Inizia subito

Setup and administration

NetApp
February 02, 2026

Sommario

Inizia subito

Scopri le nozioni di base

Scopri di più su NetApp Workload Factory

NetApp Workload Factory è una potente piattaforma di gestione del ciclo di vita progettata per aiutarti a ottimizzare i tuoi carichi di lavoro utilizzando i file system Amazon FSx for NetApp ONTAP . I carichi di lavoro che possono essere semplificati utilizzando Workload Factory e FSx per ONTAP includono database, migrazioni VMware su VMware Cloud su AWS, chatbot AI e altro ancora.

Un *carico di lavoro* comprende una combinazione di risorse, codice e servizi o applicazioni, progettati per soddisfare un obiettivo aziendale. Potrebbe trattarsi di qualsiasi cosa, da un'applicazione rivolta al cliente a un processo back-end. I carichi di lavoro possono riguardare un sottoinsieme di risorse all'interno di un singolo account AWS o estendersi su più account.

Amazon FSx for NetApp ONTAP fornisce volumi di storage NFS, SMB/CIFS e iSCSI nativi di AWS completamente gestiti per applicazioni mission-critical, database, container, datastore VMware Cloud e file utente. È possibile gestire FSx per ONTAP tramite Workload Factory e utilizzando gli strumenti di gestione nativi di AWS.

Caratteristiche

La piattaforma Workload Factory offre le seguenti funzionalità principali.

Storage flessibile e a basso costo

Scopri, implementa e gestisci i file system Amazon FSX per NetApp ONTAP nel cloud. FSX per ONTAP unisce le funzionalità complete di ONTAP in un servizio gestito nativo di AWS che offre un'esperienza di cloud ibrido coerente.

Migrazione degli ambienti vSphere on-premise in VMware Cloud su AWS

Il Migration ADVISOR di VMware Cloud su AWS ti consente di analizzare le configurazioni delle macchine virtuali correnti negli ambienti vSphere on-premise, di generare un piano per implementare i layout di VM consigliati in VMware Cloud su AWS e di utilizzare file system Amazon FSX per NetApp ONTAP customizzati come datastore esterni.

Lifecycle management del database

Scopri i carichi di lavoro dei database e analizza i risparmi sui costi con Amazon FSX per NetApp ONTAP; sfrutta i vantaggi delle applicazioni e dello storage durante la migrazione dei database di SQL Server in FSX per lo storage ONTAP; implementa server SQL, database e cloni di database che implementano le Best practice dei vendor; utilizza un co-pilot Infrastructure as Code per automatizzare le operazioni e monitora costantemente e ottimizza le proprietà di SQL Server per migliorare performance, disponibilità, protezione ed efficienza dei costi.

Sviluppo di chatbot ai

Sfrutta i file system FSX per ONTAP per memorizzare le origini dei chatbot delle tue organizzazioni e i database del motore ai. Questo ti consente di incorporare i dati non strutturati della tua organizzazione in un'applicazione chatbot aziendale.

Calcolatori del risparmio per risparmiare i costi

Analizza le tue implementazioni attuali che utilizzano lo storage Amazon Elastic Block Store (EBS) o Elastic file System (EFS) o Amazon FSX per Windows file Server, per scoprire quanto denaro puoi risparmiare passando ad Amazon FSX per NetApp ONTAP. È inoltre possibile utilizzare la calcolatrice per eseguire uno scenario "what if" per una distribuzione futura che si sta pianificando.

Account di servizio per promuovere l'automazione

Utilizza gli account di servizio per automatizzare le operazioni di NetApp Workload Factory in modo sicuro e affidabile. Gli account di servizio garantiscono un'automazione affidabile e duratura, senza alcuna restrizione nella gestione degli utenti, e sono più sicuri perché forniscono solo l'accesso API.

Chiedimi assistente AI

Poni all'assistente AI domande sulla gestione e l'utilizzo dei file system FSx for ONTAP . Utilizzando il Model Context Protocol (MCP), Ask Me interagisce in modo sicuro con ambienti esterni e interroga gli strumenti API per fornire risposte personalizzate in base al tuo specifico ambiente di archiviazione.

Cloud provider supportati

Workload Factory consente di gestire l'archiviazione cloud e di utilizzare le funzionalità dei carichi di lavoro in Amazon Web Services.

Sicurezza

La sicurezza di NetApp Workload Factory è una priorità assoluta per NetApp. Tutti i carichi di lavoro in Workload Factory vengono eseguiti su Amazon FSx for NetApp ONTAP. Oltre a tutto "Funzionalità di sicurezza di AWS", NetApp Workload Factory ha ricevuto "Conformità SOC2 Tipo 1, conformità SOC2 Tipo 2 e conformità HIPAA".

Amazon FSx for NetApp ONTAP per NetApp Workload Factory è un"Soluzione AWS per la distribuzione di app aziendali" che è stato creato tenendo a mente le migliori pratiche ben progettate.

Costo

L'utilizzo di Workload Factory è gratuito. Il costo che paghi ad Amazon Web Services (AWS) dipende dai servizi di archiviazione e dai carichi di lavoro che intendi distribuire. Ciò include il costo dei file system Amazon FSx for NetApp ONTAP , dell'infrastruttura VMware Cloud on AWS, dei servizi AWS e altro ancora.

Come funziona Workload Factory

Workload Factory include una console basata sul Web fornita tramite il livello SaaS, un account, modalità operative che controllano l'accesso al tuo ambiente cloud, collegamenti che forniscono connettività separata tra Workload Factory e un account AWS e molto altro.

Software-as-a-service

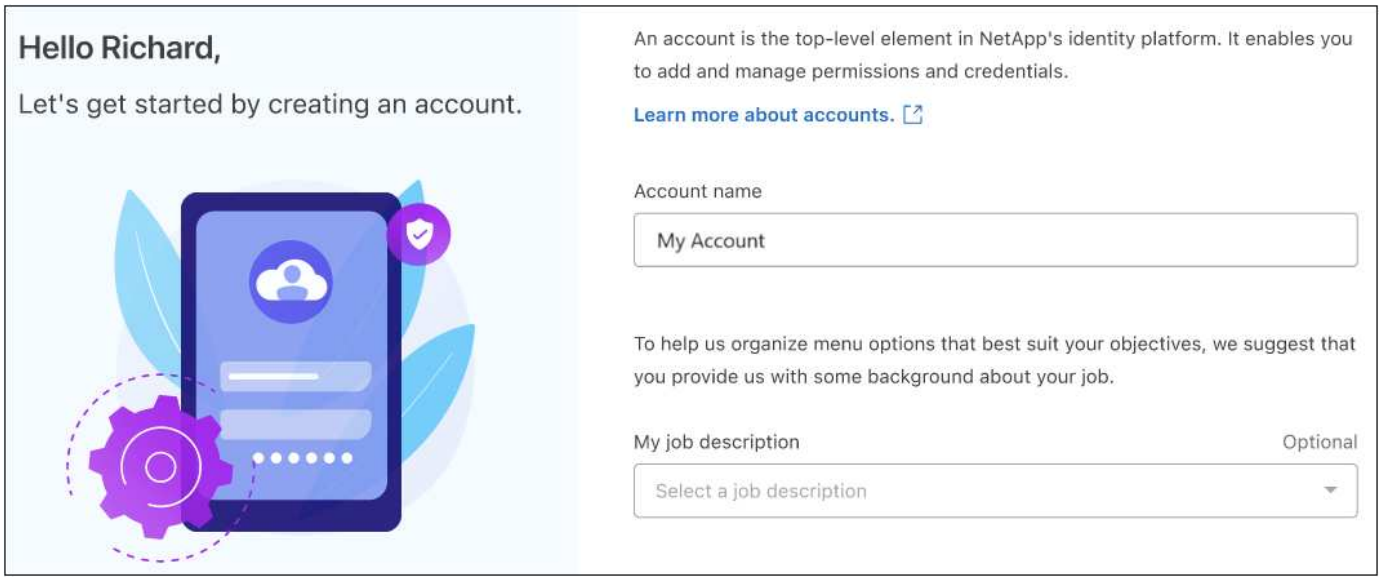
Workload Factory è accessibile tramite"Console NetApp Workload Factory" e il"Console NetApp" . Queste esperienze SaaS ti consentono di accedere automaticamente alle funzionalità più recenti non appena vengono rilasciate e di passare facilmente da un account all'altro e dai collegamenti Workload Factory.

"Scopri di più sulle diverse esperienze della console"

Account

Quando accedi a Workload Factory per la prima volta, ti verrà chiesto di creare un account. Questo account ti

consente di organizzare le risorse, i carichi di lavoro e l'accesso ai carichi di lavoro per la tua organizzazione utilizzando le credenziali.



Quando crei un account, sei il singolo utente *account admin* per quell'account.

Se la vostra organizzazione richiede una gestione aggiuntiva dell'account o dell'utente, contattateci tramite la chat in-product.

Se utilizzi la console NetApp , apparterrai già a un account perché Workload Factory sfrutta gli account NetApp .

Account di servizio

Un account di servizio funge da "utente" che può effettuare chiamate API autorizzate a NetApp Workload Factory per scopi di automazione. Ciò semplifica la gestione dell'automazione perché non è necessario creare script di automazione basati sull'account utente di una persona reale che può lasciare l'azienda in qualsiasi momento. Tutti i titolari di account in Workload Factory sono considerati amministratori dell'account. Gli amministratori degli account possono creare ed eliminare più account di servizio.

"Scopri come gestire gli account di servizio"

Permessi

Workload Factory fornisce policy di autorizzazione flessibili che consentono di controllare attentamente l'accesso al proprio ambiente cloud e di assegnare un livello di attendibilità incrementale a Workload Factory in base alle policy IT.

"Scopri di più sui criteri di autorizzazione di Workload Factory"

Collegamenti di connettività

Un collegamento Workload Factory crea una relazione di trust e connettività tra Workload Factory e uno o più file system FSx for ONTAP . Ciò consente di monitorare e gestire determinate funzionalità del file system direttamente dalle chiamate API REST ONTAP che non sono disponibili tramite l'API Amazon FSx for ONTAP .

Per iniziare a usare Workload Factory non è necessario un collegamento, ma in alcuni casi sarà necessario crearne uno per sbloccare tutte le funzionalità di Workload Factory e le capacità del carico di lavoro.

Attualmente, i link sfruttano AWS Lambda.

"Ulteriori informazioni sui collegamenti"

Automazione del codebox

Codebox è un copilota Infrastructure as Code (IaC) che aiuta gli sviluppatori e gli ingegneri DevOps a generare il codice necessario per eseguire qualsiasi operazione supportata da Workload Factory. I formati di codice includono Workload Factory REST API, AWS CLI e AWS CloudFormation.

Codebox è allineato con le modalità operative di Workload Factory (*base*, *sola lettura* e *lettura/scrittura*) e definisce un percorso chiaro per la prontezza all'esecuzione, nonché un catalogo di automazione per un rapido riutilizzo futuro.

Il riquadro Codebox mostra l'IAC generato da una specifica operazione di flusso di lavoro e associato a una procedura guidata grafica o a un'interfaccia di conversazione testuale. Anche se Codebox supporta la codifica a colori e la ricerca per una facile navigazione e analisi, non consente la modifica. È possibile solo copiare o salvare nel catalogo di automazione.

"Ulteriori informazioni su Codebox"

Calcolatori del risparmio

Workload Factory fornisce calcolatori di risparmio che ti consentono di confrontare i costi dei tuoi ambienti di archiviazione, database o carichi di lavoro VMware sui file system FSx for ONTAP rispetto ad altri servizi Amazon. A seconda delle tue esigenze di archiviazione, potresti scoprire che FSx per i file system ONTAP è l'opzione più conveniente per te.

- "Scopri come risparmiare per i tuoi ambienti storage"
- "Scopri come esplorare i risparmi per i carichi di lavoro del tuo database"
- "Scopri come esplorare i risparmi per i tuoi carichi di lavoro VMware"

Carichi di lavoro ben progettati

Workload Factory ti aiuta a gestire e gestire configurazioni di database e storage affidabili, sicure, efficienti e convenienti, in linea con AWS Well-Architected Framework. Workload Factory esegue quotidianamente la scansione di FSx per individuare i file system ONTAP , le distribuzioni di database SQL Server e Oracle, per fornire informazioni su potenziali configurazioni errate e consigliare azioni manuali o automatiche per risolvere i problemi.

"Scopri di più sui carichi di lavoro ben progettati"

Strumenti per utilizzare NetApp Workload Factory

È possibile utilizzare NetApp Workload Factory con i seguenti strumenti:

- **Console Workload Factory**: la console Workload Factory fornisce una visione visiva e olistica delle applicazioni e dei progetti.
- * NetApp Console*: la NetApp Console offre un'esperienza di interfaccia ibrida che consente di utilizzare Workload Factory insieme ad altri servizi dati NetApp .
- **Chiedimi**: utilizza l'assistente AI Chiedimi per porre domande e scoprire di più su Workload Factory senza uscire dalla console di Workload Factory. Accedi a Chiedimi dal menu della guida di Workload Factory.
- **CloudShell CLI**: Workload Factory include una CloudShell CLI per gestire e utilizzare gli ambienti AWS e

NetApp su più account da un'unica CLI basata su browser. Accedi a CloudShell dalla barra superiore della console di Workload Factory.

- **API REST**: utilizza le API REST di Workload Factory per distribuire e gestire i tuoi file system FSx for ONTAP e altre risorse AWS.
- **CloudFormation**: utilizza il codice AWS CloudFormation per eseguire le azioni definite nella console Workload Factory per modellare, fornire e gestire risorse AWS e di terze parti dallo stack CloudFormation nel tuo account AWS.
- **Provider Terraform NetApp Workload Factory**: utilizza Terraform per creare e gestire i flussi di lavoro dell'infrastruttura generati nella console Workload Factory.

API REST

Workload Factory consente di ottimizzare, automatizzare e gestire i file system FSx for ONTAP per carichi di lavoro specifici. Ogni carico di lavoro espone un'API REST associata. Nel complesso, questi carichi di lavoro e API formano una piattaforma di sviluppo flessibile ed estensibile che puoi utilizzare per amministrare i tuoi file system FSx for ONTAP .

L'utilizzo delle API REST di Workload Factory offre numerosi vantaggi:

- Le API sono state progettate sulla base della tecnologia REST e delle Best practice correnti. Le tecnologie principali includono HTTP e JSON.
- L'autenticazione di Workload Factory si basa sullo standard OAuth2. NetApp si basa sull'implementazione del servizio Auth0.
- La console basata sul Web di Workload Factory utilizza le stesse API REST principali, in modo che vi sia coerenza tra i due percorsi di accesso.

"Visualizza la documentazione dell'API REST di Workload Factory"

Esperienze di console

NetApp Workload Factory è accessibile tramite due console basate sul Web. Scopri come accedere a Workload Factory utilizzando la console Workload Factory e la console NetApp .

- * Console NetApp *: offre un'esperienza ibrida in cui puoi gestire i file system FSx for ONTAP e i carichi di lavoro in esecuzione su Amazon FSx for NetApp ONTAP nello stesso posto.
- **Console Workload Factory**: offre un'esperienza Workload Factory dedicata, focalizzata sui carichi di lavoro in esecuzione su Amazon FSx for NetApp ONTAP.

Accedi a Workload Factory nella console NetApp

È possibile accedere a Workload Factory dalla NetApp Console. Oltre a utilizzare Workload Factory per le funzionalità di archiviazione e carico di lavoro di AWS, puoi anche accedere ad altri servizi dati come NetApp Copy and Sync e altro ancora.

Fasi

1. Accedi al"Console NetApp" .
2. Dal menu NetApp Console, seleziona **Carichi di lavoro** e poi **Panoramica**.

Accedi a Workload Factory nella console Workload Factory

È possibile accedere a Workload Factory dalla console Workload Factory.

Fase

1. Accedi al"Console Workload Factory" .

Autorizzazioni per NetApp Workload Factory

Per utilizzare le funzionalità e i servizi di NetApp Workload Factory, è necessario fornire le autorizzazioni necessarie affinché Workload Factory possa eseguire operazioni nel tuo ambiente cloud.

Perché utilizzare le autorizzazioni

Quando si forniscono le autorizzazioni, Workload Factory associa una policy all'istanza con le autorizzazioni per gestire risorse e processi all'interno di quell'account AWS. Ciò consente a Workload Factory di eseguire diverse operazioni, a partire dalla scoperta degli ambienti di storage fino alla distribuzione di risorse AWS, come file system nella gestione dello storage o knowledge base per carichi di lavoro GenAI.

Ad esempio, per i carichi di lavoro del database, quando a Workload Factory vengono concesse le autorizzazioni necessarie, vengono analizzate tutte le istanze EC2 in un determinato account e in una determinata regione e vengono filtrati tutti i computer basati su Windows. Se l'agente AWS Systems Manager (SSM) è installato e in esecuzione sull'host e la rete di System Manager è configurata correttamente, Workload Factory può accedere alla macchina Windows e verificare se il software SQL Server è installato o meno.

Autorizzazioni per carico di lavoro

Ogni carico di lavoro utilizza autorizzazioni per eseguire determinate attività in Workload Factory. Le autorizzazioni sono raggruppate in criteri di autorizzazione definiti. Scorri fino al carico di lavoro che utilizzi per scoprire di più sui criteri di autorizzazione, sul JSON copiabile per i criteri di autorizzazione e su una tabella che elenca tutti i permessi, il loro scopo, dove vengono utilizzati e quali criteri di autorizzazione li supportano.

Autorizzazioni per l'archiviazione

I criteri IAM disponibili per Storage forniscono le autorizzazioni di cui Workload Factory ha bisogno per gestire risorse e processi all'interno del tuo ambiente cloud pubblico.

L'archiviazione dispone delle seguenti policy di autorizzazione tra cui scegliere:

- **Visualizzazione, pianificazione e analisi**: visualizza i file system FSx per ONTAP , scopri di più sullo stato del sistema, ottieni un'analisi ben progettata per i tuoi sistemi ed esplora i risparmi.
- **Operazioni e risoluzione**: esegui attività operative come la regolazione della capacità del file system e la risoluzione dei problemi relativi alle configurazioni del file system.
- **Creazione ed eliminazione del file system**: crea ed elimina FSx per i file system ONTAP e le VM di archiviazione.

Visualizza i criteri IAM richiesti:

Criteri IAM per l’archiviazione

Visualizzazione, pianificazione e analisi

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "fsx:DescribeFileSystems",
        "fsx:DescribeStorageVirtualMachines",
        "fsx:DescribeVolumes",
        "fsx:ListTagsForResource",
        "fsx:DescribeBackups",
        "fsx:DescribeSharedVpcConfiguration",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "elasticfilesystem:DescribeFileSystems",
        "ce:GetCostAndUsage",
        "ce:GetTags",
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:SimulatePrincipalPolicy"
      ],
      "Resource": "*"
    }
  ]
}
```

Operazioni e bonifica

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "fsx:CreateVolume",
        "fsx:DeleteVolume",
        "fsx:UpdateFileSystem",
```

```
        "fsx:UpdateStorageVirtualMachine",
        "fsx:UpdateVolume",
        "fsx:CreateBackup",
        "fsx:CreateVolumeFromBackup",
        "fsx:DeleteBackup",
        "fsx:TagResource",
        "fsx:UntagResource",
        "fsx:CreateAndAttachS3AccessPoint",
        "fsx:DetachAndDeleteS3AccessPoint",
        "s3:CreateAccessPoint",
        "s3:DeleteAccessPoint",
        "s3:GetObjectTagging",
        "bedrock:InvokeModelWithResponseStream",
        "bedrock:InvokeModel",
        "bedrock:ListInferenceProfiles",
        "bedrock:GetInferenceProfile",
        "s3tables:CreateTableBucket",
        "s3tables:ListTables",
        "s3tables:GetTable",
        "s3tables:GetTableMetadataLocation",
        "s3tables:CreateTable",
        "s3tables:GetNamespace",
        "s3tables:PutTableData",
        "s3tables:CreateNamespace",
        "s3tables:GetTableData",
        "s3tables:ListNamespaces",
        "s3tables:ListTableBuckets",
        "s3tables:GetTableBucket",
        "s3tables:UpdateTableMetadataLocation",
        "s3tables:ListTagsForResource",
        "s3tables:TagResource",
        "s3:GetObjectTagging",
        "s3:ListBucket"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:SimulatePrincipalPolicy"
      ],
      "Resource": "*"
    }
  ]
}
```

Creazione ed eliminazione del file system

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "fsx:CreateFileSystem",
        "fsx:CreateStorageVirtualMachine",
        "fsx:DeleteFileSystem",
        "fsx:DeleteStorageVirtualMachine",
        "fsx:TagResource",
        "fsx:UntagResource",
        "kms:CreateGrant",
        "iam:CreateServiceLinkedRole",
        "ec2:CreateSecurityGroup",
        "ec2:CreateTags",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeRouteTables",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVolumeStatus",
        "kms:DescribeKey",
        "kms:ListKeys",
        "kms:ListAliases"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:DeleteSecurityGroup"
      ],
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "ec2:ResourceTag/AppCreator": "NetappFSxWF"
        }
      }
    },
```

```
    {
      "Effect": "Allow",
      "Action": [
        "iam:SimulatePrincipalPolicy"
      ],
      "Resource": "*"
    }
  ]
}
```

Nella tabella seguente vengono visualizzate le autorizzazioni per l'archiviazione.

Tabella delle autorizzazioni per l'archiviazione

Scopo	Azione	Dove usato	Politica di autorizzazione
Crea un file system FSX per ONTAP	fsx:CreateFileSystem	Implementazione	Creazione ed eliminazione del file system
Creare un gruppo di sicurezza per un file system FSX per ONTAP	ec2:CreateSecurityGroup	Implementazione	Creazione ed eliminazione del file system
Aggiungere tag a un gruppo di sicurezza per un file system FSX per ONTAP	ec2:CreateTag	Implementazione	Creazione ed eliminazione del file system
Autorizzare l'uscita e l'ingresso dei gruppi di sicurezza per un file system FSX per ONTAP	ec2:AuthorizeSecurityGroupErgress	Implementazione	Creazione ed eliminazione del file system
	ec2:AuthorizeSecurityGroupIngress	Implementazione	Creazione ed eliminazione del file system
Il ruolo concesso fornisce la comunicazione tra FSX per ONTAP e altri servizi AWS	iam:CreateServiceEnumerRole	Implementazione	Creazione ed eliminazione del file system

Scopo	Azione	Dove usato	Politica di autorizzazione
Scopri come compilare il modulo di implementazione del file system FSX per ONTAP	ec2:DescripteVpcs	• Implementazione • Scopri i risparmi	Creazione ed eliminazione del file system
	ec2:DescripteSubnet	• Implementazione • Scopri i risparmi	Creazione ed eliminazione del file system
	ec2:DescripteSecurityGroups	• Implementazione • Scopri i risparmi	Creazione ed eliminazione del file system
	ec2:DescripteRouteTable	• Implementazione • Scopri i risparmi	Creazione ed eliminazione del file system
	ec2:DescripteNetworkInterfaces	• Implementazione • Scopri i risparmi	Creazione ed eliminazione del file system
	EC2:DescribeVolumeStatus	• Implementazione • Scopri i risparmi	Creazione ed eliminazione del file system

Scopo	Azione	Dove usato	Politica di autorizzazione
Ottieni dettagli chiave KMS e utilizza la crittografia per FSX for ONTAP	Km: CreateGrant	Implementazione	Creazione ed eliminazione del file system
	Km: DescribeKey	Implementazione	Creazione ed eliminazione del file system
	Km:ListKeys	Implementazione	Creazione ed eliminazione del file system
	Km:ListAlias	Implementazione	Creazione ed eliminazione del file system
Ottieni dettagli del volume per istanze EC2	ec2:DescripteVolumes	• Inventario • Scopri i risparmi	Visualizzazione, pianificazione e analisi
Ottieni dettagli per EC2 istanze	ec2:DescripbeInstances	Scopri i risparmi	Visualizzazione, pianificazione e analisi
Descrivi Elastic file System nel calcolatore del risparmio	Elasticfilesystem:Descrivi i filesystem	Scopri i risparmi	Visualizzazione, pianificazione e analisi
Elenca i tag per le risorse di FSX per ONTAP	fsx:ListTagsForResource	Inventario	Visualizzazione, pianificazione e analisi
Gestire l'uscita e l'ingresso dei gruppi di sicurezza per un file system FSX per ONTAP	ec2:RevokeSecurityGroupIngress	Operazioni di gestione	Creazione ed eliminazione del file system
	ec2: Revoca SecurityGroupEgress	Operazioni di gestione	Creazione ed eliminazione del file system
	ec2:DeleteSecurityGroup	Operazioni di gestione	Creazione ed eliminazione del file system

Scopo	Azione	Dove usato	Politica di autorizzazione
Crea, visualizza e gestisci risorse di file system FSX per ONTAP			

	fsx:CreaBackup	Operazioni di gestione	Operazioni e bonifica
Scopo	**Azione**	**Dove usato**	**Politica di autorizzazione**
	fsx:CreaVolumeDaBackup	Operazioni di gestione	Operazioni e bonifica
	fsx:EliminaBackup	Operazioni di gestione	Operazioni e bonifica
Ottieni metriche su file system e volumi	Cloudwatch:GetMetricData	Operazioni di gestione	Visualizzazione, pianificazione e analisi
	Cloudwatch:GetMetricStatistics	Operazioni di gestione	Visualizzazione, pianificazione e analisi
Simula le operazioni del carico di lavoro per validare le autorizzazioni disponibili e confrontarle con le autorizzazioni necessarie per gli account AWS	iam:SimulatePrincipalPolicy	Implementazione	Tutto
Fornire informazioni basate sull'intelligenza artificiale per FSx per gli eventi ONTAP EMS	Bedrock:ListInferenceProfiles	FSx per l'analisi ONTAP EMS	Operazioni e bonifica
	bedrock:GetInferenceProfile	FSx per l'analisi ONTAP EMS	Operazioni e bonifica
	bedrock:InvokeModelWihResponseStream	FSx per l'analisi ONTAP EMS	Operazioni e bonifica
	Bedrock:InvokeModel	FSx per l'analisi ONTAP EMS	Operazioni e bonifica
Ottieni dati sui costi e sull'utilizzo per i file system FSx for ONTAP da AWS Cost Explorer	ce:GetCostAndUsage	Analisi dei costi e dell'utilizzo	Visualizzazione, pianificazione e analisi
	ce:OttieniTag	Analisi dei costi e dell'utilizzo	Visualizzazione, pianificazione e analisi
Crea un punto di accesso S3 e lo collega a un file system FSx for ONTAP	fsx:CreateAndAttachS3AccessPoint	Gestione del punto di accesso S3	Operazioni e bonifica
Scollega un punto di accesso S3 da un file system FSx for ONTAP ed eliminalo	fsx:DetachAndDeleteS3AccessPoint	Gestione del punto di accesso S3	Operazioni e bonifica
Crea un punto di accesso S3 per una gestione semplificata dell'accesso al bucket	s3:CreateAccessPoint	Gestione del punto di accesso S3	Operazioni e bonifica
Elimina un access point S3	s3:DeleteAccessPoint	Gestione del punto di accesso S3	Operazioni e bonifica
Aggiungi tag a un punto di accesso S3	s3:TagResource	Gestione del punto di accesso S3	Operazioni e bonifica

Scopo	Azione	Dove usato	Politica di autorizzazione
Elenca e visualizza i tag su un access point S3	s3:ListTagsForResource	Gestione del punto di accesso S3	Operazioni e bonifica
Rimuovere i tag da un access point S3	s3:UntagResource	Gestione del punto di accesso S3	Operazioni e bonifica
Scopri gli oggetti in un bucket S3 access point	s3:ListBucket	Operazioni del bucket S3	Operazioni e bonifica
Elenca, crea e descrivi i bucket delle tabelle S3	s3tables:ListTableBuckets s3tables:CreateTableBucket s3tables:GetTableBucket	Gestione dei bucket delle tabelle S3	Operazioni e bonifica
Elenca, crea e recupera tabelle S3	s3tables:ListTables s3tables:CreateTable s3tables:GetTable	Operazioni sulla tabella S3	Operazioni e bonifica
Leggi la posizione dei metadati della tabella	s3tables:GetTableMetadataLocation	Operazioni sui metadati della tabella S3	Operazioni e bonifica
Aggiorna la posizione dei metadati della tabella	s3tables:UpdateTableMetadataLocation	Operazioni sui metadati della tabella S3	Operazioni e bonifica
Elenca, crea e recupera gli spazi dei nomi delle tabelle	s3tables:ListNamespaces s3tables:CreateNamespace s3tables:GetNamespace	Operazioni dello spazio dei nomi S3	Operazioni e bonifica
Leggere i dati della tabella (select, scan)	s3tables:GetTableData	Operazioni sui dati della tabella S3	Operazioni e bonifica
Scrivi dati della tabella (inserisci)	s3tables:PutTableData	Operazioni sui dati della tabella S3	Operazioni e bonifica
Elenca i tag su una tabella di inventario (ottieni FSx for NetApp ONTAP, storage VM, ID volume)	s3tables:ListTagsForResource	Operazioni sui tag della tabella S3	Operazioni e bonifica
Etichetta una tabella di inventario per la ricerca in NetApp Workload Factory	s3tables:TagResource	Operazioni sui tag della tabella S3	Operazioni e bonifica
Recupera l'etichettatura degli oggetti tramite il punto di accesso	s3:GetObjectTagging	Operazioni sugli oggetti S3	Operazioni e bonifica

Autorizzazioni per i carichi di lavoro del database

I criteri IAM disponibili per i carichi di lavoro del database forniscono le autorizzazioni di cui Workload Factory ha bisogno per gestire risorse e processi all'interno del tuo ambiente cloud pubblico.

I database dispongono delle seguenti policy di autorizzazione tra cui scegliere:

- **Visualizzazione, pianificazione e analisi**: visualizza l'inventario delle risorse del database, scopri lo stato di salute delle tue risorse, esamina l'analisi ben progettata per le configurazioni del tuo database ed esplora i risparmi, ottieni l'analisi del registro degli errori ed esplora i risparmi.
- **Operazioni e risoluzione**: esegui attività operative per le risorse del database e risolvi problemi per le configurazioni del database e per l'archiviazione del file system FSx for ONTAP sottostante.
- **Creazione dell'host del database**: distribuire gli host del database e il file system FSx sottostante per l'archiviazione ONTAP secondo le best practice.

Selezionare la modalità operativa per visualizzare i criteri IAM richiesti:

Criteri IAM per i carichi di lavoro del database

Visualizzazione, pianificazione e analisi

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "CommonGroup",
            "Effect": "Allow",
            "Action": [
                "cloudwatch:GetMetricStatistics",
                "cloudwatch:GetMetricData",
                "sns:ListTopics",
                "ec2:DescribeInstances",
                "ec2:DescribeVpcs",
                "ec2:DescribeSubnets",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeImages",
                "ec2:DescribeRegions",
                "ec2:DescribeRouteTables",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeInstanceTypes",
                "ec2:DescribeVpcEndpoints",
                "ec2:DescribeInstanceTypeOfferings",
                "ec2:DescribeSnapshots",
                "ec2:DescribeVolumes",
                "ec2:DescribeAddresses",
                "kms:ListAliases",
                "kms:ListKeys",
                "kms:DescribeKey",
                "cloudformation:ListStacks",
                "cloudformation:DescribeAccountLimits",
                "ds:DescribeDirectories",
                "fsx:DescribeVolumes",
                "fsx:DescribeBackups",
                "fsx:DescribeStorageVirtualMachines",
                "fsx:DescribeFileSystems",
                "servicequotas:ListServiceQuotas",
                "ssm:GetParametersByPath",
                "ssm:GetCommandInvocation",
                "ssm:SendCommand",
                "ssm:GetConnectionStatus",
                "ssm:DescribePatchBaselines",
                "ssm:DescribeInstancePatchStates",
                "ssm:ListCommands",
                "ssm:DescribeInstanceInformation",
```

```
                "fsx:ListTagsForResource",
                "logs:DescribeLogGroups",
                "bedrock:GetFoundationModelAvailability",
                "bedrock:ListInferenceProfiles"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Sid": "SSMParameterStore",
            "Effect": "Allow",
            "Action": [
                "ssm:GetParameter",
                "ssm:GetParameters",
                "ssm:PutParameter",
                "ssm:DeleteParameters"
            ],
            "Resource": "arn:aws:ssm:*:*:parameter/netapp/wlmdb/*"
        },
        {
            "Sid": "SSMResponseCloudWatch",
            "Effect": "Allow",
            "Action": [
                "logs:GetLogEvents",
                "logs:PutRetentionPolicy"
            ],
            "Resource": "arn:aws:logs:*:*:log-group:netapp/wlmdb/*"
        }
    ]
}
```

Operazioni e bonifica

```
[
    {
        "Sid": "FSxRemediation",
        "Effect": "Allow",
        "Action": [
            "fsx:UpdateFileSystem",
            "fsx:UpdateVolume"
        ],
        "Resource": "*"
    },
    {
        "Sid": "EC2Remediation",
        "Effect": "Allow",
        "Action": [
            "ec2:StartInstances",
            "ec2:ModifyInstanceAttribute",
            "ec2:StopInstances"
        ],
        "Resource": "*",
        "Condition": {
            "StringLike": {
                "ec2:ResourceTag/aws:cloudformation:stack-name":
"WLMDB*"
            }
        }
    }
]
```

Creazione dell'host del database

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "EC2TagGroup",
            "Effect": "Allow",
            "Action": [
                "ec2:AllocateAddress",
                "ec2:AllocateHosts",
                "ec2:AssignPrivateIpAddresses",
                "ec2:AssociateAddress",
                "ec2:AssociateRouteTable",
                "ec2:AssociateSubnetCidrBlock",
                "ec2:AssociateVpcCidrBlock",
                "ec2:AttachInternetGateway",
```

```
                "ec2:AttachNetworkInterface",
                "ec2:AttachVolume",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateVolume",
                "ec2:DeleteNetworkInterface",
                "ec2:DeleteSecurityGroup",
                "ec2:DeleteTags",
                "ec2:DeleteVolume",
                "ec2:DetachNetworkInterface",
                "ec2:DetachVolume",
                "ec2:DisassociateAddress",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:DisassociateRouteTable",
                "ec2:DisassociateSubnetCidrBlock",
                "ec2:DisassociateVpcCidrBlock",
                "ec2:ModifyInstancePlacement",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:ModifySubnetAttribute",
                "ec2:ModifyVolume",
                "ec2:ModifyVolumeAttribute",
                "ec2:ReleaseAddress",
                "ec2:ReplaceRoute",
                "ec2:ReplaceRouteTableAssociation",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/aws:cloudformation:stack-
name": "WLMDB*"
                }
            }
        },
        {
            "Sid": "FSxNGroup",
            "Effect": "Allow",
            "Action": [
                "fsx:TagResource"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "aws:ResourceTag/aws:cloudformation:stack-
name": "WLMDB*"
```

```
                }
            }
        },
        {
            "Sid": "CreationGroup",
            "Effect": "Allow",
            "Action": [
                "cloudformation:CreateStack",
                "cloudformation:DescribeStackEvents",
                "cloudformation:DescribeStacks",
                "cloudformation:ValidateTemplate",
                "ec2:CreateLaunchTemplate",
                "ec2:CreateLaunchTemplateVersion",
                "ec2:CreateNetworkInterface",
                "ec2:CreateSecurityGroup",
                "ec2:CreateTags",
                "ec2:CreateVpcEndpoint",
                "ec2:RunInstances",
                "ec2:DescribeTags",
                "ec2:DescribeLaunchTemplates",
                "ec2:ModifyVpcAttribute",
                "fsx:CreateFileSystem",
                "fsx:CreateStorageVirtualMachine",
                "fsx:CreateVolume",
                "fsx:DescribeFileSystemAliases",
                "kms:CreateGrant",
                "kms:DescribeCustomKeyStores",
                "kms:GenerateDataKey",
                "kms:Decrypt",
                "logs:CreateLogGroup",
                "logs:CreateLogStream",
                "logs:GetLogGroupFields",
                "logs:GetLogRecord",
                "logs:ListLogDeliveries",
                "logs:PutLogEvents",
                "logs:TagResource",
                "sns:Publish",
                "ssm:PutComplianceItems",
                "ssm:PutConfigurePackageResult",
                "ssm:PutInventory",
                "ssm:UpdateAssociationStatus",
                "ssm:UpdateInstanceAssociationStatus",
                "ssm:UpdateInstanceInformation",
                "ssmmessages:CreateControlChannel",
                "ssmmessages:CreateDataChannel",
                "ssmmessages:OpenControlChannel",
```

```
                "ssmmessages:OpenDataChannel",
                "compute-optimizer:GetEnrollmentStatus",
                "compute-optimizer:PutRecommendationPreferences",
                "compute-
optimizer:GetEffectiveRecommendationPreferences",
                "compute-optimizer:GetEC2InstanceRecommendations",
                "autoscaling:DescribeAutoScalingGroups",
                "autoscaling:DescribeAutoScalingInstances",
                "iam:GetPolicy",
                "iam:GetPolicyVersion",
                "iam:GetRole",
                "iam:GetRolePolicy",
                "iam:GetUser"
            ],
            "Resource": "*"
        },
        {
            "Sid": "ArnGroup",
            "Effect": "Allow",
            "Action": [
                "cloudformation:SignalResource"
            ],
            "Resource": [
                "arn:aws:cloudformation:*:*:stack/WLMDB*",
                "arn:aws:logs:*:*:log-group:WLMDB*"
            ]
        },
        {
            "Sid": "IAMGroup1",
            "Effect": "Allow",
            "Action": [
                "iam:AddRoleToInstanceProfile",
                "iam:CreateInstanceProfile",
                "iam:DeleteInstanceProfile",
                "iam:PutRolePolicy",
                "iam:RemoveRoleFromInstanceProfile"
            ],
            "Resource": [
                "arn:aws:iam::*:instance-profile/*",
                "arn:aws:iam::*:role/WLMDB*"
            ]
        },
        {
            "Sid": "IAMGroup2",
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
```

```
            "Resource": [
                "arn:aws:iam::*:instance-profile/*",
                "arn:aws:iam::*:role/WLMDB*"
            ],
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "ec2.amazonaws.com"
                }
            }
        },
        {
            "Sid": "IAMGroup3",
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": [
                "arn:aws:iam::*:instance-profile/*",
                "arn:aws:iam::*:role/WLMDB*"
            ],
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": "ec2.amazonaws.com"
                }
            }
        },
        {
            "Sid": "IAMGroup4",
            "Effect": "Allow",
            "Action": "iam:CreateRole",
            "Resource": "arn:aws:iam::*:role/WLMDB*"
        }
    ]
}
```

Nella tabella seguente vengono visualizzate le autorizzazioni per i carichi di lavoro del database.

Tabella delle autorizzazioni per i carichi di lavoro del database

Scopo	Azione	Dove usato	Politica di autorizzazione
Ottieni statistiche metriche per FSx per ONTAP, EBS e FSx per Windows File Server e per consigli sull'ottimizzazione del calcolo	Cloudwatch:GetMetricStatistics	• Inventario • Scopri i risparmi	Visualizzazione, pianificazione e analisi
Raccogli i parametri delle prestazioni salvati su Amazon CloudWatch dai nodi SQL registrati. I dati vengono generati in grafici di tendenza delle prestazioni nella schermata di gestione delle istanze SQL registrate.	Cloudwatch:GetMetricData	Inventario	Visualizzazione, pianificazione e analisi
Ottieni dettagli per EC2 istanze	ec2:DescripbeInstances	• Inventario • Scopri i risparmi	Visualizzazione, pianificazione e analisi
	ec2:DescripteKeyPairs	Implementazione	Visualizzazione, pianificazione e analisi
	ec2:DescripteNetworkInterfaces	Implementazione	Visualizzazione, pianificazione e analisi
	EC2:DescribeInstanceTypes	• Implementazione • Scopri i risparmi	Visualizzazione, pianificazione e analisi

Scopo	Azione	Dove usato	Politica di autorizzazione
Ottieni i dettagli da compilare nel modulo di distribuzione di FSX per ONTAP	ec2:DescripteVpcs	• Implementazione • Inventario	Visualizzazione, pianificazione e analisi
	ec2:DescripteSubnet	• Implementazione • Inventario	Visualizzazione, pianificazione e analisi
	ec2:DescripteSecurityGroups	Implementazione	Visualizzazione, pianificazione e analisi
	ec2:DescripteImages	Implementazione	Visualizzazione, pianificazione e analisi
	ec2:DescripteRegions	Implementazione	Visualizzazione, pianificazione e analisi
	ec2:DescripteRouteTable	• Implementazione • Inventario	Visualizzazione, pianificazione e analisi
Ottieni qualsiasi endpoint VPC esistente per determinare se è necessario creare nuovi endpoint prima delle implementazioni	ec2:DescripteVpcEndpoint	• Implementazione • Inventario	Visualizzazione, pianificazione e analisi
Creare endpoint VPC se non esistono per i servizi richiesti indipendentemente dalla connettività di rete pubblica sulle istanze EC2	EC2:CreateVpcEndpoint	Implementazione	Creazione dell'host del database
Ottieni tipi di istanza disponibili nella regione per i nodi di convalida (t2.micro/t3.micro)	EC2:DescribeInstanceTypeOfferings	Implementazione	Visualizzazione, pianificazione e analisi
Ottieni i dettagli snapshot di ogni volume EBS collegato per ottenere prezzi e stime di risparmio	ec2:DescripteSnapshot	Scopri i risparmi	Visualizzazione, pianificazione e analisi

Scopo	Azione	Dove usato	Politica di autorizzazione
Ottieni dettagli su ogni volume EBS collegato per ottenere prezzi e stime di risparmio	ec2:DescripteVolumes	• Inventario • Scopri i risparmi	Visualizzazione, pianificazione e analisi
Ottieni i dettagli delle chiavi KMS per la crittografia del file system FSX per ONTAP	Km:ListAlias	Implementazione	Visualizzazione, pianificazione e analisi
	Km:ListKeys	Implementazione	Visualizzazione, pianificazione e analisi
	Km: DescribeKey	Implementazione	Visualizzazione, pianificazione e analisi
Ottenere l'elenco degli stack di CloudFormation in esecuzione nell'ambiente per controllare il limite di quota	Cloudformation:ListStack	Implementazione	Visualizzazione, pianificazione e analisi
Controllare i limiti degli account per le risorse prima di attivare la distribuzione	Formazione del cloud:DescribeAccountLimits	Implementazione	Visualizzazione, pianificazione e analisi
Ottieni un elenco delle Active Directory gestite da AWS nella regione	ds:DescribeDirectories	Implementazione	Visualizzazione, pianificazione e analisi

Scopo	Azione	Dove usato	Politica di autorizzazione
Ottieni elenchi e dettagli di volumi, backup, SVM, file system in zone e tag per FSX per il file system ONTAP	fsx:DescribeVolumes	• Inventario • Scopri i risparmi	Visualizzazione, pianificazione e analisi
	fsx:DescribeBackups	• Inventario • Scopri i risparmi	Visualizzazione, pianificazione e analisi
	fsx:DescribeStorageVirtualMachines	• Implementazione • Operazioni di gestione • Inventario	Visualizzazione, pianificazione e analisi
	fsx:DescribeFileSystems	• Implementazione • Operazioni di gestione • Inventario • Scopri i risparmi	Visualizzazione, pianificazione e analisi
	fsx:ListTagsForResource	Operazioni di gestione	Visualizzazione, pianificazione e analisi
Ottieni limiti di quota del servizio per CloudFormation e VPC / Crea segreti in un account utente per le credenziali fornite per SQL, dominio e FSx per ONTAP	Services equotas:ListServiceQuotas	Implementazione	Visualizzazione, pianificazione e analisi
Utilizzare la query basata su SSM per ottenere l'elenco aggiornato delle aree supportate da FSX per ONTAP	ssm:GetParametersByPath	Implementazione	Visualizzazione, pianificazione e analisi

Scopo	Azione	Dove usato	Politica di autorizzazione
Verifica della risposta SSM dopo l'invio del comando per le operazioni di gestione post deployment	ssm:GetCommandInvocation	• Operazioni di gestione • Inventario • Scopri i risparmi • Ottimizzazione	Visualizzazione, pianificazione e analisi
Invia comandi tramite SSM alle istanze EC2 per l'individuazione e la gestione	ssm:SendCommand	• Operazioni di gestione • Inventario • Scopri i risparmi • Ottimizzazione	Visualizzazione, pianificazione e analisi
Ottenere lo stato di connettività SSM sulle istanze dopo la distribuzione	ssm:GetConnectionStatus	• Operazioni di gestione • Inventario • Ottimizzazione	Visualizzazione, pianificazione e analisi
Recupero dello stato di associazione SSM per un gruppo di istanze EC2 gestite (nodi SQL)	ssm:DescribeInstanceInformation	Inventario	Visualizzazione, pianificazione e analisi
Consultare l'elenco delle linee di base delle patch disponibili per la valutazione delle patch del sistema operativo	ssm:DescribePatchBaselines	Ottimizzazione	Visualizzazione, pianificazione e analisi
Ottenere lo stato di applicazione delle patch nelle istanze di Windows EC2 per la valutazione delle patch del sistema operativo	ssm:DescribeInstancePatchStates	Ottimizzazione	Visualizzazione, pianificazione e analisi
Elenca comandi eseguiti da AWS Patch Manager su istanze EC2 per la gestione delle patch del sistema operativo	ssm:ListCommander	Ottimizzazione	Visualizzazione, pianificazione e analisi

Scopo	Azione	Dove usato	Politica di autorizzazione
Verifica se l'account è registrato in AWS Compute Optimizer	Compute-Optimizer:GetEnrollmentStatus	• Scopri i risparmi • Ottimizzazione	Creazione dell'host del database
Aggiornare una preferenza di raccomandazione esistente in AWS Compute Optimizer per personalizzare i suggerimenti per i carichi di lavoro di SQL Server	Compute-Optimizer:RecommendationPreferences	• Scopri i risparmi • Ottimizzazione	Creazione dell'host del database
AWS Compute Optimizer offre le preferenze dei consigli in vigore per una determinata risorsa	Compute-Optimizer:GetEffectiveRecommendationPreferences	• Scopri i risparmi • Ottimizzazione	Creazione dell'host del database
Recupera consigli generati da AWS Compute Optimizer per le istanze di Amazon Elastic Compute Cloud (Amazon EC2)	Compute-Optimizer:GetEC2InstanceRecommendations	• Scopri i risparmi • Ottimizzazione	Creazione dell'host del database
Controllare l'associazione di esempio ai gruppi di ridimensionamento automatico	Ridimensionamento automatico:DescribeAutoScalingGroups	• Scopri i risparmi • Ottimizzazione	Creazione dell'host del database
	Ridimensionamento automatico:DescribeAutoScalingInstances	• Scopri i risparmi • Ottimizzazione	Creazione dell'host del database

Scopo	Azione	Dove usato	Politica di autorizzazione
Ottieni, elenca, crea ed elimina i parametri SSM per le credenziali utente ad, FSX per ONTAP e SQL utilizzate durante l'implementazione o gestite nell'account AWS	ssm:getParameter [1]	• Implementazione • Operazioni di gestione • Inventario	Visualizzazione, pianificazione e analisi
	ssm:GetParameters [1]	• Implementazione • Operazioni di gestione • Inventario	Visualizzazione, pianificazione e analisi
	ssm:PutParameter [1]	• Implementazione • Operazioni di gestione	Visualizzazione, pianificazione e analisi
	ssm:DeleteParameters [1]	• Implementazione • Operazioni di gestione	Visualizzazione, pianificazione e analisi

Scopo	Azione	Dove usato	Politica di autorizzazione
Associare le risorse di rete ai nodi SQL e ai nodi di convalida e aggiungere ulteriori IP secondari ai nodi SQL	EC2:AllocateAddress [1]	Implementazione	Creazione dell'host del database
	EC2:AllocateHosts [1]	Implementazione	Creazione dell'host del database
	EC2:AssignPrivateIpAddresses [1]	Implementazione	Creazione dell'host del database
	EC2:AssociateAddress [1]	Implementazione	Creazione dell'host del database
	EC2:AssociateRouteTable [1]	Implementazione	Creazione dell'host del database
	EC2:AssociateSubnetCidrBlock [1]	Implementazione	Creazione dell'host del database
	EC2:AssociateVpcCidrBlock [1]	Implementazione	Creazione dell'host del database
	EC2:AttachInternetGateway [1]	Implementazione	Creazione dell'host del database
	EC2:AttachNetworkInterface [1]	Implementazione	Creazione dell'host del database
Possibilità di collegare i volumi EBS richiesti ai nodi SQL per l'implementazione	ec2:AttachVolume	Implementazione	Creazione dell'host del database
Collega gruppi di sicurezza e modifica le regole alle istanze EC2 fornite	ec2:AuthorizeSecurityGroupEgress	Implementazione	Creazione dell'host del database
	ec2:AuthorizeSecurityGroupIngress	Implementazione	Creazione dell'host del database
Creare volumi EBS richiesti ai nodi SQL per l'implementazione	ec2:CreateVolume	Implementazione	Creazione dell'host del database

Scopo	Azione	Dove usato	Politica di autorizzazione
Rimuovere i nodi di convalida temporanea creati di tipo t2.micro e per il rollback o il nuovo tentativo di nodi SQL EC2 non riusciti	ec2:DeleteNetworkInterface	Implementazione	Creazione dell'host del database
	ec2:DeleteSecurityGroup	Implementazione	Creazione dell'host del database
	ec2:DeleteMags	Implementazione	Creazione dell'host del database
	ec2:DeleteVolume	Implementazione	Creazione dell'host del database
	EC2:DetachNetworkInterface	Implementazione	Creazione dell'host del database
	ec2:DetachVolume	Implementazione	Creazione dell'host del database
	EC2:DisassociateAddress	Implementazione	Creazione dell'host del database
	ec2:DisassociateIamInstanceProfile	Implementazione	Creazione dell'host del database
	EC2:DisassociateRouteTable	Implementazione	Creazione dell'host del database
	EC2:DisassociateSubnetCidrBlock	Implementazione	Creazione dell'host del database
	EC2:DisassociateVpcCidrBlock	Implementazione	Creazione dell'host del database

Scopo	Azione	Dove usato	Politica di autorizzazione
Modificare gli attributi per le istanze SQL create. Applicabile solo ai nomi che iniziano con WLMDB.	ec2:ModifyInstanceAttribute	Implementazione	Operazioni e bonifica
	EC2:ModifyInstancePlacement	Implementazione	Creazione dell'host del database
	ec2:ModifyNetworkInterfaceAttribute	Implementazione	Creazione dell'host del database
	EC2:ModifySubnetAttribute	Implementazione	Creazione dell'host del database
	ec2:ModifyVolume	Implementazione	Creazione dell'host del database
	ec2:ModifyVolumeAttribute	Implementazione	Creazione dell'host del database
	EC2:ModifyVpcAttribute	Implementazione	Creazione dell'host del database
Dissociare e distruggere le istanze di convalida	EC2:ReleaseAddress	Implementazione	Creazione dell'host del database
	EC2:ReplaceRoute	Implementazione	Creazione dell'host del database
	EC2:ReplaceRouteTableAssociation	Implementazione	Creazione dell'host del database
	ec2:RevokeSecurityGroupErgress	Implementazione	Creazione dell'host del database
	ec2:RevokeSecurityGroupIngress	Implementazione	Creazione dell'host del database
Avviare le istanze distribuite	ec2:StartInstances	Implementazione	Operazioni e bonifica
Arrestare le istanze distribuite	ec2:StopInstances	Implementazione	Operazioni e bonifica

Scopo	Azione	Dove usato	Politica di autorizzazione
Contrassegnare i valori personalizzati per le risorse Amazon FSX per NetApp ONTAP create da WLMDB per ottenere i dettagli di fatturazione durante la gestione delle risorse	fsx:TagResource [1]	• Implementazione • Operazioni di gestione	Creazione dell'host del database
Creare e convalidare il modello CloudFormation per la distribuzione	Cloud formation: CreateStack	Implementazione	Creazione dell'host del database
	Cloudformation:DescripbeStackEvents	Implementazione	Creazione dell'host del database
	Cloudformation:DescripteStack	Implementazione	Creazione dell'host del database
	Cloudformation:ListStack	Implementazione	Visualizzazione, pianificazione e analisi
	Cloud formation:ValidateTemplate	Implementazione	Creazione dell'host del database
Creare modelli di stack nidificati per riprovare e ripristinare	EC2:CreateLaunchTemplate	Implementazione	Creazione dell'host del database
	EC2:CreateLaunchTemplateVersion	Implementazione	Creazione dell'host del database
Gestire i tag e la sicurezza di rete sulle istanze create	ec2:CreateNetworkInterface	Implementazione	Creazione dell'host del database
	ec2:CreateSecurityGroup	Implementazione	Creazione dell'host del database
	ec2:CreateTag	Implementazione	Creazione dell'host del database
Ottieni dettagli delle istanze per il provisioning	ec2:DescriviIndirizzi	Implementazione	Visualizzazione, pianificazione e analisi
	ec2:DescribeLaunchTemplates	Implementazione	Visualizzazione, pianificazione e analisi

Scopo	Azione	Dove usato	Politica di autorizzazione
Avviare le istanze create	ec2:RunInstances	Implementazione	Creazione dell'host del database
Crea risorse FSX per ONTAP richieste per il provisioning. Per i sistemi esistenti di FSX per ONTAP, viene creata una nuova SVM per ospitare i volumi SQL.	fsx:CreateFileSystem	Implementazione	Creazione dell'host del database
	fsx:CreateStorageVirtualMachine	Implementazione	Creazione dell'host del database
	fsx:CreateVolume	• Implementazione • Operazioni di gestione	Creazione dell'host del database
Ottieni i dettagli di FSX per ONTAP	fsx:DescribeFileSystemAliases	Implementazione	Creazione dell'host del database
Ridimensiona FSX per il file system ONTAP per rimediare allo spazio a disposizione del file system	fsx:Updatefilesystem	Ottimizzazione	Operazioni e bonifica
Ridimensionamento dei volumi per correggere le dimensioni dei dischi di log e TempDB	fsx:UpdateVolume	Ottimizzazione	Operazioni e bonifica
Ottieni dettagli chiave KMS e utilizza la crittografia per FSX for ONTAP	Km: CreateGrant	Implementazione	Creazione dell'host del database
	kms:DescribeCustomKeyStores	Implementazione	Creazione dell'host del database
	Km:GenerateDataKey	Implementazione	Creazione dell'host del database

Scopo	Azione	Dove usato	Politica di autorizzazione
Creare log di CloudWatch per la convalida e il provisioning di script in esecuzione su istanze EC2	Registri:CreateLogGroup	Implementazione	Creazione dell'host del database
	Registri:CreateLogStream	Implementazione	Creazione dell'host del database
	registri:GetLogGroupFields	Implementazione	Creazione dell'host del database
	registri:GetLogRecord	Implementazione	Creazione dell'host del database
	Registri:ListLogDeliveries	Implementazione	Creazione dell'host del database
	Registri:PutLogEvents	• Implementazione • Operazioni di gestione	Creazione dell'host del database
	Registri:TagResource	Implementazione	Creazione dell'host del database
Workload Factory passa ai log di Amazon CloudWatch per l'istanza SQL quando rileva un troncamento dell'output SSM	Registri:GetLogEvents	• Valutazione dello storage (ottimizzazione) • Inventario	Visualizzazione, pianificazione e analisi
Consenti a Workload Factory di ottenere i gruppi di log correnti e verifica che la conservazione sia impostata per i gruppi di log creati da Workload Factory	Registri:DescribeLogGroups	• Valutazione dello storage (ottimizzazione) • Inventario	Visualizzazione, pianificazione e analisi
Consenti a Workload Factory di impostare un criterio di conservazione di un giorno per i gruppi di log creati da Workload Factory per evitare un accumulo non necessario di flussi di log per gli output dei comandi SSM	Registri:PutRetentionPolicy	• Valutazione dello storage (ottimizzazione) • Inventario	Visualizzazione, pianificazione e analisi

Scopo	Azione	Dove usato	Politica di autorizzazione
Elencare gli argomenti SNS dei clienti e pubblicarli su SNS back-end WLMDB e SNS dei clienti, se selezionati	sns:ListTopics	Implementazione	Visualizzazione, pianificazione e analisi
	sns: Pubblica	Implementazione	Creazione dell'host del database
Autorizzazioni SSM richieste per eseguire lo script di rilevamento sulle istanze SQL sottoposte a provisioning e per recuperare l'elenco più recente delle regioni AWS supportate da FSX per ONTAP.	ssm: PutComplianceItems	Implementazione	Creazione dell'host del database
	ssm:PutConfigurePackageResult	Implementazione	Creazione dell'host del database
	ssm:PutInventory	Implementazione	Creazione dell'host del database
	ssm:UpdateAssociationStatus	Implementazione	Creazione dell'host del database
	ssm:UpdateInstanceAssociationStatus	Implementazione	Creazione dell'host del database
	ssm:UpdateInstanceInformation	Implementazione	Creazione dell'host del database
	ssmmessages:CreateControlChannel	Implementazione	Creazione dell'host del database
	ssmmessages:CreateDataChannel	Implementazione	Creazione dell'host del database
	ssmmessages:OpenControlChannel	Implementazione	Creazione dell'host del database
	ssmmessages:OpenDataChannel	Implementazione	Creazione dell'host del database
Segnala lo stack CloudFormation in caso di successo o errore.	Formazione del cloud:SignalResource [1]	Implementazione	Creazione dell'host del database
Aggiungere il ruolo EC2 creato da modello al profilo di istanza di EC2 per consentire agli script di EC2 di accedere alle risorse necessarie per la distribuzione.	iam:AddRoleToInstanceProfile	Implementazione	Creazione dell'host del database

Scopo	Azione	Dove usato	Politica di autorizzazione
Creare un profilo di istanza per EC2 e allegare il ruolo EC2 creato.	iam:CreateInstanceProfile	Implementazione	Creazione dell'host del database
Creare un ruolo EC2 tramite il modello con le autorizzazioni elencate di seguito	iam: CreateRole	Implementazione	Creazione dell'host del database
Creare un ruolo collegato al servizio EC2	iam:CreateServiceEnumerRole [2]	Implementazione	Creazione dell'host del database
Eliminare il profilo di istanza creato durante la distribuzione specificamente per i nodi di convalida	iam:DeleteInstanceProfile	Implementazione	Creazione dell'host del database
Ottieni i dettagli del ruolo e della policy per determinare eventuali lacune nelle autorizzazioni e convalidare per la distribuzione	iam:GetPolicy	Implementazione	Creazione dell'host del database
	iam:GetPolicyVersion	Implementazione	Creazione dell'host del database
	iam: GetRole	Implementazione	Creazione dell'host del database
	iam:GetRolePolicy	Implementazione	Creazione dell'host del database
	iam:GetUser	Implementazione	Creazione dell'host del database
Passare il ruolo creato all'istanza EC2	iam:PassRole [3]	Implementazione	Creazione dell'host del database
Aggiungere policy con autorizzazioni richieste al ruolo EC2 creato	iam:PutRolePolicy	Implementazione	Creazione dell'host del database
Scollega il ruolo dal profilo di istanza EC2 di cui è stato eseguito il provisioning	iam:RemoveRoleFromInstanceProfile	Implementazione	Creazione dell'host del database
Simula le operazioni del carico di lavoro per validare le autorizzazioni disponibili e confrontarle con le autorizzazioni necessarie per gli account AWS	iam:SimulatePrincipalPolicy	Implementazione	Tutto

Scopo	Azione	Dove usato	Politica di autorizzazione
Ottieni i modelli di base disponibili per l'analisi del registro degli errori	Bedrock:GetFoundationModelAvailability	Analisi del registro degli errori	Visualizzazione, pianificazione e analisi
Elenca i profili di interfaccia disponibili in Amazon Bedrock per l'analisi del registro degli errori	Bedrock:ListInferenceProfiles	Analisi del registro degli errori	Visualizzazione, pianificazione e analisi

1. L'autorizzazione è limitata alle risorse che iniziano con WLMDB.
2. "iam:CreateServiceEnumerRole" limitato da "iam:AWSServiceName": "ec2.amazonaws.com"*
3. "iam:PassRole" limitata da "iam:PassedToService": "ec2.amazonaws.com"*

Autorizzazioni per i carichi di lavoro Genai

I criteri IAM per i carichi di lavoro VMware forniscono le autorizzazioni di cui Workload Factory per VMware ha bisogno per gestire risorse e processi all'interno dell'ambiente cloud pubblico in base alla modalità operativa in cui si opera.

I criteri GenAI IAM sono disponibili solo con autorizzazioni di lettura/scrittura:

- **Lettura/Scrittura**: esegue e automatizza le operazioni in AWS per tuo conto insieme alle credenziali assegnate che dispongono delle autorizzazioni necessarie e convalidate per l'esecuzione.

Policy IAM per i carichi di lavoro Genai

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CloudformationGroup",
      "Effect": "Allow",
      "Action": [
        "cloudformation:CreateStack",
        "cloudformation:DescribeStacks"
      ],
      "Resource": "arn:aws:cloudformation:*:*:stack/wlmai*/*"
    },
    {
      "Sid": "EC2Group",
      "Effect": "Allow",
      "Action": [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "ec2:ResourceTag/aws:cloudformation:stack-name": "wlmai*"
        }
      }
    },
    {
      "Sid": "EC2DescribeGroup",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeRegions",
        "ec2:DescribeTags",
        "ec2:CreateVpcEndpoint",
        "ec2:CreateSecurityGroup",
        "ec2:CreateTags",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeRouteTables",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeInstances",
        "ec2:DescribeImages",
        "ec2:RevokeSecurityGroupEgress",
```

```
        "ec2:RevokeSecurityGroupIngress",
        "ec2:RunInstances"
      ],
      "Resource": "*"
    },
    {
      "Sid": "IAMGroup",
      "Effect": "Allow",
      "Action": [
        "iam:CreateRole",
        "iam:CreateInstanceProfile",
        "iam:AddRoleToInstanceProfile",
        "iam:PutRolePolicy",
        "iam:GetRolePolicy",
        "iam:GetRole",
        "iam:TagRole"
      ],
      "Resource": "*"
    },
    {
      "Sid": "IAMGroup2",
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "iam:PassedToService": "ec2.amazonaws.com"
        }
      }
    },
    {
      "Sid": "FSXNGroup",
      "Effect": "Allow",
      "Action": [
        "fsx:DescribeVolumes",
        "fsx:DescribeFileSystems",
        "fsx:DescribeStorageVirtualMachines",
        "fsx:ListTagsForResource"
      ],
      "Resource": "*"
    },
    {
      "Sid": "FSXNGroup2",
      "Effect": "Allow",
      "Action": [
        "fsx:UntagResource",
```

```
        "fsx:TagResource"
      ],
      "Resource": [
        "arn:aws:fsx:*:*:volume/*/*",
        "arn:aws:fsx:*:*:storage-virtual-machine/*/*"
      ]
    },
    {
      "Sid": "SSMParameterStore",
      "Effect": "Allow",
      "Action": [
        "ssm:GetParameter",
        "ssm:PutParameter"
      ],
      "Resource": "arn:aws:ssm:*:*:parameter/netapp/wlmai/*"
    },
    {
      "Sid": "SSM",
      "Effect": "Allow",
      "Action": [
        "ssm:GetParameters",
        "ssm:GetParametersByPath"
      ],
      "Resource": "arn:aws:ssm:*:*:parameter/aws/service/*"
    },
    {
      "Sid": "SSMMessages",
      "Effect": "Allow",
      "Action": [
        "ssm:GetCommandInvocation"
      ],
      "Resource": "*"
    },
    {
      "Sid": "SSMCommandDocument",
      "Effect": "Allow",
      "Action": [
        "ssm:SendCommand"
      ],
      "Resource": [
        "arn:aws:ssm:*:*:document/AWS-RunShellScript"
      ]
    },
    {
      "Sid": "SSMCommandInstance",
      "Effect": "Allow",
```

```
      "Action": [
        "ssm:SendCommand",
        "ssm:GetConnectionStatus"
      ],
      "Resource": [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition": {
        "StringLike": {
          "ssm:resourceTag/aws:cloudformation:stack-name": "wlmai-*"
        }
      }
    },
    {
      "Sid": "KMS",
      "Effect": "Allow",
      "Action": [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource": "*"
    },
    {
      "Sid": "SNS",
      "Effect": "Allow",
      "Action": [
        "sns:Publish"
      ],
      "Resource": "*"
    },
    {
      "Sid": "CloudWatch",
      "Effect": "Allow",
      "Action": [
        "logs:DescribeLogGroups"
      ],
      "Resource": "*"
    },
    {
      "Sid": "CloudWatchAiEngine",
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogGroup",
        "logs:PutRetentionPolicy",
        "logs:TagResource",
        "logs:DescribeLogStreams"
```

```
      ],
      "Resource": "arn:aws:logs:*:*:log-group:/netapp/wlmai*"
    },
    {
      "Sid": "CloudWatchAiEngineLogStream",
      "Effect": "Allow",
      "Action": [
        "logs:GetLogEvents"
      ],
      "Resource": "arn:aws:logs:*:*:log-group:/netapp/wlmai*:*"
    },
    {
      "Sid": "BedrockGroup",
      "Effect": "Allow",
      "Action": [
        "bedrock:InvokeModelWithResponseStream",
        "bedrock:InvokeModel",
        "bedrock:ListFoundationModels",
        "bedrock:GetFoundationModelAvailability",
        "bedrock:GetModelInvocationLoggingConfiguration",
        "bedrock:PutModelInvocationLoggingConfiguration",
        "bedrock:ListInferenceProfiles"
      ],
      "Resource": "*"
    },
    {
      "Sid": "CloudWatchBedrock",
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogGroup",
        "logs:PutRetentionPolicy",
        "logs:TagResource"
      ],
      "Resource": "arn:aws:logs:*:*:log-group:/aws/bedrock*"
    },
    {
      "Sid": "BedrockLoggingAttachRole",
      "Effect": "Allow",
      "Action": [
        "iam:AttachRolePolicy",
        "iam:PassRole"
      ],
      "Resource": "arn:aws:iam::*:role/NetApp_AI_Bedrock*"
    },
    {
      "Sid": "BedrockLoggingIamOperations",
```

```
      "Effect": "Allow",
      "Action": [
        "iam:CreatePolicy"
      ],
      "Resource": "*"
    },
    {
      "Sid": "QBusiness",
      "Effect": "Allow",
      "Action": [
        "qbusiness:ListApplications"
      ],
      "Resource": "*"
    },
    {
      "Sid": "S3",
      "Effect": "Allow",
      "Action": [
        "s3:ListAllMyBuckets"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:SimulatePrincipalPolicy"
      ],
      "Resource": "*"
    }
  ]
}
```

La tabella seguente fornisce dettagli sulle autorizzazioni per i carichi di lavoro GenAI.

Tabella delle autorizzazioni per i carichi di lavoro Genai

Scopo	Azione	Dove usato	Politica di autorizzazione
Crea uno stack di formazione cloud per un motore ai durante le operazioni di implementazione e ricostruzione	Cloud formation: CreateStack	Implementazione	Lettura/scrittura
Creare lo stack di formazione del cloud del motore ai	Cloudformation:DescripteStack	Implementazione	Lettura/scrittura
Elencare le regioni per la procedura guidata di implementazione del motore ai	ec2:DescripteRegions	Implementazione	Lettura/scrittura
Visualizzare le etichette del motore ai	ec2:DescripteTag	Implementazione	Lettura/scrittura
Elenca i bucket S3	s3:ListAllMyBucket	Implementazione	Lettura/scrittura
Elenca gli endpoint VPC prima della creazione dello stack del motore ai	EC2:CreateVpcEndpoint	Implementazione	Lettura/scrittura
Creare un gruppo di sicurezza del motore ai durante la creazione dello stack del motore ai durante le operazioni di implementazione e ricostruzione	ec2:CreateSecurityGroup	Implementazione	Lettura/scrittura
Contrassegnare le risorse create dalla creazione di stack del motore ai durante le operazioni di implementazione e ricostruzione	ec2:CreateTag	Implementazione	Lettura/scrittura
Pubblicare gli eventi crittografati nel backend WLmai dallo stack del motore ai	Km:GenerateDataKey	Implementazione	Lettura/scrittura
	Km:decrittografia	Implementazione	Lettura/scrittura
Pubblicare eventi e risorse personalizzate sul backend WLmai dallo stack ai-Engine	sns: Pubblica	Implementazione	Lettura/scrittura
Elenca i VPC durante l'implementazione guidata del motore ai	ec2:DescripteVpcs	Implementazione	Lettura/scrittura
Elencare le subnet nella procedura guidata di implementazione del motore ai	ec2:DescripteSubnet	Implementazione	Lettura/scrittura
Ottenere tabelle di routing durante la distribuzione e la ricostruzione del motore ai	ec2:DescripteRouteTable	Implementazione	Lettura/scrittura

Scopo	Azione	Dove usato	Politica di autorizzazione
Elenca le coppie di chiavi durante l'implementazione guidata del motore ai	ec2:DescripteKeyPairs	Implementazione	Lettura/scrittura
Elencare i gruppi di sicurezza durante la creazione dello stack del motore ai (per trovare gruppi di sicurezza sugli endpoint privati)	ec2:DescripteSecurityGroups	Implementazione	Lettura/scrittura
Ottieni endpoint VPC per determinare se crearne uno durante l'implementazione del motore ai	ec2:DescripteVpcEndpoint	Implementazione	Lettura/scrittura
Elencare le applicazioni aziendali Amazon Q	Qbusiness:ListApplications	Implementazione	Lettura/scrittura
Elencare le istanze per scoprire lo stato del motore ai	ec2:DescripbeInstances	Risoluzione dei problemi	Lettura/scrittura
Elenca le immagini durante la creazione dello stack del motore ai durante le operazioni di implementazione e ricostruzione	ec2:DescripteImages	Implementazione	Lettura/scrittura
Creare e aggiornare l'istanza ai e il gruppo di sicurezza dell'endpoint privato durante la creazione dello stack dell'istanza ai durante le operazioni di distribuzione e ricostruzione	ec2:RevokeSecurityGroupErgress	Implementazione	Lettura/scrittura
	ec2:RevokeSecurityGroupIngress	Implementazione	Lettura/scrittura
Esegui un motore ai durante la creazione di uno stack di formazione del cloud durante le operazioni di implementazione e ricostruzione	ec2:RunInstances	Implementazione	Lettura/scrittura
Collegare il gruppo di sicurezza e modificare le regole per il motore ai durante la creazione dello stack durante le operazioni di distribuzione e ricostruzione	ec2:AuthorizeSecurityGroupErgress	Implementazione	Lettura/scrittura
	ec2:AuthorizeSecurityGroupIngress	Implementazione	Lettura/scrittura
Avviare una richiesta di chat su uno dei modelli di base	Bedrock:InvokeModelWithResponseStream	Implementazione	Lettura/scrittura
Inizia la richiesta di chat/integrazione per i modelli di base	Bedrock:InvokeModel	Implementazione	Lettura/scrittura
Mostra i modelli di base disponibili in una regione	Bedrock:ListFoundationModels	Implementazione	Lettura/scrittura
Ottieni informazioni su un modello di base	Bedrock:GetFoundationModel	Implementazione	Lettura/scrittura

Scopo	Azione	Dove usato	Politica di autorizzazione
Verifica dell'accesso al modello di base	Bedrock:GetFoundationModelAvailability	Implementazione	Lettura/scrittura
Verifica la necessità di creare un gruppo di log Amazon CloudWatch durante le operazioni di distribuzione e ricostruzione	Registri:DescribeLogGroups	Implementazione	Lettura/scrittura
Ottieni regioni che supportano FSX e Amazon Bedrock durante la procedura guidata del motore di ai	ssm:GetParametersByPath	Implementazione	Lettura/scrittura
Ottieni l'ultima immagine di Amazon Linux per l'implementazione del motore ai durante le operazioni di implementazione e ricostruzione	ssm:GetParameters	Implementazione	Lettura/scrittura
Ottenere la risposta SSM dal comando inviato al motore ai	ssm:GetCommandInvocation	Implementazione	Lettura/scrittura
Controllare il collegamento SSM al motore ai	ssm:SendCommand	Implementazione	Lettura/scrittura
	ssm:GetConnectionStatus	Implementazione	Lettura/scrittura
Creare un profilo di istanza del motore ai durante la creazione dello stack durante le operazioni di implementazione e ricostruzione	iam: CreateRole	Implementazione	Lettura/scrittura
	iam:CreateInstanceProfile	Implementazione	Lettura/scrittura
	iam:AddRoleToInstanceProfile	Implementazione	Lettura/scrittura
	iam:PutRolePolicy	Implementazione	Lettura/scrittura
	iam:GetRolePolicy	Implementazione	Lettura/scrittura
	iam: GetRole	Implementazione	Lettura/scrittura
	iam: TagRole	Implementazione	Lettura/scrittura
	iam: PassRole	Implementazione	Lettura/scrittura
Simula le operazioni del carico di lavoro per validare le autorizzazioni disponibili e confrontarle con le autorizzazioni necessarie per gli account AWS	iam:SimulatePrincipalPolicy	Implementazione	Lettura/scrittura

Scopo	Azione	Dove usato	Politica di autorizzazione
Elenca file system FSX per ONTAP durante la procedura guidata "Crea knowledgebase"	fsx:DescribeVolumes	Creazione di una Knowledge base	Lettura/scrittura
Elencare FSX per i volumi del file system ONTAP durante la procedura guidata "Crea knowledgebase"	fsx:DescribeFileSystems	Creazione di una Knowledge base	Lettura/scrittura
Gestire knowledge base sul motore ai durante le operazioni di ricostruzione	fsx:ListTagsForResource	Risoluzione dei problemi	Lettura/scrittura
Elenca FSX per le macchine virtuali di storage del file system ONTAP durante la procedura guidata "Crea knowledgebase"	fsx:DescribeStorageVirtualMachines	Implementazione	Lettura/scrittura
Spostare la knowledgebase in una nuova istanza	fsx:UntagResource	Risoluzione dei problemi	Lettura/scrittura
Gestire la knowledgebase sul motore ai durante la ricostruzione	FSX:TagResource	Risoluzione dei problemi	Lettura/scrittura
Salvare i segreti SSM (token ECR, credenziali CIFS, chiavi degli account del servizio di locazione) in modo sicuro	ssm:getParameter	Implementazione	Lettura/scrittura
	ssm: Parametro di PutMeter	Implementazione	Lettura/scrittura
Invia i log del motore ai al gruppo di log di Amazon CloudWatch durante le operazioni di implementazione e ricostruzione	Registri:CreateLogGroup	Implementazione	Lettura/scrittura
	Registri:PutRetentionPolicy	Implementazione	Lettura/scrittura
Inviare i registri del motore ai al gruppo di log di Amazon CloudWatch	Registri:TagResource	Risoluzione dei problemi	Lettura/scrittura
Ottieni la risposta SSM da Amazon CloudWatch (quando la risposta è troppo lunga)	Registri:DescribeLogStreams	Risoluzione dei problemi	Lettura/scrittura
Ottieni la risposta SSM da Amazon CloudWatch	Registri:GetLogEvents	Risoluzione dei problemi	Lettura/scrittura
Creare un gruppo di log Amazon CloudWatch per i registri Amazon Bedrock durante la creazione dello stack durante le operazioni di distribuzione e ricostruzione	Registri:CreateLogGroup	Implementazione	Lettura/scrittura
	Registri:PutRetentionPolicy	Implementazione	Lettura/scrittura
	Registri:TagResource	Implementazione	Lettura/scrittura
Elenca profili di deduzione per il modello	Bedrock:ListInferenceProfiles	Risoluzione dei problemi	Lettura/scrittura

Autorizzazioni per i carichi di lavoro VMware

Per i carichi di lavoro VMware è possibile scegliere tra le seguenti policy di autorizzazione:

- **Visualizzazione, pianificazione e analisi**: visualizza l'inventario degli ambienti di virtualizzazione EVS, ottieni un'analisi ben progettata per i tuoi sistemi ed esplora i risparmi.
- **Distribuzione e connettività del datastore**: distribuisci i layout VM consigliati sui cluster Amazon EVS, Amazon EC2 o VMware Cloud su AWS vSphere e utilizza i file system Amazon FSx for NetApp ONTAP personalizzati come datastore esterni.

Selezionare la policy di autorizzazione per visualizzare le policy IAM richieste:

Criteri IAM per i carichi di lavoro VMware

Visualizzazione, pianificazione e analisi

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeRegions",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeDhcpOptions",
        "kms:DescribeKey",
        "kms:ListKeys",
        "kms:ListAliases",
        "secretsmanager:ListSecrets",
        "evs:ListEnvironments",
        "evs:GetEnvironment",
        "evs:ListEnvironmentVlans"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:SimulatePrincipalPolicy"
      ],
      "Resource": "*"
    }
  ]
}
```

Distribuzione e connettività del datastore

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cloudformation:CreateStack"
      ],
      "Resource": "*"
```

```
    },
    {
      "Effect": "Allow",
      "Action": [
        "fsx:CreateFileSystem",
        "fsx:DescribeFileSystems",
        "fsx:CreateStorageVirtualMachine",
        "fsx:DescribeStorageVirtualMachines",
        "fsx:CreateVolume",
        "fsx:DescribeVolumes",
        "fsx:TagResource",
        "sns:Publish",
        "kms:GenerateDataKey",
        "kms:Decrypt",
        "kms:CreateGrant"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:RunInstances",
        "ec2:DescribeInstances",
        "ec2:CreateSecurityGroup",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DescribeImages"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:SimulatePrincipalPolicy"
      ],
      "Resource": "*"
    }
  ]
}
```

Nella tabella seguente vengono forniti dettagli sulle autorizzazioni per i carichi di lavoro VMware.

Tabella delle autorizzazioni per i carichi di lavoro VMware

Scopo	Azione	Dove usato	Politica di autorizzazione
Collegare i gruppi di sicurezza e modificare le regole per i nodi sottoposti a provisioning	ec2:AuthorizeSecurityGroupIngress	Implementazione	Distribuzione e connettività del datastore
Creare volumi EBS	fsx:CreateVolume	Implementazione	Distribuzione e connettività del datastore
Contrassegna i valori personalizzati per le risorse FSX per NetApp ONTAP create da carichi di lavoro VMware	FSX:TagResource	Implementazione	Distribuzione e connettività del datastore
Creare e convalidare il modello CloudFormation	Cloud formation: CreateStack	Implementazione	Distribuzione e connettività del datastore
Gestire i tag e la sicurezza di rete sulle istanze create	ec2:CreateSecurityGroup	Implementazione	Distribuzione e connettività del datastore
Avviare le istanze create	ec2:RunInstances	Implementazione	Distribuzione e connettività del datastore
Ottieni dettagli sull'istanza di EC2	ec2:DescripbeInstances	Inventario	Distribuzione e connettività del datastore
Elencare le immagini durante la creazione dello stack durante le operazioni di distribuzione e ricostruzione	ec2:DescripteImages	Inventario	Distribuzione e connettività del datastore
Visualizza i dettagli di configurazione dei set di opzioni DHCP associati alle VPC	ec2:DescriviDhcpOptions	Inventario	Visualizzazione, pianificazione e analisi
Scaricare i VPC nell'ambiente selezionato per completare il modulo di distribuzione	ec2:DescripteVpcs	• Implementazione • Inventario	Visualizzazione, pianificazione e analisi
Ottenere le subnet nell'ambiente selezionato per completare il modulo di distribuzione	ec2:DescripteSubnet	• Implementazione • Inventario	Visualizzazione, pianificazione e analisi

Scopo	Azione	Dove usato	Politica di autorizzazione
Ottenere i gruppi di protezione nell'ambiente selezionato per completare il modulo di distribuzione	ec2:DescripteSecurityGroups	Implementazione	Visualizzazione, pianificazione e analisi
Ottieni le zone di disponibilità in un ambiente selezionato	EC2:DescribeAvailabilityZones	• Implementazione • Inventario	Visualizzazione, pianificazione e analisi
Ottieni le regioni con il supporto di Amazon FSX per NetApp ONTAP	ec2:DescripteRegions	Implementazione	Visualizzazione, pianificazione e analisi
Ottieni gli alias delle chiavi KMS da utilizzare per la crittografia Amazon FSX per NetApp ONTAP	Km:ListAlias	Implementazione	Visualizzazione, pianificazione e analisi
Ottieni le chiavi KMS da utilizzare per la crittografia di Amazon FSX per NetApp ONTAP	Km:ListKeys	Implementazione	Visualizzazione, pianificazione e analisi
Ottieni i dettagli sulla scadenza delle chiavi KMS da utilizzare per la crittografia di Amazon FSX per NetApp ONTAP	Km: DescribeKey	Implementazione	Visualizzazione, pianificazione e analisi
Elenca i segreti in AWS Secrets Manager	secretmanager:ListSecrets	Inventario	Visualizzazione, pianificazione e analisi
Ottieni un elenco di ambienti da Amazon EVS	evs:ListEnvironments	Inventario	Visualizzazione, pianificazione e analisi
Ottieni informazioni dettagliate su uno specifico ambiente Amazon EVS	evs:GetEnvironment	Inventario	Visualizzazione, pianificazione e analisi
Elenca le VLAN associate a un ambiente Amazon EVS	evs:ListEnvironmentVlans	Inventario	Visualizzazione, pianificazione e analisi

Scopo	Azione	Dove usato	Politica di autorizzazione
Crea le risorse Amazon FSX per NetApp ONTAP necessarie per il provisioning	fsx:CreateFileSystem	Implementazione	Distribuzione e connettività del datastore
	fsx:CreateStorageVirtualMachine	Implementazione	Distribuzione e connettività del datastore
	fsx:CreateVolume	• Implementazione • Operazioni di gestione	Distribuzione e connettività del datastore
Ottieni i dettagli di Amazon FSX per NetApp ONTAP	fsx:descrivere*	• Implementazione • Inventario • Operazioni di gestione • Scopri i risparmi	Distribuzione e connettività del datastore
Ottieni i dettagli chiave del KMS e utilizza la crittografia per Amazon FSX per NetApp ONTAP	Km: CreateGrant	Implementazione	Distribuzione e connettività del datastore
	Km:descrivere*	Implementazione	Visualizzazione, pianificazione e analisi
	Km: Elenco*	Implementazione	Visualizzazione, pianificazione e analisi
	Km:decrittografia	Implementazione	Distribuzione e connettività del datastore
	Km:GenerateDataKey	Implementazione	Distribuzione e connettività del datastore
Elencare gli argomenti SNS dei clienti e pubblicarli su SNS back-end WLMVMC e SNS dei clienti, se selezionati	sns: Pubblica	Implementazione	Distribuzione e connettività del datastore

Scopo	Azione	Dove usato	Politica di autorizzazione
Simula le operazioni del carico di lavoro per validare le autorizzazioni disponibili e confrontarle con le autorizzazioni necessarie per gli account AWS	iam:SimulatePrincipalPolicy	Implementazione	• Distribuzione e connettività del datastore • Visualizzazione, pianificazione e analisi

Registro delle modifiche

Man mano che le autorizzazioni vengono aggiunte e rimosse, le annoteremo nelle sezioni seguenti.

1 febbraio 2025

Sono state aggiunte le seguenti autorizzazioni al carico di lavoro Archiviazione:

- `s3:TagResource`
- `s3:ListTagsForResource`
- `s3:UntagResource`
- `s3tables:CreateTableBucket`
- `s3tables:ListTables`
- `s3tables:GetTable`
- `s3tables:GetTableMetadataLocation`
- `s3tables:CreateTable`
- `s3tables:GetNamespace`
- `s3tables:PutTableData`
- `s3tables:CreateNamespace`
- `s3tables:GetTableData`
- `s3tables:ListNamespaces`
- `s3tables:ListTableBuckets`
- `s3tables:GetTableBucket`
- `s3tables:UpdateTableMetadataLocation`
- `s3tables:ListTagsForResource`
- `s3tables:TagResource`

- `s3:GetObjectTagging`
- `s3:ListBucket`

04 dicembre 2025

Sono state aggiunte le seguenti autorizzazioni al carico di lavoro Archiviazione:

- `fsx:CreateAndAttachS3AccessPoint`
- `fsx:DetachAndDeleteS3AccessPoint`
- `s3:CreateAccessPoint`
- `s3:DeleteAccessPoint`

27 novembre 2025

Sono state aggiunte le seguenti autorizzazioni al carico di lavoro Archiviazione:

- `bedrock:ListInferenceProfiles`
- `bedrock:GetInferenceProfile`
- `bedrock:InvokeModelWithResponseStream`
- `bedrock:InvokeModel`

2 novembre 2025

I criteri di autorizzazione "sola lettura" e "lettura/scrittura" sono stati sostituiti nei carichi di lavoro di archiviazione, database e VMware per garantire maggiore granularità e flessibilità nell'assegnazione delle autorizzazioni.

5 ottobre 2025

Le seguenti autorizzazioni sono state rimosse da GenAI e ora sono gestite dal motore GenAI:

- `bedrock:GetModelInvocationLoggingConfiguration`
- `bedrock:PutModelInvocationLoggingConfiguration`
- `iam:AttachRolePolicy`
- `iam:PassRole`
- `iam:CreatePolicy`

29 giugno 2025

La seguente autorizzazione è ora disponibile in modalità *sola lettura* per i database: `cloudwatch:GetMetricData` .

3 giugno 2025

La seguente autorizzazione è ora disponibile in modalità *lettura/scrittura* per GenAI: `s3:ListAllMyBuckets` .

4 maggio 2025

La seguente autorizzazione è ora disponibile in modalità *lettura/scrittura* per GenAI: `qbusiness:ListApplications` .

Le seguenti autorizzazioni sono ora disponibili in modalità *sola lettura* per i database:

- `logs:GetLogEvents`
- `logs:DescribeLogGroups`

La seguente autorizzazione è ora disponibile in modalità *lettura/scrittura* per i database: `logs:PutRetentionPolicy` .

2 aprile 2025

La seguente autorizzazione è ora disponibile in modalità *sola lettura* per i database: `ssm:DescribeInstanceInformation` .

30 marzo 2025

Aggiornamento delle autorizzazioni del carico di lavoro Genai

Le seguenti autorizzazioni sono ora disponibili in *modalità lettura/scrittura* per GenAI:

- `bedrock:PutModelInvocationLoggingConfiguration`
- `iam:AttachRolePolicy`
- `iam:PassRole`
- `iam:createPolicy`
- `bedrock:ListInferenceProfiles`

La seguente autorizzazione è stata rimossa dalla *modalità lettura/scrittura* per GenAI: `Bedrock:GetFoundationModel` .

iam:aggiornamento delle autorizzazioni di SimulatePrincipalPolicy

IL `iam:SimulatePrincipalPolicy` l'autorizzazione fa parte di tutte le policy di autorizzazione del carico di lavoro se si abilita il controllo automatico delle autorizzazioni quando si aggiungono ulteriori credenziali dell'account AWS o si aggiunge una nuova funzionalità del carico di lavoro dalla console Workload Factory. L'autorizzazione simula le operazioni del carico di lavoro e verifica se si dispone delle autorizzazioni necessarie per l'account AWS prima di distribuire le risorse da Workload Factory. L'abilitazione di questo controllo riduce il tempo e lo sforzo necessari per ripulire le risorse dalle operazioni non riuscite e per aggiungere autorizzazioni mancanti.

2 marzo 2025

La seguente autorizzazione è ora disponibile in modalità *lettura/scrittura* per GenAI: `bedrock:GetFoundationModel` .

3 febbraio 2025

La seguente autorizzazione è ora disponibile in modalità *sola lettura* per i database:

`iam:SimulatePrincipalPolicy`.

Avvio rapido per NetApp Workload Factory

Per iniziare a usare NetApp Workload Factory, registrati e crea un account, aggiungi le credenziali in modo che Workload Factory possa gestire direttamente le risorse AWS e quindi ottimizzare i tuoi carichi di lavoro utilizzando Amazon FSx for NetApp ONTAP.

NetApp Workload Factory è accessibile agli utenti come servizio cloud dalla console basata sul Web. Prima di iniziare, dovresti avere una comprensione di"Fabbrica del carico di lavoro" .

1 **Registrati e crea un account**

Vai al "Console Workload Factory" , registrati e crea un account.

"Scopri come iscriversi e creare un account".

2 **Aggiungi le credenziali AWS a Workload Factory**

Questo passaggio è facoltativo. Puoi utilizzare Workload Factory senza aggiungere credenziali per accedere al tuo account AWS. Aggiungendo le credenziali AWS a Workload Factory, il tuo account Workload Factory ottiene le autorizzazioni necessarie per creare e gestire i file system FSx for ONTAP e per distribuire e gestire carichi di lavoro specifici, come database e GenAI.

"Scopri come aggiungere credenziali al tuo account".

3 **Ottimizza i tuoi carichi di lavoro con FSX per ONTAP**

Dopo esserti registrato, aver creato un account e, facoltativamente, aver aggiunto le credenziali AWS, puoi iniziare a utilizzare Workload Factory per ottimizzare i tuoi carichi di lavoro tramite FSx for ONTAP.

"Ottimizza i tuoi carichi di lavoro con FSx per ONTAP" .

Iscriviti a NetApp Workload Factory

NetApp Workload Factory è accessibile tramite una console basata sul Web. Quando inizi a utilizzare Workload Factory, il primo passo è registrarti utilizzando le credenziali del tuo sito di supporto NetApp o creando un accesso cloud NetApp .

Puoi anche invitare altri ad unirsi al tuo account Workload Factory in modo che possano accedere e utilizzare Workload Factory.

Iscriviti a Workload Factory

Puoi registrarti a Workload Factory utilizzando una delle seguenti opzioni:

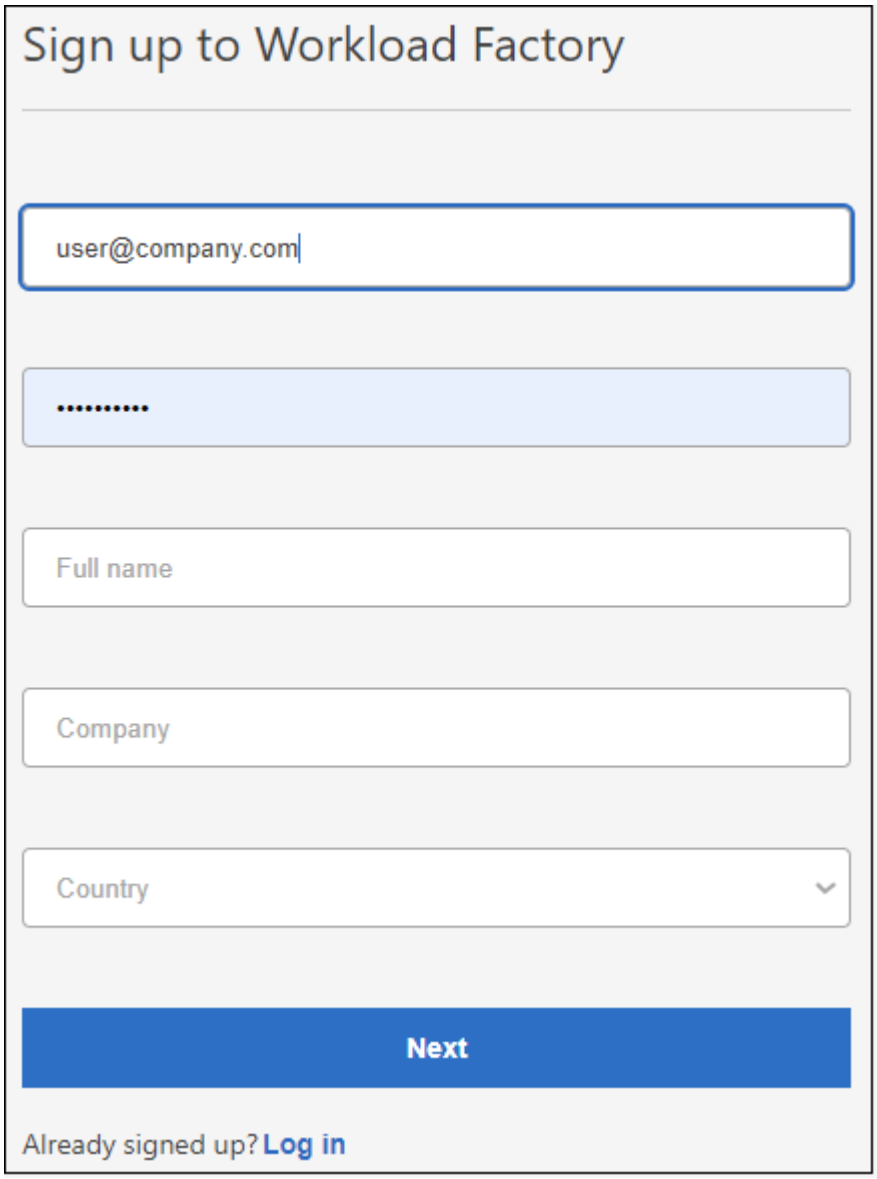
- Le tue credenziali NetApp Support Site (NSS) esistenti
- Un login cloud NetApp specificando il tuo indirizzo e-mail e una password

Fasi

1. Apri un browser web e vai su "Console Workload Factory"
2. Se disponi di un account NetApp Support Site, inserisci l'indirizzo e-mail associato al tuo account NSS direttamente nella pagina **Log in**.

   Se hai un account NSS puoi saltare la pagina di registrazione. Workload Factory ti registrerà durante questo accesso iniziale.

3. Se non disponi di un account NSS e desideri registrarti creando un login cloud NetApp, seleziona **Registrati**.



4. Nella pagina **Iscrizione**, immettere le informazioni richieste per creare un login cloud NetApp e selezionare **Avanti**.

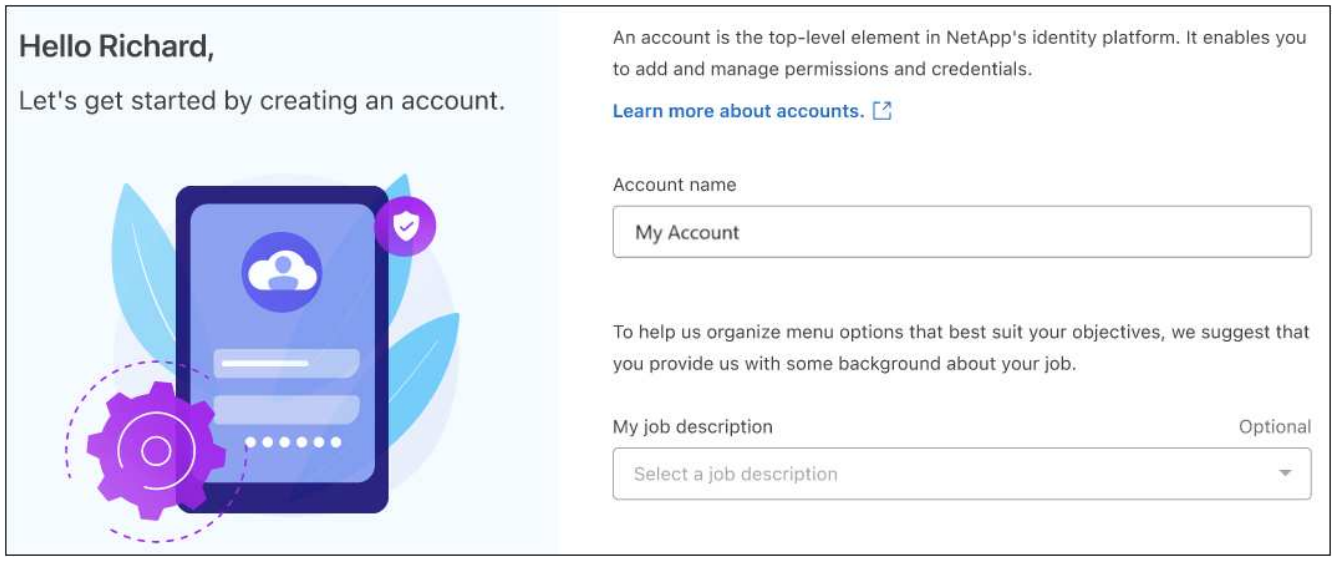
   Nel modulo di iscrizione sono consentiti solo caratteri inglesi.

5. Immettere le informazioni dettagliate relative alla società e selezionare **Iscrizione**.
6. Controlla la posta in arrivo per un messaggio e-mail da NetApp che includa le istruzioni per la verifica dell'indirizzo e-mail.

Questo passaggio è necessario prima di effettuare l'accesso.

7. Quando richiesto, leggere il Contratto di licenza per l'utente finale e accettare i termini, quindi selezionare **continua**.
8. Nella pagina **account**, immettere un nome per l'account e, se necessario, selezionare la descrizione del lavoro.

   Un account è l'elemento di primo livello della piattaforma di identità di NetApp e ti consente di aggiungere e gestire autorizzazioni e credenziali.



9. Selezionare **Crea** e verrà visualizzata la home page di Workload Factory.

Risultato

Ora hai un login e un account Workload Factory. Sei considerato un amministratore dell'account e hai accesso a tutte le funzionalità di Workload Factory.

Invita altri a unirsi a un account in Workload Factory

In qualità di amministratore dell'account, puoi invitare altri a unirsi al tuo account Workload Factory in modo che possano accedere e utilizzare Workload Factory. La gestione dell'account è possibile solo dalla NetApp Console.

Fare riferimento alla documentazione NetApp Console per "scopri come aggiungere membri (account utente)", al tuo account Workload Factory.

Risultato

L'utente invitato riceverà un'e-mail con le istruzioni per unirsi al tuo account Workload Factory.

Aggiungi le credenziali AWS a Workload Factory

Aggiungi e gestisci le credenziali AWS in modo che NetApp Workload Factory disponga delle autorizzazioni necessarie per distribuire e gestire le risorse cloud nei tuoi account AWS.

Panoramica

È possibile aggiungere le credenziali AWS a un account Workload Factory esistente dalla pagina Credenziali. Ciò fornisce a Workload Factory le autorizzazioni necessarie per gestire risorse e processi all'interno del tuo ambiente cloud AWS.

È possibile aggiungere credenziali utilizzando due metodi:

- **Manualmente**: crei la policy IAM e il ruolo IAM nel tuo account AWS mentre aggiungi le credenziali in Workload Factory.
- **Automaticamente**: È possibile acquisire una quantità minima di informazioni sulle autorizzazioni e utilizzare uno stack CloudFormation per creare i criteri e il ruolo IAM per le credenziali.

Credenziali AWS

Abbiamo progettato un flusso di registrazione con credenziali AWS presumono il ruolo che:

- Supporto di autorizzazioni degli account AWS più allineate, consentendoti di specificare le funzionalità dei workload che desideri utilizzare e fornendo requisiti di policy IAM in base a tali selezioni.
- Consente di regolare le autorizzazioni degli account AWS assegnate in base al consenso esplicito o di esclusione di funzionalità specifiche dei carichi di lavoro.
- Semplifica la creazione manuale delle policy IAM fornendo file di policy JSON personalizzati che puoi applicare nella console AWS.
- Semplifica ulteriormente il processo di registrazione delle credenziali offrendo agli utenti un'opzione automatica per la creazione di ruoli e policy IAM richieste utilizzando gli stack di AWS CloudFormation.
- Si allinea in modo migliore con FSX per gli utenti ONTAP che preferiscono avere le proprie credenziali memorizzate entro i confini dell'ecosistema cloud di AWS, consentendo lo storage delle credenziali dei servizi FSX per ONTAP in un backend di gestione segreta basato su AWS.

Una o più credenziali AWS

Quando utilizzi la tua prima funzionalità (o funzionalità) di Workload Factory, dovrai creare le credenziali utilizzando le autorizzazioni richieste per tali funzionalità del carico di lavoro. Aggiungerai le credenziali a Workload Factory, ma dovrai accedere alla AWS Management Console per creare il ruolo e la policy IAM. Queste credenziali saranno disponibili nel tuo account quando utilizzi qualsiasi funzionalità di Workload Factory.

Il set iniziale di credenziali AWS può includere una policy di autorizzazioni IAM per una o più funzionalità. Dipende dalle esigenze della tua attività.

L'aggiunta di più di un set di credenziali AWS a Workload Factory fornisce autorizzazioni aggiuntive necessarie per utilizzare funzionalità aggiuntive, come i file system FSx for ONTAP , distribuire database su FSx for ONTAP, migrare carichi di lavoro VMware e altro ancora.

Aggiungere manualmente le credenziali a un account

Puoi aggiungere manualmente le credenziali AWS a Workload Factory per concedere al tuo account Workload Factory le autorizzazioni necessarie per gestire le risorse AWS che utilizzerai per eseguire i tuoi carichi di lavoro esclusivi. Ogni set di credenziali aggiunto includerà una o più policy IAM in base alle funzionalità del carico di lavoro che si desidera utilizzare e un ruolo IAM assegnato al proprio account.

È possibile aggiungere le credenziali AWS a un account dalla console Workload Factory o dalla console NetApp .

Le credenziali vengono create in tre parti:

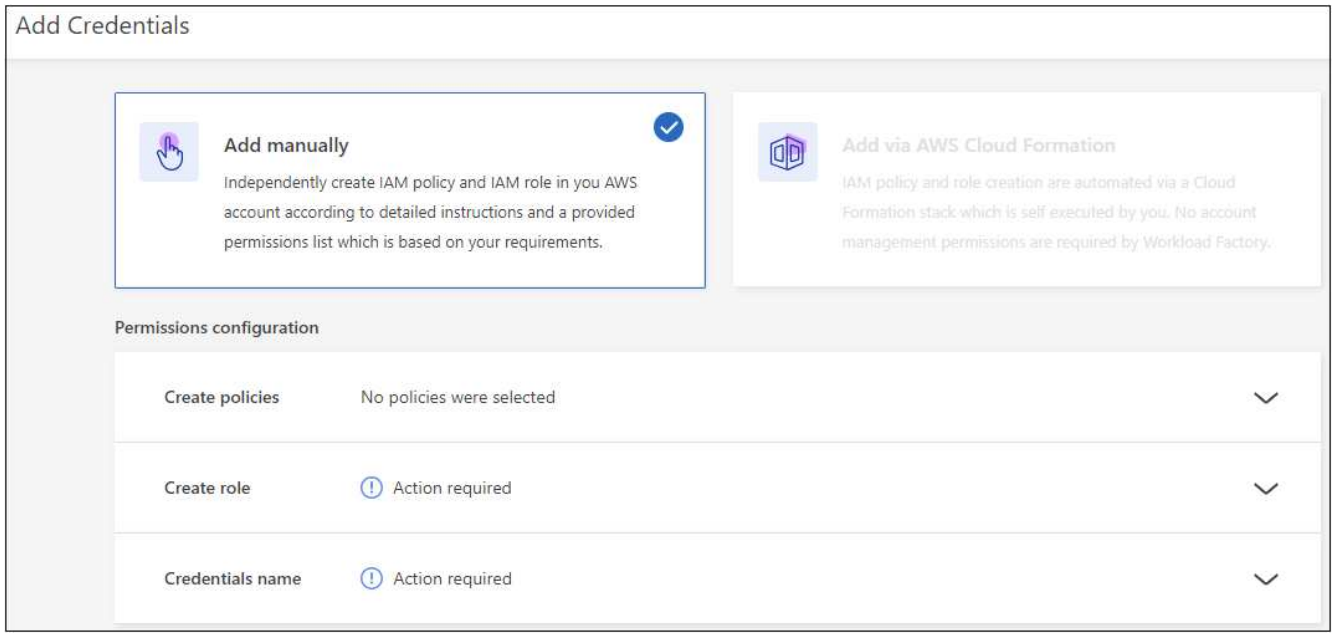
- Seleziona i servizi e i livelli di autorizzazioni che desideri utilizzare, quindi crea le policy IAM dalla Console di gestione AWS.
- Creare un ruolo IAM dalla Console di gestione AWS.
- Da Workload Factory, inserisci un nome e aggiungi le credenziali.

Prima di iniziare

Devi disporre delle credenziali per accedere al tuo account AWS.

Fasi

1. Accedi al "Console Workload Factory" .
2. Dal menu, seleziona **Amministrazione** e poi **Credenziali**.
3. Nella pagina credenziali, selezionare **Aggiungi credenziali**.
4. Nella pagina Aggiungi credenziali, selezionare **Aggiungi manualmente**, quindi attenersi alla seguente procedura per completare ogni sezione in *Configurazione autorizzazioni*.



Fase 1: Selezionare le capacità del carico di lavoro e creare i criteri IAM

In questa sezione è possibile scegliere quali tipi di funzionalità del carico di lavoro saranno gestibili come parte di queste credenziali e le autorizzazioni abilitate per ogni carico di lavoro. Per creare le policy, dovrai copiare da Codebox le autorizzazioni delle policy per ogni carico di lavoro selezionato e aggiungerle ad AWS Management Console all'interno dell'account AWS.

Fasi

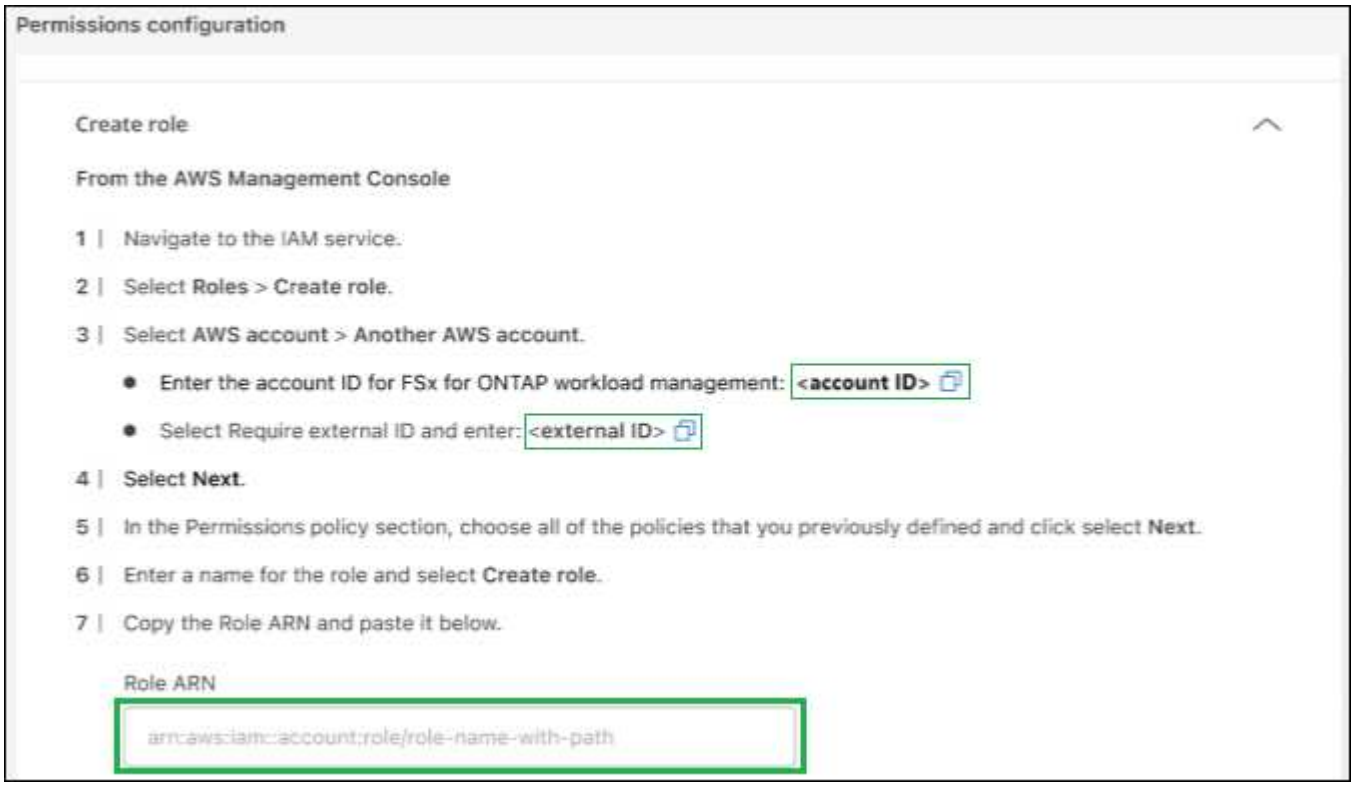
1. Nella sezione **Crea criteri**, abilitare ciascuna funzionalità del carico di lavoro che si desidera includere in queste credenziali.

Puoi aggiungere funzionalità in un secondo momento, quindi seleziona solo i carichi di lavoro da implementare e gestire.

2. Per le funzionalità del carico di lavoro che offrono una scelta di criteri di autorizzazione, selezionare il tipo di autorizzazioni che saranno disponibili con queste credenziali.
3. Facoltativo: Selezionare **Abilita controllo automatico autorizzazioni** per verificare se si dispone delle autorizzazioni necessarie per completare le operazioni del carico di lavoro. L'attivazione del segno di spunta aggiunge `iam:SimulatePrincipalPolicy permission` ai criteri di autorizzazione. Lo scopo di questa autorizzazione è solo confermare le autorizzazioni. È possibile rimuovere l'autorizzazione dopo aver aggiunto le credenziali, ma si consiglia di conservarla per evitare la creazione di risorse per operazioni parzialmente riuscite e per evitare di eliminare qualsiasi pulitura manuale delle risorse richiesta.
4. Nella finestra Codebox, copiare le autorizzazioni per il primo criterio IAM.
5. Apri un'altra finestra del browser ed effettua l'accesso al tuo account AWS in AWS Management Console.
6. Aprire il servizio IAM, quindi selezionare **Criteri** > **Crea criterio**.
7. Selezionare JSON come tipo di file, incollare le autorizzazioni copiate al passaggio 3 e selezionare **Avanti**.
8. Immettere il nome del criterio e selezionare **Crea criterio**.
9. Se nel passaggio 1 sono state selezionate più funzionalità del carico di lavoro, ripetere questi passaggi per creare un criterio per ogni gruppo di autorizzazioni del carico di lavoro.

Passaggio 2: Creare il ruolo IAM che utilizza i criteri

In questa sezione configurerai un ruolo IAM che Workload Factory assumerà e che include le autorizzazioni e i criteri appena creati.



Fasi

1. Nella Console di gestione AWS, selezionare **ruoli > Crea ruolo**.
2. In **Trusted entity type**, selezionare **AWS account**.

a. Seleziona **Un altro account AWS** e copia e incolla l'ID account per la gestione del carico di lavoro FSx for ONTAP dall'interfaccia utente di Workload Factory.
b. Selezionare **ID esterno richiesto** e copiare e incollare l'ID esterno dall'interfaccia utente di Workload Factory.

3. Selezionare **Avanti**.
4. Nella sezione Criteri autorizzazioni, scegliere tutti i criteri definiti in precedenza e selezionare **Avanti**.
5. Immettere un nome per il ruolo e selezionare **Crea ruolo**.
6. Copiare il ruolo ARN.
7. Torna alla pagina Aggiungi credenziali in Workload Factory, espandi la sezione **Crea ruolo** in **Configurazione autorizzazioni** e incolla l'ARN nel campo *ARN ruolo*.

Passaggio 3: Immettere un nome e aggiungere le credenziali

Il passaggio finale consiste nell'inserire un nome per le credenziali in Workload Factory.

Fasi

1. Dalla pagina Aggiungi credenziali in Workload Factory, espandi **Nome credenziali** in **Configurazione autorizzazioni**.
2. Immettere il nome che si desidera utilizzare per queste credenziali.
3. Selezionare **Aggiungi** per creare le credenziali.

Risultato

Le credenziali vengono create e viene visualizzata nuovamente la pagina credenziali.

Aggiungere credenziali a un account utilizzando CloudFormation

Puoi aggiungere le credenziali AWS a Workload Factory utilizzando uno stack AWS CloudFormation selezionando le funzionalità di Workload Factory che desideri utilizzare e quindi avviando lo stack AWS CloudFormation nel tuo account AWS. CloudFormation creerà i criteri IAM e il ruolo IAM in base alle capacità del carico di lavoro selezionate.

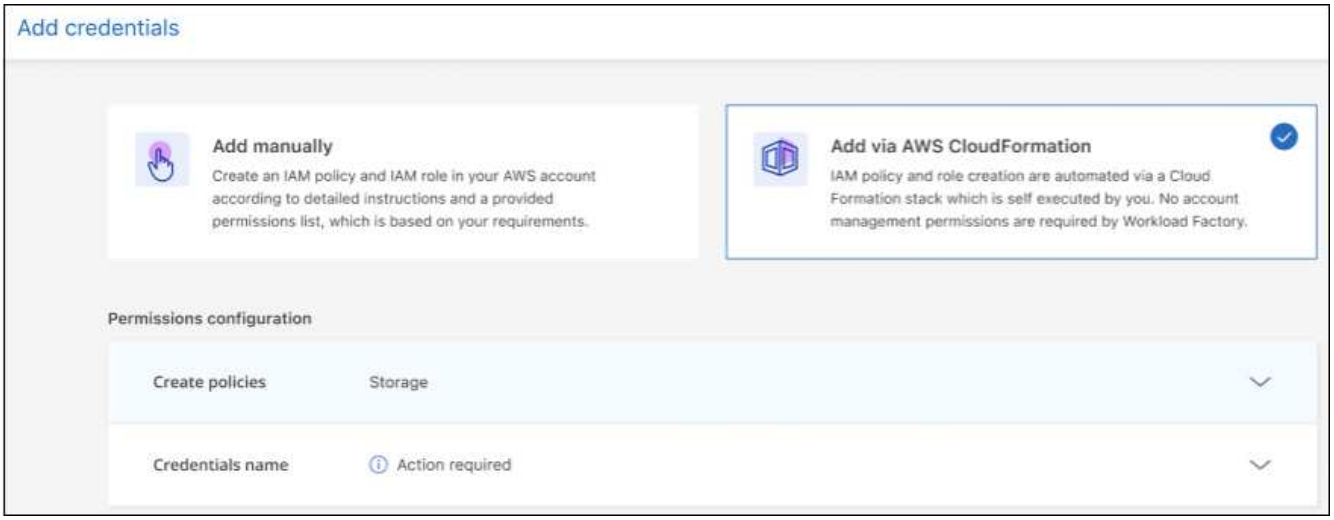
Prima di iniziare

- Devi disporre delle credenziali per accedere al tuo account AWS.
- Quando si aggiungono credenziali utilizzando uno stack CloudFormation, è necessario disporre delle seguenti autorizzazioni nell'account AWS:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cloudformation:CreateStack",
        "cloudformation:UpdateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:ListStacks",
        "cloudformation:ListStackResources",
        "cloudformation:GetTemplate",
        "cloudformation:ValidateTemplate",
        "lambda:InvokeFunction",
        "iam:PassRole",
        "iam:CreateRole",
        "iam:UpdateAssumeRolePolicy",
        "iam:AttachRolePolicy",
        "iam:CreateServiceLinkedRole"
      ],
      "Resource": "*"
    }
  ]
}
```

Fasi

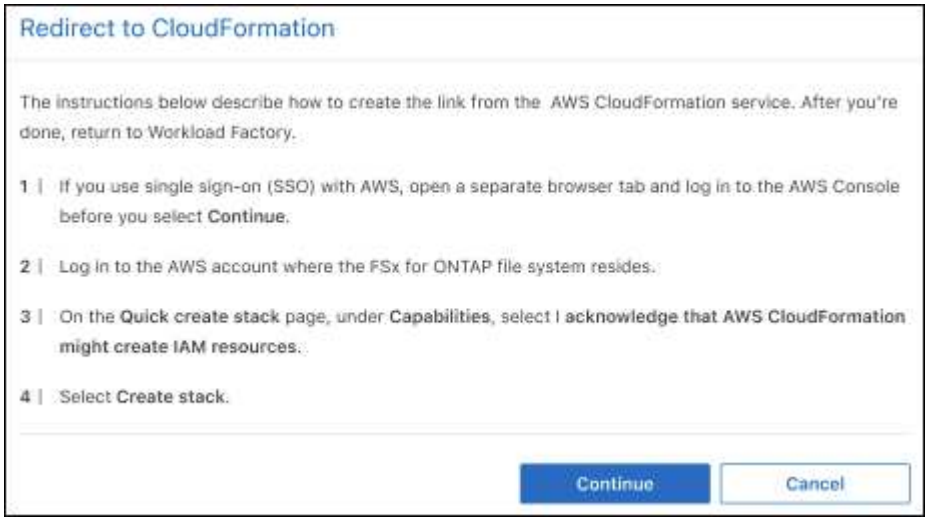
1. Accedi al "Console Workload Factory" .
2. Dal menu, seleziona **Amministrazione** e poi **Credenziali**.
3. Nella pagina credenziali, selezionare **Aggiungi credenziali**.
4. Selezionare **Aggiungi tramite AWS CloudFormation**.



5. In **Crea criteri**, abilitare tutte le funzionalità del carico di lavoro che si desidera includere in queste credenziali e scegliere un livello di autorizzazione per ogni carico di lavoro.

   Puoi aggiungere funzionalità in un secondo momento, quindi seleziona solo i carichi di lavoro da implementare e gestire.

6. Facoltativo: Selezionare **Abilita controllo automatico autorizzazioni** per verificare se si dispone delle autorizzazioni necessarie per completare le operazioni del carico di lavoro. L'attivazione del controllo aggiunge l' `iam:SimulatePrincipalPolicy`autorizzazione ai criteri di autorizzazione. Lo scopo di questa autorizzazione è solo confermare le autorizzazioni. È possibile rimuovere l'autorizzazione dopo aver aggiunto le credenziali, ma si consiglia di conservarla per evitare la creazione di risorse per operazioni parzialmente riuscite e per evitare di eliminare qualsiasi pulitura manuale delle risorse richiesta.
7. In **Nome credenziali**, immettere il nome che si desidera utilizzare per queste credenziali.
8. Aggiungi le credenziali da AWS CloudFormation:
   a. Selezionare **Aggiungi** (oppure selezionare **Reindirizza a CloudFormation**) per visualizzare la pagina Reindirizza a CloudFormation.



   b. Se si utilizza il single sign-on (SSO) con AWS, aprire una scheda separata del browser ed effettuare l'accesso alla console AWS prima di selezionare **continua**.

      Devi accedere all'account AWS in cui si trova il file system FSX per ONTAP.

c. Selezionare **continua** dalla pagina Redirect to CloudFormation.

d. Nella pagina creazione rapida stack, in funzionalità, selezionare **Acknowledge that AWS CloudFormation May create IAM resources** (riconosco che AWS CloudFormation potrebbe creare risorse IAM*).

e. Selezionare **Crea stack**.

f. Tornare a Workload Factory e monitorare la pagina Credenziali per verificare che le nuove credenziali siano in elaborazione o che siano state aggiunte.

Ottimizza i carichi di lavoro con NetApp Workload Factory

Dopo aver effettuato l'accesso e configurato NetApp Workload Factory, puoi iniziare a utilizzare diverse funzionalità di Workload Factory, come la creazione di file system Amazon FSx for ONTAP , la distribuzione di database su file system FSx for ONTAP e la migrazione delle configurazioni delle macchine virtuali su VMware Cloud on AWS utilizzando i file system FSx for ONTAP come datastore esterni.

- "Amazon FSX per NetApp ONTAP"

  Valuta e analizza gli ambienti dati correnti per ottenere potenziali risparmi sui costi usando FSX per ONTAP come infrastruttura storage, effettua il provisioning e Templatizza le implementazioni di FSX per ONTAP in base alle Best practice e accedi a funzioni di gestione avanzate.

- "Workload dei database"

  Rileva il tuo ambiente di database esistente in AWS, valuta i potenziali risparmi sui costi passando a FSX per ONTAP, implementa database end-to-end con Best practice integrate per l'ottimizzazione e automatizza il thin cloning per pipeline ci/CD.

- "Genai"

  Implementa e gestisci un'infrastruttura RAG (Retrieval-Augmented Generation) per migliorare la precisione e l'unicità delle tue applicazioni ai. Crea una knowledge base RAG su FSX per ONTAP con sicurezza e conformità dei dati integrate.

- "Workload VMware"

  Ottimizza migrazioni e operazioni con consigli smart e correzioni automatiche. Distribuire backup efficienti e un disaster recovery solido. Monitora e risolvi i problemi delle macchine virtuali.

- "Carichi di lavoro EDA"

  Ottimizza FSx per ONTAP su più file system per aumentare le prestazioni e ridurre i costi operativi tramite la gestione automatizzata dei parametri di archiviazione.

Informazioni sul copyright

Informazioni sul marchio commerciale