Guida per l'utente

Servizio Red Hat OpenShift su AWS

Servizio Red Hat OpenShift su AWS: Guida per l'utente

Table of Contents

Che cos'è Servizio Red Hat OpenShift su AWS?

Servizio Red Hat OpenShift su AWS (ROSA) è un servizio gestito che puoi utilizzare per creare, scalare e implementare applicazioni containerizzate con la piattaforma Red Hat Enterprise Kubernetes su OpenShift AWS. ROSA semplifica lo spostamento dei carichi di lavoro Red Hat locali verso OpenShift AWS e offre una stretta integrazione con altri Servizi AWS.

Funzionalità

ROSA è supportato e gestito congiuntamente da AWS e Red Hat. Ciascuno ROSA Il cluster viene fornito con il supporto di Red Hat Site Reliability Engineer (SRE) 24 ore su 24 per la gestione del cluster, supportato dall'accordo sui livelli di servizio con uptime del 99,95% di Red Hat (). SLA Per ulteriori informazioni sul modello di supporto del servizio, consulta. the section called “Ottenere supporto”

ROSA offre inoltre le seguenti funzionalità:

- Installazione del cluster, manutenzione e aggiornamenti del cluster SRE supportati da Red Hat.
- Servizio AWS le integrazioni includono AWS elaborazione, database, analisi, apprendimento automatico, networking e dispositivi mobili.
- Esegui e ridimensiona il piano di controllo di Kubernetes su più piani AWS Zone di disponibilità per garantire un'elevata disponibilità.
- Gestisci i cluster utilizzando OpenShift APIs strumenti di produttività per sviluppatori, tra cui Service Mesh, CodeReady Workspaces e Serverless.

Accesso ROSA

Puoi definire e configurare i tuoi ROSA implementazioni di servizi utilizzando le seguenti interfacce.

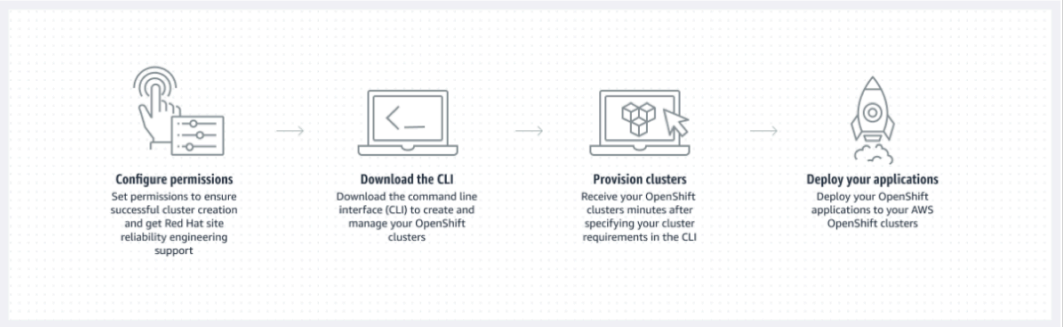
AWS

- ROSA console: fornisce un'interfaccia web per abilitare ROSA abbonamento e acquisto di un ROSA contratto software.
- AWS Command Line Interface (AWS CLI) — Fornisce comandi per un'ampia gamma di Servizi AWS ed è supportato su Windows, macOS e Linux. Per ulteriori informazioni, consulta AWS Command Line Interface.

Red Hat OpenShift

- Red Hat Hybrid Cloud Console: fornisce un'interfaccia web per creare, aggiornare e gestire ROSA cluster, installazione di componenti aggiuntivi per cluster e creazione e distribuzione di applicazioni su un ROSA ammasso.
- ROSA CLI(rosa) — Fornisce comandi per creare, aggiornare e gestire ROSA i cluster.
- OpenShift CLI(oc) — Fornisce comandi per creare applicazioni e gestire progetti OpenShift Container Platform.
- Knative CLI (kn): fornisce comandi che possono essere utilizzati per interagire con componenti OpenShift Serverless, come Knative Serving ed Eventing.
- Pipelines CLI (tkn): fornisce comandi per interagire con Pipelines utilizzando il terminale. OpenShift
- opm CLI: fornisce comandi che aiutano gli sviluppatori di operatori e gli amministratori del cluster a creare e gestire i cataloghi degli OpenShift operatori dal terminale.
- Operatore SDK CLI: fornisce comandi che uno sviluppatore di operatori può utilizzare per creare, testare e implementare un operatore. OpenShift

Come iniziare con ROSA



Di seguito viene riepilogata la procedura introduttiva per ROSA. Per istruzioni introduttive dettagliate, consultaInizia con ROSA .

AWS Management Console/AWS CLI

1. Configurare le autorizzazioni per Servizi AWS that ROSA si affida alla fornitura delle funzionalità del servizio. Per ulteriori informazioni, consulta the section called “Prerequisiti”.
2. Installa e configura la versione più recente AWS CLI strumento. Per ulteriori informazioni, consulta Installazione del nostro aggiornamento della versione più recente di AWS CLInel AWS CLI Guida per l'utente.

3. Attiva ROSA nel ROSA consolle.

Console Red Hat Hybrid Cloud/ROSA CLI

1. Scarica l'ultima versione di ROSA CLIe OpenShift CLI dalla Red Hat Hybrid Cloud Console. Per ulteriori informazioni, consulta Getting started with the ROSA CLInella documentazione di Red Hat.
2. Crea ROSA cluster nella Red Hat Hybrid Cloud Console o con ROSA CLI.
3. Quando il cluster è pronto, configura un provider di identità per concedere l'accesso degli utenti al cluster.
4. Implementa e gestisci i carichi di lavoro sul tuo ROSA raggruppa nello stesso modo in cui lo faresti con qualsiasi altro OpenShift ambiente.

Prezzi

Il costo totale di ROSA è costituito da due componenti: ROSA costi di servizio e AWS tariffe per l'infrastruttura. Per ulteriori informazioni sui prezzi, consulta Servizio Red Hat OpenShift su AWS Prezzi.

ROSA costi di servizio

Per impostazione predefinita, ROSA i costi del servizio vengono addebitati su richiesta a una tariffa oraria per 4 V CPU utilizzati dai nodi di lavoro. I costi di servizio sono uniformi per tutti i servizi supportati AWS Regioni standard. Oltre al costo del servizio Worker Node, ROSA con i cluster Hosted Control Plane (HCP) viene applicata una tariffa oraria per il cluster.

ROSA offre contratti di servizio di 1 e 3 anni che è possibile acquistare per risparmiare sui costi di servizio su richiesta per i nodi di lavoro. Per ulteriori informazioni, consulta the section called “Acquisto di un contratto ROSA”.

AWS tariffe per l'infrastruttura

AWS le tariffe per l'infrastruttura si applicano ai nodi di lavoro, ai nodi dell'infrastruttura, ai nodi del piano di controllo, allo storage e alle risorse di rete sottostanti ospitati su AWS infrastruttura globale. AWS le tariffe per l'infrastruttura variano in base Regione AWS.

Panoramica delle responsabilità per ROSA

Questa documentazione delinea le responsabilità di Amazon Web Services (AWS), Red Hat e i clienti di Servizio Red Hat OpenShift su AWS (ROSA) servizio gestito. Per ulteriori informazioni sull' ROSA e i suoi componenti, consulta Policies and service definition nella documentazione di Red Hat.

Il AWS il modello di responsabilità condivisa definisce AWS la responsabilità di proteggere l'infrastruttura che gestisce tutti i servizi offerti nel Cloud AWS, incluso ROSA. AWS l'infrastruttura include l'hardware, il software, la rete e le strutture che funzionano Cloud AWS servizi. Questo AWS la responsabilità viene comunemente definita «sicurezza del cloud». Operare ROSA in quanto servizio completamente gestito, Red Hat e il cliente sono responsabili degli elementi del servizio che AWS il modello di responsabilità si definisce come «sicurezza nel cloud».

Red Hat è responsabile della gestione e della sicurezza continue di ROSA infrastruttura del cluster, piattaforma applicativa sottostante e sistema operativo. Mentre ROSA i cluster sono ospitati su AWS risorse del cliente Account AWS, vi si accede da remoto tramite ROSA componenti di servizio e tecnici di Red Hat Site Reliability (SREs) tramite IAM ruoli creati dal cliente. Red Hat utilizza questo accesso per gestire l'implementazione e la capacità di tutti i nodi del piano di controllo e dell'infrastruttura sul cluster e mantenere le versioni per i nodi del piano di controllo, i nodi dell'infrastruttura e i nodi di lavoro.

Red Hat e il cliente condividono la responsabilità di ROSA gestione della rete, registrazione del cluster, controllo delle versioni del cluster e gestione della capacità. Mentre Red Hat gestisce ROSA servizio, il cliente è pienamente responsabile della gestione e della protezione di tutte le applicazioni, i carichi di lavoro e i dati distribuiti su ROSA.

Panoramica

La tabella seguente fornisce una panoramica di AWS, Red Hat e le responsabilità dei clienti per Servizio Red Hat OpenShift su AWS.

> **Note**
>
> Se il `cluster-admin` ruolo viene aggiunto a un utente, consulta le responsabilità e le note di esclusione nell'Appendice 4 del Red Hat Enterprise Agreement (Online Subscription Services).

Risorsa	Gestione degli incidenti e delle operazioni	Gestione delle modifiche	Autorizzazione dell'accesso e dell'identità	Sicurezza e conformità alle normative	Ripristino di emergenza
Dati dei clienti	Customer	Customer	Customer	Customer	Customer
Applicazioni per i clienti	Customer	Customer	Customer	Customer	Customer
Servizi per sviluppatori	Customer	Customer	Customer	Customer	Customer
Monitoraggio della piattaforma	Red Hat	Red Hat	Red Hat	Red Hat	Red Hat
Registrazione di log	Red Hat	Red Hat e il cliente	Red Hat e cliente	Red Hat e cliente	Red Hat
Rete delle applicazioni	Red Hat e il cliente	Red Hat e cliente	Red Hat e cliente	Red Hat	Red Hat
Rete in cluster	Red Hat	Red Hat e il cliente	Red Hat e cliente	Red Hat	Red Hat
Gestione delle reti virtuali	Red Hat e il cliente	Red Hat e cliente	Red Hat e cliente	Red Hat e cliente	Red Hat e cliente
Gestione dell'elaborazione virtuale (piano di controllo, infrastru	Red Hat	Red Hat	Red Hat	Red Hat	Red Hat

Risorsa	Gestione degli incidenti e delle operazioni	Gestione delle modifiche	Autorizzazione dell'accesso e dell'identità	Sicurezza e conformità alle normative	Ripristino di emergenza
ttura e nodi di lavoro)					
Versione cluster	Red Hat	Red Hat e il cliente	Red Hat	Red Hat	Red Hat
Gestione della capacità	Red Hat	Red Hat e i clienti	Red Hat	Red Hat	Red Hat
Gestione dello storage virtuale	Red Hat	Red Hat	Red Hat	Red Hat	Red Hat
AWS software (pubblico) Servizi AWS)	AWS	AWS	AWS	AWS	AWS
Hardware/ AWS infrastruttura globale	AWS	AWS	AWS	AWS	AWS

Compiti per responsabilità condivise per area

AWS, Red Hat e i clienti condividono la responsabilità del monitoraggio e della manutenzione di ROSA componenti. Questa documentazione definisce ROSA responsabilità di servizio per area e mansione.

Gestione degli incidenti e delle operazioni

AWS è responsabile della protezione dell'infrastruttura hardware che gestisce tutti i servizi offerti nel Cloud AWS. Red Hat è responsabile della gestione dei componenti di servizio necessari per il networking della piattaforma predefinita. Il cliente è responsabile della gestione degli incidenti e

delle operazioni dei dati delle applicazioni del cliente e di qualsiasi rete personalizzata che il cliente potrebbe aver configurato.

Risorsa	Responsabilità di servizio	Responsabilità del cliente
Rete delle applicazioni	Red Hat • Monitora OpenShift il servizio router nativo e rispondi agli avvisi.	Cliente • Monitora lo stato dei percorsi delle applicazioni e degli endpoint sottostanti. • Segnala le interruzioni a AWS e Red Hat.
Gestione delle reti virtuali	Red Hat • Monitoraggio AWS sistemi di bilanciamento del carico, Amazon VPC sottoreti e Servizio AWS componenti necessari per il networking della piattaforma predefinita. Rispondi agli avvisi.	Cliente • Monitora lo stato di AWS endpoint del sistema di bilanciamento del carico. • Monitora il traffico di rete configurato facoltativamente tramite Amazon VPC-a-connessione, VPC AWS VPN connessione, o AWS Direct Connect per potenzial i problemi o minacce alla sicurezza.
Gestione dello storage virtuale	Red Hat • Monitoraggio Amazon EBS volumi utilizzati per i nodi del cluster e Amazon S3 bucket utilizzati per ROSA registro delle immagini dei contenitori integrato nel servizio. Rispondi agli avvisi.	Cliente • Monitora lo stato dei dati delle applicazioni. • Se gestito dal cliente AWS KMS keys vengono utilizzat i, creano e controllano il ciclo di vita e le politiche chiave per Amazon EBS crittografia.

Risorsa	Responsabilità di servizio	Responsabilità del cliente
AWS software (pubblico) Servizi AWS)	AWS • Per informazioni su AWS gestione degli incidenti e delle operazioni, vedi Come AWS mantiene la resilienz a operativa e la continuità del servizio nel AWS white paper.	cliente • Monitora lo stato di AWS risorse nell'account del cliente. • Utilizzo IAM strumenti per applicare le autorizzazioni appropriate a AWS risorse nell'account cliente.
Hardware/AWS infrastruttura globale	AWS • Per informazioni su AWS gestione degli incidenti e delle operazioni, vedi Come AWS mantiene la resilienz a operativa e la continuità del servizio nel AWS white paper.	cliente • Configura, gestisci e monitora le applicazioni e i dati dei clienti per garantire che i controlli di sicurezza delle applicazioni e dei dati siano applicati correttam ente.

Gestione delle modifiche

AWS è responsabile della protezione dell'infrastruttura hardware che gestisce tutti i servizi offerti nel Cloud AWS. Red Hat è responsabile dell'abilitazione delle modifiche all'infrastruttura e ai servizi del cluster che il cliente controllerà, nonché della manutenzione delle versioni per i nodi del piano di controllo, i nodi dell'infrastruttura e i nodi di lavoro. Il cliente è responsabile dell'avvio delle modifiche all'infrastruttura. Il cliente è inoltre responsabile dell'installazione e della manutenzione dei servizi opzionali, delle configurazioni di rete sul cluster e delle modifiche ai dati e alle applicazioni del cliente.

Risorsa	Responsabilità del servizio	Responsabilità del cliente
Registrazione di log	Red Hat	Cliente • Installa l'operatore di registrazione delle applicazi

Risorsa	Responsabilità del servizio	Responsabilità del cliente
	• Aggrega e monitora centralmente i log di controllo della piattaforma. • Fornisci e gestisci un operatore di registrazione per consentire al cliente di implementare uno stack di registrazione per la registrazione predefinita delle applicazioni. • Fornisci registri di controllo su richiesta del cliente.	oni predefinito opzionale sul cluster. • Installa, configura e gestisci qualsiasi soluzione opzionale di registrazione delle app, ad esempio contenitori collaterali per la registrazione o applicazioni di registrazione di terze parti. • Ottimizza le dimensioni e la frequenza dei log delle applicazioni prodotti dalle applicazioni dei clienti se influiscono sulla stabilità dello stack di registrazione o del cluster. • Richiedi i log di controllo della piattaforma tramite un case di supporto per la ricerca di incidenti specifici.

Risorsa	Responsabilità del servizio	Responsabilità del cliente
Rete delle applicazioni	Red Hat • Configura sistemi di bilanciamento del carico pubblici. Offri la possibilità di configurare sistemi di bilanciamento del carico privati e fino a un sistema di bilanciamento del carico aggiuntivo, se necessario. • Configura il servizio router nativo OpenShift . Offri la possibilità di impostare il router come privato e aggiungere fino a uno shard di router aggiuntivo. • Installa, configura e gestisci OpenShift SDN i componenti per il traffico interno predefinito dei pod. • Offri al cliente la possibilità di gestire `NetworkPolicy` e `EgressNetworkPolicy` (firewall) gli oggetti.	Cliente • Configura le autorizzazioni di rete pod non predefinite per le reti di progetto e pod, l'ingresso e l'uscita dei pod utilizzando oggetti. `NetworkPolicy` • Utilizzate OpenShift Cluster Manager per richiedere un sistema di bilanciamento del carico privato per i percorsi applicativi predefiniti. • Utilizza OpenShift Cluster Manager per configurare fino a uno shard di router pubblico o privato aggiuntivo e il corrispondente load balancer. • Richiedi e configura eventuali service load balancer aggiuntivi per servizi specifici. • Configura tutte le regole di DNS inoltro necessarie.

Risorsa	Responsabilità del servizio	Responsabilità del cliente
Rete in cluster	Red Hat • Configura i componenti di gestione del cluster, come gli endpoint di servizi pubblici o privati e l'integrazione necessaria con Amazon VPC componenti. • Configura i componenti di rete interni necessari per la comunicazione interna del cluster tra operatore, infrastruttura e nodi del piano di controllo.	Cliente • Fornisci intervalli di indirizzi IP opzionali non predefiniti per macchina CIDRCIDR, servizio e pod, CIDR se necessario, tramite OpenShift Cluster Manager al momento del provisioning del cluster. • Richiedi che l'endpoint del API servizio sia reso pubblico o privato al momento della creazione del cluster o dopo la creazione del cluster tramite OpenShift Cluster Manager.

Risorsa	Responsabilità del servizio	Responsabilità del cliente
Gestione delle reti virtuali	Red Hat • Configura e configura Amazon VPC componenti necessari per il provisioning del cluster, come sottoreti, sistemi di bilanciamento del carico, gateway Internet e gateway. NAT • Offri al cliente la possibili tà di gestire AWS VPN connettività con risorse locali, Amazon VPC VPCconnettività -to- e AWS Direct Connect come richiesto tramite OpenShift Cluster Manager. • Consenti ai clienti di creare e implementare AWS sistemi di bilanciamento del carico da utilizzare con i servizi di bilanciamento del carico.	Cliente • Configurazione e manutenzi one facoltative Amazon VPC componenti, come Amazon VPC VPCconnes sione -a-, AWS VPN connessione, o AWS Direct Connect. • Richiedi e configura eventuali sistemi di bilanciamento del carico aggiuntivi per servizi specifici.

Risorsa	Responsabilità del servizio	Responsabilità del cliente
Gestione dell'elaborazione virtuale	Red Hat • Imposta e configura il ROSA piano di controllo e piano dati da utilizzare Amazon EC2 istanze per il calcolo in cluster. • Monitora e gestisci l'implementazione di Amazon EC2 piano di controllo e nodi dell'infr astruttura sul cluster.	Cliente • Monitora e gestisci Amazon EC2 nodi di lavoro creando un pool di macchine utilizzando OpenShift Cluster Manager oppure ROSA CLI. • Gestisci le modifiche alle applicazioni e ai dati delle applicazioni distribuite dal cliente.
Versione del cluster	Red Hat • Abilita il processo di pianificazione degli aggiornamenti. • Monitora l'avanzamento dell'aggiornamento e risolvi eventuali problemi riscontra ti. • Pubblica i registri delle modifiche e le note di rilascio per aggiornamenti minori e di manutenzione.	Cliente • Pianifica gli aggiornamenti delle versioni di manutenzi one immediatamente, per il futuro, oppure utilizza aggiornamenti automatici. • Riconosci e pianifica gli aggiornamenti delle versioni minori. • Assicurati che la versione del cluster rimanga su una versione secondaria supportata. • Testa le applicazioni dei clienti su versioni secondari e e di manutenzione per garantire la compatibilità.

Risorsa	Responsabilità del servizio	Responsabilità del cliente
Gestione della capacità	Red Hat • Monitora l'uso del piano di controllo. I piani di controllo includono i nodi del piano di controllo e i nodi dell'infr astruttura. • Ridimensiona e ridimensi ona i nodi del piano di controllo per mantenere la qualità del servizio.	Cliente • Monitora l'utilizzo del nodo di lavoro e, se appropriato, abilita la funzionalità di auto scaling. • Determina la strategia di scalabilità del cluster. • Utilizza i controlli di OpenShift Cluster Manager forniti per aggiungere o rimuovere nodi di lavoro aggiuntivi, se necessario. • Rispondi alle notifiche di Red Hat relative ai requisiti delle risorse del cluster.

Risorsa	Responsabilità del servizio	Responsabilità del cliente
Gestione dello storage virtuale	Red Hat • Configura e configura Amazon EBS per fornire lo storage su nodi locali e lo storage su volumi persistenti per il cluster. • Imposta e configura il registro delle immagini integrato da utilizzare Amazon S3 archiviazione a secchiello. • Elimina regolarmente le risorse del registro delle immagini Amazon S3 ottimizzare Amazon S3 utilizzo e prestazioni del cluster.	cliente • Facoltativamente, configura il Amazon EBS CSIdriver o Amazon EFS CSIdriver per il provisioning di volumi persistenti sul cluster.

Risorsa	Responsabilità del servizio	Responsabilità del cliente

AWS software (pubblico). AWS servizi)	AWS
	
	Calcolo
	
	• Fornire il Amazon EC2 servizio, usato per ROSA piano di controllo, infrastru ttura e nodi di lavoro.
	
	Storage
	
	• Fornire Amazon EBS per consentire il ROSA servizio per la fornitura di storage su nodi locali e storage di volumi persistenti per il cluster.
	
	Reti
	
	• Fornire quanto segue Cloud AWS servizi da soddisfare ROSA esigenze di infrastru ttura di rete virtuale:
	  • Amazon VPC
	  • Elastic Load Balancing
	  • IAM
	• Fornire quanto segue (facoltativo) Servizio AWS integrazioni per ROSA:
	  • AWS VPN
	  • AWS Direct Connect
	  • AWS PrivateLink
		Cliente
		
		• Firma le richieste utilizzan do un ID chiave di accesso e una chiave di accesso segreta associati a un IAM principale o AWS STS credenziali di sicurezza temporanee.
		• Specificare le VPC sottoreti da utilizzare per il cluster durante la creazione del cluster.
		• Facoltativamente, configura un sistema gestito dal cliente da utilizzare VPC con ROSA i cluster.

Risorsa	Responsabilità del servizio	Responsabilità del cliente
	• AWS Transit Gateway	
Hardware/AWS infrastruttura globale	AWS • Per informazioni sui controlli di gestione per AWS data center, consulta la sezione I nostri controlli sul Cloud AWS Pagina sulla sicurezza . • Per informazioni sulle migliori pratiche di gestione delle modifiche, consulta la Guida per la gestione delle modifiche su AWSnel AWS Libreria di soluzioni.	Cliente • Implementa le migliori pratiche di gestione delle modifiche per le applicazioni e i dati dei clienti ospitati su Cloud AWS.

Autorizzazione dell'accesso e dell'identità

L'autorizzazione all'accesso e all'identità include la responsabilità di gestire l'accesso autorizzato a cluster, applicazioni e risorse dell'infrastruttura. Ciò include attività come la fornitura di meccanismi di controllo degli accessi, l'autenticazione, l'autorizzazione e la gestione dell'accesso alle risorse.

Risorsa	Responsabilità di servizio	Responsabilità del cliente
Registrazione di log	Red Hat • Aderisci a un processo di accesso interno su più livelli basato sugli standard del settore per i log di controllo della piattaforma. • OpenShift RBACFornisci funzionalità native.	Cliente • Configura OpenShift RBAC per controllare l'accesso ai progetti e, per estensione, ai log delle applicazioni di un progetto. • Per le soluzioni di registraz ione delle applicazioni personalizzate o di terze

Risorsa	Responsabilità di servizio	Responsabilità del cliente
		parti, il cliente è responsab ile della gestione degli accessi.
Rete delle applicazioni	Red Hat • Fornisci `dedicated -admin` funzionalità OpenShift RBAC e funzional ità native.	Cliente • Configurare OpenShift `dedicated-admin` e RBAC controllare l'accesso alla configurazione del percorso in base alle esigenze. • Gestisci gli amministratori dell'organizzazione Red Hat per consentire a Red Hat di concedere l'accesso a OpenShift Cluster Manager. Il cluster manager viene utilizzato per configurare le opzioni del router e fornire una quota di service load balancer.

Risorsa	Responsabilità di servizio	Responsabilità del cliente
Rete in cluster	Red Hat • Fornisci il controllo degli accessi ai clienti tramite OpenShift Cluster Manager. Fornisci `dedicated -admin` funzionalità OpenShift RBAC e funzionalità native.	Cliente • Configurare OpenShift `dedicated-admin` e RBAC controllare l'accesso alla configurazione del percorso in base alle esigenze. • Gestisci l'appartenenza degli account Red Hat all'organizzazione Red Hat. • Gestisci gli amministratori dell'organizzazione per consentire a Red Hat di concedere l'accesso a OpenShift Cluster Manager.
Gestione delle reti virtuali	Red Hat • Fornisci il controllo degli accessi ai clienti tramite OpenShift Cluster Manager.	Cliente • Gestisci l'accesso opzionale degli utenti a AWS componenti tramite OpenShift Cluster Manager.
Gestione dell'elaborazione virtuale	Red Hat • Fornisci il controllo degli accessi ai clienti tramite OpenShift Cluster Manager.	Cliente • Gestisci l'accesso opzionale degli utenti a AWS componenti tramite OpenShift Cluster Manager. • Crea IAM ruoli e policy allegate necessari per l'attivazione ROSA accesso al servizio.

Risorsa	Responsabilità di servizio	Responsabilità del cliente
Gestione dello storage virtuale	Red Hat • Fornisci il controllo degli accessi ai clienti tramite OpenShift Cluster Manager.	Cliente • Gestisci l'accesso opzionale degli utenti a AWS componenti tramite OpenShift Cluster Manager. • Crea IAM ruoli e policy allegate necessari per l'attivazione ROSA accesso al servizio.

Risorsa	Responsabilità di servizio	Responsabilità del cliente
AWS software (pubblico) AWS servizi)	AWS Calcolo • Fornire il Amazon EC2 servizio, usato per ROSA piano di controllo, infrastru ttura e nodi di lavoro. Storage • Fornire Amazon EBS, usato per consentire ROSA per fornire lo storage su nodi locali e lo storage di volumi persistenti per il cluster. • Fornire Amazon S3, utilizzat o per il registro delle immagini integrato nel servizio. Reti • Fornire AWS Identity and Access Management (IAM), utilizzato dai clienti per controllare l'accesso a ROSA risorse in esecuzione sugli account dei clienti.	Cliente • Crea IAM ruoli e politiche allegate necessari per abilitare ROSA accesso al servizio. • Utilizzo IAM strumenti per applicare le autorizzazioni appropriate a AWS risorse nell'account cliente. • Per abilitare ROSA attravers o il tuo AWS organizza zione, il cliente è responsab ile della gestione AWS Organizations amministr atori. • Per abilitare ROSA attravers o il tuo AWS organizza zione, il cliente è responsab ile della distribuzione del ROSA concessione di diritti utilizzando AWS License Manager.

Risorsa	Responsabilità di servizio	Responsabilità del cliente
Hardware/AWS infrastruttura globale	AWS • Per informazioni sui controlli fisici degli accessi per AWS data center, consulta la sezione I nostri controlli sul Cloud AWS Pagina sulla sicurezza.	Cliente • Il cliente non è responsab ile per AWS infrastruttura globale.

Sicurezza e conformità alle normative

Di seguito sono elencate le responsabilità e i controlli relativi alla conformità:

Risorsa	Responsabilità di servizio	Responsabilità del cliente
Registrazione di log	Red Hat • Invia i log di controllo del cluster a un Red Hat SIEM per analizzare gli eventi di sicurezza. Conserva i log di controllo per un periodo di tempo definito per supportar e l'analisi forense.	Cliente • Analizza i log delle applicazioni per verificar e la presenza di eventi di sicurezza. • Invia i log delle applicazi oni a un endpoint esterno tramite contenitori secondari di registrazione o applicazi oni di registrazione di terze parti se è necessaria una conservazione più lunga di quella offerta dallo stack di registrazione predefinito.
Gestione delle reti virtuali	Red Hat • Monitora i componenti di rete virtuale per potenzial	Cliente • Monitora i componenti di rete virtuali configura

Risorsa	Responsabilità di servizio	Responsabilità del cliente
	i problemi e minacce alla sicurezza. • Usa pubblico AWS strumenti per il monitoraggio e la protezione aggiuntivi.	ti opzionali per potenzial i problemi e minacce alla sicurezza. • Configura le regole firewall o le protezioni del data center del cliente necessarie in base alle esigenze.
Gestione dell'elaborazione virtuale	Red Hat • Monitora i componenti di elaborazione virtuale per potenziali problemi e minacce alla sicurezza. • Usa pubblico AWS strumenti per il monitoraggio e la protezione aggiuntivi.	Cliente • Monitora i componenti di rete virtuali configura ti opzionali per potenzial i problemi e minacce alla sicurezza. • Configura le regole firewall o le protezioni del data center del cliente necessarie in base alle esigenze.

Risorsa	Responsabilità di servizio	Responsabilità del cliente
Gestione dello storage virtuale	Red Hat • Monitora i componenti di storage virtuale per potenziali problemi e minacce alla sicurezza. • Usa pubblico AWS strumenti per il monitoraggio e la protezione aggiuntivi. • Configura il ROSA servizio per crittografare i dati del piano di controllo, dell'infrastruttura e del volume del nodo di lavoro per impostazione predefinita utilizzando il AWS KMSchiave gestita che Amazon EBS fornisce. • Configura il ROSA servizio per crittografare i volumi persistenti dei clienti che utilizzano la classe di storage predefinita con AWS KMSchiave gestita che Amazon EBS fornisce. • Fornire la possibilità al cliente di utilizzare un servizio gestito dal cliente KMS key per crittografare volumi persistenti. • Configura il registro delle immagini del contenitore per crittografare i dati del registro delle immagini inattivi utilizzando la	Cliente • Fornitura Amazon EBS volumi. • Manage (Gestione) Amazon EBS spazio di archiviazione per garantire che sia disponibile spazio di archiviazione sufficiente per il montaggio come volume in ROSA. • Crea la dichiarazione di volume persistente e genera un volume persistente tramite OpenShift Cluster Manager.

Risorsa	Responsabilità di servizio	Responsabilità del cliente
	crittografia lato server con Amazon S3 chiavi gestite (-3)SSE. • Fornire la possibilità al cliente di creare un account pubblico o privato Amazon S3 registro delle immagini per proteggere le immagini dei contenitori dall'accesso non autorizzato degli utenti.	

Risorsa	Responsabilità di servizio	Responsabilità del cliente
AWS software (pubblico) AWS servizi)	AWS Calcolo • Fornire Amazon EC2, usato per ROSA piano di controllo, infrastruttura e nodi di lavoro. Per ulteriori informazioni, vedere Sicurezza dell'infrastruttura in Amazon EC2nel Amazon EC2 Guida per l'utente. Storage • Fornire Amazon EBS, usato per ROSA i volumi del piano di controllo, dell'infr astruttura e dei nodi di lavoro, nonché i volumi persistenti di Kubernetes. Per ulteriori informazioni, consulta Protezione dei dati in Amazon EC2nel Amazon EC2 Guida per l'utente. • Fornire AWS KMS, quale ROSA utilizza per crittogra fare i volumi del piano di controllo, dell'infrastruttura e dei nodi di lavoro e i volumi persistenti. Per ulteriori informazioni, consulta Amazon EBS crittografia in Amazon EC2 Guida per l'utente.	Cliente • Garantire che vengano seguite le migliori pratiche di sicurezza e il principio del privilegio minimo per proteggere i dati su Amazon EC2 istanza. Per ulteriori informazioni, vedere Sicurezza dell'infrastruttura in Amazon EC2e Protezione dei dati in Amazon EC2. • Monitora i componenti di rete virtuali configura ti opzionali per individua re potenziali problemi e minacce alla sicurezza. • Configura le regole firewall o le protezioni del data center del cliente necessarie in base alle esigenze. • Crea una KMS chiave opzionale gestita dal cliente e crittografa il Amazon EBS volume persistente che utilizza la KMS chiave. • Monitora i dati dei clienti nello storage virtuale per potenziali problemi e minacce alla sicurezza. Per ulteriori informazioni, consultare la .AWS Modello di responsabilità condivisa.

Risorsa	Responsabilità di servizio	Responsabilità del cliente
	• Fornire Amazon S3, utilizzato per il registro delle immagini dei contenitori integrato nel ROSA servizio. Per ulteriori informazioni, consulta Amazon S3 sicurezza in Amazon S3 Guida per l'utente. Reti • Fornisci funzionalità e servizi di sicurezza per aumentare la privacy e controllare l'accesso alla rete su AWS infrastruttura globale, compresi i firewall di rete integrati Amazon VPC, connessioni di rete private o dedicate e crittografia automatica di tutto il traffico sul AWS reti globali e regionali tra AWS strutture protette. Per ulteriori informazioni, consultare la .AWS Modello di responsabilità condivisa e sicurezza dell'infrastruttura nell'introduzione a AWS White paper sulla sicurezza.	

Risorsa	Responsabilità di servizio	Responsabilità del cliente
Hardware/AWS infrastruttura globale	AWS • Fornire il AWS infrastruttura globale che ROSA utilizza per fornire funzionalità di servizio. Per ulteriori informazioni sull' AWS controlli di sicurezza, vedere Sicurezza del AWS Infrastruttura in AWS white paper. • Fornisci al cliente la documentazione necessaria a per gestire le esigenze di conformità e verificarne lo stato di sicurezza in AWS utilizzando strumenti come AWS Artifact e AWS Security Hub.	Cliente • Configura, gestisci e monitora le applicazioni e i dati dei clienti per garantire che i controlli di sicurezza delle applicazioni e dei dati siano applicati correttamente. • Utilizzo IAM strumenti per applicare le autorizzazioni appropriate a AWS risorse nell'account cliente.

Ripristino di emergenza

Il disaster recovery include il backup dei dati e della configurazione, la replica dei dati e la configurazione dell'ambiente di disaster recovery e il failover in caso di eventi di emergenza.

Risorsa	Responsabilità di servizio	Responsabilità del cliente
Gestione delle reti virtuali	Red Hat • Ripristina o ricrea i componenti di rete virtuale interessati necessari per il funzionamento della piattaforma.	Cliente • Configura connessioni di rete virtuali con più di un tunnel, ove possibile, per la protezione dalle interruzioni. • Mantieni il failover DNS e il bilanciamento del carico

Risorsa	Responsabilità di servizio	Responsabilità del cliente
		se utilizzi un sistema di bilanciamento del carico globale con più cluster.
Gestione dell'elaborazione virtuale	Red Hat • Il monitoraggio e la sostituzione del cluster non sono riusciti Amazon EC2 piano di controllo o nodi dell'infrastruttura. • Offri al cliente la possibilità di sostituire manualmente o automaticamente i nodi di lavoro guasti.	Cliente • Sostituzione non riuscita Amazon EC2 nodi di lavoro modificando la configurazione del pool di macchine tramite OpenShift Cluster Manager o ROSA CLI.
Gestione dello storage virtuale	Red Hat • In ROSA cluster creati con AWS IAM credenziali utente, esegui il backup di tutti gli oggetti Kubernetes sul cluster tramite istantanee di volume orarie, giornaliere e settimanali.	Cliente • Esegui il backup delle applicazioni e dei dati delle applicazioni dei clienti.

Risorsa	Responsabilità di servizio	Responsabilità del cliente
AWS software (pubblico). AWS servizi)	AWS Calcolo • Fornire Amazon EC2 funzionalità che supportan o la resilienza dei dati come Amazon EBS istantanee e Amazon EC2 Auto Scaling. Per ulteriori informazi oni, vedere Resilience in Amazon EC2nel Amazon EC2 Guida per l'utente. Storage • Fornire la capacità di ROSA servizio e clienti per il backup di Amazon EBS volume sul cluster tramite Amazon EBS istantanee del volume. • Per informazioni su Amazon S3 funzionalità che supportano la resilienza dei dati, vedi Resilienza in Amazon S3. Reti • Per informazioni su Amazon VPC funzionalità che supportano la resilienza dei dati, vedi Resilienza in Amazon Virtual Private	Cliente • Configura ROSA Cluster Multi-AZ per migliorare la tolleranza agli errori e la disponibilità dei cluster. • Effettua il provisioning di volumi persistenti utilizzan do Amazon EBS CSIdriver per abilitare le istantanee dei volumi. • Crea istantanee CSI di volume di Amazon EBS volumi persistenti.

Risorsa	Responsabilità di servizio	Responsabilità del cliente
	Cloudnel Amazon VPC Guida per l'utente.	
Hardware/AWS infrastruttura globale	AWS • Fornire AWS infrastru ttura globale che consente ROSA per scalare il piano di controllo, l'infrastruttura e i nodi di lavoro tra le zone di disponibilità. Questa funzionalità consente ROSA per orchestrare il failover automatico tra le zone senza interruzioni. • Per ulteriori informazioni sulle migliori pratiche di disaster recovery, consulta Opzioni di disaster recovery nel cloud nel AWS Well-Architected Framework.	Cliente • Configura ROSA Cluster Multi-AZ per migliorare la tolleranza agli errori e la disponibilità dei cluster.

Responsabilità del cliente per dati e applicazioni

Il cliente è responsabile delle applicazioni, dei carichi di lavoro e dei dati in cui vengono distribuiti Servizio Red Hat OpenShift su AWS. Tuttavia, AWS e Red Hat forniscono vari strumenti per aiutare il cliente a gestire dati e applicazioni sulla piattaforma.

Risorsa	Come AWS e Red Hat aiuta	Responsabilità del cliente
Dati dei clienti	Red Hat • Mantieni gli standard a livello di piattaforma per la crittografia dei dati definiti	Cliente • Mantieni la responsabilità di tutti i dati dei clienti archiviat i sulla piattaforma e del

Risorsa	Come AWS e Red Hat aiuta	Responsabilità del cliente
	dagli standard di sicurezza e conformità del settore. • Fornisci OpenShift componenti per aiutare a gestire i dati delle applicazioni, come i segreti. • Abilita l'integrazione con servizi di dati come Amazon RDS per archiviare e gestire i dati all'esterno del cluster e/o AWS. AWS • Fornire Amazon RDS per consentire ai clienti di archiviare e gestire i dati all'esterno del cluster.	modo in cui le applicazioni dei clienti utilizzano ed espongono tali dati.

Risorsa	Come AWS e Red Hat aiuta	Responsabilità del cliente
Applicazioni per i clienti	Red Hat • Esegui il provisioning dei cluster con OpenShift componenti installati in modo che i clienti possano accedere a Kubernetes OpenShift e distribuire e gestire applicazioni APIs containerizzate. • Crea cluster con image pull secret in modo che le implementazioni dei clienti possano estrarre le immagini dal registro di Red Hat Container Catalog. • Fornisci un accesso OpenShift APIs che un cliente possa utilizzare per configurare gli operatori per aggiungere community , terze parti, AWS e i servizi Red Hat al cluster. • Fornisci classi di storage e plugin per supportare volumi persistenti da utilizzare con le applicazioni dei clienti. • Fornisci un registro delle immagini dei contenitori in modo che i clienti possano archiviare in modo sicuro le immagini dei contenitori delle applicazioni sul cluster	Cliente • Mantieni la responsabilità per le applicazioni, i dati e l'intero ciclo di vita delle applicazioni di clienti e terze parti. • Se un cliente aggiunge servizi Red Hat, della community, di terze parti, propri o di altro tipo al cluster utilizzando operatori o immagini esterne, è responsabile di questi servizi e della collabora zione con il provider appropriato (incluso Red Hat) per la risoluzione di eventuali problemi. • Utilizza gli strumenti e le funzionalità forniti per configurare e distribui re, tenerti aggiornato, impostare le richieste e i limiti delle risorse, dimensionare il cluster per disporre di risorse sufficien ti per eseguire le app, configurare le autorizza zioni, effettuare l'integra zione con altri servizi, gestire i flussi di immagini o i modelli distribuiti dal cliente, servire estername

Risorsa	Come AWS e Red Hat aiuta	Responsabilità del cliente
	per distribuire e gestire le applicazioni. AWS • Fornire Amazon EBS per supportare volumi persistenti da utilizzare con le applicazioni dei clienti. • Fornire Amazon S3 per supportare il provisioning Red Hat del registro delle immagini dei contenitori.	nte, salvare, eseguire il backup e ripristinare i dati e gestire in altro modo i carichi di lavoro ad alta disponibilità e resilienza. • Mantieni la responsab ilità del monitoraggio delle applicazioni su cui vengono eseguite Servizio Red Hat OpenShift su AWS, inclusa l'installazione e il funzionamento del software per raccogliere metriche, creare avvisi e proteggere i segreti dell'applicazione.

Modelli di architettura

Servizio Red Hat OpenShift su AWS (ROSA) presenta le seguenti topologie di cluster:

- Piano di controllo ospitato (HCP) - Il piano di controllo è ospitato all'interno di Red Hat Account AWS e gestito da Red Hat. I nodi di lavoro vengono implementati presso il cliente Account AWS.
- Classico: il piano di controllo e i nodi di lavoro vengono implementati presso il cliente. Account AWS

ROSAHCPoffre un'architettura del piano di controllo più efficiente che aiuta a ridurre i costi di AWS infrastruttura sostenuti durante il funzionamento ROSA e consente tempi di creazione dei cluster più rapidi. Nella AWS ROSA console possono essere abilitati sia ROSA with HCP che ROSA classic. Puoi scegliere l'architettura che desideri utilizzare quando esegui il provisioning dei ROSA cluster utilizzando. ROSA CLI

> **Note**
>
> ROSAwith hosted control planes (HCP) non offre le certificazioni di conformità Fed RAMP High e HIPAA Qualified. Per ulteriori informazioni, consulta la sezione Compliance nella documentazione di Red Hat.

> **Note**
>
> ROSAwith hosted control planes (HCP) non offre endpoint Federal Information Processing Standard (FIPS).

A confronto ROSA con un HCP classico ROSA

La tabella seguente mette a confronto ROSA HCP i modelli di architettura ROSA classici.

	ROSAcon HCP	ROSAclassico
Hosting di infrastrutture cluster	I componenti del piano di controllo, come etcd, API server e oauth, sono ospitati in un ambiente di proprietà di Red Hat. Account AWS	I componenti del piano di controllo, come etcd, API server e oauth, sono ospitati in un ambiente di proprietà del cliente. Account AWS
Amazon VPC	I nodi di lavoro comunicano con il piano di controllo. AWS PrivateLink	I nodi di lavoro e i nodi del piano di controllo vengono implementati presso il clienteVPC.
AWS Identity and Access Management	Utilizza politiche AWS gestite.	Utilizza politiche gestite dal cliente definite dal servizio.
Implementazione multizona	Il piano di controllo è distribui to su più zone di disponibilità ()AZs.	Il piano di controllo può essere implementato all'interno di una singola AZ o su più aree. AZs

	ROSAcon HCP	ROSAclassico
Nodi dell'infrastruttura	Non utilizza nodi di infrastruttura dedicati. I componenti della piattaforma vengono distribuiti ai nodi di lavoro.	Utilizza due nodi dedicati Single-AZ o tre Multi-AZ per ospitare i componenti della piattaforma.
OpenShift funzionalità	Il monitoraggio della piattaforma, il registro delle immagini e il controller di ingresso vengono implementati nei nodi di lavoro.	Il monitoraggio della piattaforma, il registro delle immagini e il controller di ingresso vengono implementati in nodi di infrastruttura dedicati.
Aggiornamenti del cluster	Il piano di controllo e ogni pool di macchine possono essere aggiornati separatamente.	L'intero cluster deve essere aggiornato contemporaneamente.
Ingombro minimo Amazon EC2	Sono necessarie due Amazon EC2 istanze per creare un cluster.	Per creare un cluster sono necessarie sette istanze Single-AZ o nove Amazon EC2 istanze Multi-AZ.
Regioni AWS	Per informazioni sulla Regione AWS disponibilità, consulta gli Servizio Red Hat OpenShift su AWS endpoint e le quote nella Guida di riferimento generale. AWS	Per Regione AWS la disponibilità, consulta Servizio Red Hat OpenShift su AWS endpoint e quote nella Guida di riferimento generale. AWS

Inizia con ROSA

Servizio Red Hat OpenShift su AWS (ROSA) è un servizio gestito che puoi utilizzare per creare, scalare e distribuire applicazioni containerizzate con la piattaforma Red Hat Enterprise Kubernetes. OpenShift AWS

Puoi utilizzare le seguenti guide per creare il tuo primo ROSA cluster, concedere l'accesso utente, implementare la tua prima applicazione e scoprire come revocare l'accesso degli utenti ed eliminare il cluster.

- the section called “Crea un ROSA HCPgrappolo - CLI”- Crea il tuo primo ROSA con HCP cluster usando AWS STS and the. ROSA CLI
- the section called “Crea un cluster ROSA classico - AWS PrivateLink ”- Crea il tuo primo cluster ROSA classico utilizzando AWS PrivateLink.
- the section called “Crea un cluster ROSA classico - CLI”- Crea il tuo primo cluster ROSA classico utilizzando AWS STS e il ROSA CLI.

Configurazione per l'uso ROSA

Per preparare l'ambiente alla creazione di un ROSA cluster, è necessario completare le seguenti azioni.

Prerequisiti

I seguenti prerequisiti devono essere soddisfatti per consentire la creazione di ROSA cluster.

- Installa e configura la versione più recente AWS CLI. Per ulteriori informazioni, consulta Installare o aggiornare la versione più recente della AWS CLI.
- Installa e configura la versione più recente ROSA CLI di OpenShift Container PlatformCLI. Per ulteriori informazioni, vedi Guida introduttiva a ROSA CLI.
- È necessario che le quote di servizio richieste siano impostate per Amazon EC2, Amazon VPC Amazon EBS, e Elastic Load Balancing. AWS oppure Red Hat può richiedere aumenti delle quote di servizio per vostro conto, se necessario per la risoluzione dei problemi. Per visualizzare le quote di servizio richieste ROSA, consulta gli Servizio Red Hat OpenShift su AWS endpoint e le quote nel AWS Riferimento generale.

- Per ricevere AWS supporto per ROSA, è necessario abilitare i piani di supporto AWS Business, Enterprise On-Ramp o Enterprise. Red Hat può richiedere AWS assistenza per conto dell'utente, se necessario per la risoluzione dei problemi. Per ulteriori informazioni, consulta the section called "Ottenere supporto". Per abilitarlo AWS Support, consulta la AWS Support pagina.
- Se utilizzate AWS Organizations per gestire il servizio Account AWS che ospita il ROSA servizio, la policy di controllo del servizio (SCP) dell'organizzazione deve essere configurata per consentire a Red Hat di eseguire le azioni politiche elencate nella pagina SCP senza restrizioni. Per ulteriori informazioni, consulta the section called "AWS Organizations la politica di controllo del servizio non è richiesta Marketplace AWS autorizzazioni". Per maggiori informazioni in meritoSCPs, consulta Service control policies (SCPs).
- Se si distribuisce un ROSA cluster with AWS STS in un ambiente abilitato Regione AWS che è disabilitato per impostazione predefinita, è necessario aggiornare il token di sicurezza alla versione 2 per tutte le regioni Account AWS incluse nel comando seguente.

```
aws iam set-security-token-service-preferences --global-endpoint-token-version
 v2Token
```

  Per ulteriori informazioni sull'abilitazione delle regioni, vedi link:accounts/latest/reference/manage

ROSA Abilita e configura i prerequisiti AWS

Per creare un ROSA cluster, è necessario abilitare il ROSA servizio nella AWS ROSA console. La AWS ROSA console verifica se l'utente Account AWS dispone delle Marketplace AWS autorizzazioni necessarie, delle quote di servizio e del ruolo Elastic Load Balancing (ELB) collegato al servizio denominato. `AWSServiceRoleForElasticLoadBalancing` Se manca uno di questi prerequisiti, la console fornisce indicazioni su come configurare l'account per soddisfarli.

1. Passare alla console ROSA.
2. Scegli Avvia.
3. Nella pagina Verifica i ROSA prerequisiti, seleziona Accetto di condividere le mie informazioni di contatto con Red Hat.
4. Scegli Abilita. ROSA
5. Una volta che la pagina ha verificato che le quote di servizio soddisfino ROSA i prerequisiti e creato il ruolo ELB collegato al servizio, apri una nuova sessione di terminale per crearne una prima utilizzando il. ROSA cluster ROSA CLI

Crea un HCP cluster ROSA con utilizzando ROSA CLI

Le sezioni seguenti descrivono come iniziare a utilizzare i ROSA piani di controllo ospitati (ROSAconHCP) utilizzando AWS STS e il ROSA CLI. Per i passaggi per creare un HCP cluster ROSA con Terraform, consulta la documentazione di Red Hat. Per saperne di più sul provider Terraform per la creazione ROSA cluster, consulta la documentazione Terraform.

Il ROSA CLIutilizza `auto` mode o `manual` mode per creare il IAM risorse e configurazione OpenID Connect (OIDC) necessarie per creare un ROSA cluster. `auto`la modalità crea automaticamente il necessario IAM ruoli, politiche e OIDC provider. `manual`mode emette il AWS CLI comandi necessari per creare il IAM risorse manualmente. Utilizzando la `manual` modalità, è possibile rivedere i dati generati AWS CLI comandi prima di eseguirli manualmente. Con `manual` mode, puoi anche passare i comandi a un altro amministratore o gruppo dell'organizzazione in modo che possa creare le risorse.

Le procedure descritte in questo documento utilizzano la `auto` modalità di ROSA CLIper creare il necessario IAM risorse e OIDC configurazione per ROSA withHCP. Per altre opzioni per iniziare, consultaInizia con ROSA .

Argomenti

Prerequisiti

Completa le azioni preliminari elencate inthe section called “Configurazione”.

Crea Amazon VPC architecture

La procedura seguente crea Amazon VPC architettura che può essere utilizzata per ospitare un cluster. Tutti cluster le risorse sono ospitate nella sottorete privata. La sottorete pubblica indirizza il traffico in uscita dalla sottorete privata attraverso un NAT gateway verso la rete Internet pubblica. Questo esempio utilizza il blocco per CIDR `10.0.0.0/16` Amazon VPC. Tuttavia, puoi scegliere un CIDR blocco diverso. Per ulteriori informazioni, vedi VPCdimensionamento.

> **Important**
>
> Se Amazon VPC i requisiti non sono soddisfatti, la creazione del cluster non riesce.

Example

Terraform

1. Installa TerraformCLI. Per ulteriori informazioni, consulta le istruzioni di installazione nella documentazione di Terraform.
2. Apri una sessione di terminale e clona il repository VPC Terraform.

   ```
   git clone https://github.com/openshift-cs/terraform-vpc-example
   ```

3. Passa alla directory creata.

   ```
   cd terraform-vpc-example
   ```

4. Avvia il file Terraform.

   ```
   terraform init
   ```

   Una volta completato, CLI restituisce un messaggio che indica che Terraform è stato inizializzato con successo.

5. Per creare un piano Terraform basato sul modello esistente, esegui il seguente comando. Il Regione AWS deve essere specificato. Facoltativamente, puoi scegliere di specificare un nome per il cluster.

   ```
   terraform plan -out rosa.tfplan -var region=<region>
   ```

   Una volta eseguito il comando, viene aggiunto un `rosa.tfplan` file alla `hypershift-tf` directory. Per opzioni più dettagliate, consulta il file del VPC repository Terraform. README

6. Applica il file del piano per creare il. VPC

   ```
   terraform apply rosa.tfplan
   ```

   Una volta completato, ha CLI restituito un messaggio di successo che verifica le risorse aggiunte.

   a. (Facoltativo) Crea variabili di ambiente per la sottorete IDs privata, pubblica e machinepool fornita da Terraform da utilizzare durante la creazione del cluster with. ROSA HCP

      ```
      export SUBNET_IDS=$(terraform output -raw cluster-subnets-string)
      ```

   b. (Facoltativo) Verifica che le variabili di ambiente siano state impostate correttamente.

      ```
      echo $SUBNET_IDS
      ```

Amazon VPC console

1. Aprire Amazon VPC console.
2. Nella VPC dashboard, scegli Crea VPC.
3. Per creare risorse, scegli VPCe altro ancora.
4. Mantieni selezionata la generazione automatica dei tag nome per creare i tag Nome per VPC le risorse o deselezionala per fornire i tuoi tag Nome per le VPC risorse.
5. Per IPv4CIDRblocco, inserisci un intervallo di IPv4 indirizzi per. VPC Un VPC deve avere un intervallo di IPv4 indirizzi.
6. (Facoltativo) Per supportare IPv6 il traffico, scegli IPv6CIDRblock, blocco fornito da Amazon IPv6 CIDR.
7. Lascia Tenancy come. `Default`

8. Per Numero di zone di disponibilità (AZs), scegli il numero che desideri. Per le implementazioni Multi-AZ, ROSA richiede tre zone di disponibilità. Per scegliere le AZs sottoreti, espandi Personalizza. AZs

   > **Note**
   >
   > Medio ROSA i tipi di istanza sono disponibili solo in zone di disponibilità selezionate. Puoi utilizzare il plugin ROSA CLI`rosa list instance-types`comando per elencare tutto ROSA tipi di istanze disponibili. Per verificare se un tipo di istanza è disponibile per una determinata zona di disponibilità, usa AWS CLI comando`aws ec2 describe-instance-type-offerings --location-type availability-zone --filters Name=location,Values=<availability_zone> --region <region> --output text | egrep "<instance_type>"`.

9. Per configurare le sottoreti, scegli i valori per Numero di sottoreti pubbliche e Numero di sottoreti private. Per scegliere gli intervalli di indirizzi IP per le sottoreti, espandi Personalizza i blocchi di CIDR sottoreti.

   > **Note**
   >
   > ROSAwith HCP richiede che i clienti configurino almeno una sottorete pubblica e privata per ogni zona di disponibilità utilizzata per creare i cluster.

10. Per concedere alle risorse della sottorete privata l'accesso alla rete Internet pubblica tramiteIPv4, per i NATgateway, scegli il numero di gateway AZs in cui creare i gateway. NAT In produzione, consigliamo di implementare un NAT gateway in ogni AZ con risorse che richiedono l'accesso alla rete Internet pubblica.
11. (Facoltativo) Se è necessario accedere Amazon S3 direttamente dal tuoVPC, scegli VPCendpoint, S3 Gateway.
12. Lascia selezionate le DNS opzioni predefinite. ROSA richiede DNS il supporto del nome host su. VPC
13. Espandi Tag aggiuntivi, scegli Aggiungi nuovo tag e aggiungi le seguenti chiavi di tag. ROSA utilizza controlli automatici di preflight che verificano l'utilizzo di questi tag.
    - Chiave: `kubernetes.io/role/elb`
    - Chiave: `kubernetes.io/role/internal-elb`
14. Scegli Crea VPC.

AWS CLI

1. Crea un VPC con un `10.0.0.0/16` CIDR blocco.

```
aws ec2 create-vpc \
    --cidr-block 10.0.0.0/16 \
    --query Vpc.VpcId \
    --output text
```

   Il comando precedente restituisce l'VPCID. Di seguito è riportato un esempio di output.

```
vpc-1234567890abcdef0
```

2. Memorizza l'VPCID in una variabile di ambiente.

```
export VPC_ID=vpc-1234567890abcdef0
```

3. Crea un `Name` tag perVPC, utilizzando la variabile di `VPC_ID` ambiente.

```
aws ec2 create-tags --resources $VPC_ID --tags Key=Name,Value=MyVPC
```

4. Abilita DNS il supporto del nome host su. VPC

```
aws ec2 modify-vpc-attribute \
    --vpc-id $VPC_ID \
    --enable-dns-hostnames
```

5. Crea una sottorete pubblica e privata inVPC, specificando le zone di disponibilità in cui devono essere create le risorse.

> **Important**
>
> ROSAwith HCP richiede che i clienti configurino almeno una sottorete pubblica e privata per ogni zona di disponibilità utilizzata per creare i cluster. Per le implementazioni Multi-AZ, sono necessarie tre zone di disponibilità. Se questi requisiti non vengono soddisfatti, la creazione del cluster non riesce.

> **Note**
>
> Medio ROSA i tipi di istanza sono disponibili solo in zone di disponibilità selezionate. Puoi utilizzare il plugin ROSA CLI`rosa list instance-types`comando per elencare tutto ROSA tipi di istanze disponibili. Per verificare se un tipo di istanza è disponibile per una determinata zona di disponibilità, usa AWS CLI comando`aws ec2 describe-instance-type-offerings --location-type availability-zone --filters Name=location,Values=<availability_zone> --region <region> --output text | egrep "<instance_type>"`.

```
aws ec2 create-subnet \
    --vpc-id $VPC_ID \
    --cidr-block 10.0.1.0/24 \
    --availability-zone us-east-1a \
    --query Subnet.SubnetId \
    --output text
aws ec2 create-subnet \
    --vpc-id $VPC_ID \
    --cidr-block 10.0.0.0/24 \
    --availability-zone us-east-1a \
    --query Subnet.SubnetId \
    --output text
```

6. Memorizza la sottorete pubblica e privata IDs in variabili di ambiente.

```
export PUBLIC_SUB=subnet-1234567890abcdef0
export PRIVATE_SUB=subnet-0987654321fedcba0
```

7. Crea i seguenti tag per le tue VPC sottoreti. ROSA utilizza controlli automatici di preflight che verificano l'utilizzo di questi tag.

> **Note**
>
> È necessario etichettare almeno una sottorete privata e, se applicabile, una sottorete pubblica.

```
aws ec2 create-tags --resources $PUBLIC_SUB --tags Key=kubernetes.io/role/
elb,Value=1
aws ec2 create-tags --resources $PRIVATE_SUB --tags Key=kubernetes.io/role/
internal-elb,Value=1
```

8. Crea un gateway Internet e una tabella di routing per il traffico in uscita. Crea una tabella di routing e un indirizzo IP elastico per il traffico privato.

```
aws ec2 create-internet-gateway \
    --query InternetGateway.InternetGatewayId \
    --output text
aws ec2 create-route-table \
    --vpc-id $VPC_ID \
    --query RouteTable.RouteTableId \
    --output text
aws ec2 allocate-address \
    --domain vpc \
    --query AllocationId \
    --output text
aws ec2 create-route-table \
    --vpc-id $VPC_ID \
    --query RouteTable.RouteTableId \
    --output text
```

9. IDsMemorizza le variabili di ambiente.

```
export IGW=igw-1234567890abcdef0
export PUBLIC_RT=rtb-0987654321fedcba0
export EIP=eipalloc-0be6ecac95EXAMPLE
export PRIVATE_RT=rtb-1234567890abcdef0
```

10. Collega il gateway Internet aVPC.

```
aws ec2 attach-internet-gateway \
    --vpc-id $VPC_ID \
    --internet-gateway-id $IGW
```

11. Associa la tabella delle rotte pubbliche alla sottorete pubblica e configura il traffico da indirizzare verso il gateway Internet.

```
aws ec2 associate-route-table \
    --subnet-id $PUBLIC_SUB \
    --route-table-id $PUBLIC_RT
aws ec2 create-route \
    --route-table-id $PUBLIC_RT \
    --destination-cidr-block 0.0.0.0/0 \
    --gateway-id $IGW
```

12. Crea il NAT gateway e associalo all'indirizzo IP elastico per abilitare il traffico verso la sottorete privata.

```
aws ec2 create-nat-gateway \
    --subnet-id $PUBLIC_SUB \
    --allocation-id $EIP \
    --query NatGateway.NatGatewayId \
    --output text
```

13. Associa la tabella di routing privata alla sottorete privata e configura il traffico per l'instradamento verso il NAT gateway.

```
aws ec2 associate-route-table \
    --subnet-id $PRIVATE_SUB \
    --route-table-id $PRIVATE_RT
aws ec2 create-route \
    --route-table-id $PRIVATE_RT \
    --destination-cidr-block 0.0.0.0/0 \
    --gateway-id $NATGW
```

14. (Facoltativo) Per le implementazioni Multi-AZ, ripeti i passaggi precedenti per configurare altre due zone di disponibilità con sottoreti pubbliche e private.

Crea il file richiesto IAM ruoli e configurazione OpenID Connect

Prima di creare un HCP cluster ROSA with, è necessario creare il necessario IAM ruoli e politiche e la configurazione OpenID Connect (OIDC). Per ulteriori informazioni sull' IAM ruoli e politiche per ROSA withHCP, vedithe section called “ AWS policy gestite”.

Questa procedura utilizza la `auto` modalità di ROSA CLIper creare automaticamente la OIDC configurazione necessaria per creare un HCP cluster ROSA with.

1. Crea il richiesto IAM ruoli e politiche dell'account. Il `--force-policy-creation` parametro aggiorna tutti i ruoli e le politiche esistenti presenti. Se non sono presenti ruoli e politiche, il comando crea invece queste risorse.

```
rosa create account-roles --force-policy-creation
```

> **Note**
>
> Se il token di accesso offline è scaduto, ROSA CLIemette un messaggio di errore che indica che il token di autorizzazione deve essere aggiornato. Per la procedura di risoluzione dei problemi, consulta. the section called “Risolvi i problemi relativi ai token di ROSA CLI accesso offline scaduti”

2. Crea la configurazione OpenID Connect (OIDC) che abilita l'autenticazione degli utenti nel cluster. Questa configurazione è registrata per essere utilizzata con OpenShift Cluster Manager (OCM).

```
rosa create oidc-config --mode=auto
```

3. Copia l'ID di OIDC configurazione fornito nel ROSA CLIuscita. L'ID di OIDC configurazione deve essere fornito in seguito per creare il HCP cluster ROSA with.
4. Per verificare le OIDC configurazioni disponibili per i cluster associati all'organizzazione degli utenti, esegui il comando seguente.

```
rosa list oidc-config
```

5. Crea il file richiesto IAM ruoli dell'operatore, sostituiti `<OIDC_CONFIG_ID>` con l'ID di OIDC configurazione copiato in precedenza.

   Example

> **Important**
>
> È necessario fornire un prefisso in `<PREFIX_NAME>` quando si creano i ruoli Operator. In caso contrario, si verificherà un errore.

```
rosa create operator-roles --prefix <PREFIX_NAME> --oidc-config-id <OIDC_CONFIG_ID>
 --hosted-cp
```

6. Per verificare il IAM i ruoli operatore sono stati creati, esegui il comando seguente:

```
rosa list operator-roles
```

Crea un HCP cluster ROSA with usando il ROSA CLIe AWS STS

Puoi creare ROSA un HCP cluster utilizzo di AWS Security Token Service (AWS STS) e la `auto` modalità fornita in ROSA CLI. Hai la possibilità di creare un cluster con un ingresso pubblico API e un ingresso privatoAPI.

È possibile creare un cluster con una singola zona di disponibilità (Single-AZ) o più zone di disponibilità (Multi-AZ). In entrambi i casi, il CIDR valore della macchina deve corrispondere al valore VPC del CIDR tuo.

La procedura seguente utilizza il `rosa create cluster --hosted-cp` comando per creare un Single-AZ con ROSA HCP cluster. Per creare un Multi-AZ cluster, specifica `multi-az` nel comando e nella sottorete privata IDs per ogni sottorete privata in cui desiderate effettuare la distribuzione.

1. Crea un HCP cluster ROSA with con uno dei seguenti comandi.
   - Crea un HCP cluster ROSA with con un public API e un Ingress, specificando il nome del cluster, il prefisso del ruolo dell'operatore, l'ID di OIDC configurazione e la sottorete pubblica e privata. IDs

     ```
     rosa create cluster --cluster-name=<CLUSTER_NAME> --sts --mode=auto --hosted-cp --
     operator-roles-prefix <OPERATOR_ROLE_PREFIX> --oidc-config-id <OIDC_CONFIG_ID> --
     subnet-ids=<PUBLIC_SUBNET_ID>,<PRIVATE_SUBNET_ID>
     ```

   - Crea un HCP cluster ROSA with con un cluster privato API e Ingress, specificando il nome del cluster, il prefisso del ruolo dell'operatore, l'ID di configurazione e la sottorete privata. OIDC IDs

     ```
     rosa create cluster --private --cluster-name=<CLUSTER_NAME> --sts --mode=auto --
     hosted-cp --subnet-ids=<PRIVATE_SUBNET_ID>
     ```

2. Controlla lo stato del tuo cluster.

```
rosa describe cluster -c <CLUSTER_NAME>
```

> **Note**
>
> Se il processo di creazione fallisce o il `State` campo non diventa pronto dopo 10 minuti, consultaRisoluzione dei problemi.
> Per contattare AWS Support o il supporto Red Hat per ricevere assistenza, consultathe section called “Ottenere supporto”.

3. Monitora lo stato di avanzamento del cluster creazione guardando i log dell' OpenShift installatore.

```
rosa logs install -c <CLUSTER_NAME> --watch
```

Configura un provider di identità e concedi cluster accedi

ROSA include un OAuth server integrato. Dopo il tuo cluster è stato creato, è necessario configurarlo OAuth per utilizzare un provider di identità. Puoi quindi aggiungere utenti al tuo provider di identità configurato per concedere loro l'accesso al tuo cluster. È possibile concedere tali utenti `cluster-admin` o `dedicated-admin` autorizzazioni in base alle esigenze.

Puoi configurare diversi tipi di provider di identità per ROSA cluster. I tipi supportati includono GitHub Enterprise GitHub GitLab, GoogleLDAP, OpenID Connect e provider di HTPasswd identità.

> **Important**
>
> Il provider di HTPasswd identità è incluso solo per consentire la creazione di un singolo utente amministratore statico. HTPasswdnon è supportato come provider di identità di uso generico per ROSA.

La procedura seguente configura un provider di GitHub identità come esempio. Per istruzioni su come configurare ciascuno dei tipi di provider di identità supportati, vedere Configurazione dei provider di identità per AWS STS.

1. Vai su github.com e accedi al tuo account. GitHub

2. Se non disponi di un' GitHub organizzazione da utilizzare per la fornitura di identità per il tuo cluster, creane uno. Per ulteriori informazioni, consulta i passaggi indicati nella GitHub documentazione.
3. Utilizzo di ROSA CLI, configura un provider di identità per il tuo cluster.

```
rosa create idp --cluster=<CLUSTER_NAME> --interactive
```

4. Segui le istruzioni di configurazione nell'output per limitare cluster accesso ai membri della tua GitHub organizzazione.

```
I: Interactive mode enabled.
Any optional fields can be left empty and a default will be selected.
? Type of identity provider: github
? Identity provider name: github-1
? Restrict to members of: organizations
? GitHub organizations: <GITHUB_ORG_NAME>
? To use GitHub as an identity provider, you must first register the application:
  - Open the following URL:
    https://github.com/organizations/<GITHUB_ORG_NAME>/settings/
applications/new?oauth_application%5Bcallback_url%5D=https%3A%2F%2Foauth-
openshift.apps.<CLUSTER_NAME>/<RANDOM_STRING>.p1.openshiftapps.com%2Foauth2callback
%2Fgithub-1&oauth_application%5Bname%5D=<CLUSTER_NAME>&oauth_application
%5Burl%5D=https%3A%2F%2Fconsole-openshift-console.apps.<CLUSTER_NAME>/
<RANDOM_STRING>.p1.openshiftapps.com
  - Click on 'Register application'
...
```

5. Apri il file URL nell'output, sostituendolo <GITHUB_ORG_NAME> con il nome della tua GitHub organizzazione.
6. Nella pagina GitHub web, scegli Registra applicazione per registrare una nuova OAuth applicazione nella tua GitHub organizzazione.
7. Utilizza le informazioni della GitHub OAuth pagina per compilare i prompt `rosa create idp` interattivi rimanenti eseguendo il comando seguente. Sostituisci <GITHUB_CLIENT_ID> e <GITHUB_CLIENT_SECRET> con le credenziali dell'applicazione. GitHub OAuth

```
...
? Client ID: <GITHUB_CLIENT_ID>
? Client Secret: [? for help] <GITHUB_CLIENT_SECRET>
? GitHub Enterprise Hostname (optional):
? Mapping method: claim
```

```
I: Configuring IDP for cluster '<CLUSTER_NAME>'
I: Identity Provider 'github-1' has been created.
   It will take up to 1 minute for this configuration to be enabled.
   To add cluster administrators, see 'rosa grant user --help'.
   To login into the console, open https://console-openshift-
console.apps.<CLUSTER_NAME>.<RANDOM_STRING>.p1.openshiftapps.com and click on
 github-1.
```

> **Note**
>
> Potrebbero essere necessari circa due minuti prima che la configurazione del provider di identità diventi attiva. Se hai configurato un `cluster-admin` utente, puoi correre `oc get pods -n openshift-authentication --watch` a guardare i OAuth pod ridistribuirsi con la configurazione aggiornata.

8. Verifica che il provider di identità sia configurato correttamente.

```
rosa list idps --cluster=<CLUSTER_NAME>
```

Concedi all'utente l'accesso a cluster

Puoi concedere a un utente l'accesso a cluster aggiungendoli al provider di identità configurato.

La procedura seguente aggiunge un utente a un' GitHub organizzazione configurata per il provisioning delle identità al cluster.

1. Vai su github.com e accedi al tuo account. GitHub
2. Invita gli utenti che lo richiedono cluster accesso alla tua GitHub organizzazione. Per ulteriori informazioni, vedi Invitare gli utenti a entrare a far parte della tua organizzazione nella GitHub documentazione.

Configura le **`cluster-admin`** autorizzazioni

1. Concedi le `cluster-admin` autorizzazioni eseguendo il comando seguente. Sostituisci `<IDP_USER_NAME>` e `<CLUSTER_NAME>` con il nome utente e del cluster.

```
rosa grant user cluster-admin --user=<IDP_USER_NAME> --cluster=<CLUSTER_NAME>
```

2. Verifica che l'utente sia elencato come membro del `cluster-admins` gruppo.

```
rosa list users --cluster=<CLUSTER_NAME>
```

Configura le **`dedicated-admin`** autorizzazioni

1. Concedi le `dedicated-admin` autorizzazioni utilizzando il seguente comando. Sostituisci `<IDP_USER_NAME>` e `<CLUSTER_NAME>` con il tuo utente e cluster nome eseguendo il comando seguente.

```
rosa grant user dedicated-admin --user=<IDP_USER_NAME> --cluster=<CLUSTER_NAME>
```

2. Verifica che l'utente sia elencato come membro del `cluster-admins` gruppo.

```
rosa list users --cluster=<CLUSTER_NAME>
```

Accedere a cluster tramite la console Red Hat Hybrid Cloud

Accedi al tuo cluster tramite la Red Hat Hybrid Cloud Console.

1. Procurati la console URL per cluster usando il seguente comando. Sostituisci `<CLUSTER_NAME>` con il nome del tuo cluster.

```
rosa describe cluster -c <CLUSTER_NAME> | grep Console
```

2. Vai alla console URL nell'output e accedi.

   Nella finestra di dialogo Accedi con..., scegli il nome del provider di identità e completa tutte le richieste di autorizzazione presentate dal provider.

Distribuisci un'applicazione dal Developer Catalog

Dalla Red Hat Hybrid Cloud Console, puoi implementare un'applicazione di test del Developer Catalog ed esporla con un percorso.

1. Accedi a Red Hat Hybrid Cloud Console e scegli il cluster in cui vuoi implementare l'app.
2. Nella pagina del cluster, scegli Open console.

3. Nella prospettiva dell'amministratore, scegli Home > Progetti > Crea progetto.
4. Immettete un nome per il progetto e, facoltativamente, aggiungete un nome visualizzato e una descrizione.
5. Scegli Crea per creare il progetto.
6. Passa alla prospettiva dello sviluppatore e scegli +Aggiungi. Assicurati che il progetto selezionato sia quello appena creato.
7. Nella finestra di dialogo Developer Catalog, scegli Tutti i servizi.
8. Nella pagina del catalogo per sviluppatori, scegliete Lingue > JavaScriptdal menu.
9. Scegliete Node.js, quindi scegliete Crea applicazione per aprire la pagina Crea applicazione Source-to-Image.

> **Note**
>
> Potrebbe essere necessario scegliere Cancella tutti i filtri per visualizzare l'opzione Node.js.

10. Nella sezione Git, scegli Try Sample.
11. Nel campo Nome, aggiungi un nome univoco.
12. Scegli Create (Crea) .

> **Note**
>
> La distribuzione della nuova applicazione richiede diversi minuti.

13. Una volta completata la distribuzione, scegli il percorso URL per l'applicazione.

    Si apre una nuova scheda nel browser con un messaggio simile al seguente.

```
Welcome to your Node.js application on OpenShift
```

14. (Facoltativo) Eliminare l'applicazione e ripulire le risorse:
    a. Nella prospettiva dell'amministratore, scegliete Home > Progetti.
    b. Apri il menu delle azioni per il tuo progetto e scegli Elimina progetto.

Revoca le **`cluster-admin`** autorizzazioni a un utente

1. Revoca le `cluster-admin` autorizzazioni utilizzando il seguente comando. Sostituisci `<IDP_USER_NAME>` e `<CLUSTER_NAME>` con il tuo utente e cluster nome.

```
rosa revoke user cluster-admin --user=<IDP_USER_NAME> --cluster=<CLUSTER_NAME>
```

2. Verifica che l'utente non sia elencato come membro del `cluster-admins` gruppo.

```
rosa list users --cluster=<CLUSTER_NAME>
```

Revoca le **`dedicated-admin`** autorizzazioni a un utente

1. Revoca le `dedicated-admin` autorizzazioni utilizzando il seguente comando. Sostituisci `<IDP_USER_NAME>` e `<CLUSTER_NAME>` con il tuo utente e cluster nome.

```
rosa revoke user dedicated-admin --user=<IDP_USER_NAME> --cluster=<CLUSTER_NAME>
```

2. Verifica che l'utente non sia elencato come membro del `dedicated-admins` gruppo.

```
rosa list users --cluster=<CLUSTER_NAME>
```

Revoca l'accesso utente a cluster

Puoi revocare cluster accedere a un utente del provider di identità rimuovendolo dal provider di identità configurato.

Puoi configurare diversi tipi di provider di identità per i tuoi cluster. La seguente procedura revoca cluster accesso per un membro di un' GitHub organizzazione.

1. Vai su github.com e accedi al tuo account. GitHub
2. Rimuovi l'utente dalla tua organizzazione. GitHub Per ulteriori informazioni, consulta Rimuovere un membro dall'organizzazione nella GitHub documentazione.

Eliminare un cluster e AWS STS risorse

Puoi utilizzare il plugin ROSA CLIeliminare un cluster che usa AWS Security Token Service (AWS STS). Puoi anche usare il ROSA CLIper eliminare il IAM ruoli e OIDC provider creati da ROSA. Per eliminare il IAM politiche create da ROSA, è possibile utilizzare il IAM console.

> **Note**
>
> IAM ruoli e politiche creati da ROSA potrebbe essere usato da altri ROSA cluster nello stesso account.

1. Elimina le foto o i video cluster e guarda i log. Sostituisci `<CLUSTER_NAME>` con il nome o l'ID del tuo cluster.

   ```
   rosa delete cluster --cluster=<CLUSTER_NAME> --watch
   ```

   > **Important**
   >
   > Devi aspettare il cluster da eliminare completamente prima di rimuovere il IAM ruoli, politiche e OIDC provider. I IAM ruoli dell'account sono necessari per eliminare le risorse create dal programma di installazione. I IAM ruoli degli operatori sono necessari per ripulire le risorse create dagli OpenShift operatori. Gli operatori utilizzano il OIDC provider per l'autenticazione.

2. Eliminare il OIDC provider che cluster gli operatori utilizzano per autenticarsi eseguendo il comando seguente.

   ```
   rosa delete oidc-provider -c <CLUSTER_ID> --mode auto
   ```

3. Eliminare l'operatore specifico del cluster IAM ruoli.

   ```
   rosa delete operator-roles -c <CLUSTER_ID> --mode auto
   ```

4. Eliminare i IAM ruoli dell'account utilizzando il seguente comando. Sostituisci `<PREFIX>` con il prefisso dei IAM ruoli dell'account da eliminare. Se hai specificato un prefisso personalizzato durante la creazione dei IAM ruoli dell'account, specifica il prefisso predefinito`ManagedOpenShift`.

```
rosa delete account-roles --prefix <PREFIX> --mode auto
```

5. Elimina le foto o i video IAM politiche create da ROSA.
   a. Effettua il login a IAM console.
   b. Nel menu a sinistra in Gestione degli accessi, scegli Politiche.
   c. Seleziona la politica che desideri eliminare e scegli Azioni > Elimina.
   d. Inserisci il nome della politica e scegli Elimina.
   e. Ripeti questo passaggio per eliminare ciascuna delle IAM politiche per cluster.

Crea un cluster ROSA classico utilizzando ROSA CLI

Le sezioni seguenti descrivono come iniziare a usare la ROSA versione classica AWS STS e il ROSA CLI. Per i passaggi per creare un cluster ROSA classico utilizzando Terraform, consulta la documentazione di Red Hat. Per saperne di più sul provider Terraform per la creazione ROSA cluster, consulta la documentazione Terraform.

Il ROSA CLIutilizza `auto` mode o `manual` mode per creare il IAM risorse necessarie per fornire a ROSA cluster. `auto`la modalità crea immediatamente il necessario IAM ruoli e politiche e un provider OpenID Connect (OIDC). `manual`mode emette il AWS CLI comandi necessari per creare il IAM risorse. Utilizzando la `manual` modalità, è possibile rivedere i dati generati AWS CLI comandi prima di eseguirli manualmente. Con `manual` mode, puoi anche passare i comandi a un altro amministratore o gruppo dell'organizzazione in modo che possa creare le risorse.

Per altre opzioni per iniziare, consultaInizia con ROSA .

Argomenti

- Prerequisiti
- Crea un cluster ROSA classico utilizzando il ROSA CLIe AWS STS
- Configura un provider di identità e concedi cluster accedi
- Concedi all'utente l'accesso a un cluster
- Configura le cluster-admin autorizzazioni
- Configura le dedicated-admin autorizzazioni
- Accedere a cluster tramite la console Red Hat Hybrid Cloud
- Distribuisci un'applicazione dal Developer Catalog

- Revoca le cluster-admin autorizzazioni a un utente
- Revoca le dedicated-admin autorizzazioni a un utente
- Revoca l'accesso utente a un cluster
- Eliminare un cluster e AWS STS risorse

Prerequisiti

Completa le azioni preliminari elencate inthe section called “Configurazione”.

Crea un cluster ROSA classico utilizzando il ROSA CLIe AWS STS

Puoi creare un ROSA classico cluster utilizzando il ROSA CLIe AWS STS.

1. Crea il richiesto IAM ruoli e politiche dell'account che utilizzano `--mode auto` o`--mode manual`.
   - ```
     rosa create account-roles --classic --mode auto
     ```
   - ```
     rosa create account-roles --classic --mode manual
     ```

     > **Note**
     >
     > Se il token di accesso offline è scaduto, ROSA CLIemette un messaggio di errore che indica che il token di autorizzazione deve essere aggiornato. Per la procedura di risoluzione dei problemi, consulta. the section called “Risolvi i problemi relativi ai token di ROSA CLI accesso offline scaduti”
2. Crea un cluster utilizzando `--mode auto` o`--mode manual`. `auto`la modalità consente di creare un cluster più rapidamente. `manual`mode richiede di specificare impostazioni personalizzate per il cluster.
   - ```
     rosa create cluster --cluster-name <CLUSTER_NAME> --sts --mode auto
     ```
     ```

> **Note**
>
> Quando si specifica `--mode auto`, il `rosa create cluster` comando crea l'operatore specifico del cluster IAM ruoli e OIDC provider automaticamente. Gli operatori utilizzano il OIDC provider per l'autenticazione.

> **Note**
>
> Quando si utilizzano le `--mode auto` impostazioni predefinite, viene installata l'ultima OpenShift versione stabile.

- ```
  rosa create cluster --cluster-name <CLUSTER_NAME> --sts --mode manual
  ```

> **Important**
>
> Se si abilita la crittografia etcd in `manual` modalità, si incorre in un sovraccarico di prestazioni di circa il 20%. L'overhead è il risultato dell'introduzione di questo secondo livello di crittografia, oltre alla EBS crittografia Amazon predefinita che crittografa i volumi etcd.

> **Note**
>
> Dopo aver eseguito la `manual` modalità di creazione del cluster, è necessario creare manualmente i IAM ruoli operatore specifici del cluster e il provider OpenID Connect utilizzato dagli operatori del cluster per l'autenticazione.

3. Controlla lo stato del tuo cluster.

```
rosa describe cluster -c <CLUSTER_NAME>
```
```

> **Note**
>
> Se il processo di provisioning fallisce o il `State` campo non diventa pronto dopo 40 minuti, consultaRisoluzione dei problemi. Per contattare AWS Support o il supporto Red Hat per ricevere assistenza, consultathe section called “Ottenere supporto”.

4. Monitora lo stato di avanzamento del cluster creazione guardando i log dell' OpenShift installatore.

```
rosa logs install -c <CLUSTER_NAME> --watch
```

Configura un provider di identità e concedi cluster accedi

ROSA include un OAuth server integrato. Dopo il tuo cluster è stato creato, è necessario configurarlo OAuth per utilizzare un provider di identità. È quindi possibile aggiungere utenti al provider di identità configurato per concedere loro l'accesso al cluster. È possibile concedere tali utenti `cluster-admin` o `dedicated-admin` autorizzazioni in base alle esigenze.

Puoi configurare diversi tipi di provider di identità per ROSA cluster. I tipi supportati includono GitHub Enterprise GitHub GitLab, GoogleLDAP, OpenID Connect e provider di HTPasswd identità.

> **Important**
>
> Il provider di HTPasswd identità è incluso solo per consentire la creazione di un singolo utente amministratore statico. HTPasswdnon è supportato come provider di identità di uso generico per ROSA.

La procedura seguente configura un provider di GitHub identità come esempio. Per istruzioni su come configurare ciascuno dei tipi di provider di identità supportati, vedere Configurazione dei provider di identità per AWS STS.

1. Vai su github.com e accedi al tuo account. GitHub
2. Se non disponi di un' GitHub organizzazione da utilizzare per la fornitura di identità per cluster, creane uno. Per ulteriori informazioni, consulta i passaggi indicati nella GitHub documentazione.
3. Utilizzo di ROSA CLI, configura un provider di identità per il tuo cluster.

```
rosa create idp --cluster=<CLUSTER_NAME> --interactive
```

4. Segui le istruzioni di configurazione nell'output per limitare cluster accesso ai membri della tua GitHub organizzazione.

```
I: Interactive mode enabled.
Any optional fields can be left empty and a default will be selected.
? Type of identity provider: github
? Identity provider name: github-1
? Restrict to members of: organizations
? GitHub organizations: <GITHUB_ORG_NAME>
? To use GitHub as an identity provider, you must first register the application:
  - Open the following URL:
    https://github.com/organizations/<GITHUB_ORG_NAME>/settings/
applications/new?oauth_application%5Bcallback_url%5D=https%3A%2F%2Foauth-
openshift.apps.<CLUSTER_NAME>/<RANDOM_STRING>.p1.openshiftapps.com%2Foauth2callback
%2Fgithub-1&oauth_application%5Bname%5D=<CLUSTER_NAME>&oauth_application
%5Burl%5D=https%3A%2F%2Fconsole-openshift-console.apps.<CLUSTER_NAME>/
<RANDOM_STRING>.p1.openshiftapps.com
  - Click on 'Register application'
...
```

5. Apri il file URL nell'output, sostituendolo <GITHUB_ORG_NAME> con il nome della tua GitHub organizzazione.
6. Nella pagina GitHub web, scegli Registra applicazione per registrare una nuova OAuth applicazione nella tua GitHub organizzazione.
7. Utilizza le informazioni della GitHub OAuth pagina per compilare i prompt `rosa create idp` interattivi rimanenti eseguendo il comando seguente. Sostituisci <GITHUB_CLIENT_ID> e <GITHUB_CLIENT_SECRET> con le credenziali dell'applicazione. GitHub OAuth

```
...
? Client ID: <GITHUB_CLIENT_ID>
? Client Secret: [? for help] <GITHUB_CLIENT_SECRET>
? GitHub Enterprise Hostname (optional):
? Mapping method: claim
I: Configuring IDP for cluster '<CLUSTER_NAME>'
I: Identity Provider 'github-1' has been created.
   It will take up to 1 minute for this configuration to be enabled.
   To add cluster administrators, see 'rosa grant user --help'.
```

```
   To login into the console, open https://console-openshift-
console.apps.<CLUSTER_NAME>.<RANDOM_STRING>.p1.openshiftapps.com and click on
 github-1.
```

> **Note**
>
> Potrebbero essere necessari circa due minuti prima che la configurazione del provider di identità diventi attiva. Se hai configurato un `cluster-admin` utente, puoi correre `oc get pods -n openshift-authentication --watch` a guardare i OAuth pod ridistribuirsi con la configurazione aggiornata.

8. Verifica che il provider di identità sia configurato correttamente.

```
rosa list idps --cluster=<CLUSTER_NAME>
```

Concedi all'utente l'accesso a un cluster

Puoi concedere a un utente l'accesso al tuo cluster aggiungendoli al provider di identità configurato.

La procedura seguente aggiunge un utente a un' GitHub organizzazione configurata per il provisioning delle identità al cluster.

1. Vai su github.com e accedi al tuo account. GitHub
2. Invita gli utenti che lo richiedono cluster accesso alla tua GitHub organizzazione. Per ulteriori informazioni, vedi Invitare gli utenti a entrare a far parte della tua organizzazione nella GitHub documentazione.

Configura le **`cluster-admin`** autorizzazioni

1. Concedi le `cluster-admin` autorizzazioni eseguendo il comando seguente. Sostituisci `<IDP_USER_NAME>` e `<CLUSTER_NAME>` con il nome utente e del cluster.

```
rosa grant user cluster-admin --user=<IDP_USER_NAME> --cluster=<CLUSTER_NAME>
```

2. Verifica che l'utente sia elencato come membro del `cluster-admins` gruppo.

```
rosa list users --cluster=<CLUSTER_NAME>
```

Configura le **`dedicated-admin`** autorizzazioni

1. Concedi le `dedicated-admin` autorizzazioni utilizzando il seguente comando. Sostituisci `<IDP_USER_NAME>` e `<CLUSTER_NAME>` con il tuo utente e cluster nome eseguendo il comando seguente.

```
rosa grant user dedicated-admin --user=<IDP_USER_NAME> --cluster=<CLUSTER_NAME>
```

2. Verifica che l'utente sia elencato come membro del `cluster-admins` gruppo.

```
rosa list users --cluster=<CLUSTER_NAME>
```

Accedere a cluster tramite la console Red Hat Hybrid Cloud

Dopo aver creato un cluster utente amministratore o aggiunto un utente al provider di identità configurato, puoi accedere al cluster tramite la Red Hat Hybrid Cloud Console.

1. Procurati la console URL per il tuo cluster usando il seguente comando. Sostituisci `<CLUSTER_NAME>` con il nome del tuo cluster.

```
rosa describe cluster -c <CLUSTER_NAME> | grep Console
```

2. Vai alla console URL nell'output e accedi.
   - Se hai creato un `cluster-admin` utente, accedi utilizzando le credenziali fornite.
   - Se hai configurato un provider di identità per il tuo cluster, scegli il nome del provider di identità nella finestra di dialogo Accedi con... e completa tutte le richieste di autorizzazione presentate dal provider.

Distribuisci un'applicazione dal Developer Catalog

Dalla Red Hat Hybrid Cloud Console, puoi implementare un'applicazione di test del Developer Catalog ed esporla con un percorso.

1. Accedi a Red Hat Hybrid Cloud Console e scegli il cluster in cui vuoi implementare l'app.
2. Nella pagina del cluster, scegli Open console.
3. Nella prospettiva dell'amministratore, scegli Home > Progetti > Crea progetto.

4. Immettete un nome per il progetto e, facoltativamente, aggiungete un nome visualizzato e una descrizione.
5. Scegli Crea per creare il progetto.
6. Passa alla prospettiva dello sviluppatore e scegli +Aggiungi. Assicurati che il progetto selezionato sia quello appena creato.
7. Nella finestra di dialogo Developer Catalog, scegli Tutti i servizi.
8. Nella pagina del catalogo per sviluppatori, scegliete Lingue > JavaScriptdal menu.
9. Scegliete Node.js, quindi scegliete Crea applicazione per aprire la pagina Crea applicazione Source-to-Image.

> **Note**
>
> Potrebbe essere necessario scegliere Cancella tutti i filtri per visualizzare l'opzione Node.js.

10. Nella sezione Git, scegli Try Sample.
11. Nel campo Nome, aggiungi un nome univoco.
12. Scegli Create (Crea) .

> **Note**
>
> La distribuzione della nuova applicazione richiede diversi minuti.

13. Una volta completata la distribuzione, scegli il percorso URL per l'applicazione.

    Si apre una nuova scheda nel browser con un messaggio simile al seguente.

```
Welcome to your Node.js application on OpenShift
```

14. (Facoltativo) Eliminare l'applicazione e ripulire le risorse:
    a. Nella prospettiva dell'amministratore, scegliete Home > Progetti.
    b. Apri il menu delle azioni per il tuo progetto e scegli Elimina progetto.

Revoca le **`cluster-admin`** autorizzazioni a un utente

1. Revoca le `cluster-admin` autorizzazioni utilizzando il seguente comando. Sostituisci `<IDP_USER_NAME>` e `<CLUSTER_NAME>` con il tuo utente e cluster nome.

```
rosa revoke user cluster-admin --user=<IDP_USER_NAME> --cluster=<CLUSTER_NAME>
```

2. Verifica che l'utente non sia elencato come membro del `cluster-admins` gruppo.

```
rosa list users --cluster=<CLUSTER_NAME>
```

Revoca le **`dedicated-admin`** autorizzazioni a un utente

1. Revoca le `dedicated-admin` autorizzazioni utilizzando il seguente comando. Sostituisci `<IDP_USER_NAME>` e `<CLUSTER_NAME>` con il tuo utente e cluster nome.

```
rosa revoke user dedicated-admin --user=<IDP_USER_NAME> --cluster=<CLUSTER_NAME>
```

2. Verifica che l'utente non sia elencato come membro del `dedicated-admins` gruppo.

```
rosa list users --cluster=<CLUSTER_NAME>
```

Revoca l'accesso utente a un cluster

Puoi revocare cluster accedere a un utente del provider di identità rimuovendolo dal provider di identità configurato.

Puoi configurare diversi tipi di provider di identità per cluster. La seguente procedura revoca cluster accesso per un membro di un' GitHub organizzazione.

1. Vai su github.com e accedi al tuo account. GitHub
2. Rimuovi l'utente dalla tua organizzazione. GitHub Per ulteriori informazioni, consulta Rimuovere un membro dall'organizzazione nella GitHub documentazione.

Eliminare un cluster e AWS STS risorse

Puoi utilizzare il plugin ROSA CLIeliminare un cluster che usa AWS Security Token Service (AWS STS). Puoi anche usare il ROSA CLIper eliminare il IAM ruoli e OIDC provider creati da ROSA. Per eliminare il IAM politiche create da ROSA, è possibile utilizzare il IAM console.

> **Important**
>
> IAM ruoli e politiche creati da ROSA potrebbe essere usato da altri ROSA cluster nello stesso account.

1. Elimina le foto o i video cluster e guarda i log. Sostituisci <CLUSTER_NAME> con il nome o l'ID del tuo cluster.

   ```
   rosa delete cluster --cluster=<CLUSTER_NAME> --watch
   ```

   > **Important**
   >
   > Devi aspettare il cluster da eliminare completamente prima di rimuovere il IAM ruoli, politiche e OIDC provider. I IAM ruoli dell'account sono necessari per eliminare le risorse create dall'installatore. I IAM ruoli degli operatori sono necessari per ripulire le risorse create dagli OpenShift operatori. Gli operatori utilizzano il OIDC provider per l'autenticazione.

2. Eliminare il OIDC provider che cluster gli operatori utilizzano per autenticarsi eseguendo il comando seguente.

   ```
   rosa delete oidc-provider -c <CLUSTER_ID> --mode auto
   ```

3. Eliminare l'operatore specifico del cluster IAM ruoli.

   ```
   rosa delete operator-roles -c <CLUSTER_ID> --mode auto
   ```

4. Eliminare i IAM ruoli dell'account utilizzando il seguente comando. Sostituisci <PREFIX> con il prefisso dei IAM ruoli dell'account da eliminare. Se hai specificato un prefisso personalizzato durante la creazione dei IAM ruoli dell'account, specifica il prefisso predefinitoManaged0penShift.

```
rosa delete account-roles --prefix <PREFIX> --mode auto
```

5. Elimina le foto o i video IAM politiche create da ROSA.
   a. Effettua il login a IAM console.
   b. Nel menu a sinistra in Gestione degli accessi, scegli Politiche.
   c. Seleziona la politica che desideri eliminare e scegli Azioni > Elimina.
   d. Inserisci il nome della politica e scegli Elimina.
   e. Ripeti questo passaggio per eliminare ciascuna delle IAM politiche per cluster.

Crea un cluster ROSA classico che utilizza AWS PrivateLink

ROSAi cluster classici possono essere implementati in diversi modi: pubblici, privati o privati con AWS PrivateLink. Per ulteriori informazioni sulla ROSA versione classica, consultathe section called “Modelli di architettura”. Sia per uso pubblico che privato cluster configurazioni, il OpenShift cluster ha accesso a Internet e la privacy è impostata sui carichi di lavoro delle applicazioni a livello di applicazione.

Se hai bisogno di entrambi cluster e che i carichi di lavoro delle applicazioni siano privati, puoi configurare AWS PrivateLink con ROSA classic. AWS PrivateLink è una tecnologia scalabile e altamente disponibile che ROSA utilizza per creare una connessione privata tra ROSA servizio e risorse del cluster in AWS account cliente. Con AWS PrivateLink, il team di Red Hat site Reliability Engineering (SRE) può accedere al cluster per scopi di supporto e riparazione utilizzando una sottorete privata connessa al cluster AWS PrivateLink endpoint.

Per ulteriori informazioni sull' AWS PrivateLink, vedi Cos'è AWS PrivateLink?

Argomenti

- Prerequisiti
- Crea Amazon VPC architecture
- Crea un cluster classico utilizzando ROSA ROSA CLIe AWS PrivateLink
- Configura AWS PrivateLink DNSinoltro
- Configura un provider di identità e concedi cluster accedi
- Concedi all'utente l'accesso a cluster
- Configura le cluster-admin autorizzazioni

- Configura le dedicated-admin autorizzazioni
- Accedere a cluster tramite la console Red Hat Hybrid Cloud
- Distribuisci un'applicazione dal Developer Catalog
- Revoca le cluster-admin autorizzazioni a un utente
- Revoca le dedicated-admin autorizzazioni a un utente
- Revoca l'accesso utente a cluster
- Eliminare un cluster e AWS STS risorse

Prerequisiti

Completa le azioni preliminari elencate inthe section called “Configurazione”.

Crea Amazon VPC architecture

La procedura seguente crea Amazon VPC architettura che può essere utilizzata per ospitare un cluster. Tutti cluster le risorse sono ospitate nella sottorete privata. La sottorete pubblica indirizza il traffico in uscita dalla sottorete privata attraverso un NAT gateway verso la rete Internet pubblica. Questo esempio utilizza il blocco per CIDR `10.0.0.0/16` Amazon VPC. Tuttavia, puoi scegliere un CIDR blocco diverso. Per ulteriori informazioni, vedi VPCdimensionamento.

> **Important**
>
> Se Amazon VPC i requisiti non sono soddisfatti, la creazione del cluster non riesce.

Example

Amazon VPC console

1. Aprire Amazon VPC console.
2. Nella VPC dashboard, scegli Crea VPC.
3. Per Risorse da creare, scegli VPCe altro ancora.
4. Mantieni selezionata la generazione automatica dei tag nome per creare i tag Nome per VPC le risorse o deselezionala per fornire i tuoi tag Nome per le VPC risorse.
5. Per IPv4CIDRblocco, inserisci un intervallo di IPv4 indirizzi per. VPC Un VPC deve avere un intervallo di IPv4 indirizzi.

6. (Facoltativo) Per supportare IPv6 il traffico, scegli IPv6CIDRblock, blocco fornito da Amazon IPv6 CIDR.
7. Lascia Tenancy come. `Default`
8. Per Numero di zone di disponibilità (AZs), scegli il numero che desideri. Per le implementazioni Multi-AZ, ROSA richiede tre zone di disponibilità. Per scegliere le AZs sottoreti, espandi Personalizza. AZs

   > **Note**
   >
   > Medio ROSA i tipi di istanza sono disponibili solo in zone di disponibilità selezionate. Puoi utilizzare il plugin ROSA CLI`rosa list instance-types`comando per elencare tutto ROSA tipi di istanze disponibili. Per verificare se un tipo di istanza è disponibile per una determinata zona di disponibilità, usa AWS CLI comando`aws ec2 describe-instance-type-offerings --location-type availability-zone --filters Name=location,Values=<availability_zone> --region <region> --output text | egrep "<instance_type>"`.

9. Per configurare le sottoreti, scegli i valori per Numero di sottoreti pubbliche e Numero di sottoreti private. Per scegliere gli intervalli di indirizzi IP per le sottoreti, espandi Personalizza i blocchi di CIDR sottoreti.

   > **Note**
   >
   > ROSA richiede che i clienti configurino almeno una sottorete privata per zona di disponibilità utilizzata per creare i cluster.

10. Per concedere alle risorse della sottorete privata l'accesso alla rete Internet pubblicaIPv4, per i NATgateway, scegli il numero di gateway AZs in cui creare i gateway. NAT In produzione, consigliamo di implementare un NAT gateway in ogni AZ con risorse che richiedono l'accesso alla rete Internet pubblica.
11. (Facoltativo) Se è necessario accedere Amazon S3 direttamente dal tuoVPC, scegli VPCendpoint, S3 Gateway.
12. Lascia selezionate le DNS opzioni predefinite. ROSA richiede DNS il supporto del nome host su. VPC
13. Scegli Crea VPC.

AWS CLI

1. Crea un VPC con un `10.0.0.0/16` CIDR blocco.

```
aws ec2 create-vpc \
    --cidr-block 10.0.0.0/16 \
    --query Vpc.VpcId \
    --output text
```

   Il comando precedente restituisce l'VPCID. Di seguito è riportato un esempio di output.

```
vpc-1234567890abcdef0
```

2. Memorizza l'VPCID in una variabile di ambiente.

```
export VPC_ID=vpc-1234567890abcdef0
```

3. Crea un `Name` tag perVPC, utilizzando la variabile di `VPC_ID` ambiente.

```
aws ec2 create-tags --resources $VPC_ID --tags Key=Name,Value=MyVPC
```

4. Abilita DNS il supporto del nome host su. VPC

```
aws ec2 modify-vpc-attribute \
    --vpc-id $VPC_ID \
    --enable-dns-hostnames
```

5. Crea una sottorete pubblica e privata inVPC, specificando le zone di disponibilità in cui devono essere create le risorse.

> **Important**
>
> ROSA richiede che i clienti configurino almeno una sottorete privata per ogni zona di disponibilità utilizzata per creare i cluster. Per le implementazioni Multi-AZ, sono necessarie tre zone di disponibilità. Se questi requisiti non vengono soddisfatti, la creazione del cluster non riesce.

> **Note**
>
> Medio ROSA i tipi di istanza sono disponibili solo in zone di disponibilità selezionate. Puoi utilizzare il plugin ROSA CLI`rosa list instance-types`comando per elencare tutto ROSA tipi di istanze disponibili. Per verificare se un tipo di istanza è disponibile per una determinata zona di disponibilità, usa AWS CLI comando`aws ec2 describe-instance-type-offerings --location-type availability-zone --filters Name=location,Values=<availability_zone> --region <region> --output text | egrep "<instance_type>"`.

```
aws ec2 create-subnet \
    --vpc-id $VPC_ID \
    --cidr-block 10.0.1.0/24 \
    --availability-zone us-east-1a \
    --query Subnet.SubnetId \
    --output text
aws ec2 create-subnet \
    --vpc-id $VPC_ID \
    --cidr-block 10.0.0.0/24 \
    --availability-zone us-east-1a \
    --query Subnet.SubnetId \
    --output text
```

6. Memorizza la sottorete pubblica e privata IDs in variabili di ambiente.

```
export PUBLIC_SUB=subnet-1234567890abcdef0
export PRIVATE_SUB=subnet-0987654321fedcba0
```

7. Crea un gateway Internet e una tabella di routing per il traffico in uscita. Crea una tabella di routing e un indirizzo IP elastico per il traffico privato.

```
aws ec2 create-internet-gateway \
    --query InternetGateway.InternetGatewayId \
    --output text
aws ec2 create-route-table \
    --vpc-id $VPC_ID \
    --query RouteTable.RouteTableId \
    --output text
```

```
aws ec2 allocate-address \
    --domain vpc \
    --query AllocationId \
    --output text
aws ec2 create-route-table \
    --vpc-id $VPC_ID \
    --query RouteTable.RouteTableId \
    --output text
```

8. IDsMemorizza le variabili di ambiente.

```
export IGW=igw-1234567890abcdef0
export PUBLIC_RT=rtb-0987654321fedcba0
export EIP=eipalloc-0be6ecac95EXAMPLE
export PRIVATE_RT=rtb-1234567890abcdef0
```

9. Collega il gateway Internet aVPC.

```
aws ec2 attach-internet-gateway \
    --vpc-id $VPC_ID \
    --internet-gateway-id $IGW
```

10. Associa la tabella delle rotte pubbliche alla sottorete pubblica e configura il traffico da instradare verso il gateway Internet.

```
aws ec2 associate-route-table \
    --subnet-id $PUBLIC_SUB \
    --route-table-id $PUBLIC_RT
aws ec2 create-route \
    --route-table-id $PUBLIC_RT \
    --destination-cidr-block 0.0.0.0/0 \
    --gateway-id $IGW
```

11. Crea il NAT gateway e associalo all'indirizzo IP elastico per abilitare il traffico verso la sottorete privata.

```
aws ec2 create-nat-gateway \
    --subnet-id $PUBLIC_SUB \
    --allocation-id $EIP \
    --query NatGateway.NatGatewayId \
    --output text
```

12 Associa la tabella di routing privata alla sottorete privata e configura il traffico per l'instradamento verso il NAT gateway.

```
aws ec2 associate-route-table \
    --subnet-id $PRIVATE_SUB \
    --route-table-id $PRIVATE_RT
aws ec2 create-route \
    --route-table-id $PRIVATE_RT \
    --destination-cidr-block 0.0.0.0/0 \
    --gateway-id $NATGW
```

13 (Facoltativo) Per le implementazioni Multi-AZ, ripeti i passaggi precedenti per configurare altre due zone di disponibilità con sottoreti pubbliche e private.

Crea un cluster classico utilizzando ROSA ROSA CLIe AWS PrivateLink

Puoi utilizzare il plugin ROSA CLIe AWS PrivateLink per creare un cluster con una singola zona di disponibilità (Single-AZ) o più zone di disponibilità (Multi-AZ). In entrambi i casi, il CIDR valore della macchina deve corrispondere al valore VPC del CIDR tuo.

La procedura seguente utilizza il `rosa create cluster` comando per creare un ROSA classico cluster. Per creare un Multi-AZ cluster, specificate `--multi-az` nel comando, quindi selezionate la sottorete privata IDs che desiderate utilizzare quando richiesto.

> **Note**
>
> Se si utilizza un firewall, è necessario configurarlo in modo che ROSA può accedere ai siti necessari per funzionare.
> Per ulteriori informazioni, consulta AWS prerequisiti del firewall nella OpenShift documentazione di Red Hat.

1. Crea il file richiesto IAM ruoli e politiche dell'account che utilizzano `--mode auto` o `--mode manual`.
   -
     ```
     rosa create account-roles --classic --mode auto
     ```
   -
     ```
     rosa create account-roles --classic --mode manual
     ```

> **Note**
>
> Se il token di accesso offline è scaduto, ROSA CLIemette un messaggio di errore che indica che il token di autorizzazione deve essere aggiornato. Per la procedura di risoluzione dei problemi, consulta. the section called “Risolvi i problemi relativi ai token di ROSA CLI accesso offline scaduti”

2. Crea un cluster eseguendo uno dei seguenti comandi.

   - Single-AZ

   ```
   rosa create cluster --private-link --cluster-name=<CLUSTER_NAME> --machine-
   cidr=10.0.0.0/16 --subnet-ids=<PRIVATE_SUBNET_ID>
   ```

   - Multi-AZ

   ```
   rosa create cluster --private-link --multi-az --cluster-name=<CLUSTER_NAME> --
   machine-cidr=10.0.0.0/16
   ```

   > **Note**
   >
   > Per creare un cluster che utilizza AWS PrivateLink con AWS Security Token Service (AWS STS) credenziali di breve durata, aggiungono `--sts --mode auto` o `--sts --mode manual` alla fine del comando. `rosa create cluster`

3. Crea il cluster operatore IAM ruoli seguendo le istruzioni interattive.

   ```
   rosa create operator-roles --interactive -c <CLUSTER_NAME>
   ```

4. Creare il provider OpenID Connect (OIDC) il cluster gli operatori utilizzano per autenticarsi.

   ```
   rosa create oidc-provider --interactive -c <CLUSTER_NAME>
   ```

5. Controlla lo stato del tuo cluster.

   ```
   rosa describe cluster -c <CLUSTER_NAME>
   ```

> **Note**
>
> Potrebbero essere necessari fino a 40 minuti per cluster `State`campo per mostrare lo `ready` stato. Se il provisioning fallisce o non viene visualizzato `ready` dopo 40 minuti, vediRisoluzione dei problemi. Per contattare AWS Support o il supporto Red Hat per ricevere assistenza, consultathe section called “Ottenere supporto”.

6. Monitora lo stato di avanzamento del cluster creazione guardando i log dell' OpenShift installatore.

```
rosa logs install -c <CLUSTER_NAME> --watch
```

Configura AWS PrivateLink DNSinoltro

Cluster che utilizzano AWS PrivateLink crea una zona ospitata pubblica e una zona ospitata privata in Route 53. Record all'interno del Route 53 la zona ospitata privata è risolvibile solo all'interno della zona a VPC cui è assegnata.

La convalida Let's Encrypt DNS -01 richiede una zona pubblica in modo che possano essere emessi certificati validi e pubblicamente attendibili per il dominio. I record di convalida vengono eliminati dopo il completamento della convalida di Let's Encrypt. La zona è ancora necessaria per l'emissione e il rinnovo di questi certificati, che in genere sono richiesti ogni 60 giorni. Sebbene queste zone appaiano generalmente vuote, un'area pubblica svolge un ruolo fondamentale nel processo di convalida.

Per ulteriori informazioni sull' AWS zone private ospitate, vedi Lavorare con le zone private. Per ulteriori informazioni sulle zone ospitate pubbliche, consulta Lavorare con le zone ospitate pubbliche.

Configurare un Route 53 Resolver endpoint in entrata

1. Per consentire la memorizzazione `api.<cluster_domain>` e la risoluzione di record `*.apps.<cluster_domain>` al di fuori diVPC, configura un Route 53 Resolver endpoint in entrata.

> **Note**
>
> Quando si configura un endpoint in entrata, è necessario specificare un minimo di due indirizzi IP per la ridondanza. Consigliamo di specificare indirizzi IP in almeno due zone di

disponibilità. È anche possibile specificare facoltativamente ulteriori indirizzi IP in quelle o in altre zone di disponibilità.

2. Quando configuri l'endpoint in entrata, seleziona le sottoreti private VPC utilizzate durante la creazione del cluster.

Configura l'inoltro per il cluster DNS

Dopo il Route 53 Resolver un endpoint interno è associato e operativo, configurate l'DNSinoltro in modo che DNS le interrogazioni possano essere gestite dai server designati sulla rete.

1. Configurate la rete aziendale per inoltrare DNS le query a quegli indirizzi IP per il dominio di primo livello, ad esempio. `drow-pl-01.htno.p1.openshiftapps.com`
2. Se stai inoltrando DNS le richieste da uno VPC all'altroVPC, segui le istruzioni in Gestione delle regole di inoltro.
3. Se stai configurando il server di rete remoto, consulta la documentazione specifica DNS del server per configurare l'inoltro selettivo DNS per il dominio DNS del cluster installato.

Configura un provider di identità e concedi cluster accedi

ROSA include un OAuth server integrato. Dopo il tuo ROSA cluster è stato creato, è necessario configurarlo OAuth per utilizzare un provider di identità. Puoi quindi aggiungere utenti al tuo provider di identità configurato per concedere loro l'accesso al cluster. È possibile concedere tali utenti `cluster-admin` o `dedicated-admin` autorizzazioni in base alle esigenze.

Puoi configurare diversi tipi di provider di identità per cluster. I tipi supportati includono GitHub Enterprise GitHub GitLab, GoogleLDAP, OpenID Connect e provider di HTPasswd identità.

Important

Il provider di HTPasswd identità è incluso solo per consentire la creazione di un singolo utente amministratore statico. HTPasswdnon è supportato come provider di identità di uso generico per ROSA.

La procedura seguente configura un provider di GitHub identità come esempio. Per istruzioni su come configurare ciascuno dei tipi di provider di identità supportati, vedere Configurazione dei provider di identità per AWS STS.

1. Vai su github.com e accedi al tuo account. GitHub
2. Se non disponi di un' GitHub organizzazione da utilizzare per la fornitura di identità per ROSA cluster, creane uno. Per ulteriori informazioni, consulta i passaggi indicati nella GitHub documentazione.
3. Utilizzo di ROSA CLI, configura un provider di identità per il tuo cluster eseguendo il comando seguente.

```
rosa create idp --cluster=<CLUSTER_NAME> --interactive
```

4. Segui le istruzioni di configurazione nell'output per limitare cluster accesso ai membri della tua GitHub organizzazione.

```
I: Interactive mode enabled.
Any optional fields can be left empty and a default will be selected.
? Type of identity provider: github
? Identity provider name: github-1
? Restrict to members of: organizations
? GitHub organizations: <GITHUB_ORG_NAME>
? To use GitHub as an identity provider, you must first register the application:
  - Open the following URL:
    https://github.com/organizations/<GITHUB_ORG_NAME>/settings/
applications/new?oauth_application%5Bcallback_url%5D=https%3A%2F%2Foauth-
openshift.apps.<CLUSTER_NAME>/<RANDOM_STRING>.p1.openshiftapps.com%2Foauth2callback
%2Fgithub-1&oauth_application%5Bname%5D=<CLUSTER_NAME>&oauth_application
%5Burl%5D=https%3A%2F%2Fconsole-openshift-console.apps.<CLUSTER_NAME>/
<RANDOM_STRING>.p1.openshiftapps.com
  - Click on 'Register application'
...
```

5. Apri il file URL nell'output, sostituendolo <GITHUB_ORG_NAME> con il nome della tua GitHub organizzazione.
6. Nella pagina GitHub web, scegli Registra applicazione per registrare una nuova OAuth applicazione nella tua GitHub organizzazione.

7. Utilizza le informazioni contenute nella GitHub OAuth pagina per compilare i prompt `rosa create idp` interattivi rimanenti, sostituendo `<GITHUB_CLIENT_ID>` e `<GITHUB_CLIENT_SECRET>` con le credenziali dell'applicazione. GitHub OAuth

```
...
? Client ID: <GITHUB_CLIENT_ID>
? Client Secret: [? for help] <GITHUB_CLIENT_SECRET>
? GitHub Enterprise Hostname (optional):
? Mapping method: claim
I: Configuring IDP for cluster '<CLUSTER_NAME>'
I: Identity Provider 'github-1' has been created.
   It will take up to 1 minute for this configuration to be enabled.
   To add cluster administrators, see 'rosa grant user --help'.
   To login into the console, open https://console-openshift-
console.apps.<CLUSTER_NAME>.<RANDOM_STRING>.p1.openshiftapps.com and click on
 github-1.
```

> **Note**
>
> Potrebbero essere necessari circa due minuti prima che la configurazione del provider di identità diventi attiva. Se hai configurato un `cluster-admin` utente, puoi eseguire il `oc get pods -n openshift-authentication --watch` comando per guardare i OAuth pod ridistribuirsi con la configurazione aggiornata.

8. Verifica che il provider di identità sia stato configurato correttamente.

```
rosa list idps --cluster=<CLUSTER_NAME>
```

Concedi all'utente l'accesso a cluster

Puoi concedere a un utente l'accesso al tuo cluster aggiungendoli al provider di identità configurato.

La procedura seguente aggiunge un utente a un' GitHub organizzazione configurata per il provisioning delle identità al cluster.

1. Vai su github.com e accedi al tuo account. GitHub
2. Invita gli utenti che lo richiedono cluster accesso alla tua GitHub organizzazione. Per ulteriori informazioni, vedi Invitare gli utenti a entrare a far parte della tua organizzazione nella GitHub documentazione.

Configura le **`cluster-admin`** autorizzazioni

1. Concedi le `cluster-admin` autorizzazioni utilizzando il seguente comando. Sostituisci `<IDP_USER_NAME>` e `<CLUSTER_NAME>` con il nome utente e del cluster.

```
rosa grant user cluster-admin --user=<IDP_USER_NAME> --cluster=<CLUSTER_NAME>
```

2. Verifica che l'utente sia elencato come membro del `cluster-admins` gruppo.

```
rosa list users --cluster=<CLUSTER_NAME>
```

Configura le **`dedicated-admin`** autorizzazioni

1. Concedi le `dedicated-admin` autorizzazioni con il seguente comando. Sostituisci `<IDP_USER_NAME>` e `<CLUSTER_NAME>` con il tuo utente e cluster nome.

```
rosa grant user dedicated-admin --user=<IDP_USER_NAME> --cluster=<CLUSTER_NAME>
```

2. Verifica che l'utente sia elencato come membro del `cluster-admins` gruppo.

```
rosa list users --cluster=<CLUSTER_NAME>
```

Accedere a cluster tramite la console Red Hat Hybrid Cloud

Dopo aver creato un cluster utente amministratore o aggiunto un utente al provider di identità configurato, puoi accedere al cluster tramite la Red Hat Hybrid Cloud Console.

1. Procurati la console URL per cluster usando il seguente comando. Sostituisci `<CLUSTER_NAME>` con il nome del tuo cluster.

```
rosa describe cluster -c <CLUSTER_NAME> | grep Console
```

2. Vai alla console URL nell'output e accedi.
   - Se hai creato un `cluster-admin` utente, accedi utilizzando le credenziali fornite.
   - Se hai configurato un provider di identità per il tuo cluster, scegli il nome del provider di identità nella finestra di dialogo Accedi con... e completa tutte le richieste di autorizzazione presentate dal provider.

Distribuisci un'applicazione dal Developer Catalog

Dalla Red Hat Hybrid Cloud Console, puoi implementare un'applicazione di test del Developer Catalog ed esporla con un percorso.

1. Accedi a Red Hat Hybrid Cloud Console e scegli il cluster in cui vuoi implementare l'app.
2. Nella pagina del cluster, scegli Open console.
3. Nella prospettiva dell'amministratore, scegli Home > Progetti > Crea progetto.
4. Immettete un nome per il progetto e, facoltativamente, aggiungete un nome visualizzato e una descrizione.
5. Scegli Crea per creare il progetto.
6. Passa alla prospettiva dello sviluppatore e scegli +Aggiungi. Assicurati che il progetto selezionato sia quello appena creato.
7. Nella finestra di dialogo Developer Catalog, scegli Tutti i servizi.
8. Nella pagina del catalogo per sviluppatori, scegliete Lingue > JavaScriptdal menu.
9. Scegliete Node.js, quindi scegliete Crea applicazione per aprire la pagina Crea applicazione Source-to-Image.

> **Note**
>
> Potrebbe essere necessario scegliere Cancella tutti i filtri per visualizzare l'opzione Node.js.

10. Nella sezione Git, scegli Try Sample.
11. Nel campo Nome, aggiungi un nome univoco.
12. Scegli Create (Crea) .

> **Note**
>
> La distribuzione della nuova applicazione richiede diversi minuti.

13. Una volta completata la distribuzione, scegli il percorso URL per l'applicazione.

    Si apre una nuova scheda nel browser con un messaggio simile al seguente.

```
Welcome to your Node.js application on OpenShift
```

14. (Facoltativo) Eliminare l'applicazione e ripulire le risorse.
    a. Nella prospettiva dell'amministratore, scegliete Home > Progetti.
    b. Apri il menu delle azioni per il tuo progetto e scegli Elimina progetto.

Revoca le **`cluster-admin`** autorizzazioni a un utente

1. Revoca le `cluster-admin` autorizzazioni utilizzando il seguente comando. Sostituisci `<IDP_USER_NAME>` e `<CLUSTER_NAME>` con il tuo utente e cluster nome.

```
rosa revoke user cluster-admin --user=<IDP_USER_NAME> --cluster=<CLUSTER_NAME>
```

2. Verifica che l'utente non sia elencato come membro del `cluster-admins` gruppo.

```
rosa list users --cluster=<CLUSTER_NAME>
```

Revoca le **`dedicated-admin`** autorizzazioni a un utente

1. Revoca le `dedicated-admin` autorizzazioni utilizzando il seguente comando. Sostituisci `<IDP_USER_NAME>` e `<CLUSTER_NAME>` con il tuo utente e cluster nome.

```
rosa revoke user dedicated-admin --user=<IDP_USER_NAME> --cluster=<CLUSTER_NAME>
```

2. Verifica che l'utente non sia elencato come membro del `dedicated-admins` gruppo.

```
rosa list users --cluster=<CLUSTER_NAME>
```

Revoca l'accesso utente a cluster

Puoi revocare cluster accedere a un utente del provider di identità rimuovendolo dal provider di identità configurato.

Puoi configurare diversi tipi di provider di identità per cluster. La seguente procedura revoca cluster accesso per un membro di un' GitHub organizzazione.

1. Vai su github.com e accedi al tuo account. GitHub

2. Rimuovi l'utente dalla tua organizzazione. GitHub Per ulteriori informazioni, consulta Rimuovere un membro dall'organizzazione nella GitHub documentazione.

Eliminare un cluster e AWS STS risorse

Puoi utilizzare il plugin ROSA CLIeliminare un cluster che usa AWS Security Token Service (AWS STS). Puoi anche usare il ROSA CLIper eliminare il IAM ruoli e OIDC provider creati da ROSA. Per eliminare il IAM politiche create da ROSA, è possibile utilizzare il IAM console.

> **Important**
>
> IAM ruoli e politiche creati da ROSA potrebbe essere usato da altri ROSA cluster nello stesso account.

1. Elimina le foto o i video cluster e guarda i log. Sostituisci <CLUSTER_NAME> con il nome o l'ID del tuo cluster.

```
rosa delete cluster --cluster=<CLUSTER_NAME> --watch
```

> **Important**
>
> Devi aspettare il cluster da eliminare completamente prima di rimuovere il IAM ruoli, politiche e OIDC provider. I IAM ruoli dell'account sono necessari per eliminare le risorse create dal programma di installazione. I IAM ruoli degli operatori sono necessari per ripulire le risorse create dagli OpenShift operatori. Gli operatori utilizzano il OIDC provider per l'autenticazione.

2. Eliminare il OIDC provider che cluster gli operatori utilizzano per autenticarsi eseguendo il comando seguente.

```
rosa delete oidc-provider -c <CLUSTER_ID> --mode auto
```

3. Eliminare l'operatore specifico del cluster IAM ruoli.

```
rosa delete operator-roles -c <CLUSTER_ID> --mode auto
```

4. Eliminare i IAM ruoli dell'account utilizzando il seguente comando. Sostituisci `<PREFIX>` con il prefisso dei IAM ruoli dell'account da eliminare. Se hai specificato un prefisso personalizzato durante la creazione dei IAM ruoli dell'account, specifica il prefisso predefinito`ManagedOpenShift`.

```
rosa delete account-roles --prefix <PREFIX> --mode auto
```

5. Elimina le foto o i video IAM politiche create da ROSA.
   a. Effettua il login a IAM console.
   b. Nel menu a sinistra in Gestione degli accessi, scegli Politiche.
   c. Seleziona la politica che desideri eliminare e scegli Azioni > Elimina.
   d. Inserisci il nome della politica e scegli Elimina.
   e. Ripeti questo passaggio per eliminare ciascuna delle IAM politiche per cluster.

Sicurezza in ROSA

Sicurezza nel cloud presso AWS è la massima priorità. Come AWS cliente, trarrai vantaggio da un'architettura di data center e rete progettata per soddisfare i requisiti delle organizzazioni più sensibili alla sicurezza.

La sicurezza è una responsabilità condivisa tra AWS e tu. Il modello di responsabilità condivisa descrive questo come sicurezza del cloud e sicurezza nel cloud:

- Sicurezza del cloud — AWS è responsabile della protezione dell'infrastruttura in esecuzione AWS servizi in Cloud AWS. AWS fornisce inoltre servizi che è possibile utilizzare in modo sicuro. I revisori di terze parti testano e verificano regolarmente l'efficacia della nostra sicurezza nell'ambito del AWS Programmi di conformità. Per saperne di più sui programmi di conformità applicabili a ROSA, vedi Servizi AWS in Scope by Compliance Program.
- Sicurezza nel cloud: la tua responsabilità è determinata dal Servizio AWS che usi. Sei anche responsabile di altri fattori, tra cui la riservatezza dei dati, i requisiti della tua azienda e le leggi e normative vigenti.

Questa documentazione aiuta a capire come applicare il modello di responsabilità condivisa durante l'utilizzo ROSA. Ti mostra come configurare ROSA per soddisfare i tuoi obiettivi di sicurezza e conformità. Imparerai anche a usarne altri Servizi AWS che ti aiutano a monitorare e proteggere i tuoi ROSA risorse.

Indice

Protezione dei dati in ROSA

La the section called “Responsabilità” documentazione e AWS il modello di responsabilità condivisa definisce la protezione dei dati in ROSA. AWS è responsabile della protezione dell'infrastruttura globale che gestisce tutte le Cloud AWS. Red Hat è responsabile della protezione dell'infrastruttura del cluster e della piattaforma di servizio sottostante. Il cliente è responsabile del mantenimento

del controllo sui contenuti ospitati su questa infrastruttura. Questo contenuto include le attività di configurazione e gestione della sicurezza per Servizi AWS che usi. Per ulteriori informazioni sulla privacy dei dati, consulta la sezione Privacy dei dati FAQ. Per informazioni sulla protezione dei dati in Europa, consulta il AWS Modello di responsabilità condivisa e post sul GDPR blog sul AWS Blog sulla sicurezza.

Ai fini della protezione dei dati, ti consigliamo di proteggere Account AWS credenziali e configura i singoli utenti con AWS Identity and Access Management (IAM). In questo modo, a ciascun utente vengono concesse solo le autorizzazioni necessarie per adempiere alle proprie mansioni lavorative. Ti suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- UsaSSL/TLSper comunicare con AWS risorse. Richiediamo TLS 1.2 e consigliamo TLS 1.3.
- Configurazione API e registrazione delle attività degli utenti con AWS CloudTrail.
- Utilizzo AWS soluzioni di crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno Servizi AWS.
- Utilizza servizi di sicurezza gestiti avanzati come Amazon Macie, che aiuta a scoprire e proteggere i dati sensibili archiviati in Amazon S3.
- Se sono necessari FIPS 140-2 moduli crittografici convalidati per l'accesso AWS tramite un'interfaccia a riga di comando o unAPI, utilizza un endpoint. FIPS Per ulteriori informazioni sugli FIPS endpoint disponibili, vedere Federal Information Processing Standard (FIPS) 140-2.

Consigliamo di non inserire mai informazioni identificative sensibili, ad esempio i numeri di account dei clienti, in campi a formato libero come un campo Nome. Ciò include quando lavori con ROSA o altro Servizi AWS utilizzando la consoleAPI, AWS CLI, oppure AWS SDKs. Tutti i dati che inserisci ROSA o altri servizi potrebbero essere scelti per essere inclusi nei registri di diagnostica. Quando fornite un messaggio URL a un server esterno, non includete le informazioni sulle credenziali URL per convalidare la richiesta a quel server.

Argomenti

- Protezione dei dati tramite crittografia

Protezione dei dati tramite crittografia

La protezione dei dati si riferisce alla protezione dei dati durante il transito (mentre viaggiano da e verso) ROSA) e a riposo (mentre sono archiviati su dischi in AWS centri dati).

Servizio Red Hat OpenShift su AWS fornisce un accesso sicuro a Amazon Elastic Block Store (Amazon EBS) volumi di archiviazione collegati a Amazon EC2 istanze per ROSA piano di controllo, infrastruttura e nodi di lavoro, nonché volumi persistenti Kubernetes per lo storage persistente. ROSA crittografa i dati di volume a riposo e in transito e utilizza AWS Key Management Service (AWS KMS) per proteggere i dati crittografati. Il servizio utilizza Amazon S3 per l'archiviazione del registro delle immagini del contenitore, che per impostazione predefinita è crittografato a riposo.

> **Important**
>
> Perché ROSA è un servizio gestito, AWS e Red Hat gestiscono l'infrastruttura che ROSA usi. I clienti non devono tentare di spegnere manualmente il Amazon EC2 casi che ROSA utilizza dal AWS console oCLI. Questa azione può portare alla perdita dei dati dei clienti.

Crittografia dei dati per Amazon EBS-volumi di archiviazione supportati

Servizio Red Hat OpenShift su AWS utilizza il framework Kubernetes persistent volume (PV) per consentire agli amministratori del cluster di fornire un cluster con storage persistente. I volumi persistenti, così come il piano di controllo, l'infrastruttura e i nodi di lavoro, sono supportati da Amazon Elastic Block Store (Amazon EBS) volumi di archiviazione collegati a Amazon EC2 istanze.

In ROSA volumi e nodi persistenti supportati da Amazon EBS, le operazioni di crittografia avvengono sui server che ospitano EC2 le istanze, garantendo la sicurezza sia dei dati inattivi che dei dati in transito tra un'istanza e lo storage collegato. Per ulteriori informazioni, consulta Amazon EBS crittografia in Amazon EC2 Guida per l'utente.

Crittografia dei dati per Amazon EBS CSIautista e Amazon EFS CSIautista

ROSA per impostazione predefinita utilizza il Amazon EBS CSIdriver per la fornitura Amazon EBS archiviazione. Il Amazon EBS CSIautista e Amazon EBS CSIDriver Operator sono installati nel cluster per impostazione predefinita nello `openshift-cluster-csi-drivers` spazio dei nomi. Il Amazon EBS CSIdriver e operatore consentono di effettuare il provisioning dinamico di volumi persistenti e di creare istantanee di volume.

ROSA è anche in grado di effettuare il provisioning di volumi persistenti utilizzando Amazon EFS CSIdriver e Amazon EFS CSIOperatore di guida. Il Amazon EFS driver e operatore consentono inoltre di condividere i dati del file system tra pod o con altre applicazioni all'interno o all'esterno di Kubernetes.

I dati di volume sono protetti durante il transito per entrambi i Amazon EBS CSIautista e Amazon EFS CSIautista. Per maggiori informazioni, consultate Using Container Storage Interface (CSI) nella documentazione di Red Hat.

> **Important**
>
> Durante il provisioning dinamico ROSA volumi persistenti che utilizzano il Amazon EFS CSIautista, Amazon EFS considera l'ID utente, l'ID di gruppo (GID) e il gruppo secondario del punto IDs di accesso durante la valutazione delle autorizzazioni del file system. Amazon EFS sostituisce l'utente e il gruppo IDs sui file con l'utente e il gruppo IDs sul punto di accesso e ignora il client. NFS IDs Di conseguenza, Amazon EFS ignora silenziosamente le `fsGroup` impostazioni. ROSA non è in grado di sostituire i GIDs file utilizzando. `fsGroup` Qualsiasi pod che può accedere a un file montato Amazon EFS un punto di accesso può accedere a qualsiasi file del volume. Per ulteriori informazioni, vedere Lavorare con Amazon EFS punti di accesso in Amazon EFS Guida per l'utente.

crittografia etcd

ROSA offre la possibilità di abilitare la crittografia dei valori `etcd` chiave all'interno del `etcd` volume durante la creazione del cluster, aggiungendo un ulteriore livello di crittografia. Una volta `etcd` crittografato, si verificherà un sovraccarico di prestazioni aggiuntivo di circa il 20%. Ti consigliamo di abilitare la `etcd` crittografia solo se la richiedi specificamente per il tuo caso d'uso. Per ulteriori informazioni, vedere etcd encryption nel ROSA definizione del servizio.

Gestione delle chiavi

ROSA utilizza KMS keys per gestire in modo sicuro i volumi di dati del piano di controllo, dell'infrastruttura e dei lavoratori e i volumi persistenti per le applicazioni dei clienti. Durante la creazione del cluster, puoi scegliere di utilizzare l'impostazione predefinita AWS gestiti KMS key fornito da Amazon EBS o specificando la propria chiave gestita dal cliente. Per ulteriori informazioni, consulta the section called “Gestione delle chiavi”.

Crittografia dei dati per il registro delle immagini integrato

ROSA fornisce un registro di immagini del contenitore integrato per archiviare, recuperare e condividere le immagini del contenitore tramite Amazon S3 stoccaggio a secchiello. Il registro è configurato e gestito dall' OpenShift Image Registry Operator. Fornisce agli utenti una out-

of-the-box soluzione per gestire le immagini che eseguono i loro carichi di lavoro e funziona sulla base dell'infrastruttura cluster esistente. Per ulteriori informazioni, consultate Registry nella documentazione di Red Hat.

ROSA offre registri di immagini pubblici e privati. Per le applicazioni aziendali, consigliamo di utilizzare un registro privato per proteggere le immagini dall'utilizzo da parte di utenti non autorizzati. Per proteggere i dati del registro quando sono inattivi, ROSA utilizza la crittografia lato server per impostazione predefinita con Amazon S3 chiavi gestite (SSE-S3). Questa operazione non richiede alcuna azione da parte dell'utente ed è offerta senza costi aggiuntivi. Per ulteriori informazioni, vedere Protezione dei dati utilizzando la crittografia lato server con Amazon S3 chiavi di crittografia gestite (SSE-S3) in Amazon S3 Guida per l'utente.

ROSA utilizza il protocollo Transport Layer Security (TLS) per proteggere i dati in transito da e verso il registro delle immagini. Per ulteriori informazioni, consultate Registry nella documentazione di Red Hat.

Riservatezza del traffico Internet

Servizio Red Hat OpenShift su AWS utilizza Amazon Virtual Private Cloud (Amazon VPC) per creare confini tra le risorse del tuo ROSA raggruppa e controlla il traffico tra queste ultime, la tua rete locale e Internet. Per ulteriori informazioni sull' Amazon VPC sicurezza, vedi Privacy del traffico Internet in Amazon VPC nella Amazon VPC Guida per l'utente.

All'interno diVPC, puoi configurare il tuo ROSA cluster per utilizzare un server HTTP o HTTPS proxy per negare l'accesso diretto a Internet. Se sei un amministratore del cluster, puoi anche definire politiche di rete a livello di pod che limitino il traffico interrete ai pod del tuo ROSA ammasso. Per ulteriori informazioni, consulta the section called “Sicurezza dell'infrastruttura”.

Crittografia dei dati utilizzando KMS

ROSA utilizza AWS KMS per gestire in modo sicuro le chiavi per i dati crittografati. I volumi del piano di controllo, dell'infrastruttura e dei nodi di lavoro sono crittografati per impostazione predefinita utilizzando AWS gestiti KMS key fornito da Amazon EBS. Questo KMS key ha lo pseudonimo`aws/ebs`. Anche i volumi persistenti che utilizzano la classe di archiviazione gp3 predefinita vengono crittografati di default utilizzando questo KMS key.

Appena creato ROSA i cluster sono configurati per utilizzare la classe di archiviazione gp3 predefinita per crittografare i volumi persistenti. I volumi persistenti creati utilizzando qualsiasi altra classe di archiviazione vengono crittografati solo se la classe di archiviazione è configurata per

essere crittografata. Per ulteriori informazioni sull' ROSA classi di storage predefinite, consultate Configurazione dello storage persistente nella documentazione di Red Hat.

Durante la creazione del cluster, è possibile scegliere di crittografare i volumi persistenti del cluster utilizzando l'impostazione predefinita Amazon EBS-chiave fornita o specifica la chiave simmetrica gestita dal cliente KMS key. Per ulteriori informazioni sulla creazione di chiavi, vedere Creazione di KMS chiavi di crittografia simmetriche nella AWS KMS Guida per gli sviluppatori.

È inoltre possibile crittografare i volumi persistenti per singoli contenitori all'interno di un cluster definendo un KMS key. Ciò è utile quando si dispone di linee guida esplicite in materia di conformità e sicurezza durante la distribuzione su AWS. Per ulteriori informazioni, vedere Crittografia dei volumi persistenti dei contenitori su AWS con un KMS keynella documentazione di Red Hat.

I seguenti punti devono essere considerati quando si crittografano volumi persistenti utilizzando i propri KMS keys:

- Quando si utilizza KMS la crittografia con la propria KMS key, la chiave deve esistere nella stessa Regione AWS come tuo cluster.
- È previsto un costo associato alla creazione e all'utilizzo del proprio KMS keys Per ulteriori informazioni, consulta .AWS Key Management Service prezzi.

Gestione delle identità e degli accessi per ROSA

AWS Identity and Access Management (IAM) è un Servizio AWS che aiuta un amministratore a controllare in modo sicuro l'accesso a AWS risorse. IAM gli amministratori controllano chi può essere autenticato (effettuato l'accesso) e autorizzato (dispone delle autorizzazioni) all'uso ROSA risorse. IAM è un Servizio AWS che puoi utilizzare senza costi aggiuntivi.

Argomenti

- Destinatari
- Autenticazione con identità
- Gestione dell'accesso con policy
- ROSA esempi di politiche basate sull'identità
- AWS politiche gestite per ROSA
- Risoluzione dei problemi ROSA identità e accesso

Destinatari

Come si usa AWS Identity and Access Management (IAM) differisce, a seconda del lavoro svolto ROSA.

Utente del servizio: se si utilizza il ROSA per svolgere il proprio lavoro, l'amministratore fornisce all'utente le credenziali e le autorizzazioni necessarie. Man mano che ne usi di più ROSA per eseguire il tuo lavoro, potresti aver bisogno di autorizzazioni aggiuntive. La comprensione della gestione dell'accesso ti consente di richiedere le autorizzazioni corrette all'amministratore. Se non è possibile accedere a una funzionalità in ROSA, consulta the section called “Risoluzione dei problemi”.

Amministratore del servizio: se sei responsabile di ROSA le risorse della tua azienda, probabilmente hai pieno accesso a ROSA. Spetta a te determinare quale ROSA funzionalità e risorse a cui gli utenti del servizio devono accedere. È quindi necessario inviare le richieste al IAM amministratore per modificare le autorizzazioni degli utenti del servizio. Consulta le informazioni contenute in questa pagina per comprendere i concetti di base di IAM.

IAM administrator - Se sei un IAM amministratore, potresti voler conoscere i dettagli sulle politiche utilizzate per gestire l'accesso a ROSA. Per visualizzare un esempio ROSA politiche basate sull'identità che è possibile utilizzare in IAM, consulta the section called “ ROSA esempi di politiche basate sull'identità”.

Autenticazione con identità

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

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

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

Se accedi AWS programmaticamente, AWS fornisce un kit di sviluppo software (SDK) e un'interfaccia a riga di comando (CLI) per firmare crittograficamente le richieste utilizzando le credenziali dell'utente. Se non usi AWS strumenti, devi firmare tu stesso le richieste. Per ulteriori informazioni sull'utilizzo del metodo consigliato per firmare autonomamente le richieste, vedi Firma AWS APIrichieste in IAM Guida per l'utente.

Indipendentemente dal metodo di autenticazione utilizzato, potrebbe essere necessario specificare ulteriori informazioni sulla sicurezza. Ad esempio, AWS consiglia di utilizzare l'autenticazione a più fattori (MFA) per aumentare la sicurezza del proprio account. Per ulteriori informazioni, consulta Autenticazione a più fattori nel AWS IAMIdentity Center (successore di AWS Guida per l'utente (Single Sign-On) e utilizzo dell'autenticazione a più fattori () in MFA AWS nella Guida per l'utente di IAM.

Account AWS utente root

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

Identità federata

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

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

Per la gestione centralizzata degli accessi, si consiglia di utilizzare AWS IAM Identity Center. È possibile creare utenti e gruppi in IAM Identity Center oppure connettersi e sincronizzarsi con un set di utenti e gruppi nella propria fonte di identità per utilizzarli su tutti i Account AWS e applicazioni. Per informazioni su IAM Identity Center, vedi Cos'è IAM Identity Center? nel AWS IAMIdentity Center (successore di AWS Guida per l'utente (Single Sign-On).

Utenti IAM e gruppi

Un Utente IAMè un'identità all'interno della tua Account AWS che dispone di autorizzazioni specifiche per una singola persona o applicazione. Laddove possibile, consigliamo di fare affidamento su credenziali temporanee anziché creare Utenti IAM che dispongono di credenziali a lungo termine come password e chiavi di accesso. Tuttavia, se hai casi d'uso specifici che richiedono credenziali a lungo termine con Utenti IAM, ti consigliamo di ruotare le chiavi di accesso. Per ulteriori informazioni, consulta Ruotare regolarmente le chiavi di accesso per i casi d'uso che richiedono credenziali a lungo termine nella Guida per l'IAMutente.

Un IAM gruppo è un'identità che specifica una raccolta di Utenti IAM. Non puoi accedere come gruppo. È possibile utilizzare gruppi per specificare le autorizzazioni per più utenti alla volta. I gruppi semplificano la gestione delle autorizzazioni per set di utenti di grandi dimensioni. Ad esempio, potresti avere un gruppo denominato IAMAdminse concedere a quel gruppo le autorizzazioni di amministrazione IAM risorse.

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

IAM roles

Un IAM il ruolo è un'identità all'interno della tua Account AWS che dispone di autorizzazioni specifiche. È simile a un Utente IAM, ma non è associato a una persona specifica. È possibile assumere temporaneamente un IAM ruolo nel AWS Management Console cambiando ruolo. Puoi assumere un ruolo chiamando un AWS CLI oppure AWS APIoperazione o utilizzando un comando personalizzatoURL. Per ulteriori informazioni sui metodi di utilizzo dei ruoli, vedere Utilizzo IAM ruoli nella Guida IAM per l'utente.

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

- Accesso utente federato: per assegnare autorizzazioni a un'identità federata, è necessario creare un ruolo e definire le autorizzazioni per il ruolo. Quando un'identità federata viene autenticata, l'identità viene associata al ruolo e ottiene le autorizzazioni da esso definite. Per informazioni sui ruoli per la federazione, consulta Creazione di un ruolo per un provider di identità di terze parti nella Guida per l'utente. IAM Se utilizzi IAM Identity Center, configuri un set di autorizzazioni. Per controllare a cosa possono accedere le identità dopo l'autenticazione, IAM Identity Center correla

il set di autorizzazioni a un ruolo in IAM. Per informazioni sui set di autorizzazioni, vedere Set di autorizzazioni nel AWS IAMIdentity Center (successore di AWS Guida per l'utente (Single Sign-On).

- Temporaneo Utente IAM autorizzazioni - Un Utente IAM può assumere un IAM ruolo per assumere temporaneamente autorizzazioni diverse per un'attività specifica.
- Accesso su più account: puoi usare un IAM ruolo che consente a qualcuno (un titolare fidato) di un altro account di accedere alle risorse del tuo account. I ruoli sono lo strumento principale per concedere l'accesso multi-account. Tuttavia, con alcuni Servizi AWS, è possibile allegare una policy direttamente a una risorsa (anziché utilizzare un ruolo come proxy). Per scoprire la differenza tra i ruoli e le politiche basate sulle risorse per l'accesso tra account diversi, vedi Come IAM i ruoli differiscono dalle politiche basate sulle risorse riportate nella Guida per l'utente. IAM
- Accesso a più servizi: alcuni Servizi AWS usa le funzionalità in altri Servizi AWS. Ad esempio, quando si effettua una chiamata in un servizio, è normale che quel servizio esegua applicazioni in Amazon EC2 o memorizza oggetti in Amazon S3. Un servizio può eseguire questa operazione utilizzando le autorizzazioni del principale chiamante, utilizzando un ruolo di servizio o utilizzando un ruolo collegato al servizio.
  - Sessioni di accesso diretto (FAS): quando si utilizza un Utente IAM o ruolo in cui eseguire azioni AWS, sei considerato un preside. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra operazione in un servizio diverso. FASutilizza le autorizzazioni del principale che chiama un Servizio AWS, in combinazione con la richiesta Servizio AWS per effettuare richieste ai servizi a valle. FASle richieste vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse da completare. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli FAS delle politiche relative alle richieste, consulta Forward access sessions.
  - Ruolo di servizio: un ruolo di servizio è IAM ruolo che un servizio assume per eseguire azioni per conto dell'utente. Un record IAM l'amministratore può creare, modificare ed eliminare un ruolo di servizio dall'interno IAM. Per ulteriori informazioni, vedere Creazione di un ruolo per delegare le autorizzazioni a un Servizio AWS nella Guida per l'utente di IAM.
  - Ruolo collegato al servizio: un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un Servizio AWS. Il servizio può assumere il ruolo di eseguire un'azione per conto dell'utente. I ruoli collegati ai servizi vengono visualizzati nel IAM account e sono di proprietà del servizio. Un record IAM l'amministratore può visualizzare, ma non modificare le autorizzazioni per i ruoli collegati al servizio.
- Applicazioni in esecuzione su Amazon EC2 - È possibile utilizzare un IAM ruolo per gestire le credenziali temporanee per le applicazioni in esecuzione su un Amazon EC2 istanza e creazione

AWS CLI oppure AWS APIrichieste. Ciò è preferibile rispetto alla memorizzazione delle chiavi di accesso all'interno del Amazon EC2 istanza. Per assegnare un AWS ruolo a un Amazon EC2 per renderla disponibile per tutte le relative applicazioni, si crea un profilo di istanza collegato all'istanza. Un profilo di istanza contiene il ruolo e abilita i programmi in esecuzione su Amazon EC2 istanza per ottenere credenziali temporanee. Per ulteriori informazioni, vedere Utilizzo di un IAM ruolo per concedere le autorizzazioni alle applicazioni in esecuzione su Amazon EC2 istanze nella Guida per l'IAMutente.

Per sapere se usare IAM ruoli o IAM utenti, vedi Quando creare un IAM ruolo (anziché utente) nella Guida per l'IAMutente.

Gestione dell'accesso con policy

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

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

Per impostazione predefinita, utenti e ruoli non dispongono di autorizzazioni. Per concedere agli utenti il permesso di eseguire azioni sulle risorse di cui hanno bisogno, IAM l'amministratore può creare IAM politiche. L'amministratore può quindi aggiungere IAM le politiche ai ruoli e gli utenti possono assumerli.

IAM le politiche definiscono le autorizzazioni per un'azione indipendentemente dal metodo utilizzato per eseguire l'operazione. Ad esempio, supponiamo di disporre di una policy che consente l'operazione `iam:GetRole`. Un utente con tale criterio può ottenere informazioni sul ruolo da AWS Management Console, il AWS CLI, o AWS API.

Policy basate su identità

Le politiche basate sull'identità sono documenti relativi alle politiche di JSON autorizzazione che è possibile allegare a un'identità, ad esempio Utente IAM, ruolo o gruppo. Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su

come creare una politica basata sull'identità, vedi Creazione IAM politiche nella Guida per l'utente. IAM

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

Policy basate su risorse

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

Le policy basate sulle risorse sono policy inline che si trovano in tale servizio. Non puoi usare AWS politiche gestite da IAM in una politica basata sulle risorse.

Elenchi di controllo degli accessi () ACLs

Le liste di controllo degli accessi (ACLs) controllano quali principali (membri dell'account, utenti o ruoli) dispongono delle autorizzazioni per accedere a una risorsa. ACLssono simili alle politiche basate sulle risorse, sebbene non utilizzino il formato del documento di policy. JSON

Amazon S3, AWS WAF e Amazon VPC sono esempi di servizi che supportano. ACLs Per ulteriori informazioniACLs, consulta la panoramica di Access Control List (ACL) nella Guida per l'utente di Amazon Simple Storage Service.

Altri tipi di policy

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

- Limiti delle autorizzazioni: un limite di autorizzazioni è una funzionalità avanzata in cui si impostano le autorizzazioni massime che una politica basata sull'identità può concedere a un IAM entità

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

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

Più tipi di policy

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

ROSA esempi di politiche basate sull'identità

Per impostazione predefinita, Utenti IAM e i ruoli non sono autorizzati a creare o modificare AWS risorse. Inoltre, non possono eseguire attività utilizzando AWS Management Console, AWS CLI, oppure AWS API. Un record IAM l'amministratore deve creare IAM politiche che concedono a utenti e ruoli il permesso di eseguire API operazioni specifiche sulle risorse specificate di cui hanno bisogno. L'amministratore deve quindi allegare tali politiche al Utenti IAM o gruppi che richiedono tali autorizzazioni.

Per imparare a creare un IAM politica basata sull'identità che utilizza questi documenti di esempioJSON, consulta Creazione di politiche nella JSON scheda della Guida per l'utente. IAM

Utilizzo di ROSA console

Per abbonarsi a ROSA dalla console, il IAM principale deve disporre dei dati richiesti Marketplace AWS autorizzazioni. Le autorizzazioni consentono al principale di sottoscrivere e annullare l'iscrizione a ROSA elenco di prodotti in Marketplace AWS e visualizza Marketplace AWS abbonamenti. Per aggiungere le autorizzazioni richieste, vai a ROSA console e collega il AWS politica gestita `ROSAManageSubscription` al tuo IAM preside. Per ulteriori informazioni su `ROSAManageSubscription`, consulta the section called “AWS politica gestita: ROSAManageSubscription”.

Autorizzazione ROSA con HCP to manage AWS risorse

ROSAcon piani di controllo ospitati (HCP) usi AWS politiche gestite con le autorizzazioni necessarie per il funzionamento e il supporto del servizio. Si utilizza il ROSA CLIo IAM console per collegare queste politiche ai ruoli di servizio nel tuo Account AWS.

Per ulteriori informazioni, consulta the section called “ AWS policy gestite”.

Autorizzazione ROSA classica alla gestione AWS risorse

ROSAclassic utilizza IAM politiche gestite dai clienti con autorizzazioni predefinite dal servizio. Si utilizza il ROSA CLIper creare queste politiche e associarle ai ruoli di servizio nel Account AWS. ROSA richiede che queste politiche siano configurate come definito dal servizio per garantire il funzionamento e il supporto continui del servizio.

> **Note**
>
> Non dovreste modificare le policy ROSA classiche senza prima consultare Red Hat. Ciò potrebbe invalidare l'accordo sul livello di servizio di uptime del cluster del 99,95% di Red Hat. ROSAcon piani di controllo ospitati (usi) AWS politiche gestite con un set più limitato di autorizzazioni. Per ulteriori informazioni, consulta the section called “ AWS policy gestite”.

Esistono due tipi di politiche gestite dai clienti per ROSA: politiche relative agli account e politiche degli operatori. Le politiche dell'account sono allegate a IAM ruoli utilizzati dal servizio per stabilire un rapporto di fiducia con Red Hat per il supporto dei tecnici dell'affidabilità del sito (SRE), la creazione di cluster e le funzionalità di calcolo. Le politiche degli operatori sono allegate a IAM ruoli utilizzati

OpenShift dagli operatori per le operazioni del cluster relative all'ingresso, allo storage, al registro delle immagini e alla gestione dei nodi. Le politiche dell'account vengono create una volta per Account AWS, mentre le policy degli operatori vengono create una volta per cluster.

Per ulteriori informazioni, consulta the section called “ROSApolitiche di account classiche” e the section called “ROSApolitiche classiche degli operatori”.

Consentire agli utenti di visualizzare le loro autorizzazioni

Questo esempio mostra come è possibile creare una politica che consenta Utenti IAM per visualizzare le politiche in linea e gestite allegate alla loro identità utente. Questa politica include le autorizzazioni per completare questa azione sulla console o utilizzando a livello di codice il AWS CLI.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
```

```
    ]
}
```

ROSApolitiche di account classiche

Questa sezione fornisce dettagli sulle politiche dell'account richieste per la ROSA versione classica. Queste autorizzazioni sono necessarie affinché la ROSA versione classica gestisca il AWS risorse su cui vengono eseguiti i cluster e abilitano il supporto tecnico di Red Hat Site Reliability per i cluster. È possibile assegnare un prefisso personalizzato ai nomi delle policy, ma altrimenti tali policy dovrebbero essere denominate come definito in questa pagina (ad esempio,). `ManagedOpenShift-Installer-Role-Policy`

Le politiche dell'account sono specifiche di una versione OpenShift secondaria e sono compatibili con le versioni precedenti. Prima di creare o aggiornare un cluster, è necessario verificare che la versione della policy e la versione del cluster coincidano eseguendo. `rosa list account-roles` Se la versione della policy è precedente alla versione del cluster, esegui `rosa upgrade account-roles` per aggiornare i ruoli e le policy associate. È possibile utilizzare le stesse politiche e gli stessi ruoli dell'account per più cluster della stessa versione secondaria.

[Prefisso] -Installer-Role-Policy

Puoi collegarti alle tue entità. `[Prefix]-Installer-Role-Policy` IAM Prima di poter creare un cluster ROSA classico, è necessario associare questa politica a un IAM ruolo denominato`[Prefix]-Installer-Role`. Questa politica concede le autorizzazioni necessarie che consentono ROSA programma di installazione per gestire il AWS risorse necessarie per la creazione di cluster.

Policy delle autorizzazioni

Le autorizzazioni definite in questo documento di policy specificano quali azioni sono consentite o negate.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "autoscaling:DescribeAutoScalingGroups",
                "ec2:AllocateAddress",
                "ec2:AssociateAddress",
                "ec2:AssociateDhcpOptions",
```

```
                "ec2:AssociateRouteTable",
                "ec2:AttachInternetGateway",
                "ec2:AttachNetworkInterface",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CopyImage",
                "ec2:CreateDhcpOptions",
                "ec2:CreateInternetGateway",
                "ec2:CreateNatGateway",
                "ec2:CreateNetworkInterface",
                "ec2:CreateRoute",
                "ec2:CreateRouteTable",
                "ec2:CreateSecurityGroup",
                "ec2:CreateSubnet",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:CreateVpc",
                "ec2:CreateVpcEndpoint",
                "ec2:DeleteDhcpOptions",
                "ec2:DeleteInternetGateway",
                "ec2:DeleteNatGateway",
                "ec2:DeleteNetworkInterface",
                "ec2:DeleteRoute",
                "ec2:DeleteRouteTable",
                "ec2:DeleteSecurityGroup",
                "ec2:DeleteSnapshot",
                "ec2:DeleteSubnet",
                "ec2:DeleteTags",
                "ec2:DeleteVolume",
                "ec2:DeleteVpc",
                "ec2:DeleteVpcEndpoints",
                "ec2:DeregisterImage",
                "ec2:DescribeAccountAttributes",
                "ec2:DescribeAddresses",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeDhcpOptions",
                "ec2:DescribeImages",
                "ec2:DescribeInstanceAttribute",
                "ec2:DescribeInstanceCreditSpecifications",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:DescribeInstanceTypeOfferings",
                "ec2:DescribeInstanceTypes",
                "ec2:DescribeInternetGateways",
```

```
                "ec2:DescribeKeyPairs",
                "ec2:DescribeNatGateways",
                "ec2:DescribeNetworkAcls",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribePrefixLists",
                "ec2:DescribeRegions",
                "ec2:DescribeReservedInstancesOfferings",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSecurityGroupRules",
                "ec2:DescribeSubnets",
                "ec2:DescribeTags",
                "ec2:DescribeVolumes",
                "ec2:DescribeVpcAttribute",
                "ec2:DescribeVpcClassicLink",
                "ec2:DescribeVpcClassicLinkDnsSupport",
                "ec2:DescribeVpcEndpoints",
                "ec2:DescribeVpcs",
                "ec2:DetachInternetGateway",
                "ec2:DisassociateRouteTable",
                "ec2:GetConsoleOutput",
                "ec2:GetEbsDefaultKmsKeyId",
                "ec2:ModifyInstanceAttribute",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:ModifySubnetAttribute",
                "ec2:ModifyVpcAttribute",
                "ec2:ReleaseAddress",
                "ec2:ReplaceRouteTableAssociation",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:RunInstances",
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances",
                "elasticloadbalancing:AddTags",
                "elasticloadbalancing:ApplySecurityGroupsToLoadBalancer",
                "elasticloadbalancing:AttachLoadBalancerToSubnets",
                "elasticloadbalancing:ConfigureHealthCheck",
                "elasticloadbalancing:CreateListener",
                "elasticloadbalancing:CreateLoadBalancer",
                "elasticloadbalancing:CreateLoadBalancerListeners",
                "elasticloadbalancing:CreateTargetGroup",
                "elasticloadbalancing:DeleteLoadBalancer",
                "elasticloadbalancing:DeleteTargetGroup",
```

```
                "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
                "elasticloadbalancing:DeregisterTargets",
                "elasticloadbalancing:DescribeAccountLimits",
                "elasticloadbalancing:DescribeInstanceHealth",
                "elasticloadbalancing:DescribeListeners",
                "elasticloadbalancing:DescribeLoadBalancerAttributes",
                "elasticloadbalancing:DescribeLoadBalancers",
                "elasticloadbalancing:DescribeTags",
                "elasticloadbalancing:DescribeTargetGroupAttributes",
                "elasticloadbalancing:DescribeTargetGroups",
                "elasticloadbalancing:DescribeTargetHealth",
                "elasticloadbalancing:ModifyLoadBalancerAttributes",
                "elasticloadbalancing:ModifyTargetGroup",
                "elasticloadbalancing:ModifyTargetGroupAttributes",
                "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
                "elasticloadbalancing:RegisterTargets",
                "elasticloadbalancing:SetLoadBalancerPoliciesOfListener",
                "iam:AddRoleToInstanceProfile",
                "iam:CreateInstanceProfile",
                "iam:DeleteInstanceProfile",
                "iam:GetInstanceProfile",
                "iam:TagInstanceProfile",
                "iam:GetRole",
                "iam:GetRolePolicy",
                "iam:GetUser",
                "iam:ListAttachedRolePolicies",
                "iam:ListInstanceProfiles",
                "iam:ListInstanceProfilesForRole",
                "iam:ListRolePolicies",
                "iam:ListRoles",
                "iam:ListUserPolicies",
                "iam:ListUsers",
                "iam:PassRole",
                "iam:RemoveRoleFromInstanceProfile",
                "iam:SimulatePrincipalPolicy",
                "iam:TagRole",
                "iam:UntagRole",
                "route53:ChangeResourceRecordSets",
                "route53:ChangeTagsForResource",
                "route53:CreateHostedZone",
                "route53:DeleteHostedZone",
                "route53:GetAccountLimit",
                "route53:GetChange",
                "route53:GetHostedZone",
```

```
                "route53:ListHostedZones",
                "route53:ListHostedZonesByName",
                "route53:ListResourceRecordSets",
                "route53:ListTagsForResource",
                "route53:UpdateHostedZoneComment",
                "s3:CreateBucket",
                "s3:DeleteBucket",
                "s3:DeleteObject",
                "s3:DeleteObjectVersion",
                "s3:GetAccelerateConfiguration",
                "s3:GetBucketAcl",
                "s3:GetBucketCORS",
                "s3:GetBucketLocation",
                "s3:GetBucketLogging",
                "s3:GetBucketObjectLockConfiguration",
                "s3:GetBucketPolicy",
                "s3:GetBucketReplication",
                "s3:GetBucketRequestPayment",
                "s3:GetBucketTagging",
                "s3:GetBucketVersioning",
                "s3:GetBucketWebsite",
                "s3:GetEncryptionConfiguration",
                "s3:GetLifecycleConfiguration",
                "s3:GetObject",
                "s3:GetObjectAcl",
                "s3:GetObjectTagging",
                "s3:GetObjectVersion",
                "s3:GetReplicationConfiguration",
                "s3:ListBucket",
                "s3:ListBucketVersions",
                "s3:PutBucketAcl",
                "s3:PutBucketTagging",
                "s3:PutBucketVersioning",
                "s3:PutEncryptionConfiguration",
                "s3:PutObject",
                "s3:PutObjectAcl",
                "s3:PutObjectTagging",
                "servicequotas:GetServiceQuota",
                "servicequotas:ListAWSDefaultServiceQuotas",
                "sts:AssumeRole",
                "sts:AssumeRoleWithWebIdentity",
                "sts:GetCallerIdentity",
                "tag:GetResources",
                "tag:UntagResources",
```

```
                "ec2:CreateVpcEndpointServiceConfiguration",
                "ec2:DeleteVpcEndpointServiceConfigurations",
                "ec2:DescribeVpcEndpointServiceConfigurations",
                "ec2:DescribeVpcEndpointServicePermissions",
                "ec2:DescribeVpcEndpointServices",
                "ec2:ModifyVpcEndpointServicePermissions",
                "kms:DescribeKey",
                "cloudwatch:GetMetricData"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "secretsmanager:GetSecretValue"
            ],
            "Effect": "Allow",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/red-hat-managed": "true"
                }
            }
        }
    ]
}
```

[Prefisso] - -Role-Policy ControlPlane

Puoi allegare `[Prefix]-ControlPlane-Role-Policy` alle tue entità. IAM Prima di poter creare un cluster ROSA classico, è necessario associare questa politica a un IAM ruolo denominato`[Prefix]-ControlPlane-Role`. Questa politica concede le autorizzazioni necessarie a ROSA Classic to Manage Amazon EC2 e Elastic Load Balancing risorse che ospitano il ROSA piano di controllo, oltre a leggere KMS keys.

Policy delle autorizzazioni

Le autorizzazioni definite in questo documento di policy specificano quali azioni sono consentite o negate.

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

```
        {
            "Action": [
                "ec2:AttachVolume",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateSecurityGroup",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DeleteSecurityGroup",
                "ec2:DeleteVolume",
                "ec2:Describe*",
                "ec2:DetachVolume",
                "ec2:ModifyInstanceAttribute",
                "ec2:ModifyVolume",
                "ec2:RevokeSecurityGroupIngress",
                "elasticloadbalancing:AddTags",
                "elasticloadbalancing:AttachLoadBalancerToSubnets",
                "elasticloadbalancing:ApplySecurityGroupsToLoadBalancer",
                "elasticloadbalancing:CreateListener",
                "elasticloadbalancing:CreateLoadBalancer",
                "elasticloadbalancing:CreateLoadBalancerPolicy",
                "elasticloadbalancing:CreateLoadBalancerListeners",
                "elasticloadbalancing:CreateTargetGroup",
                "elasticloadbalancing:ConfigureHealthCheck",
                "elasticloadbalancing:DeleteListener",
                "elasticloadbalancing:DeleteLoadBalancer",
                "elasticloadbalancing:DeleteLoadBalancerListeners",
                "elasticloadbalancing:DeleteTargetGroup",
                "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
                "elasticloadbalancing:DeregisterTargets",
                "elasticloadbalancing:Describe*",
                "elasticloadbalancing:DetachLoadBalancerFromSubnets",
                "elasticloadbalancing:ModifyListener",
                "elasticloadbalancing:ModifyLoadBalancerAttributes",
                "elasticloadbalancing:ModifyTargetGroup",
                "elasticloadbalancing:ModifyTargetGroupAttributes",
                "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
                "elasticloadbalancing:RegisterTargets",
                "elasticloadbalancing:SetLoadBalancerPoliciesForBackendServer",
                "elasticloadbalancing:SetLoadBalancerPoliciesOfListener",
                "kms:DescribeKey"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
```

```
    ]
}
```

[Prefisso] -Worker-Role-Policy

Puoi allegare alle tue entità. `[Prefix]-Worker-Role-Policy` IAM Prima di poter creare un cluster ROSA classico, è necessario associare questa politica a un IAM ruolo denominato`[Prefix]-Worker-Role`. Questa politica concede le autorizzazioni necessarie a ROSA classic per descrivere le EC2 istanze in esecuzione come nodi di lavoro.

Policy delle autorizzazioni

Le autorizzazioni definite in questo documento di policy specificano quali azioni sono consentite o negate.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeRegions"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

[Prefisso] -Support-Role-Policy

Puoi allegare alle tue entità. `[Prefix]-Support-Role-Policy` IAM Prima di poter creare un cluster ROSA classico, è necessario associare questa politica a un IAM ruolo denominato`[Prefix]-Support-Role`. Questa policy concede le autorizzazioni necessarie all'ingegneria dell'affidabilità del sito Red Hat per osservare, diagnosticare e supportare AWS risorse utilizzate dai cluster ROSA classici, inclusa la possibilità di modificare lo stato dei nodi del cluster.

Policy delle autorizzazioni

Le autorizzazioni definite in questo documento di policy specificano quali azioni sono consentite o negate.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "cloudtrail:DescribeTrails",
                "cloudtrail:LookupEvents",
                "cloudwatch:GetMetricData",
                "cloudwatch:GetMetricStatistics",
                "cloudwatch:ListMetrics",
                "ec2-instance-connect:SendSerialConsoleSSHPublicKey",
                "ec2:CopySnapshot",
                "ec2:CreateNetworkInsightsPath",
                "ec2:CreateSnapshot",
                "ec2:CreateSnapshots",
                "ec2:CreateTags",
                "ec2:DeleteNetworkInsightsAnalysis",
                "ec2:DeleteNetworkInsightsPath",
                "ec2:DeleteTags",
                "ec2:DescribeAccountAttributes",
                "ec2:DescribeAddresses",
                "ec2:DescribeAddressesAttribute",
                "ec2:DescribeAggregateIdFormat",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeByoipCidrs",
                "ec2:DescribeCapacityReservations",
                "ec2:DescribeCarrierGateways",
                "ec2:DescribeClassicLinkInstances",
                "ec2:DescribeClientVpnAuthorizationRules",
                "ec2:DescribeClientVpnConnections",
                "ec2:DescribeClientVpnEndpoints",
                "ec2:DescribeClientVpnRoutes",
                "ec2:DescribeClientVpnTargetNetworks",
                "ec2:DescribeCoipPools",
                "ec2:DescribeCustomerGateways",
                "ec2:DescribeDhcpOptions",
                "ec2:DescribeEgressOnlyInternetGateways",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DescribeIdentityIdFormat",
                "ec2:DescribeIdFormat",
                "ec2:DescribeImageAttribute",
                "ec2:DescribeImages",
                "ec2:DescribeInstanceAttribute",
```

```
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:DescribeInstanceTypeOfferings",
                "ec2:DescribeInstanceTypes",
                "ec2:DescribeInternetGateways",
                "ec2:DescribeIpv6Pools",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeLaunchTemplates",
                "ec2:DescribeLocalGatewayRouteTables",
                "ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations",
                "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
                "ec2:DescribeLocalGateways",
                "ec2:DescribeLocalGatewayVirtualInterfaceGroups",
                "ec2:DescribeLocalGatewayVirtualInterfaces",
                "ec2:DescribeManagedPrefixLists",
                "ec2:DescribeNatGateways",
                "ec2:DescribeNetworkAcls",
                "ec2:DescribeNetworkInsightsAnalyses",
                "ec2:DescribeNetworkInsightsPaths",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribePlacementGroups",
                "ec2:DescribePrefixLists",
                "ec2:DescribePrincipalIdFormat",
                "ec2:DescribePublicIpv4Pools",
                "ec2:DescribeRegions",
                "ec2:DescribeReservedInstances",
                "ec2:DescribeRouteTables",
                "ec2:DescribeScheduledInstances",
                "ec2:DescribeSecurityGroupReferences",
                "ec2:DescribeSecurityGroupRules",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSnapshotAttribute",
                "ec2:DescribeSnapshots",
                "ec2:DescribeSpotFleetInstances",
                "ec2:DescribeStaleSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeTags",
                "ec2:DescribeTransitGatewayAttachments",
                "ec2:DescribeTransitGatewayConnectPeers",
                "ec2:DescribeTransitGatewayConnects",
                "ec2:DescribeTransitGatewayMulticastDomains",
                "ec2:DescribeTransitGatewayPeeringAttachments",
                "ec2:DescribeTransitGatewayRouteTables",
                "ec2:DescribeTransitGateways",
```

```
                "ec2:DescribeTransitGatewayVpcAttachments",
                "ec2:DescribeVolumeAttribute",
                "ec2:DescribeVolumes",
                "ec2:DescribeVolumesModifications",
                "ec2:DescribeVolumeStatus",
                "ec2:DescribeVpcAttribute",
                "ec2:DescribeVpcClassicLink",
                "ec2:DescribeVpcClassicLinkDnsSupport",
                "ec2:DescribeVpcEndpointConnectionNotifications",
                "ec2:DescribeVpcEndpointConnections",
                "ec2:DescribeVpcEndpoints",
                "ec2:DescribeVpcEndpointServiceConfigurations",
                "ec2:DescribeVpcEndpointServicePermissions",
                "ec2:DescribeVpcEndpointServices",
                "ec2:DescribeVpcPeeringConnections",
                "ec2:DescribeVpcs",
                "ec2:DescribeVpnConnections",
                "ec2:DescribeVpnGateways",
                "ec2:GetAssociatedIpv6PoolCidrs",
                "ec2:GetConsoleOutput",
                "ec2:GetManagedPrefixListEntries",
                "ec2:GetSerialConsoleAccessStatus",
                "ec2:GetTransitGatewayAttachmentPropagations",
                "ec2:GetTransitGatewayMulticastDomainAssociations",
                "ec2:GetTransitGatewayPrefixListReferences",
                "ec2:GetTransitGatewayRouteTableAssociations",
                "ec2:GetTransitGatewayRouteTablePropagations",
                "ec2:ModifyInstanceAttribute",
                "ec2:RebootInstances",
                "ec2:RunInstances",
                "ec2:SearchLocalGatewayRoutes",
                "ec2:SearchTransitGatewayMulticastGroups",
                "ec2:SearchTransitGatewayRoutes",
                "ec2:StartInstances",
                "ec2:StartNetworkInsightsAnalysis",
                "ec2:StopInstances",
                "ec2:TerminateInstances",
                "elasticloadbalancing:ConfigureHealthCheck",
                "elasticloadbalancing:DescribeAccountLimits",
                "elasticloadbalancing:DescribeInstanceHealth",
                "elasticloadbalancing:DescribeListenerCertificates",
                "elasticloadbalancing:DescribeListeners",
                "elasticloadbalancing:DescribeLoadBalancerAttributes",
                "elasticloadbalancing:DescribeLoadBalancerPolicies",
```

```
                "elasticloadbalancing:DescribeLoadBalancerPolicyTypes",
                "elasticloadbalancing:DescribeLoadBalancers",
                "elasticloadbalancing:DescribeRules",
                "elasticloadbalancing:DescribeSSLPolicies",
                "elasticloadbalancing:DescribeTags",
                "elasticloadbalancing:DescribeTargetGroupAttributes",
                "elasticloadbalancing:DescribeTargetGroups",
                "elasticloadbalancing:DescribeTargetHealth",
                "iam:GetRole",
                "iam:ListRoles",
                "kms:CreateGrant",
                "route53:GetHostedZone",
                "route53:GetHostedZoneCount",
                "route53:ListHostedZones",
                "route53:ListHostedZonesByName",
                "route53:ListResourceRecordSets",
                "s3:GetBucketTagging",
                "s3:GetObjectAcl",
                "s3:GetObjectTagging",
                "s3:ListAllMyBuckets",
                "sts:DecodeAuthorizationMessage",
                "tiros:CreateQuery",
                "tiros:GetQueryAnswer",
                "tiros:GetQueryExplanation"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "s3:ListBucket"
            ],
            "Effect": "Allow",
            "Resource": [
                "arn:aws:s3:::managed-velero*",
                "arn:aws:s3:::*image-registry*"
            ]
        }
    ]
}
```

ROSApolitiche classiche degli operatori

Questa sezione fornisce dettagli sulle politiche degli operatori necessarie per la ROSA versione classica. Prima di poter creare un cluster ROSA classico, è necessario collegare queste politiche ai ruoli di operatore pertinenti. È richiesto un set unico di ruoli di operatore per ogni cluster.

Queste autorizzazioni sono necessarie per consentire agli OpenShift operatori di gestire i ROSA classici nodi del cluster. È possibile assegnare un prefisso personalizzato ai nomi delle politiche per semplificare la gestione delle politiche (ad esempio,). `ManagedOpenShift-openshift-ingress-operator-cloud-credentials`

[Prefisso] - -credenziali openshift-ingress-operator-cloud

Puoi collegarti alle tue entità`[Prefix]-openshift-ingress-operator-cloud-credentials`. IAM Questa politica concede le autorizzazioni necessarie all'Ingress Operator per fornire e gestire i sistemi di bilanciamento del carico e le DNS configurazioni per l'accesso al cluster esterno. La policy consente inoltre all'Ingress Operator di leggere e filtrare Route 53 valori dei tag di risorsa per scoprire le zone ospitate. Per ulteriori informazioni sull'operatore, consulta OpenShift Ingress Operator nella OpenShift GitHub documentazione.

Policy delle autorizzazioni

Le autorizzazioni definite in questo documento di policy specificano quali azioni sono consentite o negate.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "elasticloadbalancing:DescribeLoadBalancers",
                "route53:ListHostedZones",
                "route53:ListTagsForResources",
                "route53:ChangeResourceRecordSets",
                "tag:GetResources"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

[Prefisso] - - openshift-cluster-csi-drivers ebs-cloud-credentials

Puoi collegarti `[Prefix]-openshift-cluster-csi-drivers-ebs-cloud-credentials` alle tue IAM entità. Questa politica concede le autorizzazioni necessarie a Amazon EBS CSIDriver Operator per l'installazione e la manutenzione di Amazon EBS CSIdriver su un cluster ROSA classico. Per ulteriori informazioni sull'operatore, vedere aws-ebs-csi-driver-operator nella OpenShift GitHub documentazione.

Policy delle autorizzazioni

Le autorizzazioni definite in questo documento di policy specificano quali azioni sono consentite o negate.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:AttachVolume",
                "ec2:CreateSnapshot",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DeleteSnapshot",
                "ec2:DeleteTags",
                "ec2:DeleteVolume",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeInstances",
                "ec2:DescribeSnapshots",
                "ec2:DescribeTags",
                "ec2:DescribeVolumes",
                "ec2:DescribeVolumesModifications",
                "ec2:DetachVolume",
                "ec2:EnableFastSnapshotRestores",
                "ec2:ModifyVolume"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

[Prefisso] - -cloud-credentials openshift-machine-api-aws

Puoi collegarti alle tue entità. `[Prefix]-openshift-machine-api-aws-cloud-credentials` IAM Questa politica concede le autorizzazioni necessarie all'operatore Machine Config per descrivere, eseguire e terminare Amazon EC2 istanze gestite come nodi di lavoro. Questa politica concede inoltre le autorizzazioni per consentire la crittografia del disco del volume radice del nodo di lavoro utilizzando AWS KMS keys. Per ulteriori informazioni sull'operatore, machine-config-operatorconsulta la OpenShift GitHub documentazione.

Policy delle autorizzazioni

Le autorizzazioni definite in questo documento di policy specificano quali azioni sono consentite o negate.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:CreateTags",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeDhcpOptions",
                "ec2:DescribeImages",
                "ec2:DescribeInstances",
                "ec2:DescribeInternetGateways",
                "ec2:DescribeInstanceTypes",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeRegions",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:RunInstances",
                "ec2:TerminateInstances",
                "elasticloadbalancing:DescribeLoadBalancers",
                "elasticloadbalancing:DescribeTargetGroups",
                "elasticloadbalancing:DescribeTargetHealth",
                "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
                "elasticloadbalancing:RegisterTargets",
                "elasticloadbalancing:DeregisterTargets",
                "iam:PassRole",
                "iam:CreateServiceLinkedRole"
            ],
            "Effect": "Allow",
            "Resource": "*"
```

```
        },
        {
            "Action": [
                "kms:Decrypt",
                "kms:Encrypt",
                "kms:GenerateDataKey",
                "kms:GenerateDataKeyWithoutPlainText",
                "kms:DescribeKey"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "kms:RevokeGrant",
                "kms:CreateGrant",
                "kms:ListGrants"
            ],
            "Effect": "Allow",
            "Resource": "*",
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": true
                }
            }
        }
    ]
}
```

[Prefisso] - -cloud-credentials openshift-cloud-credential-operator

Puoi collegarti alle tue entità. `[Prefix]-openshift-cloud-credential-operator-cloud-credentials` IAM Questa policy concede le autorizzazioni necessarie al Cloud Credential Operator per il recupero Utente IAM dettagli, tra cui chiave di accessoIDs, documenti di policy in linea allegati, data di creazione dell'utente, percorso, ID utente e Amazon Resource Name (ARN). Per ulteriori informazioni sull'operatore, consulta cloud-credential-operatorla OpenShift GitHub documentazione.

Policy delle autorizzazioni

Le autorizzazioni definite in questo documento di policy specificano quali azioni sono consentite o negate.

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "iam:GetUser",
                "iam:GetUserPolicy",
                "iam:ListAccessKeys"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

[Prefisso] - -cloud-credentials openshift-image-registry-installer

Puoi collegarti alle tue entità. `[Prefix]-openshift-image-registry-installer-cloud-credentials` IAM Questa politica concede le autorizzazioni necessarie all'Image Registry Operator per fornire e gestire le risorse per il registro di immagini interno al cluster della ROSA versione classica e per i servizi dipendenti, tra cui Amazon S3. Ciò è necessario per consentire all'operatore di installare e gestire il registro interno di un cluster ROSA classico. Per ulteriori informazioni sull'operatore, vedere Image Registry Operator nella OpenShift GitHub documentazione.

Policy delle autorizzazioni

Le autorizzazioni definite in questo documento di policy specificano quali azioni sono consentite o negate.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:CreateBucket",
                "s3:DeleteBucket",
                "s3:PutBucketTagging",
                "s3:GetBucketTagging",
                "s3:PutBucketPublicAccessBlock",
                "s3:GetBucketPublicAccessBlock",
                "s3:PutEncryptionConfiguration",
                "s3:GetEncryptionConfiguration",
                "s3:PutLifecycleConfiguration",
```

```
                "s3:GetLifecycleConfiguration",
                "s3:GetBucketLocation",
                "s3:ListBucket",
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject",
                "s3:ListBucketMultipartUploads",
                "s3:AbortMultipartUpload",
                "s3:ListMultipartUploadParts"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

[Prefisso] - - openshift-cloud-network-config controller-cloud-cr

Puoi collegarti `[Prefix]-openshift-cloud-network-config-controller-cloud-cr` alle tue IAM entità. Questa politica concede le autorizzazioni necessarie all'operatore del controller di Cloud Network Config per fornire e gestire le risorse di rete da utilizzare con il ROSA classico overlay di rete del cluster. L'operatore utilizza queste autorizzazioni per gestire gli indirizzi IP privati per Amazon EC2 istanze come parte del cluster ROSA classico. Per ulteriori informazioni sull'operatore, vedere C loud-network-config-controller nella OpenShift GitHub documentazione.

Policy delle autorizzazioni

Le autorizzazioni definite in questo documento di policy specificano quali azioni sono consentite o negate.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:DescribeInstanceTypes",
                "ec2:UnassignPrivateIpAddresses",
                "ec2:AssignPrivateIpAddresses",
                "ec2:UnassignIpv6Addresses",
                "ec2:AssignIpv6Addresses",
                "ec2:DescribeSubnets",
```

```
                "ec2:DescribeNetworkInterfaces"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

AWS politiche gestite per ROSA

Un record AWS la politica gestita è una politica autonoma creata e amministrata da AWS. AWS le politiche gestite sono progettate per fornire autorizzazioni per molti casi d'uso comuni, in modo da poter iniziare ad assegnare autorizzazioni a utenti, gruppi e ruoli.

Tieni presente che AWS le politiche gestite potrebbero non concedere le autorizzazioni con il privilegio minimo per i casi d'uso specifici perché sono disponibili per tutti AWS clienti da utilizzare. Ti consigliamo pertanto di ridurre ulteriormente le autorizzazioni definendo policy gestite dal cliente specifiche per i tuoi casi d'uso.

Non è possibile modificare le autorizzazioni definite in AWS politiche gestite. Se AWS aggiorna le autorizzazioni definite in un AWS politica gestita, l'aggiornamento riguarda tutte le identità principali (utenti, gruppi e ruoli) a cui è associata la politica. AWS è più probabile che aggiorni un AWS politica gestita quando è nuova Servizio AWS viene avviata o nuove API operazioni diventano disponibili per i servizi esistenti. Per ulteriori informazioni, consulta AWS politiche gestite in IAM Guida per l'utente.

AWS politica gestita: ROSAManageSubscription

Puoi allegare la `ROSAManageSubscription` politica al tuo IAM entità. Prima di abilitare ROSA nel AWS ROSA console, è necessario innanzitutto collegare questo criterio a un ruolo di console.

Questa politica garantisce il Marketplace AWS autorizzazioni necessarie per gestire il ROSA abbonamento.

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `aws-marketplace:Subscribe`- Concede il permesso di sottoscrivere il Marketplace AWS prodotto per ROSA.
- `aws-marketplace:Unsubscribe`- Consente ai responsabili di rimuovere gli abbonamenti a Marketplace AWS prodotti.

- `aws-marketplace:ViewSubscriptions`- Consente ai mandanti di visualizzare gli abbonamenti da Marketplace AWS. Ciò è necessario affinché IAM il principale può visualizzare il disponibile Marketplace AWS abbonamenti.

Per visualizzare il documento JSON politico completo, consulta ROSAManageSubscriptionla AWS Guida di riferimento sulle policy gestite.

ROSAcon politiche relative HCP all'account

Questa sezione fornisce dettagli sulle politiche dell'account necessarie per i piani ROSA di controllo ospitati (HCP). Questi AWS le politiche gestite aggiungono le autorizzazioni utilizzate ROSA dai HCP IAM ruoli. Le autorizzazioni sono necessarie per il supporto tecnico di Red Hat Site Reliability Engineering (SRE), l'installazione del cluster e il piano di controllo e le funzionalità di calcolo.

> **Note**
>
> AWS le policy gestite sono destinate all'uso ROSA con piani di controllo ospitati ()HCP. ROSAi cluster classici utilizzano IAM politiche gestite dal cliente. Per ulteriori informazioni sulle politiche ROSA classiche, consulta the section called “ROSApolitiche di account classiche” ethe section called “ROSApolitiche classiche degli operatori”.

AWS politica gestita: ROSAWorkerInstancePolicy

Puoi allegare `ROSAWorkerInstancePolicy` al tuo IAM entità. Prima di creare un cluster ROSA con piani di controllo ospitati, è necessario innanzitutto collegare questa politica a un IAM ruolo di lavoratore.

Dettagli dell'autorizzazione

Questa politica include le seguenti autorizzazioni che consentono di ROSA servizio per completare le seguenti attività:

- `ec2`— Revisione Regione AWS e Amazon EC2 dettagli dell'istanza come parte della gestione del ciclo di vita dei nodi di lavoro in un ROSA cluster.

Per visualizzare il documento JSON programmatico completo, vedere ROSAWorkerInstancePolicynel AWS Guida di riferimento sulle policy gestite.

AWS politica gestita: ROSASRESupportPolicy

Puoi collegarti `ROSASRESupportPolicy` alle tue IAM entità.

Prima di creare un cluster ROSA con piani di controllo ospitati, è necessario collegare questa politica a un IAM ruolo di supporto. Questa policy concede le autorizzazioni necessarie ai tecnici di Red Hat Site Reliability (SREs) per osservare, diagnosticare e supportare direttamente AWS risorse associate a ROSA cluster, inclusa la possibilità di modificare ROSA stato del nodo del cluster.

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni che consentono SREs a Red Hat di completare le seguenti attività:

- `cloudtrail`— Leggi AWS CloudTrail eventi e percorsi pertinenti al cluster.
- `cloudwatch`— Leggi Amazon CloudWatch metriche pertinenti al cluster.
- `ec2`— Leggi, descrivi e rivedi Amazon EC2 componenti relativi allo stato del cluster, come i gruppi di sicurezza, le connessioni VPC degli endpoint e lo stato del volume. Avvia, arresta, riavvia e termina Amazon EC2 istanze.
- `elasticloadbalancing`— Leggi, descrivi e rivedi Elastic Load Balancing parametri relativi allo stato di salute del cluster.
- `iam`— Valuta IAM ruoli relativi allo stato del cluster.
- `route53`— Rivedi DNS le impostazioni relative allo stato del cluster.
- `sts`— `DecodeAuthorizationMessage` — Leggi IAM messaggi per scopi di debug.

Per visualizzare il documento JSON politico completo, vedere nel ROSASRESupportPolicy AWS Guida di riferimento sulle policy gestite.

AWS politica gestita: ROSAInstallerPolicy

Puoi allegare `ROSAInstallerPolicy` al tuo IAM entità.

Prima di creare un cluster ROSA con piani di controllo ospitati, è necessario innanzitutto collegare questa politica a un IAM ruolo denominato`[Prefix]-ROSA-Worker-Role`. Questa politica consente alle entità di aggiungere qualsiasi ruolo che segua lo `[Prefix]-ROSA-Worker-Role` schema a un profilo di istanza. Questa politica concede all'installatore le autorizzazioni necessarie per la gestione AWS risorse che supportano ROSA installazione di cluster.

Dettagli dell'autorizzazione

Questa politica include le seguenti autorizzazioni che consentono all'installatore di completare le seguenti attività:

- `ec2`— Esegui Amazon EC2 istanze che utilizzano AMIs hosted in Account AWS possedute e gestite da Red Hat. Describe Amazon EC2 istanze, volumi e risorse di rete associate a Amazon EC2 nodi. Questa autorizzazione è necessaria affinché il piano di controllo di Kubernetes possa unire le istanze a un cluster e il cluster possa valutarne la presenza all'interno Amazon VPC. Etichetta le sottoreti utilizzando la corrispondenza delle chiavi dei tag. `"kubernetes.io/cluster/*"` Ciò è necessario per garantire che il load balancer utilizzato per l'ingresso del cluster venga creato solo nelle sottoreti applicabili.
- `elasticloadbalancing`— Aggiungere sistemi di bilanciamento del carico ai nodi di destinazione di un cluster. Rimuovi i sistemi di bilanciamento del carico dai nodi di destinazione su un cluster. Questa autorizzazione è necessaria affinché il piano di controllo Kubernetes possa fornire dinamicamente i bilanciatori del carico richiesti dai servizi e dai servizi applicativi Kubernetes. OpenShift
- `kms`— Leggi un AWS KMS chiave, crea e gestisci sovvenzioni per Amazon EC2 e restituisce una chiave dati simmetrica unica da utilizzare al di fuori di AWS KMS. Ciò è necessario per l'utilizzo di `etcd` dati crittografati quando la `etcd` crittografia è abilitata al momento della creazione del cluster.
- `iam`— Convalida IAM ruoli e politiche. Fornitura e gestione in modo dinamico Amazon EC2 profili di istanza pertinenti al cluster. Aggiungi tag a un profilo di IAM istanza utilizzando l'`iam:TagInstanceProfile`autorizzazione. Fornisci messaggi di errore all'installatore quando l'installazione del cluster non riesce a causa della mancanza di un provider di cluster specificato dal cliente. OIDC
- `route53`— Gestisci Route 53 risorse necessarie per creare cluster.
- `servicequotas`— Valuta le quote di servizio necessarie per creare un cluster.
- `sts`— Crea un file temporaneo AWS STS credenziali per ROSA componenti. Assumi le credenziali per la creazione del cluster.
- `secretsmanager`— Leggi un valore segreto per consentire in modo sicuro la OIDC configurazione gestita dal cliente come parte del provisioning del cluster.

Per visualizzare il documento di JSON policy completo, consulta la ROSAInstallerPolicy AWS Guida di riferimento sulle policy gestite.

ROSAcon le politiche HCP degli operatori

Questa sezione fornisce dettagli sulle politiche dell'operatore necessarie per i piani ROSA di controllo ospitati (HCP). È possibile allegare questi AWS politiche gestite ai ruoli di operatore necessari per l'utilizzo ROSA conHCP. Le autorizzazioni sono necessarie per consentire agli OpenShift operatori di gestire ROSA i nodi HCP del cluster.

> **Note**
>
> AWS le politiche gestite sono destinate all'uso ROSA con piani di controllo ospitati (HCP). ROSAi cluster classici utilizzano IAM politiche gestite dal cliente. Per ulteriori informazioni sulle politiche ROSA classiche, consulta the section called “ROSApolitiche di account classiche” ethe section called “ROSApolitiche classiche degli operatori”.

AWS politica gestita: ROSAAmazonEBSCSIDriverOperatorPolicy

Puoi allegare `ROSAAmazonEBSCSIDriverOperatorPolicy` al tuo IAM entità. È necessario collegare questa politica a un IAM ruolo di operatore per consentire a un cluster ROSA con piani di controllo ospitati di effettuare chiamate verso altri Servizi AWS. È richiesto un set unico di ruoli operatore per ogni cluster.

Questa politica concede le autorizzazioni necessarie a Amazon EBS CSIDriver Operator per l'installazione e la manutenzione di Amazon EBS CSIdriver su un ROSA grappolo. Per ulteriori informazioni sull'operatore, vedere aws-ebs-csi-driver operatore nella OpenShift GitHub documentazione.

Dettagli dell'autorizzazione

Questa politica include le seguenti autorizzazioni che consentono di Amazon EBS Driver Operator di completare le seguenti attività:

- `ec2`— Creare, modificare, allegare, scollegare ed eliminare Amazon EBS volumi che sono allegati a Amazon EC2 istanze. Creare ed eliminare Amazon EBS istantanee ed elenco dei volumi Amazon EC2 istanze, volumi e istantanee.

Per visualizzare il documento di JSON policy completo, consulta la ROSAAmazonEBSCSIDriverOperatorPolicy AWS Guida di riferimento sulle policy gestite.

AWS politica gestita: ROSAIngressOperatorPolicy

Puoi allegare `ROSAIngressOperatorPolicy` al tuo IAM entità. È necessario collegare questa politica a un IAM ruolo di operatore per consentire a un cluster ROSA con piani di controllo ospitati di effettuare chiamate verso altri Servizi AWS. È richiesto un set unico di ruoli operatore per ogni cluster.

Questa politica concede le autorizzazioni necessarie all'Ingress Operator per fornire e gestire i sistemi di bilanciamento del carico e le configurazioni per DNS ROSA i cluster. La policy consente l'accesso in lettura ai valori dei tag. L'operatore filtra quindi i valori dei tag per Route 53 risorse per scoprire le zone ospitate. Per ulteriori informazioni sull'operatore, consulta OpenShift Ingress Operator nella OpenShift GitHub documentazione.

Dettagli dell'autorizzazione

Questa politica include le seguenti autorizzazioni che consentono all'operatore di ingresso di completare le seguenti attività:

- `elasticloadbalancing`— Descrivere lo stato dei sistemi di bilanciamento del carico predisposti.
- `route53`: List Route 53 zone ospitate e modifica i record che gestiscono i dati DNS controllati dal cluster. ROSA
- `tag`— Gestisci le risorse contrassegnate utilizzando l'`tag:GetResources`autorizzazione.

Per visualizzare il documento JSON normativo completo, ROSAIngressOperatorPolicyconsulta la AWS Guida di riferimento sulle policy gestite.

AWS politica gestita: ROSAImageRegistryOperatorPolicy

Puoi allegare `ROSAImageRegistryOperatorPolicy` al tuo IAM entità. È necessario collegare questa politica a un IAM ruolo di operatore per consentire a un cluster ROSA con piani di controllo ospitati di effettuare chiamate verso altri Servizi AWS. È richiesto un set unico di ruoli operatore per ogni cluster.

Questa politica concede le autorizzazioni necessarie all'Image Registry Operator per fornire e gestire le risorse per ROSA registro delle immagini all'interno del cluster e servizi dipendenti, incluso S3. Ciò è necessario per consentire all'operatore di installare e gestire il registro interno di un ROSA grappolo. Per ulteriori informazioni sull'operatore, vedere Image Registry Operator nella OpenShift GitHub documentazione.

Dettagli dell'autorizzazione

Questa politica include le seguenti autorizzazioni che consentono all'Image Registry Operator di completare le seguenti azioni:

- `s3`— Gestire e valutare Amazon S3 bucket come storage persistente per il contenuto delle immagini dei container e i metadati del cluster.

Per visualizzare il documento JSON normativo completo, consulta la ROSAImageRegistryOperatorPolicy AWS Guida di riferimento sulle policy gestite.

AWS politica gestita: ROSACloudNetworkConfigOperatorPolicy

Puoi allegare `ROSACloudNetworkConfigOperatorPolicy` al tuo IAM entità. È necessario collegare questa politica a un IAM ruolo di operatore per consentire a un cluster ROSA con piani di controllo ospitati di effettuare chiamate verso altri Servizi AWS. È richiesto un set unico di ruoli operatore per ogni cluster.

Questa politica concede le autorizzazioni necessarie all'operatore del controller di Cloud Network Config per fornire e gestire le risorse di rete per ROSA overlay di rete per cluster. L'operatore utilizza queste autorizzazioni per gestire gli indirizzi IP privati per Amazon EC2 istanze come parte di ROSA grappolo. Per ulteriori informazioni sull'operatore, vedere C loud-network-config-controller nella OpenShift GitHub documentazione.

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni che consentono all'operatore del Cloud Network Config Controller di completare le seguenti attività:

- `ec2`— Leggere, assegnare e descrivere le configurazioni per la connessione Amazon EC2 istanze, Amazon VPC sottoreti e interfacce di rete elastiche in un ROSA cluster.

Per visualizzare il documento JSON programmatico completo, vedere ROSACloudNetworkConfigOperatorPolicynel AWS Guida di riferimento alle policy gestite.

AWS politica gestita: ROSAKubeControllerPolicy

Puoi allegare `ROSAKubeControllerPolicy` al tuo IAM entità. È necessario collegare questa politica a un IAM ruolo di operatore per consentire a un cluster ROSA con piani di controllo ospitati di effettuare chiamate verso altri Servizi AWS. È richiesto un set unico di ruoli operatore per ogni cluster.

Questa politica concede le autorizzazioni necessarie al controller kube per la gestione Amazon EC2, Elastic Load Balancing e AWS KMS risorse per un cluster ROSA con piani di controllo ospitati. Per ulteriori informazioni su questo controller, consulta l'architettura del controller nella OpenShift documentazione.

Dettagli dell'autorizzazione

Questa politica include le seguenti autorizzazioni che consentono al controller kube di completare le seguenti attività:

- `ec2`— Creare, eliminare e aggiungere tag a Amazon EC2 gruppi di sicurezza di istanze. Aggiungere regole in entrata ai gruppi di sicurezza. Descrivi le zone di disponibilità, Amazon EC2 istanze, tabelle di routingVPCs, gruppi di sicurezza e sottoreti.
- `elasticloadbalancing`— Crea e gestisci i sistemi di bilanciamento del carico e le relative politiche. Crea e gestisci i listener di load balancer. Registra gli obiettivi con i gruppi target e gestisci i gruppi target. Registrazione e cancellazione Amazon EC2 istanze con sistema di bilanciamento del carico e aggiunta di tag ai sistemi di bilanciamento del carico.
- `kms`— Recupera informazioni dettagliate su un AWS KMS chiave. Ciò è necessario per l'utilizzo di `etcd` dati crittografati quando la `etcd` crittografia è abilitata al momento della creazione del cluster.

Per visualizzare il documento JSON politico completo, ROSAKubeControllerPolicyconsulta la AWS Guida di riferimento alle policy gestite.

AWS politica gestita: ROSANodePoolManagementPolicy

Puoi allegare `ROSANodePoolManagementPolicy` al tuo IAM entità. È necessario collegare questa politica a un IAM ruolo di operatore per consentire a un cluster ROSA con piani di controllo ospitati di effettuare chiamate verso altri AWS servizi. È richiesto un set unico di ruoli operatore per ogni cluster.

Questa politica concede le autorizzazioni necessarie al NodePool controller per descrivere, eseguire e terminare Amazon EC2 istanze gestite come nodi di lavoro. Questa politica concede inoltre le autorizzazioni per consentire la crittografia del disco del volume radice del nodo di lavoro utilizzando AWS KMS chiavi. Per ulteriori informazioni su questo controller, consulta l'architettura del controller nella OpenShift documentazione.

Dettagli dell'autorizzazione

Questa politica include le seguenti autorizzazioni che consentono al NodePool controller di completare le seguenti attività:

- `ec2`— Esegui Amazon EC2 istanze che utilizzano AMIs hosted in Account AWS possedute e gestite da Red Hat. Gestisci i EC2 cicli di vita in ROSA cluster. Crea e integra dinamicamente nodi di lavoro con Elastic Load Balancing, Amazon VPC, Route 53, Amazon EBS e Amazon EC2.
- `iam`— Usa Elastic Load Balancing tramite il ruolo collegato al servizio denominato. `AWSServiceRoleForElasticLoadBalancing` Assegna ruoli a Amazon EC2 profili di istanza.
- `kms`— Leggi un AWS KMS chiave, crea e gestisci sovvenzioni per Amazon EC2 e restituisce una chiave dati simmetrica unica da utilizzare al di fuori di AWS KMS. Ciò è necessario per consentire la crittografia del disco del volume radice del nodo di lavoro.

Per visualizzare il documento di JSON policy completo, ROSANodePoolManagementPolicyconsulta la AWS Guida di riferimento alle policy gestite.

AWS politica gestita: ROSAKMSProviderPolicy

Puoi allegare `ROSAKMSProviderPolicy` al tuo IAM entità. È necessario collegare questa politica a un IAM ruolo di operatore per consentire a un cluster ROSA con piani di controllo ospitati di effettuare chiamate verso altri Servizi AWS. È richiesto un set unico di ruoli operatore per ogni cluster.

Questa politica concede le autorizzazioni necessarie al sistema integrato AWS Provider di crittografia da gestire AWS KMS chiavi che supportano la crittografia `etcd` dei dati. Questa politica consente Amazon EC2 di utilizzare KMS chiavi che AWS Encryption Provider fornisce la crittografia e la decrittografia dei `etcd` dati. Per ulteriori informazioni su questo provider, vedere AWS Encryption Provider nella documentazione di Kubernetes GitHub .

Dettagli dell'autorizzazione

Questa politica include le seguenti autorizzazioni che consentono di AWS Encryption Provider può completare le seguenti attività:

- `kms`— Crittografa, decrittografa e recupera un AWS KMS chiave. Ciò è necessario per l'utilizzo di `etcd` dati crittografati quando la `etcd` crittografia è abilitata al momento della creazione del cluster.

Per visualizzare il documento JSON politico completo, ROSAKMSProviderPolicyconsulta la AWS Guida di riferimento alle policy gestite.

AWS politica gestita: ROSAControlPlaneOperatorPolicy

Puoi allegare `ROSAControlPlaneOperatorPolicy` al tuo IAM entità. È necessario collegare questa politica a un IAM ruolo di operatore per consentire a un cluster ROSA con piani di controllo

ospitati di effettuare chiamate verso altri Servizi AWS. È richiesto un set unico di ruoli operatore per ogni cluster.

Questa politica concede le autorizzazioni necessarie all'operatore del piano di controllo per la gestione Amazon EC2 e Route 53 risorse per i cluster ROSA con piani di controllo ospitati. Per ulteriori informazioni su questo operatore, consulta l'architettura del controller nella OpenShift documentazione.

Dettagli dell'autorizzazione

Questa politica include le seguenti autorizzazioni che consentono all'operatore del piano di controllo di completare le seguenti attività:

- `ec2`— Creare e gestire Amazon VPC endpoint.
- `route53`— Elenca e modifica Route 53 set di record ed elenca zone ospitate.

Per visualizzare il documento JSON politico completo, ROSAControlPlaneOperatorPolicyconsulta la AWS Guida di riferimento alle policy gestite.

ROSA aggiornamenti a AWS policy gestite

Visualizza i dettagli sugli aggiornamenti di AWS politiche gestite per ROSA da quando questo servizio ha iniziato a tracciare queste modifiche. Per ricevere avvisi automatici sulle modifiche a questa pagina, iscriviti al RSS feed sulla Cronologia dei documenti pagina.

Modifica	Descrizione	Data
ROSANodePoolManagementPolicy— Politica aggiornata	ROSA ha aggiornato la politica per consentire il ROSA gestore del pool di nodi per descrivere i set di DHCP opzioni al fine di impostare i DNS nomi privati corretti. Per ulteriori informazioni, consulta the section called “AWS politica gestita: ROSANodePoolManagementPolicy”.	2 maggio 2024

Modifica	Descrizione	Data
ROSAInstallerPolicy— Politica aggiornata	ROSA ha aggiornato la politica per consentire il ROSA programma di installazione per aggiungere tag alle sottoreti utilizzando le chiavi dei tag corrispondenti. `"kubernetes.io/cluster/*"` Per ulteriori informazioni, consulta the section called “AWS politica gestita: ROSAInstallerPolicy”.	24 aprile 2024
ROSASRESupportPolicy— Politica aggiornata	ROSA ha aggiornato la policy per consentire al SRE ruolo di recuperare informazioni sui profili di istanza che sono stati taggati da ROSA come `red-hat-managed` . Per ulteriori informazioni, consulta the section called “AWS politica gestita: ROSASRESupportPolicy”.	10 aprile 2024

Modifica	Descrizione	Data
ROSAInstallerPolicy— Politica aggiornata	ROSA ha aggiornato la politica per consentire il ROSA programma di installazione per convalidarlo AWS politiche gestite per ROSA sono allegati a IAM ruoli usati da ROSA. Questo aggiornamento consente inoltre all'installatore di identificare se le politiche gestite dal cliente sono state allegate a ROSA ruoli. Per ulteriori informazioni, consulta the section called “AWS politica gestita: ROSAInstallerPolicy”.	10 aprile 2024
ROSAInstallerPolicy— Politica aggiornata	ROSA ha aggiornato la politica per consentire al servizio di fornire messaggi di avviso all'installatore quando l'installazione del cluster non riesce a causa della mancanza di un provider di cluster specifica to dal cliente. OIDC Questo aggiornamento consente inoltre al servizio di recuperare i DNS name server esistenti in modo che le operazioni di provisioning del cluster siano idempotenti. Per ulteriori informazioni, consulta the section called “AWS politica gestita: ROSAInstallerPolicy”.	26 gennaio 2024

Modifica	Descrizione	Data
ROSASRESupportPolicy— Politica aggiornata	ROSA ha aggiornato la policy per consentire al servizio di eseguire operazioni di lettura sui gruppi di sicurezza utilizzando il DescribeS ecurityGroups API. Per ulteriori informazioni, consulta the section called “AWS politica gestita: ROSASRESupportPolicy”.	22 gennaio 2024
ROSAImageRegistryOperatorPolicy— Politica aggiornata	ROSA ha aggiornato la politica per consentire all'Image Registry Operator di intraprendere azioni su Amazon S3 bucket nelle regioni con nomi di 14 caratteri. Per ulteriori informazioni, consulta the section called “AWS politica gestita: ROSAImageRegistryOperatorPolicy”.	12 dicembre 2023
ROSAKubeControllerPolicy— Politica aggiornata	ROSA ha aggiornato la politica per consentire di kube-controller-manager descriver e le zone di disponibilità, Amazon EC2 istanze, tabelle di routingVPCs, gruppi di sicurezza e sottoreti. Per ulteriori informazioni, consulta the section called “AWS politica gestita: ROSAKubeControllerPolicy”.	16 ottobre 2023

Modifica	Descrizione	Data
ROSAManageSubscription—Politica aggiornata	ROSA ha aggiornato la politica per aggiungerla ROSA con i piani di controllo ospitati ProductId. Per ulteriori informazioni, consulta the section called “AWS politica gestita: ROSAManageSubscription”.	1° agosto 2023
ROSAKubeControllerPolicy—Politica aggiornata	ROSA ha aggiornato la politica per consentire la creazione di Network kube-controller-manager Load Balancer come bilanciatori del carico del servizio Kubernetes. I Network Load Balancer offrono una maggiore capacità di gestire carichi di lavoro volatili e supportano indirizzi IP statici per il load balancer. Per ulteriori informazioni, consulta the section called “AWS politica gestita: ROSAKubeControllerPolicy”.	13 luglio 2023

Modifica	Descrizione	Data
ROSANodePoolManagementPolicy— Aggiunta una nuova politica	ROSA ha aggiunto una nuova politica per consentire al NodePool controller di descrivere, eseguire e terminare Amazon EC2 istanze gestite come nodi di lavoro. Questa politica consente inoltre la crittografia del disco del volume radice del nodo di lavoro utilizzando AWS KMS chiavi. Per ulteriori informazioni, consulta the section called “AWS politica gestita: ROSANodePoolManagementPolicy”.	8 giugno 2023
ROSAInstallerPolicy— Aggiunta una nuova politica	ROSA ha aggiunto una nuova politica per consentire all'installatore di gestire AWS risorse che supportano l'installazione del cluster. Per ulteriori informazioni, consulta the section called “AWS politica gestita: ROSAInstallerPolicy”.	6 giugno 2023

Modifica	Descrizione	Data
ROSASRESupportPolicy— Aggiunta una nuova politica	ROSA ha aggiunto una nuova policy per consentire SREs a Red Hat di osservare, diagnosticare e supportare direttamente AWS risorse associate a ROSA cluster, inclusa la possibilità di modificare ROSA stato del nodo del cluster. Per ulteriori informazioni, consulta the section called “AWS politica gestita: ROSASRESupportPolicy”.	1 giugno 2023
ROSAKMSProviderPolicy— Aggiunta una nuova politica	ROSA ha aggiunto una nuova politica per consentire la funzionalità integrata AWS Provider di crittografia da gestire AWS KMS chiavi per supportare la crittografia dei dati etcd. Per ulteriori informazioni, consulta the section called “AWS politica gestita: ROSAKMSProviderPolicy”.	27 aprile 2023

Modifica	Descrizione	Data
ROSAKubeControllerPolicy— Aggiunta una nuova politica	ROSA aggiunta una nuova politica per consentire al controller kube di gestire Amazon EC2, Elastic Load Balancing e AWS KMS risorse per ROSA con cluster di piani di controllo ospitati. Per ulteriori informazioni, consulta the section called “AWS politica gestita: ROSAKubeControllerPolicy”.	27 aprile 2023
ROSAImageRegistryOperatorPolicy— Aggiunta una nuova politica	ROSA ha aggiunto una nuova politica per consentire all'Image Registry Operator di fornire e gestire le risorse per ROSA registro delle immagini all'interno del cluster e servizi dipendenti, incluso S3. Per ulteriori informazioni, consulta the section called “AWS politica gestita: ROSAImageRegistryOperatorPolicy”.	27 aprile 2023
ROSAControlPlaneOperatorPolicy— Aggiunta una nuova policy	ROSA ha aggiunto una nuova politica per consentire al Control Plane Operator di gestire Amazon EC2 e Route 53 risorse per ROSA con cluster di piani di controllo ospitati. Per ulteriori informazioni, consulta the section called “AWS politica gestita: ROSAControlPlaneOperatorPolicy”.	24 aprile 2023

Modifica	Descrizione	Data
ROSACloudNetworkConfigOperatorPolicy— Aggiunta una nuova politica	ROSA ha aggiunto una nuova policy per consentire al Cloud Network Config Controller Operator di fornire e gestire le risorse di rete per ROSA overlay di rete per cluster. Per ulteriori informazioni, consulta the section called “AWS politica gestita: ROSACloudNetworkConfigOperatorPolicy”.	20 aprile 2023
ROSAIngressOperatorPolicy— Aggiunta una nuova politica	ROSA ha aggiunto una nuova politica per consentire a Ingress Operator di fornire e gestire sistemi di bilanciamento del carico e configurazioni per DNS ROSA i cluster. Per ulteriori informazioni, consulta the section called “AWS politica gestita: ROSAIngressOperatorPolicy”.	20 aprile 2023
ROSAAmazonEBSCSIDriverOperatorPolicy— Aggiunta una nuova politica	ROSA ha aggiunto una nuova politica per consentire il Amazon EBS CSIDriver Operator per installare e mantenere il Amazon EBS CSIdriver su un ROSA grappolo. Per ulteriori informazioni, consulta the section called “AWS politica gestita: ROSAAmazonEBSCSIDriverOperatorPolicy”.	20 aprile 2023

Modifica	Descrizione	Data
ROSAWorkerInstancePolicy— Aggiunta una nuova politica	ROSA ha aggiunto una nuova politica per consentire al servizio di gestire le risorse del cluster. Per ulteriori informazioni, consulta the section called “AWS politica gestita: ROSAWorkerInstancePolicy”.	20 aprile 2023
ROSAManageSubscription— Aggiunta una nuova politica	ROSA ha aggiunto una nuova politica per concedere il Marketplace AWS autorizzazioni necessarie per gestire il ROSA abbonamento. Per ulteriori informazioni, consulta the section called “AWS politica gestita: ROSAManageSubscription”.	11 aprile 2022
Servizio Red Hat OpenShift su AWS ha iniziato a tenere traccia delle modifiche	Servizio Red Hat OpenShift su AWS ha iniziato a tracciare le modifiche per suo AWS politiche gestite.	2 marzo 2022

Risoluzione dei problemi ROSA identità e accesso

Utilizza le seguenti informazioni per aiutarti a diagnosticare e risolvere i problemi più comuni che potresti riscontrare quando lavori con ROSA e IAM.

AWS Organizations la politica di controllo del servizio non è richiesta Marketplace AWS autorizzazioni

Se le ricette di AWS Organizations la policy di controllo del servizio (SCP) non consente quanto richiesto Marketplace AWS autorizzazioni di abbonamento quando si tenta di abilitare ROSA, si verifica il seguente errore di console.

```
An error occurred while enabling ROSA, because a service control policy (SCP) is
 denying required permissions. Contact your management account administrator, and
 consult the documentation for troubleshooting.
```

Se si riceve questo errore, è necessario contattare l'amministratore per ricevere assistenza. L'amministratore è la persona che gestisce gli account dell'organizzazione. Chiedi a quella persona di fare quanto segue:

1. Configura SCP le `aws-marketplace:Subscribe` `aws-marketplace:ViewSubscriptions` autorizzazioni per consentire e. `aws-marketplace:Unsubscribe` Per ulteriori informazioni, vedere Aggiornamento SCP di un AWS Organizations Guida per l'utente.
2. Attiva ROSA nell'account di gestione dell'organizzazione.
3. Condividi il ROSA abbonamento agli account dei membri che richiedono l'accesso all'interno dell'organizzazione. Per ulteriori informazioni, vedere Condivisione delle sottoscrizioni in un'organizzazione nel Marketplace AWS Guida all'acquisto.

L'utente o il ruolo non dispone dei requisiti richiesti Marketplace AWS autorizzazioni

Se le ricette di IAM il preside non ha i requisiti Marketplace AWS autorizzazioni di abbonamento quando si tenta di abilitare ROSA, si verifica il seguente errore di console.

```
An error occurred while enabling ROSA, because your user or role does not have the
 required permissions.
```

Per risolvere il problema, eseguire queste fasi:

1. Vai al IAM console e collega il AWS politica gestita `ROSAManageSubscription` per la tua IAM identità. Per ulteriori informazioni, ROSAManageSubscriptionconsulta la AWS Guida di riferimento alle policy gestite.
2. Segui la procedura riportata in the section called “ROSA Abilita e configura i prerequisiti AWS”.

Se non disponi dell'autorizzazione per visualizzare o aggiornare l'autorizzazione impostata in IAM oppure ricevi un errore, contatta l'amministratore per ricevere assistenza. Chiedi a quella persona di collegarsi `ROSAManageSubscription` al tuo IAM identifica e segui la procedura inthe section called “ROSA Abilita e configura i prerequisiti AWS”. Quando un amministratore esegue questa azione, abilita ROSA aggiornando il set di autorizzazioni per tutti IAM identità ai sensi del Account AWS.

Richiesto Marketplace AWS autorizzazioni bloccate da un amministratore

Se l'amministratore dell'account ha bloccato il file richiesto Marketplace AWS le autorizzazioni di abbonamento, si verifica il seguente errore della console quando si tenta di abilitare ROSA.

```
An error occurred while enabling ROSA because required permissions have been blocked by
 an administrator. ROSAManageSubscription includes the permissions required to enable
 ROSA. Consult the documentation and try again.
```

Se si riceve questo errore, è necessario contattare l'amministratore per ricevere assistenza. Chiedi a quella persona di fare quanto segue:

1. Vai al ROSA console e collega il AWS politica gestita `ROSAManageSubscription` per la tua IAM identità. Per ulteriori informazioni, ROSAManageSubscriptionconsulta la AWS Guida di riferimento alle policy gestite.
2. Segui la procedura riportata di seguito the section called “ROSA Abilita e configura i prerequisiti AWS” per abilitare ROSA. Questa procedura consente ROSA aggiornando il set di autorizzazioni per tutti IAM identità ai sensi del Account AWS.

Errore durante la creazione del sistema di bilanciamento del carico: AccessDenied

Se non hai creato un load balancer, il ruolo `AWSServiceRoleForElasticLoadBalacing` collegato al servizio potrebbe non esistere nel tuo account. Il seguente errore si verifica se si tenta di creare un ROSA cluster senza il `AWSServiceRoleForElasticLoadBalacing` ruolo nel tuo account.

```
Error creating network Load Balancer: AccessDenied
```

Per risolvere il problema, eseguire queste fasi:

1. Verifica se il tuo account ha il `AWSServiceRoleForElasticLoadBalancing` ruolo.

   ```
   aws iam get-role --role-name "AWSServiceRoleForElasticLoadBalancing"
   ```

2. Se non ricopri questo ruolo, segui le istruzioni per creare il ruolo che trovi in Creare il ruolo collegato al servizio nella Elastic Load Balancing Guida per l'utente.

Resilienza in ROSA

AWS resilienza dell'infrastruttura globale

Il AWS l'infrastruttura globale è costruita attorno Regioni AWS e zone di disponibilità. Regioni AWS forniscono più zone di disponibilità fisicamente separate e isolate, collegate tramite reti a bassa latenza, ad alto throughput e altamente ridondanti. Con le zone di disponibilità, puoi progettare e gestire applicazioni e database che eseguono automaticamente il failover tra zone di disponibilità senza interruzioni. Le zone di disponibilità sono più disponibili, tolleranti ai guasti e scalabili rispetto alle infrastrutture a data center singolo o multiplo tradizionali.

ROSA offre ai clienti la possibilità di eseguire il piano di controllo e il piano dati di Kubernetes in un unico piano AWS Zona di disponibilità o su più zone di disponibilità. Sebbene i cluster Single-AZ possano essere utili per la sperimentazione, i clienti sono incoraggiati a eseguire i propri carichi di lavoro in più di una zona di disponibilità. Ciò garantisce che le applicazioni possano resistere anche a un guasto completo della zona di disponibilità, un evento di per sé molto raro.

Per ulteriori informazioni sull' Regioni AWS e zone di disponibilità, vedi AWS Infrastruttura globale.

ROSA resilienza dei cluster

Il ROSA il piano di controllo è costituito da almeno tre nodi OpenShift del piano di controllo. Ogni nodo del piano di controllo è composto da un'istanza del API server, un'`etcd`distanza e dei controller. In caso di guasto di un nodo del piano di controllo, tutte le API richieste vengono indirizzate automaticamente agli altri nodi disponibili per garantire la disponibilità del cluster.

Il ROSA il piano dati è costituito da almeno due nodi di OpenShift infrastruttura e due OpenShift nodi di lavoro. I nodi di infrastruttura eseguono pod che supportano componenti dell'infrastruttura del OpenShift cluster come il router predefinito, il OpenShift registro integrato e i componenti per le metriche e il monitoraggio del cluster. OpenShift i nodi di lavoro eseguono i pod delle applicazioni per gli utenti finali.

I tecnici di Red Hat Site Reliability (SREs) gestiscono completamente il piano di controllo e i nodi dell'infrastruttura. Red Hat monitora SREs in modo proattivo ROSA raggruppano e sono responsabili della sostituzione di eventuali nodi del piano di controllo e nodi dell'infrastruttura guasti. Per ulteriori informazioni, consulta the section called “Responsabilità”.

> **Important**
>
> Perché ROSA è un servizio gestito, Red Hat è responsabile della gestione del sottostante AWS infrastruttura che ROSA usi. I clienti non devono tentare di spegnere manualmente il Amazon EC2 casi che ROSA utilizza dal AWS console o AWS CLI. Questa azione può portare alla perdita dei dati dei clienti.

Se un nodo di lavoro si guasta sul piano dati, il piano di controllo riposiziona i pod non programmati sui nodi di lavoro funzionanti fino al ripristino o alla sostituzione del nodo guasto. I nodi di lavoro guasti possono essere sostituiti manualmente o automaticamente abilitando il ridimensionamento automatico delle macchine in un cluster. Per maggiori informazioni, consulta Cluster autoscaling nella documentazione di Red Hat.

Resilienza delle applicazioni implementate dal cliente

Sebbene ROSA fornisce molte protezioni per garantire un'elevata disponibilità del servizio, i clienti hanno la responsabilità di creare le applicazioni implementate in modo da garantire l'elevata disponibilità per proteggere i carichi di lavoro dai tempi di inattività. Per ulteriori informazioni, vedere Informazioni sulla disponibilità per ROSAnella documentazione di Red Hat.

Sicurezza dell'infrastruttura in ROSA

Come servizio gestito, Servizio Red Hat OpenShift su AWS è protetto dal AWS sicurezza di rete globale. Per informazioni su AWS servizi di sicurezza e come AWS protegge l'infrastruttura, vedi AWS Sicurezza nel cloud. Per progettare il tuo AWS ambiente che utilizza le migliori pratiche per la sicurezza dell'infrastruttura, vedi Infrastructure Protection in Security Pillar — AWS Well-Architected Framework.

Tu usi AWS APIchiamate pubblicate per accedere ROSA tramite il AWS rete. I client devono supportare quanto segue:

- Sicurezza del livello di trasporto (TLS). Richiediamo TLS 1.2 e consigliamo TLS 1.3.
- Suite di cifratura con Perfect Forward Secrecy (PFS) come (Ephemeral Diffie-Hellman) o DHE (Elliptic Curve Ephemeral Diffie-Hellman). ECDHE La maggior parte dei sistemi moderni, come Java 7 e versioni successive, supporta tali modalità.

Inoltre, le richieste devono essere firmate utilizzando un ID chiave di accesso e una chiave di accesso segreta associata a un principale. IAM Oppure puoi usare il AWS Security Token Service (AWS STS) per generare credenziali di sicurezza temporanee per firmare le richieste.

Isolamento della rete di cluster

I tecnici di Red Hat Site Reliability (SREs) sono responsabili della gestione continua e della sicurezza di rete del cluster e della piattaforma applicativa sottostante. Per ulteriori informazioni sulle responsabilità di Red Hat per ROSA, consulta the section called “Responsabilità”.

Quando crei un nuovo cluster, ROSA offre la possibilità di creare un endpoint del API server Kubernetes pubblico e route di applicazione o un endpoint API Kubernetes privato e route di applicazione. Questa connessione viene utilizzata per comunicare con il cluster (utilizzando OpenShift strumenti di gestione come and). ROSA CLI OpenShift CLI Una connessione privata consente a tutte le comunicazioni tra i nodi e il API server di rimanere all'interno dell'utenteVPC. Se abiliti l'accesso privato al API server e ai percorsi delle applicazioni, devi utilizzare un percorso esistente VPC e AWS PrivateLink per connetterlo VPC al servizio di OpenShift backend.

L'accesso al API server Kubernetes è protetto utilizzando una combinazione di AWS Identity and Access Management (IAM) e controllo degli accessi nativo basato sui ruoli di Kubernetes (). RBAC Per ulteriori informazioni su Kubernetes, consulta Using Authorization nella documentazione di Kubernetes. RBAC RBAC

ROSA consente di creare percorsi applicativi sicuri utilizzando diversi tipi di TLS terminazione per fornire certificati al client. Per maggiori informazioni, consulta Percorsi protetti nella documentazione di Red Hat.

Se crei un ROSA in un cluster esistenteVPC, è necessario specificare le VPC sottoreti e le zone di disponibilità da utilizzare per il cluster. È inoltre possibile definire gli CIDR intervalli da utilizzare per la rete di cluster e abbinare questi CIDR intervalli alle sottoreti. VPC Per ulteriori informazioni, consultate le definizioni degli CIDR intervalli nella documentazione di Red Hat.

Per i cluster che utilizzano l'APIendpoint pubblico, ROSA richiede che l'utente VPC sia configurato con una sottorete pubblica e privata per ogni zona di disponibilità in cui si desidera distribuire il cluster. Per i cluster che utilizzano l'APIendpoint privato, sono necessarie solo sottoreti private.

Se ne stai usando uno esistenteVPC, puoi configurare il ROSA cluster per utilizzare un server HTTPS proxy durante HTTP o dopo la creazione del cluster per crittografare il traffico Web del cluster, aggiungendo un altro livello di sicurezza per i dati. Quando si abilita un proxy, ai componenti principali

del cluster viene negato l'accesso diretto a Internet. Il proxy non nega l'accesso a Internet per i carichi di lavoro degli utenti. Per maggiori informazioni, consultate Configurazione di un proxy a livello di cluster nella documentazione di Red Hat.

Isolamento della rete Pod

Se sei un amministratore del cluster, puoi definire politiche di rete a livello di pod che limitino il traffico ai pod del tuo ROSA raggruppamento.

ROSA quote di servizio

Servizio Red Hat OpenShift su AWS (ROSA) utilizza le quote di servizio per Amazon EC2, Amazon Virtual Private Cloud Amazon Elastic Block Store, e per il provisioning dei Elastic Load Balancing cluster. Per ulteriori informazioni, consulta Servizio Red Hat OpenShift su AWS Endpoint and Quotas nella Guida di riferimento generale. AWS

AWS servizi integrati con ROSA

ROSA collabora con altri Servizi AWS per fornire soluzioni aggiuntive per le sfide aziendali. Questo argomento identifica i servizi che vengono utilizzati ROSA per aggiungere funzionalità o i servizi ROSA utilizzati per eseguire attività.

Argomenti

Come ROSA funziona con Marketplace AWS

Marketplace AWS è un catalogo digitale curato che puoi utilizzare per trovare, acquistare, distribuire e gestire software, dati e servizi di terze parti necessari per creare soluzioni e gestire la tua attività. Marketplace AWS semplifica le licenze e l'approvvigionamento del software con opzioni di prezzo flessibili e diversi metodi di implementazione.

ROSA usi Marketplace AWS per la misurazione e la fatturazione del servizio. ROSAclassic viene misurato e fatturato tramite un prodotto basato su Marketplace AWS Amazon Machine Image (AMI), mentre ROSA con piani di controllo ospitati (HCP) viene misurato e fatturato tramite un prodotto basato su Marketplace AWS Software as a Service (SaaS).

Questa pagina spiega come ROSA funziona Marketplace AWS per i pagamenti, la fatturazione, gli abbonamenti e gli acquisti contrattuali.

Terminologia

Questa pagina utilizza i seguenti termini quando si parla ROSA dell'integrazione con. Marketplace AWS

Immagine della macchina Amazon (AMI)

: Un'immagine di un server, incluso un sistema operativo e software aggiuntivo, su cui è in esecuzione AWS.

AMIabbonamento

: Nei Marketplace AWS prodotti software AMI basati su software come ROSA Classic viene utilizzato un modello di tariffazione oraria con abbonamento annuale. La tariffa oraria è il modello

di prezzo predefinito, ma hai la possibilità di acquistare in anticipo un anno di utilizzo per un solo Amazon EC2 tipo di istanza.

Abbonamento SaaS

In Marketplace AWS, i prodotti software-as-a-service (SaaS) come ROSA with HCP adottano un modello di abbonamento basato sull'utilizzo. Il venditore del software monitora il tuo utilizzo e paghi solo per quello che usi.

Offerta pubblica

Le offerte pubbliche consentono di acquistare Marketplace AWS software e servizi direttamente da AWS Management Console.

Offerta privata

Le offerte private sono un programma di acquisto che consente a venditori e acquirenti di negoziare prezzi personalizzati e termini del contratto di licenza con l'utente finale (EULA) per gli acquisti in. Marketplace AWS

ROSA costi di servizio

Commissioni ROSA addebitate per la gestione del OpenShift software e del cluster da parte dei tecnici di Red Hat Site Reliability (SREs). ROSA i costi del servizio vengono contabilizzati Marketplace AWS e appaiono sulla AWS fattura.

AWS tariffe per l'infrastruttura

Commissioni standard AWS addebitate per ROSA i cluster Servizi AWS sottostanti, tra cui Amazon EC2, Amazon EBS Amazon S3, e Elastic Load Balancing. Le tariffe vengono contabilizzate al Servizio AWS momento dell'utilizzo e appaiono sulla fattura AWS .

ROSA pagamenti e fatturazione

ROSA si integra con Marketplace AWS per consentire la misurazione e la fatturazione dei costi di servizio. ROSA ROSA i costi del servizio coprono l'accesso al OpenShift software e la gestione dei cluster da parte dei tecnici di Red Hat Site Reliability (). SREs ROSA i costi di servizio sono uniformi in tutte le regioni AWS standard supportate. ROSAcon i costi di HCP servizio maturati su richiesta per impostazione predefinita, a una tariffa oraria fissa in base al numero di cluster in esecuzione e di nodi di lavoro in vCPUs esecuzione in tali cluster. ROSAi costi di servizio classici vengono calcolati su richiesta in base al numero di nodi di lavoro. vCPUs ROSAclassic non addebita costi di servizio per il piano di controllo o i nodi dell'infrastruttura richiesti.

ROSA i clienti pagano anche le tariffe di AWS infrastruttura standard per ROSA i cluster Servizi AWS sottostanti, tra cui Amazon EC2 Amazon EBS, Amazon S3, e Elastic Load Balancing. AWS i costi di infrastruttura sono una voce di fatturazione distinta dai costi di ROSA servizio che vengono contabilizzati. Marketplace AWS AWS le tariffe per l'infrastruttura variano di default Regione AWS e si basano sull'utilizzo orario. Per ulteriori risparmi sui costi AWS dell'infrastruttura, puoi acquistare piani di Amazon EC2 risparmio o istanze riservate. Per ulteriori informazioni, consulta Compute Savings Plans and Reserved Instances nella Guida per Amazon EC2 l'utente.

ROSA non addebita commissioni fino alla creazione di un ROSA cluster o all'acquisto di un ROSA contratto. Per ulteriori informazioni, consultare Prezzi di Servizio Red Hat OpenShift su AWS.

Puoi visualizzare i costi ROSA di servizio e i costi AWS dell'infrastruttura e gestire i pagamenti nella AWS Billing console. È inoltre possibile visualizzare i costi e monitorare l'utilizzo utilizzando l' AWS Cost Explorer Service interfaccia gratuitamente. Per ulteriori informazioni, consulta Visualizzazione della fattura nella Guida per l' AWS Billing and Cost Management utente e Analisi dei costi AWS Cost Explorer Service nella Guida per l'utente di AWS Cost Management.

Iscrizione alle inserzioni ROSA del Marketplace tramite la console

Quando lo attivi ROSA nella ROSA console, sei abbonato alla ROSA versione classica e le HCP inserzioni sono ROSA attive. Account AWS Marketplace AWS Non è previsto alcun costo per l'attivazione ROSA degli abbonamenti.

Per AWS Organizations gli utenti, ROSA consente di condividere gli abbonamenti ROSA classici con altri account dell'organizzazione. Per ulteriori informazioni, consulta Condivisione degli abbonamenti in un'organizzazione nella Guida all' Marketplace AWS acquisto.

Acquisto di un contratto ROSA

ROSA utilizza Marketplace AWS per fornire contratti opzionali per ROSA with HCP and ROSA classic. I contratti consentono di risparmiare sui costi di servizio del ROSA Worker Node. ROSA i contratti non influiscono sulle tariffe addebitate per l' AWS infrastruttura.

contratti di 12 mesi

Puoi acquistare contratti di offerta pubblica di 12 mesi per la ROSA versione classica e ROSA con HCP dalla ROSA console.

> **Note**
>
> ROSAclassic deve essere abilitato sul tuo account prima di poter acquistare contratti di 12 mesi dalla console.

> **Note**
>
> I contratti di 12 mesi non possono essere trasferiti a un'offerta privata.

Acquisto di un contratto ROSA classico di 12 mesi

Quando acquisti un contratto ROSA classico di 12 mesi, effettui un pagamento anticipato per un periodo annuale e non paghi alcun costo orario di servizio per i 12 mesi successivi per le istanze coperte. Il costo del contratto si basa sul tipo di Amazon EC2 istanza e sul numero di istanze selezionate. Il contratto non copre i costi di AWS infrastruttura ROSA addebitati per Servizi AWS il sottostante utilizzato. Per ulteriori informazioni, consulta la sezione Prezzi di Servizio Red Hat OpenShift su AWS.

Il contratto copre solo i tipi di istanza specificati durante la creazione del contratto (ad esempio m5.xlarge). È possibile acquistare contratti aggiuntivi di 12 mesi per risparmiare sui costi su più di un tipo di istanza. Amazon EC2 L'utilizzo al di fuori del contratto di 12 mesi comporta costi di ROSA servizio alla tariffa on demand.

> **Note**
>
> ROSAi contratti classici di 12 mesi non si rinnovano automaticamente.

Per acquistare un contratto di 12 mesi per la versione classica ROSA

> **Note**
>
> Se utilizzi la ROSA console in un'area geografica che non supporta ROSA ancora il protocolloHCP, questo flusso di lavoro non è ancora disponibile. Per un elenco delle regioni che supportano ROSA conHCP, consultathe section called “A confronto ROSA con un HCP classico ROSA”.

Per acquistare contratti ROSA classici nelle regioni ROSA senza HCP assistenza, vai alla ROSA console e scegli Acquista un contratto software e visualizza i contratti esistenti.

1. Accedere alla console ROSA.
2. Nel riquadro di navigazione a sinistra, scegli Contratti.
3. Scegli Contratti per la ROSA versione classica.
4. Scegli Contratto di acquisto.
5. Seleziona il tipo di EC2 istanza e il numero di istanze di cui hai bisogno.
6. Scegli Rivedi il contratto.
7. Controlla i dettagli del contratto e scegli Contratto di acquisto.

Note

ROSA I contratti di 12 mesi non possono essere declassati o annullati dopo la creazione tramite la console. Se devi effettuare il downgrade o annullare il contratto durante la durata del contratto attivo, vai al AWS Support Centro e apri una richiesta di assistenza.

Acquisto di un contratto ROSA con HCP 12 mesi

Quando abiliti ROSA con HCP nella console, sul tuo account viene inizialmente creato un HCP contratto gratuito di 12 mesi ROSA per facilitare la fatturazione su richiesta. Se scegli di acquistare un HCP contratto ROSA with per risparmiare sui costi di servizio del Worker Node, il contratto iniziale viene modificato per coprire i costi di utilizzo del Worker Node vCPUs e i piani di controllo specificati.

Quando acquisti un ROSA contratto di HCP 12 mesi, effettui un pagamento anticipato per un periodo annuale e non paghi alcuna tariffa di utilizzo oraria per i 12 mesi successivi per il nodo di lavoro coperto vCPUs e i piani di controllo. Il costo del contratto si basa sul numero di nodi di lavoro vCPUs e piani di controllo selezionati. Il contratto copre solo il nodo di lavoro vCPUs e i piani di controllo specificati durante la creazione del contratto. Il contratto non copre i costi di AWS infrastruttura ROSA addebitati per Servizi AWS il sottostante utilizzato. Per ulteriori informazioni, consulta la sezione Prezzi di Servizio Red Hat OpenShift su AWS.

Quota di utilizzo mensile

Al momento dell'acquisto, i tuoi piani prepagati vCPUs e di controllo vengono convertiti in una quota di utilizzo mensile. Per l'utilizzo di v CPU e control plane che supera la quota mensile si applicano tariffe orarie di utilizzo on demand. ROSAwith HCP utilizza le seguenti formule per calcolare la quota mensile associata al contratto:

- Nodo lavoratorevCPUs: numero di vCPUs x 24 ore x 365 giorni/12 mesi
- Piani di controllo: numero di piani di controllo x 24 ore x 365 giorni/12 mesi

Ad esempio, un acquisto di 4.000 nodi di lavoro vCPUs e 8 piani di controllo verrebbe convertito in una quota mensile di 2.920.000 nodi di lavoro per CPU ore e 5.840 ore di piano di controllo consumabili al mese.

Per HCP acquistare ROSA un contratto con 12 mesi

> **Note**
>
> Se utilizzi la Servizio Red Hat OpenShift su AWS console in una regione che non supporta ROSA ancora i piani di controllo ospitati, questo flusso di lavoro non è ancora disponibile. Per un elenco delle regioni che supportano ROSA conHCP, consultathe section called “A confronto ROSA con un HCP classico ROSA”.

1. Accedere alla console ROSA.
2. Nel riquadro di navigazione a sinistra, scegli Contratti.
3. Scegli Contratti per ROSA con HCP.
4. Scegli Contratto di acquisto.
5. Inserisci il numero di vCPUs da acquistare. Specificare in multipli di 4.
6. Inserire il numero di piani di controllo da acquistare.
7. Scegli Rivedi contratto.
8. Controlla i dettagli del contratto e scegli Contratto di acquisto.

> **Note**
>
> ROSA I contratti di 12 mesi non possono essere declassati o annullati dopo la creazione tramite la console. Se devi effettuare il downgrade o annullare il contratto durante la durata del contratto attivo, vai al AWS Support Centro e apri una richiesta di assistenza.

Aggiornamento di un contratto di 12 mesi ROSA HCP

Puoi aggiornare il tuo contratto attivo ROSA con un contratto di HCP 12 mesi in qualsiasi momento con un nodo vCPUs di lavoro e piani di controllo aggiuntivi. Quando effettui l'upgrade ROSA a un contratto di HCP 12 mesi, effettui un pagamento anticipato proporzionale per le risorse aggiuntive. Gli importi ripartiti proporzionalmente vengono calcolati in base al numero di giorni rimanenti del contratto. Il contratto copre solo il nodo di lavoro vCPUs e i piani di controllo specificati durante la creazione del contratto. Gli aggiornamenti contrattuali non influiscono sulle tariffe addebitate per l' AWS infrastruttura.

Al momento dell'upgrade, i piani aggiunti vCPUs e di controllo vengono convertiti in una quota di utilizzo mensile utilizzando le stesse formule del contratto di acquisto originale. Per l'utilizzo di v CPU e control plane che supera la quota mensile si applicano tariffe orarie di utilizzo on demand. Per ulteriori informazioni, consulta the section called “Quota di utilizzo mensile”.

Per aggiornare un contratto con durata di 12 mesi ROSA HCP

1. Accedere alla console ROSA.
2. Nel riquadro di navigazione a sinistra, scegli Contratti.
3. Scegli Contratti per ROSA con HCP.
4. Seleziona Upgrade (Aggiorna).
5. Inserisci il numero di vCPUs da aggiungere. Specificare in multipli di 4.
6. Inserire il numero di piani di controllo da aggiungere al contratto.
7. Scegli Review upgrade.
8. Controlla i dettagli del contratto e scegli Acquista upgrade.

> **Note**
>
> ROSAi contratti classici di 12 mesi non possono essere aggiornati. I contratti ROSA classici aggiuntivi di 12 mesi possono essere acquistati in qualsiasi momento utilizzando la console. ROSA

Ottenere un'offerta privata

Puoi richiedere un'offerta Marketplace AWS privata per ROSA with HCP or ROSA classic per ricevere i prezzi del prodotto e i termini del contratto di licenza per l'utente finale (EULA) negoziati con Red Hat. Per ulteriori informazioni, consulta la sezione Offerte private nella Marketplace AWS Buyer Guide.

Per ottenere un'offerta ROSA privata

> **Note**
>
> Se sei un AWS Organizations utente e hai ricevuto un'offerta privata sui tuoi account paganti e soci, segui la procedura seguente per iscriverti ROSA direttamente su ogni account della tua organizzazione.
> Se ricevi un'offerta privata ROSA classica che è stata emessa solo sull'account del AWS Organizations pagante, dovrai condividere l'abbonamento con gli account dei membri della tua organizzazione. Per ulteriori informazioni, consulta Condivisione degli abbonamenti in un'organizzazione nella Guida all' Marketplace AWS acquisto.

1. Una volta emessa un'offerta privata, accedi alla Marketplace AWS console.
2. Apri l'e-mail con il link di un'offerta ROSA privata.
3. Segui il link per accedere direttamente all'offerta privata.

   > **Note**
   >
   > Se segui questo link prima di accedere all'account corretto, verrà visualizzato l'errore Page note found (404).

4. Consulta i termini e le condizioni.
5. Scegli Accetta i termini.

> **Note**
>
> Se un'offerta Marketplace AWS privata non viene accettata, i costi di ROSA servizio Marketplace AWS continueranno a essere fatturati alla tariffa oraria pubblica.

6. Per verificare i dettagli dell'offerta, seleziona Mostra dettagli nell'elenco dei prodotti.
7. Per iniziare a utilizzare ROSA, scegli Continua con la configurazione. Verrai reindirizzato alla ROSA console.

Marketplace privato

Private Marketplace consente agli amministratori di creare cataloghi digitali personalizzati di prodotti approvati da. Marketplace AWS Gli amministratori possono creare set unici di software testato, acquistabili Marketplace AWS per unità AWS organizzative o diversi Account AWS all'interno dell'organizzazione.

Se l'organizzazione utilizza un marketplace privato, un amministratore deve aggiungere le Marketplace AWS offerte ROSA al marketplace privato prima che gli utenti possano abilitare il servizio. Per ulteriori informazioni, consulta la sezione Guida introduttiva al marketplace privato nella Guida Marketplace AWS all'acquisto.

Risoluzione dei problemi

La pagina seguente descrive alcuni problemi comuni riscontrati durante la creazione o la gestione dei cluster. ROSA

Argomenti

Accedi ai log di ROSA debug dei cluster

Per iniziare a risolvere i problemi relativi all'applicazione, esaminate innanzitutto i log di debug. I log di ROSA CLI debug forniscono dettagli sui messaggi di errore che vengono prodotti quando la creazione di un file non riesce. cluster

Per visualizzare le informazioni di cluster debug, esegui il comando seguente. ROSA CLI Nel comando, sostituiscilo `<cluster_name>` con il nome del tuo cluster.

```
rosa describe cluster -c <cluster_name> --debug
```

ROSA il cluster non riesce a controllare la quota di AWS servizio durante la cluster creazione

Per utilizzarlo ROSA, potrebbe essere necessario aumentare le quote di servizio per l'account. Per ulteriori informazioni, consulta Endpoint e quote per Servizio Red Hat OpenShift su AWS.

1. Esegui il comando seguente per identificare le quote del tuo account.

   ```
   rosa verify quota
   ```

> **Note**
>
> Le quote sono diverse in modo diverso. Regioni AWS Assicurati di verificare ciascuna delle quote per le tue regioni.

2. Se devi aumentare la tua quota, accedi alla Service Quotas console.
3. Nel riquadro di navigazione, scegli AWS servizi.
4. Scegli il servizio che richiede un aumento della quota.
5. Seleziona la quota che deve essere aumentata e scegli Richiedi un aumento della quota.
6. Per Richiedi un aumento della quota, inserisci l'importo totale che desideri assegnare alla quota e scegli Richiedi.

Risolvi i problemi relativi ai token di ROSA CLI accesso offline scaduti

Se utilizzi il token di accesso offline api.openshift.com ROSA CLI e il token di accesso offline api.openshift.com scade, viene visualizzato un messaggio di errore. Ciò accade quando sso.redhat.com invalida il token.

1. Vai alla pagina del token di OpenShift Cluster Manager API e scegli Load Token.
2. Copia e incolla il seguente comando di autenticazione nel terminale.

```
rosa login --token="<api_token>"
```

Impossibile creare un messaggio cluster con un osdCcsAdmin errore

> **Note**
>
> Questo errore si verifica solo quando non si utilizza il STS metodo di provisioning dei ROSA cluster. Per evitare questo problema, esegui il provisioning dei ROSA cluster utilizzando. AWS STS Per ulteriori informazioni, consulta the section called “Crea un cluster ROSA classico - CLI”.

Se cluster non riesci a creare, potresti ricevere il seguente messaggio di errore:

```
Failed to create cluster: Unable to create cluster spec: Failed to get access keys for
 user 'osdCcsAdmin': NoSuchEntity: The user with name osdCcsAdmin cannot be found.
```

1. Eliminare lo stack.

   ```
   rosa init --delete-stack
   ```

2. Reinizializza il tuo account.

   ```
   rosa init
   ```

Passaggi successivi

- Consulta la documentazione. OpenShift
- Apri una AWS Support custodia o una custodia Red Hat Support.
- Trova le risposte alle domande frequenti su Servizio Red Hat OpenShift su AWS.
- Per ulteriori informazioni sul modello ROSA di supporto, consultathe section called “Ottenere supporto”.

Ottenere ROSA assistenza

Con ROSA, puoi ricevere supporto da AWS Support e dai team di supporto di Red Hat. I casi di supporto possono essere aperti con entrambe le organizzazioni e indirizzati al team corretto per risolvere il problema.

Apri qualsiasi caso AWS Support

È necessario un piano di supporto per gli AWS sviluppatori per aprire casi ROSA tecnici, ma si consiglia un piano di supporto AWS Business, Enterprise o Enterprise On-Ramp per l'accesso continuo al supporto ROSA tecnico e alle linee guida sull'architettura. Red Hat lo utilizza AWS Support API per aprire casi ai clienti quando necessario. AWS I piani di supporto Business, Enterprise ed Enterprise On-Ramp consentono l'accesso continuo al telefono, al Web e alla chat ai tecnici dell'assistenza. Per ulteriori informazioni sui AWS Support piani, consulta. AWS Support

Per i passaggi per abilitare un AWS Support piano, vedi Come posso iscrivermi a un AWS Support piano?

Per informazioni sulla creazione di un AWS Support caso, consulta Creazione di casi di supporto e gestione dei casi.

Apri un caso Red Hat Support

ROSA include Red Hat Premium Support. Per ricevere Red Hat Premium Support, accedi al Red Hat Customer Portal e utilizza lo strumento Support Case per creare un ticket di supporto. Per ulteriori informazioni, consulta Come interagire con il supporto Red Hat.

Cronologia dei documenti

Nella seguente tabella sono descritte importanti modifiche alla documentazione . Per ricevere notifiche sugli aggiornamenti di questa documentazione, puoi iscriverti a un RSS feed.

Modifica	Descrizione	Data
ROSAcon HCP Regione AWS espansione	ROSAcon piani di controllo ospitati (HCP) è ora disponibile in Medio Oriente (UAE) Regione AWS.	13 maggio 2024
ROSAcon HCP Regione AWS espansione	ROSAwith hosted control planes (HCP) è ora disponibile in Europa (Parigi) Regione AWS.	6 maggio 2024
Aggiornato ROSANodePoolManagementPolicy	Aggiornato il AWS politica gestitaROSANodePoolManagementPolicy.	2 maggio 2024
ROSAcon HCP Regione AWS espansione	ROSAcon piani di controllo ospitati (HCP) è ora disponibile in Europa (Spagna) Regione AWS.	29 aprile 2024
Aggiornato ROSAInstallerPolicy	Aggiornato il AWS politica gestitaROSAInstallerPolicy.	24 aprile 2024
ROSAcon HCP Regione AWS espansione	ROSAwith hosted control planes (HCP) è ora disponibile in Europa (Zurigo) Regione AWS.	19 aprile 2024
ROSAcon HCP Regione AWS espansione	ROSAwith hosted control planes (HCP) è ora disponibile nella regione Asia-Pacifico (Osaka) Regione AWS.	17 aprile 2024

Aggiornato ROSAInstallerPolicy e ROSASRESupportPolicy	Aggiornato il AWS politiche gestite ROSAInstallerPolicy eROSASRESupportPolicy.	10 aprile 2024
ROSAcon HCP Regione AWS espansione	ROSAcon piani di controllo ospitati (HCP) è ora disponibile nella regione Asia-Pacifico (Hong Kong) Regione AWS.	8 aprile 2024
ROSAcon HCP Regione AWS espansione	ROSAcon piani di controllo ospitati (HCP) è ora disponibile in Sud America (San Paolo) Regione AWS.	1 aprile 2024
ROSAcon HCP Regione AWS espansione	ROSAwith hosted control planes (HCP) è ora disponibile in Medio Oriente (Bahrain) Regione AWS.	25 marzo 2024
ROSAcon HCP Regione AWS espansione	ROSAwith hosted control planes (HCP) è ora disponibile nella regione Asia-Pacifico (Seoul) Regione AWS.	14 marzo 2024
ROSAcon HCP Regione AWS espansione	ROSAwith hosted control planes (HCP) è ora disponibile in Africa (Città del Capo) Regione AWS.	5 marzo 2024
Aggiornato ROSAInstallerPolicy	Aggiornato il AWS politica gestitaROSAInstallerPolicy.	26 gennaio 2024
Aggiornato ROSASRESupportPolicy	Aggiornato il AWS politica gestitaROSASRESupportPolicy.	22 gennaio 2024

Aggiornato ROSAImage RegistryOperatorPolicy	Aggiornato il AWS politica gestitaROSAImageRe gistryOperatorPolicy.	12 dicembre 2023
Aggiornato ROSAKubeC ontrollerPolicy	Aggiornato il AWS politica gestitaROSAKubeControllerPo licy.	16 ottobre 2023
Aggiornato ROSAManag eSubscription	Aggiornato il AWS politica gestitaROSAManageS ubscription.	1° agosto 2023
Aggiornato ROSAKubeC ontrollerPolicy	Aggiornato il AWS politica gestitaROSAKubeControllerPo licy.	13 luglio 2023
Pagine ROSA di sicurezza aggiunte	Sono state aggiunte le ROSA pagine Resilience in ROSAROSA, Infrastructure Security in e Data Protection in.	30 giugno 2023
È stata aggiunta la pagina delle opzioni di distribuzione	È stata aggiunta la pagina delle opzioni di distribuzione.	9 giugno 2023
È stata aggiunta una nuova AWS politica gestita ROSANodePoolManage mentPolicy	Novità AWS è ROSANodeP oolManagementPolicy stata aggiunta una politica gestita.	8 giugno 2023
Aggiunto nuovo AWS politica gestita ROSAInstallerPolicy	Novità AWS è ROSAInsta llerPolicy stata aggiunta una politica gestita.	6 giugno 2023
Aggiunto nuovo AWS politica gestita ROSASRESupportPoli cy	Novità AWS è ROSASRESu pportPolicy stata aggiunta una politica gestita.	1 giugno 2023

È stata aggiunta una panoramica delle responsabilità per ROSA	È stata aggiunta una panoramica delle responsabilità per la ROSA pagina.	26 maggio 2023
Aggiornato Cos'è Servizio Red Hat OpenShift su AWS?	Aggiornato il What is Servizio Red Hat OpenShift su AWS pagina.	24 maggio 2023
Aggiunto nuovo AWS politiche gestite per i ruoli ROSA degli operatori	Novità AWS politiche ROSAImageRegistryOperatorPolicy gestite ROSAKubeControllerPolicy e ROSAKMSProviderPolicy sono state aggiunte.	27 aprile 2023
Aggiunto nuovo AWS politica gestita ROSAControlPlaneOperatorPolicy	Novità AWS è ROSAControlPlaneOperatorPolicy stata aggiunta una politica gestita.	24 aprile 2023
Aggiunto nuovo AWS politiche gestite per i ruoli ROSA degli account	Novità AWS sono state aggiunte pagine di policy gestite per la pagina dei ruoli dell'ROSAaccount e dell'operatore.	20 aprile 2023
È stata aggiunta la ROSA pagina delle quote di servizio	È stata ROSA aggiunta la pagina delle quote di servizio.	22 dicembre 2022
Aggiunte pagine di risoluzione dei problemi	Sono state aggiunte pagine per la risoluzione dei problemi.	1 novembre 2022
Sono state aggiunte pagine introduttive	Sono state aggiunte pagine introduttive.	12 agosto 2022
Aggiunte nuove AWS politica gestita ROSAManageSubscription	Novità AWS è ROSAManageSubscription stata aggiunta una politica gestita.	11 aprile 2022

Versione iniziale	La versione iniziale di Servizio Red Hat OpenShift su AWS Guida per l'utente.	24 marzo 2021

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