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 distribuire applicazioni containerizzate con la piattaforma Red Hat Enterprise Kubernetes. OpenShift AWS ROSA semplifica lo spostamento dei OpenShift carichi di lavoro Red Hat on-premise verso e offre una stretta integrazione con altri. AWS Servizi AWS

Funzionalità

ROSA è supportato e gestito congiuntamente da e Red Hat. AWS Ogni ROSA cluster è dotato del supporto Red Hat Site Reliability Engineer (SRE) 24 ore su 24 per la gestione del cluster, supportato dal contratto di servizio (SLA) con uptime del 99,95% di Red Hat. 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 supportati da Red Hat SRE.
- Servizio AWS le integrazioni includono AWS elaborazione, database, analisi, machine learning, networking e dispositivi mobili.
- Esegui e ridimensiona il piano di controllo Kubernetes su più zone di disponibilità per garantire un' AWS elevata disponibilità.
- Gestisci i cluster utilizzando strumenti di produttività per sviluppatori, tra cui Service Mesh, CodeReady Workspaces OpenShift APIs e Serverless.

Accedere ROSA

È possibile definire e configurare le distribuzioni dei ROSA servizi utilizzando le seguenti interfacce.

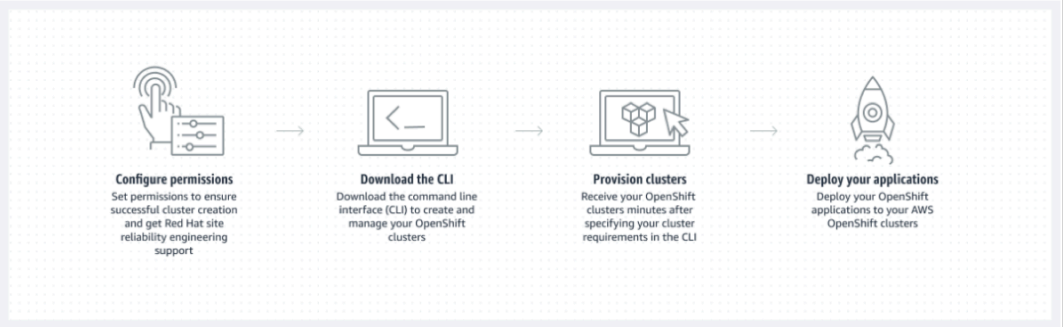
AWS

- ROSA console: fornisce un'interfaccia web per abilitare l' ROSA abbonamento e acquistare un ROSA contratto software.
- AWS Command Line Interface (AWS CLI) — Fornisce comandi per un ampio set 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 i cluster, installare componenti aggiuntivi del cluster e creare e distribuire applicazioni in un cluster. ROSA
- 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 OpenShift con componenti serverless, come Knative Serving ed Eventing.
- Pipelines CLI (tkn): fornisce comandi per interagire OpenShift con Pipelines utilizzando il terminale.
- opm CLI: fornisce comandi che aiutano gli sviluppatori di operatori e gli amministratori del cluster a creare e OpenShift gestire i cataloghi degli operatori dal terminale.
- Operator SDK CLI: fornisce comandi che uno sviluppatore Operator può utilizzare per creare, testare e implementare OpenShift un operatore.

Come iniziare con ROSA



Di seguito viene riepilogato il processo introduttivo di ROSA. Per istruzioni introduttive dettagliate, consultaInizia con ROSA .

Console di gestione AWS/AWS CLI

1. Configura le autorizzazioni su Servizi AWS cui ROSA si basa l'erogazione delle funzionalità del servizio. Per ulteriori informazioni, consulta the section called “Prerequisiti”.
2. Installa e configura lo strumento più recente AWS CLI . Per ulteriori informazioni, consulta Installazione dell'aggiornamento della versione più recente di AWS CLI nella Guida per l' AWS CLI utente.

3. Abilita ROSA nella ROSA console.

ROSA Console/CLI Red Hat Hybrid Cloud

1. Scarica l'ultima versione della ROSA CLI e della OpenShift CLI dalla Red Hat Hybrid Cloud Console. Per maggiori informazioni, consulta Guida introduttiva alla ROSA CLI nella documentazione di Red Hat.
2. Crea ROSA cluster nella Red Hat Hybrid Cloud Console o con la 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 cluster nello stesso modo in cui faresti con qualsiasi altro OpenShift ambiente.

Prezzi

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

ROSA costi di servizio

Per impostazione predefinita, i costi di ROSA servizio vengono addebitati su richiesta a una tariffa oraria per 4 vCPU utilizzate dai nodi di lavoro. I costi di servizio sono uniformi in tutte le regioni standard supportate AWS . Oltre al costo del servizio worker node, i cluster ROSA con piani di controllo ospitati (HCP) prevedono 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 ospitate sull'infrastruttura AWS 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 dei clienti per il servizio gestito Servizio Red Hat OpenShift su AWS (ROSA). Per ulteriori informazioni sui componenti ROSA e sui relativi componenti, consultate Policies and service definition nella documentazione di Red Hat.

Il modello di responsabilitàAWS condivisa definisce la AWS responsabilità di proteggere l'infrastruttura che gestisce tutti i servizi offerti nel Cloud AWS, inclusi ROSA. AWS l'infrastruttura include l'hardware, il software, la rete e le strutture che eseguono Cloud AWS i servizi. Questa AWS responsabilità viene comunemente definita «sicurezza del cloud». Per operare ROSA come servizio completamente gestito, Red Hat e il cliente sono responsabili degli elementi del servizio che il modello di AWS responsabilità definisce come «sicurezza nel cloud».

Red Hat è responsabile della gestione e della sicurezza continue dell'infrastruttura del ROSA cluster, della piattaforma applicativa sottostante e del sistema operativo. Sebbene ROSA i cluster siano ospitati su AWS risorse del cliente Account AWS, i componenti del ROSA servizio e gli ingegneri di Red Hat Site Reliability vi accedono in remoto (SREs) attraverso 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 della gestione della ROSA rete, della registrazione dei cluster, del controllo delle versioni del cluster e della gestione della capacità. Mentre Red Hat gestisce il ROSA servizio, il cliente è pienamente responsabile della gestione e della protezione di tutte le applicazioni, i carichi di lavoro e i dati distribuiti. ROSA

Panoramica di

La tabella seguente fornisce una panoramica delle responsabilità di AWS Red Hat e 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	Cliente
Applicazioni per i clienti	Customer	Customer	Customer	Customer	Cliente
Servizi per sviluppatori	Customer	Customer	Customer	Customer	Cliente
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/ infrastruttura globale AWS	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 dei ROSA componenti. Questa documentazione definisce le responsabilità di ROSA servizio per area e attività.

Gestione degli incidenti e delle operazioni

AWS è responsabile della protezione dell'infrastruttura hardware che gestisce tutti i servizi offerti in 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 Red Hat AWS e Red Hat.
Gestione delle reti virtuali	Red Hat • Monitora i sistemi di bilanciamento del AWS carico, le Amazon VPC sottoreti e i Servizio AWS componenti necessari per il networking della piattafor ma predefinita. Rispondi agli avvisi.	Cliente • Monitora lo stato degli endpoint del sistema di AWS bilanciamento del carico. • Monitora il traffico di rete configurato opzionalm ente tramite connessione Amazon VPC-to-VPC, Site-to-Site VPN connessione o Direct Connect per potenzial i problemi o minacce alla sicurezza.
Gestione dello storage virtuale	Red Hat • Monitora Amazon EBS i volumi utilizzati per i nodi del cluster e Amazon S3 i bucket utilizzati per il registro delle immagini dei container integrato nel ROSA servizio. Rispondi agli avvisi.	Cliente • Monitora lo stato dei dati delle applicazioni. • Se AWS KMS keys si utilizza Customer Managed, è possibile creare e controllare il ciclo di vita delle chiavi e le politiche

Risorsa	Responsabilità di servizio	Responsabilità del cliente
		chiave per la Amazon EBS crittografia.
AWS software (pubblico) Servizi AWS	AWS • Per informazioni sulla gestione AWS degli incidenti e delle operazioni, vedi Come AWS mantiene la resilienza operativa e la continuità del servizio nel AWS white paper.	Cliente • Monitora lo stato delle AWS risorse nell'account cliente. • Utilizza IAM gli strumenti per applicare le autorizza zioni appropriate alle AWS risorse dell'account cliente.
Hardware/infrastruttura globale AWS	AWS • Per informazioni sulla gestione AWS degli incidenti e delle operazioni, vedi Come AWS mantiene la resilienza operativa e la continuità del servizio nel white paper. AWS	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 in. 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

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.	• Installa l'operatore di registrazione dell'appl icazione predefinito opzionale sul cluster. • Installa, configura e gestisci qualsiasi soluzione opzionale di registrazione delle app, ad esempio contenitori collaterali per la registrazione o applicazi oni 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 i componenti OpenShift SDN 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 di 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 inoltro DNS necessarie.

Risorsa	Responsabilità del servizio	Responsabilità del cliente
Rete in cluster	Red Hat • Configura i componenti di gestione del cluster, come gli endpoint dei servizi pubblici o privati e l'integrazione necessaria con Amazon VPC i 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 il CIDR della macchina, il CIDR del servizio e il pod CIDR, se necessario, tramite OpenShift Cluster Manager al momento del provisioning del cluster. • Richiedi che l'endpoint del servizio API sia reso pubblico o privato al momento della creazione del cluster o dopo la creazione del cluster tramite Cluster Manager. OpenShift

Risorsa	Responsabilità del servizio	Responsabilità del cliente
Gestione delle reti virtuali	Red Hat • Imposta e configura Amazon VPC i 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 la Site-to-Site VPN connettività con risorse locali, connettività Amazon VPC a VPC e, se necessari o, tramite Direct Connect OpenShift Cluster Manager. • Consenti ai clienti di creare e implementare sistemi di AWS bilanciamento del carico da utilizzare con i service load balancer.	Cliente • Configura e gestisci Amazon VPC component i opzionali, ad esempio connessione Amazon VPC-to-VPC, Site-to-Site VPN connessione o. Direct Connect • Richiedi e configura eventuali bilanciatori di carico aggiuntivi per servizi specifici.
Gestione dell'elaborazione virtuale	Red Hat • Imposta e configura il piano ROSA di controllo e il piano dati per utilizzare Amazon EC2 le istanze per il calcolo del cluster. • Monitora e gestisci l'implementazione del piano di Amazon EC2 controllo e dei nodi dell'infrastruttura sul cluster.	Cliente • Monitora e gestisci i Amazon EC2 nodi di lavoro creando un pool di macchine utilizzando OpenShift Cluster Manager o ROSA CLI. • Gestisci le modifiche alle applicazioni e ai dati delle applicazioni distribuite dai clienti.

Risorsa	Responsabilità del servizio	Responsabilità del cliente
Versione del cluster	Red Hat • Abilita il processo di pianificazione degli aggiornamenti. • Monitora l'avanzamento dell'aggiornamento e risolvi eventuali problemi riscontrati. • Pubblica i registri delle modifiche e le note di rilascio per aggiornamenti minori e di manutenzione.	Cliente • Pianifica gli aggiornamenti delle versioni di manutenzione 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 secondarie 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 • Imposta e configura Amazon EBS per il provisioning dello storage su nodi locali e dello storage su volumi persistenti per il cluster. • Imposta e configura il registro delle immagini integrato per utilizzare lo storage Amazon S3 con bucket. • Potenzia regolarmente le risorse del registro delle immagini Amazon S3 per ottimizzare l' Amazon S3 utilizzo e le prestazioni del cluster.	Cliente • Facoltativamente, configura il driver Amazon EBS CSI o il driver Amazon EFS CSI per effettuare il provisioning di volumi persistenti sul cluster.

Risorsa	Responsabilità del servizio	Responsabilità del cliente

AWS software (servizi pubblici) AWS	AWS
	
	Calcolo
	
	• Fornisci il Amazon EC2 servizio, utilizzato per il piano ROSA di controllo , l'infrastruttura e i nodi di lavoro.
	
	Storage
	
	• Amazon EBS Fornire per consentire al ROSA servizio di fornire lo storage su nodi locali e lo storage di volumi persistenti per il cluster.
	
	Reti
	
	• Fornisci i seguenti Cloud AWS servizi per soddisfare le esigenze dell'infrastruttura di rete ROSA virtuale:
	  • Amazon VPC
	  • Elastic Load Balancing
	  • IAM
	• Fornisci le seguenti Servizio AWS integrazioni opzionali per ROSA:
	  • Site-to-Site VPN
	  • Direct Connect
	  • AWS PrivateLink
		Cliente
		
		• Firma le richieste utilizzan do un ID chiave di accesso e una chiave di accesso segreta associata a credenziali di sicurezza IAM principali o AWS STS temporanee.
		• Specificare le sottoreti VPC per il cluster da utilizzare durante la creazione del cluster.
		• Configura facoltativamente un VPC gestito dal cliente per l'utilizzo con i cluster. ROSA

Risorsa	Responsabilità del servizio	Responsabilità del cliente
	• AWS Transit Gateway	
AWS Hardware/infrastruttura globale	AWS • Per informazioni sui controlli di gestione per AWS i data center, consulta la pagina I nostri controlli sulla Cloud AWS sicurezza. • Per informazioni sulle migliori pratiche di gestione delle modifiche, consulta la Guida per la gestione delle modifiche AWS nella Libreria delle AWS 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. • Fornisci OpenShift funzionalità RBAC native.	Cliente • Configura OpenShift RBAC per controllare l'accesso ai progetti e, per estensione, i log delle applicazioni di un progetto. • Per le soluzioni di registrazione 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 funzionalità e OpenShift `dedicated-admin` RBAC nativi.	Cliente • Configure OpenShift `dedicated-admin` e RBAC per 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 funzionalità e OpenShift `dedicated-admin` RBAC nativi.	Cliente • Configure OpenShift `dedicated-admin` e RBAC per 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 ai 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 ai AWS componenti tramite OpenShift Cluster Manager. • Crea IAM i ruoli e le politiche allegate necessari per abilitare l'accesso al ROSA 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 ai AWS componenti tramite OpenShift Cluster Manager. • Crea IAM i ruoli e le politiche allegate necessari per abilitare l'accesso al ROSA servizio.

Risorsa	Responsabilità di servizio	Responsabilità del cliente
AWS software (AWS servizi pubblici)	AWS Calcolo • Fornisci il Amazon EC2 servizio, utilizzato per il piano ROSA di controllo , l'infrastruttura e i nodi di lavoro. Storage • Fornisce Amazon EBS, utilizzato ROSA per consentire il provisioning dello storage su nodi locali e dello storage di volumi persistenti per il cluster. • Amazon S3 Fornisce, utilizzato per il registro delle immagini integrato nel servizio. Reti • Provide AWS Identity and Access Management (IAM), utilizzato dai clienti per controllare l'accesso alle ROSA risorse in esecuzione sugli account dei clienti.	Cliente • Crea IAM i ruoli e le politiche allegate necessari per consentire l'accesso al ROSA servizio. • Utilizza IAM gli strumenti per applicare le autorizza zioni appropriate alle AWS risorse dell'account cliente. • Per garantire l' ROSA operatività in tutta l' AWS organizzazione, il cliente è responsabile della gestione degli AWS Organizations amministratori. • A fini di attivazione ROSA in tutta l' AWS organizza zione, il cliente è responsab ile della distribuzione della ROSA concessione di diritto utilizzando. AWS License Manager

Risorsa	Responsabilità di servizio	Responsabilità del cliente
Hardware/infrastruttura globale AWS	AWS • Per informazioni sui controlli fisici degli accessi per AWS i data center, consulta la pagina I nostri controlli sulla Cloud AWS sicurezza.	Cliente • Il cliente non è responsab ile dell'infrastruttura AWS 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 ti opzionali per potenzial

Risorsa	Responsabilità di servizio	Responsabilità del cliente
	i problemi e minacce alla sicurezza. • Utilizza AWS strumenti pubblici per un monitoraggio e una protezione aggiuntivi.	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. • Utilizza AWS strumenti pubblici per un monitoraggio e una 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. • Utilizza AWS strumenti pubblici per un monitoraggio e una protezione aggiuntivi. • Per impostazione predefinita, configura il ROSA servizio per crittografare i dati del piano di controllo, dell'infrastruttura e del volume del nodo di lavoro utilizzando la chiave KMS AWS gestita che Amazon EBS fornisce. • Configura il ROSA servizio per crittografare i volumi persistenti dei clienti che utilizzano la classe di storage predefinita con la chiave KMS AWS gestita che fornisce. Amazon EBS • Offri al cliente la possibilità di utilizzare un client gestito per KMS key crittografare i volumi persistenti. • Configura il registro delle immagini del contenitore per crittografare i dati del registro delle immagini inattivi utilizzando la	Cliente • Amazon EBS Volumi di fornitura. • Gestisci lo storage di Amazon EBS volume per assicurarti 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 chiavi Amazon S3 gestite (SSE-3). • Offri al cliente la possibili tà di creare un registro di immagini pubblico o privato per proteggere le Amazon S3 immagini del contenitore dall'accesso non autorizzato degli utenti.	

Risorsa	Responsabilità di servizio	Responsabilità del cliente
AWS software (AWS servizi pubblici)	AWS Calcolo • Fornisce Amazon EC2, utilizzato per ROSA il piano di controllo, l'infrastruttura e i nodi di lavoro. Per ulteriori informazioni, consulta la sezione Sicurezza dell'infrastruttura Amazon EC2 nella Guida Amazon EC2 per l'utente. Storage • Provide Amazon EBS, utilizzato per i volumi ROSA del piano di controllo, dell'infrastruttura e dei nodi di lavoro, nonché per i volumi persistenti di Kubernetes. Per ulteriori informazioni, consulta la sezione Protezione dei dati Amazon EC2 nella Guida per l' Amazon EC2 utente. • Provide AWS KMS, che ROSA consente di crittografare i volumi del piano di controllo, dell'infrastruttura e dei nodi di lavoro e i volumi persistenti. Per ulteriori informazioni, vedere la Amazon EBS crittografia	Cliente • Assicurati che vengano seguite le migliori pratiche di sicurezza e il principio del privilegio minimo per proteggere i dati sull'istanza. Amazon EC2 Per ulteriori informazioni, consulta Sicurezza dell'infrastruttura in Amazon EC2 e Protezione dei dati in Amazon EC2. • Monitora i componenti di rete virtuali configurati opzionali per individuare 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 chiave KMS opzionale gestita dal cliente e crittografa il volume Amazon EBS persistente utilizzando la chiave KMS. • Monitora i dati dei clienti nello storage virtuale per potenziali problemi e minacce alla sicurezza. Per ulteriori informazioni, consultare il AWS Shared Responsibility Model

Risorsa	Responsabilità di servizio	Responsabilità del cliente
	nella Guida per l' Amazon EC2 utente. • Provide Amazon S3, utilizzato per il registro delle immagini dei container integrato nel servizio ROSA. Per ulteriori informazioni, consulta Amazon S3 la sezione Sicurezza nella Guida Amazon S3 per l'utente. Reti • Fornisci funzionalità e servizi di sicurezza per aumentare la privacy e controllare l'accesso alla rete sull'infrastruttura AWS globale, inclusi firewall di rete integrati Amazon VPC, connessioni di rete private o dedicate e crittografia automatica di tutto il traffico sulle reti AWS globali e regionali tra strutture AWS protette. Per ulteriori informazioni, consulta il modello di responsabilitàAWS condivisa e la sicurezza dell'infrastruttura nel white paper Introduzione alla AWS sicurezza.	(Modello di responsabilità condivisa).

Risorsa	Responsabilità di servizio	Responsabilità del cliente
Hardware/infrastruttura globale AWS	AWS • Fornisci l'infrastruttura AWS globale che ROSA utilizza per fornire le funzionalità del servizio. Per ulteriori informazioni sui controlli AWS di sicurezza, consulta la sezione Sicurezza dell' AWS infrastruttura nel AWS white paper. • Fornisci al cliente la documentazione necessari a per gestire le esigenze di conformità e verificarne lo stato di sicurezza AWS utilizzando strumenti come AWS Artifact 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 correttam ente. • Utilizza IAM gli strumenti per applicare le autorizza zioni appropriate alle AWS risorse dell'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.

Risorsa	Responsabilità di servizio	Responsabilità del cliente
		• Mantieni il DNS di failover e il bilanciamento del carico se utilizzi un sistema di bilanciamento del carico globale con più cluster.
Gestione dell'elaborazione virtuale	Red Hat • Monitora il cluster e sostituis ci il piano Amazon EC2 di controllo o i nodi dell'infr astruttura guasti. • Offri al cliente la possibilità di sostituire manualmente o automaticamente i nodi di lavoro guasti.	Cliente • Sostituisci i Amazon EC2 nodi di lavoro guasti modificando la configura zione del pool di macchine tramite OpenShift Cluster Manager o la ROSA CLI.
Gestione dello storage virtuale	Red Hat • Per ROSA i cluster creati con credenziali AWS IAM utente, esegui il backup di tutti gli oggetti Kubernetes sul cluster tramite istantane e di volume orarie, giornalie re e settimanali.	Cliente • Esegui il backup delle applicazioni e dei dati delle applicazioni dei clienti.

Risorsa	Responsabilità di servizio	Responsabilità del cliente
AWS software (AWS servizi pubblici)	AWS Calcolo • Fornisci Amazon EC2 funzionalità che supportano la resilienza dei dati, come Amazon EBS istantanee e. Amazon EC2 Auto Scaling Per ulteriori informazioni, consulta Resilience Amazon EC2 nella Guida per l' Amazon EC2 utente. Storage • Offri la possibilità al ROSA servizio e ai clienti di eseguire il backup del Amazon EBS volume sul cluster tramite istantanee Amazon EBS del volume. • Per informazioni sulle Amazon S3 funzionalità che supportano la resilienza dei dati, consulta Resilience in. Amazon S3 Reti • Per informazioni sulle Amazon VPC funzionalità che supportano la resilienz a dei dati, consulta Resilienc e Amazon Virtual Private	Cliente • Configura i cluster ROSA Multi-AZ per migliorare la tolleranza agli errori e la disponibilità dei cluster. • Esegui il provisioning di volumi persistenti utilizzan do il driver Amazon EBS CSI per abilitare le istantane e dei volumi. • Crea istantanee di volume CSI di volumi persistenti. Amazon EBS

Risorsa	Responsabilità di servizio	Responsabilità del cliente
	Cloud nella Guida per l'utente. Amazon VPC	
Hardware/infrastruttura globale AWS	AWS • Fornisci un'infrastruttura AWS globale che ROSA consenta di scalare il piano di controllo, l'infrastruttura e i nodi di lavoro tra le zone di disponibilità. Questa funzionalità consente di ROSA 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 i cluster ROSA 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 su cui vengono distribuiti. Servizio Red Hat OpenShift su AWS Tuttavia, AWS Red Hat fornisce vari strumenti per aiutare il cliente a gestire i dati e le applicazioni sulla piattaforma.

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

Risorsa	In che modo AWS e Red Hat aiuta	Responsabilità del cliente
	crittografia dei dati definiti 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 i servizi di dati, Amazon RDS ad esempio per archiviare e gestire i dati all'esterno del cluster e/o AWS. AWS • Amazon RDS Fornire per consentire ai clienti di archiviare e gestire i dati all'esterno del cluster.	i sulla piattaforma e del modo in cui le applicazioni dei clienti utilizzano ed espongono questi dati.

Risorsa	In che modo 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 può utilizzare per configurare gli operatori per aggiungere servizi Red Hat AWS, di community e di terze parti 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

Risorsa	In che modo AWS e Red Hat aiuta	Responsabilità del cliente
	per distribuire e gestire le applicazioni. AWS • Fornisci Amazon EBS il supporto di volumi persistenti da utilizzare con le applicazioni dei clienti. • Amazon S3 Fornire supporto al provisioning Red Hat del registro delle immagini dei container.	cliente, servire esternamente, salvare, eseguire il backup e ripristinare i dati e gestire in altro modo i carichi di lavoro ad alta disponibilità e resilienza. • Mantieni la responsabilità 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 nell'applicazione.

ROSA 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

ROSA con HCP offre un'architettura del piano di controllo più efficiente che aiuta a ridurre i costi di AWS infrastruttura sostenuti durante l'esecuzione ROSA e consente tempi di creazione dei cluster più rapidi. Sia ROSA with HCP che ROSA classic possono essere abilitati nella console. AWS ROSA Hai la possibilità di selezionare l'architettura che desideri utilizzare quando esegui il provisioning dei ROSA cluster utilizzando la ROSA CLI.

> **Note**
>
> ROSA con piani di controllo ospitati (HCP) offre le certificazioni di conformità FedRAMP High e HIPAA Qualified. Per ulteriori informazioni, consulta la sezione Compliance nella documentazione di Red Hat.

Confronto tra ROSA e HCP e ROSA classic

La tabella seguente mette a confronto ROSA con i modelli di architettura classica HCP e ROSA.

	ROSA con HCP	ROSA classica
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 nel VPC del cliente.
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
Nodi dell'infrastruttura	Non utilizza nodi di infrastru ttura dedicati. I component i 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 piattafor ma, il registro delle immagini	Il monitoraggio della piattafor ma, il registro delle immagini

	ROSA con HCP	ROSA classica
	e il controller di ingresso vengono implementati nei nodi di lavoro.	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 contempor aneamente.
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 disponibi lità, consulta Servizio Red Hat OpenShift su AWS endpoint e quote nella Guida di riferimen to 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 "Creare un cluster ROSA HCP - CLI"- Crea il tuo primo cluster ROSA con HCP utilizzando AWS STS e la ROSA CLI.
- the section called "Crea un cluster ROSA classic - AWS PrivateLink "- Crea il tuo primo cluster ROSA classic utilizzando. AWS PrivateLink
- the section called "Crea un cluster ROSA classic - CLI"- Crea il tuo primo cluster ROSA classic utilizzando AWS STS e la 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 CLI e la ROSA CLI di OpenShift Container Platform più recenti. Per ulteriori informazioni, consulta Guida introduttiva alla 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 Supporto, consulta la Supporto 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 nell'SCP senza restrizioni. Per ulteriori informazioni, consulta the section called "AWS Organizations la politica di controllo del servizio nega le autorizzazioni richieste Marketplace AWS". Per ulteriori informazioni in merito SCPs, 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, consulta il link: accounts/latest/reference/ manage

Abilita ROSA e configura i AWS prerequisiti

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 e delle quote di servizio necessarie 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 collegato al servizio ELB, apri una nuova sessione terminale per crearne una prima utilizzando la CLI. ROSA cluster ROSA

Crea un cluster ROSA con HCP utilizzando la CLI ROSA

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

La ROSA CLI utilizza la `auto` modalità o la `manual` modalità per creare IAM le risorse e la configurazione OpenID Connect (OIDC) necessarie per creare un. ROSA cluster`auto`mode crea automaticamente i IAM ruoli e le politiche richiesti e il provider OIDC. `manual`mode emette i AWS CLI comandi necessari per creare le IAM risorse manualmente. Utilizzando `manual` mode, è possibile rivedere i AWS CLI comandi generati prima di eseguirli manualmente. Con `manual` la modalità, 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 ROSA CLI per creare le IAM risorse richieste e la configurazione OIDC per ROSA con HCP. Per ulteriori opzioni per iniziare, consulta. Inizia con ROSA

Argomenti

Prerequisiti

Completa le azioni preliminari elencate inthe section called "Configurazione".

Creare un'architettura Amazon VPC

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

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

Example

Terraform

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

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

3. Vai alla directory creata.

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

4. Avvia il file Terraform.

   ```
   terraform init
   ```

   Una volta completata, la CLI restituisce un messaggio indicante che Terraform è stato inizializzato con successo.

5. Per creare un piano Terraform basato sul modello esistente, esegui il seguente comando. Regione AWS Deve essere specificato. Facoltativamente, è possibile scegliere di specificare un nome di 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 README del repository VPC di Terraform.

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

```
terraform apply rosa.tfplan
```

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

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

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

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

```
echo $SUBNET_IDS
```

Amazon VPC console

1. Apri la Amazon VPC console.
2. Nella scheda VPC, scegli Create VPC (Crea modulo VPC).
3. Per Risorse da creare, scegli VPC e altro.
4. Per creare tag dei nomi per le risorse VPC, tieni selezionata Generazione automatica dei tag dei nomi altrimenti deselezionala per scegliere autonomamente tag dei nomi per le risorse VPC.
5. Per il blocco IPv4 CIDR, inserisci un intervallo di IPv4 indirizzi per il VPC. Un VPC deve avere un intervallo di IPv4 indirizzi.
6. (Facoltativo) Per supportare il IPv6 traffico, scegli il blocco IPv6 CIDR, il blocco CIDR fornito da Amazon IPv6 .

7. Lascia Tenancy come. `Default`
8. Per Numero di zone di disponibilità (AZs), scegli il numero che desideri. Per le implementazioni Multi-AZ, sono ROSA necessarie tre zone di disponibilità. Per scegliere le AZs sottoreti, espandi Personalizza. AZs

   > **Note**
   >
   > Alcuni tipi di ROSA istanze sono disponibili solo in zone di disponibilità selezionate. È possibile utilizzare il `rosa list instance-types` comando ROSA CLI per elencare tutti i tipi di ROSA istanze disponibili. Per verificare se un tipo di istanza è disponibile per una determinata zona di disponibilità, usa il 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 delle sottoreti, espandi Personalizza i blocchi CIDR delle sottoreti.

   > **Note**
   >
   > ROSA con 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 IPv4, per i gateway NAT, scegliete il numero di gateway NAT AZs in cui creare i gateway NAT. In fase di produzione, è preferibile implementare un gateway NAT in ogni zona di disponibilità con risorse che richiedono l'accesso alla rete Internet pubblica.
11. (Facoltativo) Se devi accedere Amazon S3 direttamente dal tuo VPC, scegli gli endpoint VPC, S3 Gateway.
12. Lascia selezionate le opzioni DNS predefinite. ROSA richiede il supporto del nome host DNS sul 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. Seleziona Crea VPC.

AWS CLI

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

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

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

```
vpc-1234567890abcdef0
```

2. Memorizza l'ID VPC in una variabile di ambiente.

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

3. Crea un `Name` tag per il VPC, utilizzando la variabile di `VPC_ID` ambiente.

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

4. Abilita il supporto dei nomi host DNS sul VPC.

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

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

> **Important**
>
> ROSA con 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**
>
> Alcuni tipi di ROSA istanze sono disponibili solo in zone di disponibilità selezionate. È possibile utilizzare il `rosa list instance-types` comando ROSA CLI per elencare tutti i tipi di ROSA istanze disponibili. Per verificare se un tipo di istanza è disponibile per una determinata zona di disponibilità, usa il 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 sottoreti VPC. 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. IDs Memorizza 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 al VPC.

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

11. Associate la tabella delle rotte pubbliche alla sottorete pubblica e configurate 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 gateway NAT 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 gateway NAT.

```
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.

Creare i IAM ruoli richiesti e la configurazione OpenID Connect

Prima di creare un cluster ROSA con HCP, è necessario creare i IAM ruoli e le politiche necessari e la configurazione OpenID Connect (OIDC). Per ulteriori informazioni sui IAM ruoli e le politiche di ROSA con HCP, vedere. the section called " AWS politiche gestite"

Questa procedura utilizza la `auto` modalità ROSA CLI per creare automaticamente la configurazione OIDC necessaria per creare un cluster ROSA con HCP.

1. Crea i ruoli e le politiche dell' IAM account richiesti. 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, la ROSA CLI emette 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 accesso offline scaduti della ROSA CLI"

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 configurazione OIDC fornito nell'output della ROSA CLI. L'ID di configurazione OIDC deve essere fornito in seguito per creare il cluster ROSA con HCP.
4. Per verificare le configurazioni OIDC disponibili per i cluster associati all'organizzazione degli utenti, esegui il comando seguente.

```
rosa list oidc-config
```

5. Crea i ruoli IAM operatore richiesti, sostituendoli `<OIDC_CONFIG_ID>` con l'ID di configurazione OIDC copiato in precedenza.

   Example

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

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

6. Per verificare che i ruoli IAM dell'operatore siano stati creati, esegui il comando seguente:

```
rosa list operator-roles
```

Crea un cluster ROSA con HCP utilizzando la ROSA CLI e AWS STS

È possibile creare un ROSA con HCP cluster utilizzando AWS Security Token Service (AWS STS) e la `auto` modalità fornita nella ROSA CLI. Hai la possibilità di creare un cluster con un'API pubblica e Ingress o un'API privata e Ingress.

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

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

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

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

2. cluster Controlla lo stato del tuo.

```
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 il Supporto nostro supporto Red Hat per ricevere assistenza, consultathe section called "Ottenere supporto".

3. Tieni traccia dello stato di avanzamento della cluster creazione guardando i log dell' OpenShift installatore.

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

Configura un provider di identità e concedi l'accesso cluster

ROSA include un OAuth server integrato. Dopo la creazione, cluster è necessario configurare l'utilizzo OAuth di un provider di identità. Puoi quindi aggiungere utenti al tuo provider di identità configurato per concedere loro l'accesso al tuo cluster. Puoi concedere a questi utenti `cluster-admin` o `dedicated-admin` autorizzazioni come richiesto.

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

> **Important**
>
> Il provider di HTPasswd identità è incluso solo per consentire la creazione di un singolo utente amministratore statico. HTPasswd non 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 hai un' GitHub organizzazione da utilizzare per la fornitura di identità per la tua cluster azienda, creane una. Per ulteriori informazioni, consulta i passaggi indicati nella GitHub documentazione.
3. Utilizzando la modalità interattiva della 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 l' cluster accesso ai membri della tua organizzazione. GitHub

```
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 l'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 aggiungendolo al provider di identità configurato.

La procedura seguente aggiunge un utente a un' GitHub organizzazione configurata per la fornitura di identità al cluster.

1. Vai su github.com e accedi al tuo account. GitHub
2. Invita gli utenti che richiedono cluster l'accesso alla tua organizzazione. GitHub Per ulteriori informazioni, consulta Invitare gli utenti a unirsi alla propria organizzazione nella GitHub documentazione.

Configurazione delle autorizzazioni **`cluster-admin`**

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>
```

Configurazione delle autorizzazioni **`dedicated-admin`**

1. Concedi le `dedicated-admin` autorizzazioni utilizzando il comando seguente. 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. Verificate che l'utente sia elencato come membro del `cluster-admins` gruppo.

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

Accedi a cluster tramite la Red Hat Hybrid Cloud Console

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

1. Ottieni l'URL della console cluster utilizzando il seguente comando. Sostituiscilo `<CLUSTER_NAME>` con il nome del tuo cluster.

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

2. Vai all'URL della console 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 Source-to-Image applicazione.

> **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 l'URL del percorso 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 nome utente. cluster

```
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 nome utente. cluster

```
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

È possibile revocare cluster l'accesso a un utente del provider di identità rimuovendolo dal provider di identità configurato.

Puoi configurare diversi tipi di provider di identità per il tuo. cluster La procedura seguente revoca cluster l'accesso a 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 delle risorse

È possibile utilizzare la ROSA CLI per eliminare un messaggio cluster che utilizza AWS Security Token Service ()AWS STS. Puoi anche utilizzare la ROSA CLI per eliminare i IAM ruoli e il provider OIDC creati da. ROSA Per eliminare le IAM politiche create da ROSA, puoi utilizzare la console. IAM

> **Note**
>
> IAM i ruoli e le politiche creati da ROSA potrebbero essere utilizzati da altri ROSA cluster nello stesso account.

1. Elimina 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**
>
> È necessario attendere l' cluster eliminazione completa prima di rimuovere i IAM ruoli, le politiche e il provider OIDC. I ruoli IAM dell'account sono necessari per eliminare le risorse create dal programma di installazione. I ruoli IAM dell'operatore sono necessari per ripulire le risorse create dagli OpenShift operatori. Gli operatori utilizzano il provider OIDC per l'autenticazione.

2. Eliminare il provider OIDC utilizzato cluster dagli operatori per l'autenticazione eseguendo il comando seguente.

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

3. Eliminare i ruoli degli operatori specifici del cluster. IAM

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

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

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

5. Elimina le IAM politiche create da. ROSA
   a. Accedi alla console di IAM.
   b. Nel menu a sinistra, sotto 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 policy IAM per cluster.

Crea un cluster ROSA classic utilizzando la ROSA CLI

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

La ROSA CLI utilizza la `auto` modalità o la `manual` modalità per creare IAM le risorse necessarie per il provisioning a. ROSA cluster`auto`mode crea immediatamente i IAM ruoli e le politiche richiesti e un provider OpenID Connect (OIDC). `manual`mode emette i AWS CLI comandi necessari per creare le risorse. IAM Utilizzando `manual` mode, è possibile rivedere i AWS CLI comandi generati prima di eseguirli manualmente. Con `manual` la modalità, 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 classic utilizzando la ROSA CLI e AWS STS
- Configura un provider di identità e concedi l'accesso cluster
- Concedi all'utente l'accesso a un cluster
- Configurazione delle autorizzazioni cluster-admin
- Configurazione delle autorizzazioni dedicated-admin
- Accedi a cluster tramite la Red Hat Hybrid Cloud Console
- 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 delle risorse

Prerequisiti

Completa le azioni preliminari elencate inthe section called "Configurazione".

Crea un cluster ROSA classic utilizzando la ROSA CLI e AWS STS

È possibile creare un classico ROSA cluster utilizzando la ROSA CLI e. AWS STS

1. Crea i ruoli e le politiche IAM dell'account richiesti utilizzando `--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, la ROSA CLI emette 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 accesso offline scaduti della ROSA CLI"
2. Crea un file 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 automaticamente i IAM ruoli operatore specifici del cluster e il provider OIDC. Gli operatori utilizzano il provider OIDC per l'autenticazione.

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

- ```
  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 crittografia Amazon EBS predefinita che crittografa i volumi etcd.

> **Note**
>
> Dopo aver eseguito la `manual` modalità di creazione del cluster, è necessario creare manualmente i ruoli IAM dell'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 il Supporto nostro supporto Red Hat per ricevere assistenza, consultathe section called "Ottenere supporto".

4. Tieni traccia dello stato di avanzamento della cluster creazione guardando i log dell' OpenShift installatore.

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

Configura un provider di identità e concedi l'accesso cluster

ROSA include un OAuth server integrato. Dopo la creazione, cluster è necessario configurare l'utilizzo OAuth di un provider di identità. Puoi quindi aggiungere utenti al tuo provider di identità configurato per concedere loro l'accesso al tuo cluster. Puoi concedere a questi utenti `cluster-admin` o `dedicated-admin` autorizzazioni come richiesto.

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

> **Important**
>
> Il provider di HTPasswd identità è incluso solo per consentire la creazione di un singolo utente amministratore statico. HTPasswd non 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 hai un' GitHub organizzazione da utilizzare per la fornitura di identità per la tua cluster azienda, creane una. Per ulteriori informazioni, consulta i passaggi indicati nella GitHub documentazione.

3. Utilizzando la modalità interattiva della 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 l' cluster accesso ai membri della tua organizzazione. GitHub

```
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 l'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 aggiungendolo al provider di identità configurato.

La procedura seguente aggiunge un utente a un' GitHub organizzazione configurata per la fornitura di identità al cluster.

1. Vai su github.com e accedi al tuo account. GitHub
2. Invita gli utenti che richiedono cluster l'accesso alla tua organizzazione. GitHub Per ulteriori informazioni, consulta Invitare gli utenti a unirsi alla propria organizzazione nella GitHub documentazione.

Configurazione delle autorizzazioni **`cluster-admin`**

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>
```

Configurazione delle autorizzazioni **`dedicated-admin`**

1. Concedi le `dedicated-admin` autorizzazioni utilizzando il comando seguente. 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. Verificate che l'utente sia elencato come membro del `cluster-admins` gruppo.

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

Accedi a cluster tramite la Red Hat Hybrid Cloud Console

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

1. Ottieni l'URL della console per te cluster usando il seguente comando. Sostituiscilo `<CLUSTER_NAME>` con il nome del tuo cluster.

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

2. Vai all'URL della console 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 tuo 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 Source-to-Image applicazione.

> **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, scegliete l'URL del percorso 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 nome. cluster

```
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 nome utente e nome. cluster

```
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

È possibile revocare cluster l'accesso a un utente del provider di identità rimuovendolo dal provider di identità configurato.

Puoi configurare diversi tipi di provider di identità per il tuo. cluster La procedura seguente revoca cluster l'accesso a 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 delle risorse

È possibile utilizzare la ROSA CLI per eliminare un messaggio cluster che utilizza AWS Security Token Service ()AWS STS. Puoi anche utilizzare la ROSA CLI per eliminare i IAM ruoli e il provider OIDC creati da. ROSA Per eliminare le IAM politiche create da ROSA, puoi utilizzare la console. IAM

> **Important**
>
> IAM i ruoli e le politiche creati da ROSA potrebbero essere utilizzati da altri ROSA cluster nello stesso account.

1. Elimina 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**
>
> È necessario attendere l' cluster eliminazione completa prima di rimuovere i IAM ruoli, le politiche e il provider OIDC. I ruoli IAM dell'account sono necessari per eliminare le risorse create dal programma di installazione. I ruoli IAM dell'operatore sono necessari per ripulire le risorse create dagli OpenShift operatori. Gli operatori utilizzano il provider OIDC per l'autenticazione.

2. Eliminare il provider OIDC utilizzato cluster dagli operatori per l'autenticazione eseguendo il comando seguente.

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

3. Eliminare i ruoli degli operatori specifici del cluster. IAM

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

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

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

5. Elimina le IAM politiche create da. ROSA
   a. Accedi alla console di IAM.
   b. Nel menu a sinistra, sotto 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 policy IAM per cluster.

Crea un cluster ROSA classico che utilizza AWS PrivateLink

I cluster ROSA classic possono essere implementati in diversi modi: pubblici, privati o privati con. AWS PrivateLink Per ulteriori informazioni su ROSA classic, vedere. the section called "Architecture" Sia per cluster le configurazioni pubbliche che private, OpenShift cluster ha accesso a Internet e la privacy è impostata sui carichi di lavoro delle applicazioni a livello di applicazione.

Se desideri che cluster sia il carico di lavoro che quello dell'applicazione siano privati, puoi eseguire la configurazione AWS PrivateLink con ROSA classic. AWS PrivateLink è una tecnologia scalabile e altamente disponibile che ROSA consente di creare una connessione privata tra il ROSA servizio e le risorse del cluster nell'account del AWS 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 all'endpoint del cluster. AWS PrivateLink

Per ulteriori informazioni su AWS PrivateLink, consulta What is? AWS PrivateLink

Argomenti

- Prerequisiti
- Creare un'architettura Amazon VPC
- Crea un cluster ROSA classic utilizzando la ROSA CLI e AWS PrivateLink
- Configura l'inoltro AWS PrivateLink DNS
- Configura un provider di identità e concedi l'accesso cluster
- Concedi all'utente l'accesso a un cluster
- Configurazione delle autorizzazioni cluster-admin
- Configurazione delle autorizzazioni dedicated-admin

- Accedi a cluster tramite la Red Hat Hybrid Cloud Console
- 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 delle risorse

Prerequisiti

Completa le azioni prerequisite elencate inthe section called "Configurazione".

Creare un'architettura Amazon VPC

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

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

Example

Amazon VPC console

1. Apri la Amazon VPC console.
2. Nella scheda VPC, scegli Create VPC (Crea modulo VPC).
3. Per Risorse da creare, scegli VPC e altro.
4. Per creare tag dei nomi per le risorse VPC, tieni selezionata Generazione automatica dei tag dei nomi altrimenti deselezionala per scegliere autonomamente tag dei nomi per le risorse VPC.
5. Per il blocco IPv4 CIDR, inserisci un intervallo di IPv4 indirizzi per il VPC. Un VPC deve avere un intervallo di IPv4 indirizzi.

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

> **Note**
>
> Alcuni tipi di ROSA istanze sono disponibili solo in zone di disponibilità selezionate. È possibile utilizzare il `rosa list instance-types` comando ROSA CLI per elencare tutti i tipi di ROSA istanze disponibili. Per verificare se un tipo di istanza è disponibile per una determinata zona di disponibilità, usa il 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 delle sottoreti, espandi Personalizza i blocchi CIDR delle sottoreti.

> **Note**
>
> ROSA richiede che i clienti configurino almeno una sottorete 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 IPv4, per i gateway NAT, scegli il numero di gateway NAT AZs in cui creare i gateway NAT. In fase di produzione, è preferibile implementare un gateway NAT in ogni zona di disponibilità con risorse che richiedono l'accesso alla rete Internet pubblica.
11. (Facoltativo) Se devi accedere Amazon S3 direttamente dal tuo VPC, scegli gli endpoint VPC, S3 Gateway.
12. Lascia selezionate le opzioni DNS predefinite. ROSA richiede il supporto del nome host DNS sul VPC.
13. Seleziona Crea VPC.

AWS CLI

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

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

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

```
vpc-1234567890abcdef0
```

2. Memorizza l'ID VPC in una variabile di ambiente.

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

3. Crea un `Name` tag per il VPC, utilizzando la variabile di `VPC_ID` ambiente.

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

4. Abilita il supporto dei nomi host DNS sul VPC.

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

5. Crea una sottorete pubblica e privata nel VPC, 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**
>
> Alcuni tipi di ROSA istanze sono disponibili solo in zone di disponibilità selezionate. È possibile utilizzare il `rosa list instance-types` comando ROSA CLI per elencare tutti i tipi di ROSA istanze disponibili. Per verificare se un tipo di istanza è disponibile per una determinata zona di disponibilità, usa il 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. IDs Memorizza 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 al VPC.

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

10. Associate la tabella delle rotte pubbliche alla sottorete pubblica e configurate 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
```

11. Crea il gateway NAT 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 gateway NAT.

```
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 ROSA classic utilizzando la ROSA CLI e AWS PrivateLink

È possibile utilizzare la ROSA CLI e AWS PrivateLink creare una cluster zona di disponibilità singola (Single-AZ) o più zone di disponibilità (Multi-AZ). In entrambi i casi, il valore CIDR della macchina deve corrispondere al valore CIDR del VPC.

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

> **Note**
>
> Se si utilizza un firewall, è necessario configurarlo in modo da ROSA poter accedere ai siti necessari per funzionare.
> Per maggiori informazioni, consulta Requisiti per l'utilizzo AWS PrivateLink dei cluster nella documentazione di Red Hat.

1. Crea i ruoli e le policy degli IAM account richiesti utilizzando `--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, la ROSA CLI emette 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 accesso offline scaduti della ROSA CLI"

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 credenziali AWS PrivateLink with AWS Security Token Service (AWS STS) di breve durata, aggiungi `--sts --mode auto` o `--sts --mode manual` alla fine del comando. `rosa create cluster`

3. Crea i IAM ruoli dell' cluster operatore seguendo le istruzioni interattive.

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

4. Crea il provider OpenID Connect (OIDC) che cluster gli operatori utilizzano per l'autenticazione.

   ```
   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 prima che il cluster `State` campo mostri `ready` lo stato. Se il provisioning fallisce o non viene visualizzato `ready` dopo 40 minuti, consultaRisoluzione dei problemi. Per contattare il Supporto nostro supporto Red Hat per ricevere assistenza, consultathe section called "Ottenere supporto".

6. Tieni traccia dello stato di avanzamento della cluster creazione guardando i log dell' OpenShift installatore.

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

Configura l'inoltro AWS PrivateLink DNS

I cluster che utilizzano AWS PrivateLink creano una zona ospitata pubblica e una zona ospitata privata in. Route 53 I record all'interno della zona ospitata Route 53 privata sono risolvibili solo all'interno del VPC a cui è assegnato.

La convalida DNS-01 di Let's Encrypt 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 sulle zone ospitate AWS private, consulta Lavorare con le zone private. Per ulteriori informazioni sulle zone ospitate pubbliche, consulta Lavorare con le zone ospitate pubbliche.

Configura un Route 53 Resolver endpoint in entrata

1. Per consentire la risoluzione di record come quelli `api.<cluster_domain>` esterni al VPC, configura un endpoint Route 53 Resolver in ingresso. `*.apps.<cluster_domain>`

> **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 ulteriori indirizzi IP in quelle o in altre zone di disponibilità.

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

Configura l'inoltro DNS per il cluster

Dopo che l'endpoint Route 53 Resolver interno è stato associato e reso operativo, configurate l'inoltro DNS in modo che le query DNS possano essere gestite dai server designati sulla rete.

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

Configura un provider di identità e concedi l'accesso cluster

ROSA include un OAuth server integrato. Dopo la creazione, ROSA cluster è necessario configurare l'utilizzo OAuth di un provider di identità. Puoi quindi aggiungere utenti al tuo provider di identità configurato per concedere loro l'accesso al tuo cluster. Puoi concedere a questi utenti `cluster-admin` o `dedicated-admin` autorizzazioni come richiesto.

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

Important

Il provider di HTPasswd identità è incluso solo per consentire la creazione di un singolo utente amministratore statico. HTPasswd non 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 hai un' GitHub organizzazione da utilizzare per la fornitura di identità per la tua ROSA cluster azienda, creane una. Per ulteriori informazioni, consulta i passaggi indicati nella GitHub documentazione.
3. Utilizzando la modalità interattiva della ROSA CLI, configura un provider di identità per il cluster eseguendo il comando seguente.

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

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

```
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 l'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 un cluster

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

La procedura seguente aggiunge un utente a un' GitHub organizzazione configurata per la fornitura di identità al cluster.

1. Vai su github.com e accedi al tuo account. GitHub
2. Invita gli utenti che richiedono cluster l'accesso alla tua organizzazione. GitHub Per ulteriori informazioni, consulta Invitare gli utenti a unirsi alla propria organizzazione nella GitHub documentazione.

Configurazione delle autorizzazioni **`cluster-admin`**

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>
```

Configurazione delle autorizzazioni **`dedicated-admin`**

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

```
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>
```

Accedi a cluster tramite la Red Hat Hybrid Cloud Console

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

1. Ottieni l'URL della console per te cluster usando il seguente comando. Sostituiscilo `<CLUSTER_NAME>` con il nome del tuo cluster.

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

2. Vai all'URL della console 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 tuo 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 Source-to-Image applicazione.

> **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, scegliete l'URL del percorso 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 nome utente. cluster

```
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 nome utente. cluster

```
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

È possibile revocare cluster l'accesso a un utente del provider di identità rimuovendolo dal provider di identità configurato.

Puoi configurare diversi tipi di provider di identità per il tuo. cluster La procedura seguente revoca cluster l'accesso a 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 delle risorse

È possibile utilizzare la ROSA CLI per eliminare un messaggio cluster che utilizza AWS Security Token Service ()AWS STS. Puoi anche utilizzare la ROSA CLI per eliminare i IAM ruoli e il provider OIDC creati da. ROSA Per eliminare le IAM politiche create da ROSA, puoi utilizzare la console. IAM

> **Important**
>
> IAM i ruoli e le politiche creati da ROSA potrebbero essere utilizzati da altri ROSA cluster nello stesso account.

1. Elimina 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**
>
> È necessario attendere l' cluster eliminazione completa prima di rimuovere i IAM ruoli, le politiche e il provider OIDC. I ruoli IAM dell'account sono necessari per eliminare le risorse create dal programma di installazione. I ruoli IAM dell'operatore sono necessari per ripulire le risorse create dagli OpenShift operatori. Gli operatori utilizzano il provider OIDC per l'autenticazione.

2. Eliminare il provider OIDC utilizzato cluster dagli operatori per l'autenticazione eseguendo il comando seguente.

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

3. Eliminare i ruoli degli operatori specifici del cluster. IAM

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

4. Eliminare i ruoli IAM dell'account utilizzando il seguente comando. Sostituiscili <PREFIX> con il prefisso dei ruoli IAM dell'account da eliminare. Se hai specificato un prefisso

personalizzato durante la creazione dei ruoli IAM dell'account, specifica il prefisso predefinitoManagedOpenShift.

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

5. Elimina le IAM politiche create da. ROSA
   a. Accedi alla console di IAM.
   b. Nel menu a sinistra, sotto 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 policy IAM per cluster.

Sicurezza in ROSA

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

La sicurezza è una responsabilità condivisa tra AWS te e te. 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 che gestisce AWS i 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 sicurezza come parte dei programmi di conformitàAWS. Per maggiori informazioni sui programmi di conformità applicabili ROSA, consulta Servizi AWS la sezione Scope by Compliance Program.
- Sicurezza nel cloud: la tua responsabilità è determinata dall'uso Servizio AWS che utilizzi. L'utente è anche responsabile di altri fattori, tra cui la riservatezza dei dati, i requisiti della propria 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 per ROSA soddisfare i tuoi obiettivi di sicurezza e conformità. Imparerai anche a utilizzarne altri Servizi AWS che ti aiutano a monitorare e proteggere ROSA le tue risorse.

Indice

Protezione dei dati in ROSA

La the section called "Responsabilità" documentazione e il modello di responsabilitàAWS condivisa definiscono la protezione dei dati in ROSA. AWS è responsabile della protezione dell'infrastruttura globale che gestisce tutti i 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 ciò che utilizzi. Per ulteriori informazioni sulla privacy dei dati, consulta Domande frequenti sulla privacy dei dati. Per ulteriori informazioni sulla protezione dei dati, consulta il post del blog Modello di responsabilità condivisa di AWS e GDPR sul Blog della sicurezza di AWS .

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

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

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 ROSA o Servizi AWS utilizzi la console, l'API o. AWS CLI AWS SDKs Tutti i dati che inserisci ROSA o altri servizi potrebbero essere raccolti per essere inclusi nei registri di diagnostica. Quando fornisci un URL a un server esterno, non includere informazioni sulle credenziali nell'URL per convalidare la tua richiesta a tale server.

Argomenti

- Protezione dei dati tramite crittografia

Protezione dei dati tramite crittografia

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

Servizio Red Hat OpenShift su AWS fornisce un accesso sicuro a Amazon Elastic Block Store (Amazon EBS) volumi di storage collegati alle Amazon EC2 istanze per il piano di ROSA controllo, l'infrastruttura e i nodi di lavoro, nonché ai 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 l'archiviazione del registro delle immagini dei container, che Amazon S3 per impostazione predefinita è crittografata a riposo.

> **Important**
>
> ROSA Because è un servizio gestito AWS e Red Hat gestisce l'infrastruttura che ROSA utilizza. I clienti non devono tentare di chiudere manualmente le Amazon EC2 istanze ROSA utilizzate dalla AWS console o dalla CLI. 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 storage collegati alle istanze. Amazon EC2

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

Crittografia dei dati per il driver Amazon EBS CSI e il driver Amazon EFS CSI

ROSA per impostazione predefinita utilizza il Amazon EBS driver CSI per il provisioning dello storage. Amazon EBS Il driver Amazon EBS CSI e Amazon EBS CSI Driver Operator sono installati nel cluster per impostazione predefinita nel namespace. `openshift-cluster-csi-drivers` Il driver e l'operatore Amazon EBS CSI 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 il driver CSI e Amazon EFS CSI Driver Operator. Amazon EFS Il Amazon EFS driver e l'operatore consentono inoltre di condividere i dati del file system tra i pod o con altre applicazioni all'interno o all'esterno di Kubernetes.

I dati di volume sono protetti in transito sia per il driver CSI che per il driver Amazon EBS CSI. Amazon EFS Per maggiori informazioni, consulta Using Container Storage Interface (CSI) nella documentazione di Red Hat.

> **Important**
>
> Durante il provisioning dinamico di volumi ROSA persistenti utilizzando il driver Amazon EFS CSI, nella valutazione delle autorizzazioni del file system, Amazon EFS considera l'ID utente, l'ID di gruppo (GID) e il gruppo secondario IDs del punto di accesso. Amazon EFS sostituisce l'utente e il gruppo IDs sui file con l'utente e il gruppo sul punto di accesso e ignora il client IDs NFS. IDs Di conseguenza, ignora Amazon EFS silenziosamente le impostazioni. `fsGroup` ROSA non è in grado di sostituire i GIDs file utilizzando. `fsGroup` Qualsiasi pod in grado di accedere a un punto di Amazon EFS accesso montato può accedere a qualsiasi file sul volume. Per ulteriori informazioni, vedete Lavorare con i punti di Amazon EFS accesso nella Guida Amazon EFS 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 la crittografia etcd nella definizione del ROSA 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, è possibile scegliere di utilizzare la chiave AWS gestita predefinita KMS key fornita da Amazon EBS o specificare 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 dei contenitori tramite Amazon S3 bucket storage. 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, per impostazione predefinita ROSA utilizza la crittografia lato server con chiavi Amazon S3 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 mediante la crittografia lato server con chiavi di crittografia Amazon S3 gestite (SSE-S3) nella Guida per l'utente. Amazon S3

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 usa Amazon Virtual Private Cloud (Amazon VPC) per creare confini tra le risorse del ROSA cluster e controllare il traffico tra queste, la rete locale e Internet. Per ulteriori informazioni sulla Amazon VPC sicurezza, consulta la sezione Privacy del traffico Internet Amazon VPC nella Guida per l' Amazon VPC utente.

All'interno del VPC, puoi configurare ROSA i cluster per utilizzare un server proxy HTTP o HTTPS 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 di rete ai pod del cluster. ROSA Per ulteriori informazioni, consulta the section called “Sicurezza dell’infrastruttura”.

Crittografia dei dati tramite 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 la funzionalità AWS gestita KMS key fornita da Amazon EBS. Questo KMS key ha l'alias`aws/ebs`. Anche i volumi persistenti che utilizzano la classe di archiviazione gp3 predefinita vengono crittografati di default utilizzando questo. KMS key

ROSA I cluster appena creati 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 maggiori informazioni sulle classi di storage ROSA predefinite, consultate Configurazione dello storage persistente nella documentazione di Red Hat.

Durante la creazione del cluster, è possibile scegliere di crittografare i volumi persistenti presenti nel cluster utilizzando la chiave Amazon EBS fornita di default, oppure specificare una soluzione simmetrica gestita dal cliente. KMS keyPer ulteriori informazioni sulla creazione di chiavi, consulta Creazione di chiavi KMS di crittografia simmetrica nella Guida per gli sviluppatori. AWS KMS

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 di conformità e sicurezza durante la distribuzione in. AWS Per maggiori informazioni, consulta Encrypting container persistent volumes on AWS with KMS key a nella documentazione di Red Hat.

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

- Quando utilizzi la crittografia KMS con la tua KMS key, la chiave deve esistere nello Regione AWS stesso del cluster.
- La creazione e l'utilizzo di una soluzione personalizzata KMS keys comportano un costo. Per ulteriori informazioni, consultare Prezzi di AWS Key Management Service.

Gestione delle identità e degli accessi per ROSA

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

Argomenti

- AWS politiche gestite per ROSA
- Risoluzione dei problemi di ROSA identità e accesso

Destinatari

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

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

Amministratore del servizio: se sei responsabile delle ROSA risorse della tua azienda, probabilmente hai pieno accesso a ROSA. È tuo compito determinare a quali ROSA funzionalità e risorse devono accedere gli utenti del servizio. È quindi necessario inviare richieste all' 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 amministratore: se sei un IAM amministratore, potresti voler conoscere i dettagli sulle politiche utilizzate per gestire l'accesso a ROSA. Per visualizzare esempi di policy ROSA basate sull'identità che puoi utilizzare in IAM, consulta. the section called " ROSA esempi di politiche basate sull'identità"

Autenticazione con identità

L'autenticazione è il modo in cui accedi AWS utilizzando le tue credenziali di identità. È necessario autenticarsi (accedere a AWS) come utente Account AWS root Utente IAM, o assumendo un ruolo. IAM

È possibile accedere 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 i ruoli. IAM Quando si accede AWS utilizzando la federazione, si assume indirettamente un ruolo.

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

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

Indipendentemente dal metodo di autenticazione utilizzato, potrebbe essere necessario specificare ulteriori informazioni sulla sicurezza. Ad esempio, ti AWS consiglia di utilizzare l'autenticazione a più fattori (MFA) per aumentare la sicurezza del tuo account. Per ulteriori informazioni, consulta l'autenticazione a più fattori nella Guida per l'utente di AWS IAM Identity Center (successore di AWS Single Sign-On) e Using multi-factor authentication (MFA) AWS nella IAM User Guide.

Account AWS utente root

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

Identità federata

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

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

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

informazioni su IAM Identity Center, consulta Cos'è IAM Identity Center? nella Guida per l' AWS utente di IAM Identity Center (successore di AWS Single Sign-On).

Utenti IAM e gruppi

An Utente IAMè un'identità interna all'utente 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 utenti con credenziali a lungo termine come password e chiavi di accesso. Tuttavia, se hai casi d'uso specifici che richiedono credenziali a lungo termine Utenti IAM, ti consigliamo di ruotare le chiavi di accesso. Per ulteriori informazioni, consulta la pagina Rotazione periodica delle chiavi di accesso per casi d'uso che richiedono credenziali a lungo termine nella Guida per l'utente IAM.

Un IAM gruppo è un'identità che specifica un insieme di. Utenti IAM Non è possibile eseguire l'accesso come gruppo. È possibile utilizzare gruppi per specificare le autorizzazioni per più utenti alla volta. I gruppi semplificano la gestione delle autorizzazioni di set di utenti di grandi dimensioni. Ad esempio, è possibile assegnare un nome a un gruppo IAMAdminse concedere a tale gruppo le autorizzazioni per IAM amministrare le 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 permanenti a lungo termine, ma i ruoli forniscono credenziali temporanee. Per ulteriori informazioni, consulta Quando creare un Utente IAM (anziché un ruolo) nella Guida per l'utente IAM.

IAM ruoli

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

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 ulteriori informazioni sulla federazione dei ruoli, consulta Creazione di un ruolo per un provider di identità

di terza parte nella Guida per l'utente IAM. Se utilizzi IAM Identity Center, configura un set di autorizzazioni. Centro identità IAM mette in correlazione il set di autorizzazioni con un ruolo in IAM per controllare le risorse alle quali le identità possono accedere dopo l'autenticazione. Per informazioni sui set di autorizzazioni, consulta Set di autorizzazioni nella Guida per l'utente di AWS IAM Identity Center (successore del Single Sign-On). AWS

- Utente IAM Autorizzazioni temporanee: An Utente IAM può assumere il IAM ruolo di assumere temporaneamente autorizzazioni diverse per un'attività specifica.
- Accesso su più account: puoi utilizzare un IAM ruolo per consentire a qualcuno (un responsabile 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 conoscere la differenza tra i ruoli e le politiche basate sulle risorse per l'accesso tra account diversi, consulta How IAM roles differiscono dalle policy basate sulle risorse nella IAM User Guide.
- Accesso tra servizi: alcuni utilizzano funzionalità in altri. Servizi AWS Servizi AWS Ad esempio, quando si effettua una chiamata in un servizio, è normale che quel servizio esegua applicazioni Amazon EC2 o in cui memorizzi oggetti. Amazon S3 Un servizio può eseguire questa operazione utilizzando le autorizzazioni dell'entità chiamante, un ruolo di servizio oppure un ruolo collegato al servizio.
  - Sessioni di accesso inoltrato (FAS): quando utilizzi un ruolo Utente IAM or per eseguire azioni in AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra operazione in un servizio diverso. FAS utilizza le autorizzazioni del principale che chiama an Servizio AWS, combinate con la richiesta Servizio AWS per effettuare richieste ai servizi downstream. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli delle policy relative alle richieste FAS, consulta Forward access sessions.
  - Ruolo di servizio: un ruolo di servizio è un IAM ruolo che un servizio assume per eseguire azioni per conto dell'utente. Un IAM amministratore può creare, modificare ed eliminare un ruolo di servizio dall'interno IAM. Per ulteriori informazioni, consulta la sezione 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 per eseguire un'operazione per tuo conto. I ruoli collegati al servizio vengono visualizzati nell' IAM account e sono di proprietà del servizio. Un IAM amministratore può visualizzare, ma non modificare le autorizzazioni per i ruoli collegati al servizio.

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

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

Gestione dell'accesso tramite policy

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

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale entità principale può eseguire operazioni 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, un IAM amministratore può creare IAM policy. L'amministratore può quindi aggiungere le IAM 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 policy può ottenere informazioni sul ruolo dall' Console di gestione AWS AWS CLI, dall'o dall' AWS API.

Policy basate sull'identità

Le politiche basate sull'identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità, ad esempio un ruolo o un gruppo Utente IAM. Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per scoprire come creare una policy basata sull'identità, consulta Creating policies nella IAM User Guide. IAM

Le policy basate sull'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 policy gestite sono policy autonome che puoi allegare a più utenti, gruppi e ruoli all'interno del tuo. Account AWS Le politiche gestite includono politiche AWS gestite e politiche gestite dai clienti. Per informazioni su come scegliere tra una policy gestita o una policy inline, consulta Scelta fra policy gestite e policy inline nella Guida per l'utente IAM.

Policy basate su risorse

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Gli esempi più comuni di policy basate su risorse sono le policy di trust dei ruoli IAM e le policy dei bucket Amazon S3 . Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le operazioni che un principale può eseguire su tale risorsa e a quali condizioni. In una policy basata sulle risorse è obbligatorio specificare un'entità principale. 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 è possibile utilizzare le policy AWS gestite contenute IAM in una policy 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. ACLs sono 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 informazioni ACLs, consulta la panoramica dell'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 più tipi di policy 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'entità (o ruolo). IAM Utente IAM 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 le entità nella Guida per l'utente IAM. IAM
- Policie di controllo del servizio (SCPs): SCPs sono politiche JSON che specificano le autorizzazioni massime per un'organizzazione o un'unità organizzativa (OU) in. AWS Organizations AWS Organizations è un servizio per il raggruppamento e la gestione centralizzata di più di proprietà dell' Account AWS 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. L'SCP limita le autorizzazioni per le entità negli account dei membri, incluso ogni utente Account AWS root. Per ulteriori informazioni su Organizations and SCPs, vedere Service control policies (SCPs) nella Guida per l' AWS Organizations 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 Policy di sessione nella Guida per l'utente IAM.

Più tipi di policy

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

ROSA esempi di policy basate sull'identità

Per impostazione predefinita, Utenti IAM i ruoli non dispongono dell'autorizzazione per creare o modificare risorse. AWS Inoltre, non possono eseguire attività utilizzando l' AWS API Console di gestione AWS AWS CLI, o. Un IAM amministratore deve creare IAM politiche che concedano a utenti e ruoli l'autorizzazione a eseguire operazioni API specifiche sulle risorse specifiche di cui ha bisogno. L'amministratore deve quindi allegare tali politiche agli Utenti IAM o ai gruppi che richiedono tali autorizzazioni.

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

Utilizzo della console ROSA

Per abbonarsi ROSA dalla console, il responsabile IAM deve disporre delle Marketplace AWS autorizzazioni richieste. Le autorizzazioni consentono al principale di sottoscrivere e annullare l'iscrizione all'elenco dei ROSA prodotti Marketplace AWS e di visualizzare gli abbonamenti. Marketplace AWS Per aggiungere le autorizzazioni richieste, vai alla ROSA console e collega la policy AWS `ROSAManageSubscription` gestita al tuo principale IAM. Per ulteriori informazioni su `ROSAManageSubscription`, consultare the section called "AWS politica gestita: ROSAManage abbonamento".

Autorizzazione di ROSA con HCP alla gestione delle risorse AWS

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

Per ulteriori informazioni, consulta the section called " AWS politiche gestite".

Autorizzazione di ROSA classic alla gestione delle risorse AWS

ROSA classic utilizza politiche IAM gestite dal cliente con autorizzazioni predefinite dal servizio. Utilizzi la ROSA CLI per creare queste politiche e collegarle ai ruoli di servizio nel tuo. 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 di ROSA classic senza prima consultare Red Hat. Ciò potrebbe invalidare l'accordo sul livello di servizio di uptime del cluster del 99,95% di Red Hat. ROSA con piani di controllo ospitati utilizza policy AWS gestite con un set di autorizzazioni più limitato. Per ulteriori informazioni, consulta the section called " AWS politiche gestite".

Esistono due tipi di politiche gestite dai clienti per ROSA: politiche dell'account e politiche dell'operatore. Le policy relative agli account sono associate ai IAM ruoli utilizzati dal servizio per stabilire una relazione di fiducia con Red Hat per il supporto dei Site Reliability Engineer (SRE), la creazione di cluster e le funzionalità di calcolo. Le policy degli operatori sono associate ai IAM ruoli che OpenShift gli operatori utilizzano per le operazioni del cluster relative all'ingresso, allo storage, al registro delle immagini e alla gestione dei nodi. Le politiche degli account vengono create una volta per Account AWS cluster, mentre le politiche degli operatori vengono create una volta per cluster.

Per ulteriori informazioni, consultare the section called "Politiche relative all'account ROSA classic" e the section called "POLICY ROSA classic per gli operatori".

Consentire agli utenti di visualizzare le loro autorizzazioni

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

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Effect": "Allow",
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
```

```
        {
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

Politiche relative agli account ROSA classic

Questa sezione fornisce dettagli sulle politiche degli account necessarie per ROSA classic. Queste autorizzazioni sono necessarie a ROSA classic per gestire AWS le risorse su cui vengono eseguiti i cluster e abilitare il supporto di Red Hat Site Reliability Engineer per i cluster. È possibile assegnare un prefisso personalizzato ai nomi delle policy, ma altrimenti queste politiche 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

È possibile collegare `[Prefix]-Installer-Role-Policy` alle entità IAM. Prima di poter creare un cluster ROSA classic, è necessario collegare questa policy a un ruolo IAM denominato. `[Prefix]-Installer-Role` Questa politica concede le autorizzazioni necessarie che consentono all' ROSA installatore di gestire AWS le risorse necessarie per la creazione 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": [
                "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: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:GetReplicationConfiguration",
                "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

È possibile collegare `[Prefix]-ControlPlane-Role-Policy` alle entità IAM. Prima di poter creare un cluster ROSA classic, è necessario collegare questa policy a un ruolo IAM denominato. `[Prefix]-ControlPlane-Role` Questa policy concede a ROSA classic le autorizzazioni necessarie per la gestione Amazon EC2 e la Elastic Load Balancing lettura delle risorse che ospitano il piano di ROSA controllo. 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

È possibile collegare `[Prefix]-Worker-Role-Policy` alle entità IAM. Prima di poter creare un cluster ROSA classic, è necessario collegare questa policy a un ruolo IAM denominato. `[Prefix]-Worker-Role` Questa policy concede le autorizzazioni necessarie a ROSA classic per descrivere le istanze EC2 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

È possibile collegare `[Prefix]-Support-Role-Policy` alle entità IAM. Prima di poter creare un cluster ROSA classic, è necessario collegare questa policy a un ruolo IAM denominato. `[Prefix]-Support-Role` Questa policy concede le autorizzazioni necessarie all'ingegneria dell'affidabilità del sito Red Hat per osservare, diagnosticare e supportare le AWS risorse utilizzate dai cluster ROSA classic, 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*"
            ]
        }
    ]
}
```

POLITICHE OPERATIVE CLASSICHE DI ROSA

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

Queste autorizzazioni sono necessarie per consentire agli OpenShift operatori di gestire i nodi del cluster ROSA classic. 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

È possibile collegare `[Prefix]-openshift-ingress-operator-cloud-credentials` alle entità IAM. Questa politica concede le autorizzazioni necessarie all'operatore di ingresso per fornire e gestire i sistemi di bilanciamento del carico e le configurazioni DNS per l'accesso al cluster esterno. La policy consente inoltre all'Ingress Operator di leggere e filtrare i valori dei tag delle risorse per scoprire le zone ospitate Route 53 . 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

È possibile collegare `[Prefix]-openshift-cluster-csi-drivers-ebs-cloud-credentials` alle entità IAM. Questa politica concede le autorizzazioni necessarie a Amazon EBS CSI Driver Operator per installare e gestire il driver Amazon EBS CSI su un cluster ROSA classic. Per ulteriori informazioni sull'operatore, vedere aws-ebs-csi-driver-operator nella documentazione. OpenShift GitHub

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

È possibile collegare `[Prefix]-openshift-machine-api-aws-cloud-credentials` alle entità IAM. Questa politica concede le autorizzazioni necessarie all'operatore Machine Config per descrivere, eseguire e terminare le Amazon EC2 istanze gestite come nodi di lavoro. Questa politica concede inoltre le autorizzazioni per consentire la crittografia del disco del volume root del nodo di lavoro utilizzato. AWS KMS keys Per ulteriori informazioni sull'operatore, consulta la machine-config-operator 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: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

È possibile collegare `[Prefix]-openshift-cloud-credential-operator-cloud-credentials` alle entità IAM. Questa policy concede le autorizzazioni necessarie al Cloud

Credential Operator per recuperare Utente IAM i dettagli, tra cui la chiave di accesso, i documenti di policy in linea allegati IDs, la data di creazione dell'utente, il percorso, l'ID utente e Amazon Resource Name (ARN). Per ulteriori informazioni sull'operatore, consulta la documentazione. cloud-credential-operator OpenShift GitHub

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

È possibile collegare `[Prefix]-openshift-image-registry-installer-cloud-credentials` alle entità IAM. Questa politica concede le autorizzazioni necessarie all'Image Registry Operator per fornire e gestire le risorse per il registro di immagini integrato nel cluster di ROSA classic e i servizi dipendenti, tra cui. Amazon S3 Ciò è necessario affinché l'operatore possa installare e gestire il registro interno di un cluster ROSA classic. 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

È possibile collegare `[Prefix]-openshift-cloud-network-config-controller-cloud-cr` alle entità IAM. 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 classico overlay di rete per cluster ROSA. L'operatore utilizza queste autorizzazioni per gestire gli indirizzi IP privati per le Amazon EC2 istanze come parte del cluster ROSA classic. 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

Una politica AWS 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 le policy AWS gestite potrebbero non concedere le autorizzazioni con il privilegio minimo per i tuoi casi d'uso specifici, poiché sono disponibili per tutti i clienti. AWS Si consiglia pertanto di ridurre ulteriormente le autorizzazioni definendo policy gestite dal cliente specifiche per i propri casi d'uso.

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

AWS politica gestita: ROSAManage abbonamento

Puoi allegare la `ROSAManageSubscription` politica alle tue IAM entità. Prima di abilitarla ROSA nella AWS ROSA console, devi prima collegare questa policy a un ruolo IAM.

Questa policy concede le Marketplace AWS autorizzazioni necessarie per gestire l' ROSA abbonamento.

Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- `aws-marketplace:Subscribe`- Concede l'autorizzazione a sottoscrivere il Marketplace AWS prodotto per. ROSA
- `aws-marketplace:Unsubscribe`- Consente ai responsabili di rimuovere gli abbonamenti ai prodotti. Marketplace AWS
- `aws-marketplace:ViewSubscriptions`- Consente ai mandanti di visualizzare gli abbonamenti da. Marketplace AWS Ciò è necessario affinché il IAM principale possa visualizzare gli abbonamenti disponibili Marketplace AWS .

Per visualizzare il documento completo sulla policy JSON, consulta ROSAManageSubscription nella AWS Managed Policy Reference Guide.

ROSA con politiche dell'account HCP

Questa sezione fornisce dettagli sulle politiche dell'account richieste per ROSA con piani di controllo ospitati (HCP). Queste politiche AWS gestite aggiungono le autorizzazioni utilizzate da ROSA con i ruoli HCP IAM. 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 da parte di ROSA con piani di controllo ospitati (HCP). I cluster classici ROSA utilizzano politiche IAM gestite dal cliente. Per ulteriori informazioni sulle politiche ROSA classic, consulta the section called "Politiche relative all'account ROSA classic" ethe section called "POLICY ROSA classic per gli operatori".

AWS politica gestita: ROSAWorker InstancePolicy

Puoi collegarti `ROSAWorkerInstancePolicy` alle tue IAM entità. Prima di creare un cluster, devi avere un ruolo IAM con questa policy allegata. Un servizio ROSA effettua chiamate verso altri utenti Servizi AWS per conto dell'utente. Lo fanno per gestire le risorse utilizzate con ogni cluster.

Dettagli delle autorizzazioni

Questa politica include le seguenti autorizzazioni che consentono ai nodi di lavoro ROSA di completare le seguenti attività:

- `ec2`— Valuta i dettagli Regione AWS e le Amazon EC2 istanze come parte della gestione del ciclo di vita del nodo di lavoro del cluster ROSA.
- `ecr`- Valuta e ottieni immagini dai repository ECR gestiti da ROSA necessarie per l'installazione del cluster e la gestione del ciclo di vita dei nodi di lavoro.

Per visualizzare il documento completo sulla policy JSON, consulta la Managed Policy Reference Guide ROSAWorkerInstancePolicy. AWS

AWS politica gestita: ROSASRESupport politica

È possibile collegare `ROSASRESupportPolicy` alle entità IAM.

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

Dettagli delle autorizzazioni

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

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

Per visualizzare il documento completo sulla policy JSON, consulta Policy nella AWS Managed ROSASRESupport Policy Reference Guide.

AWS politica gestita: ROSAInstaller politica

Puoi collegarti `ROSAInstallerPolicy` alle tue IAM entità.

Prima di creare un cluster ROSA con piani di controllo ospitati, è necessario collegare questa policy a un ruolo IAM denominato`[Prefix]-ROSA-Worker-Role`. Questa policy 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 gestire le AWS risorse che supportano ROSA l'installazione del cluster.

Dettagli delle autorizzazioni

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

- `ec2`— Esegui Amazon EC2 istanze utilizzando un AMIs server ospitato in Account AWS proprietà e gestito da Red Hat. Amazon EC2 Descrivi le istanze, i volumi e le risorse di rete associate Amazon EC2 ai 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 Controlla le prenotazioni di capacità di Amazon EC2 per supportare la nuova funzionalità di prenotazione della capacità in ROSA. Etichetta ed elimina i tag sulle sottoreti utilizzando le chiavi dei tag corrispondenti. `"kubernetes.io/cluster/*"` Ciò è necessario per garantire che il load balancer utilizzato per l'ingresso del cluster venga creato solo nelle sottoreti applicabili e per gestire i tag di identificazione del cluster Kubernetes.
- `elasticloadbalancing`— Aggiungere sistemi di bilanciamento del carico ai nodi di destinazione su 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 una AWS KMS chiave, crea e gestisci le concessioni e restituisci una chiave dati simmetrica unica da Amazon EC2 utilizzare all'esterno di. AWS KMS Ciò è necessario per l'uso di `etcd` dati crittografati quando la `etcd` crittografia è abilitata al momento della creazione del cluster.
- `iam`— Convalida i ruoli e le politiche IAM. Fornisci e gestisci dinamicamente i profili di Amazon EC2 istanza pertinenti al cluster. Aggiungi tag a un profilo di istanza IAM 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 OIDC del cluster specificato dal cliente.

- `route53`— Gestisci le Route 53 risorse necessarie per creare cluster.
- `servicequotas`— Valuta le quote di servizio necessarie per creare un cluster.
- `sts`— Creare AWS STS credenziali temporanee per i ROSA componenti. Assumi le credenziali per la creazione del cluster.
- `secretsmanager`— Leggi un valore segreto per consentire in modo sicuro la configurazione OIDC gestita dal cliente come parte del provisioning del cluster.

Per visualizzare il documento completo sulla policy JSON, consulta Policy nella Managed Policy Reference ROSAInstallerGuide. AWS

AWS politica gestita: ROSAShared VPCRoute53 politica

Puoi collegarti `ROSASharedVPCRoute53Policy` alle tue IAM entità. È necessario collegare questa policy a un ruolo IAM per consentire a un cluster ROSA di effettuare chiamate ad altri Servizi AWS in ambienti VPC condivisi.

Questa politica consente all'installatore ROSA di configurare i record della Route 53. Questa policy è pensata per essere utilizzata su un VPC condiviso e fornisce un sottoinsieme di autorizzazioni Route 53 su misura per casi d'uso VPC condivisi.

Dettagli delle autorizzazioni

Questa politica include le seguenti autorizzazioni che consentono al programma di installazione ROSA di completare le seguenti attività:

- `route53`— Leggi le informazioni sulla zona DNS e i record DNS esistenti per comprendere la configurazione DNS corrente. Crea, modifica ed elimina i record DNS, ma solo per modelli di dominio specifici relativi a ROSA, tra cui `.hypershift.local`,, e. `.openshiftapps.com` `.devshift.org` `.openshiftusgov.com` `.devshiftusgov.com` Aggiungi, modifica o rimuovi tag sulle risorse della Route 53 per la gestione e l'organizzazione delle risorse.
- `tag`— Scopri ed elenca AWS le risorse in base ai relativi tag, utile per identificare le risorse gestite da ROSA.

Per visualizzare maggiori dettagli sulla policy, inclusa l'ultima versione del documento sulla policy JSON, consulta Policy nella AWS Managed ROSASharedVPCRoute53Policy Reference Guide.

AWS politica gestita: ROSAShared VPCEndpoint politica

Puoi collegarti `ROSASharedVPCEndpointPolicy` alle tue IAM entità. È necessario collegare questa policy a un ruolo IAM per consentire a un cluster ROSA di effettuare chiamate ad altri Servizi AWS in ambienti VPC condivisi.

Questa policy consente all'installatore ROSA di configurare endpoint VPC e gruppi di sicurezza in ambienti VPC condivisi.

Dettagli delle autorizzazioni

Questa politica include le seguenti autorizzazioni che consentono al programma di installazione ROSA di completare le seguenti attività:

- `ec2`— Autorizzazioni di sola lettura per descrivere le risorse relative al VPC, inclusi gli endpoint VPC e i gruppi di sicurezza per comprendere l'ambiente di VPCs rete. Crea, elimina e modifica gruppi di sicurezza con restrizioni basate su tag, permettendo a ROSA di creare e gestire gruppi di sicurezza per reti di cluster, limitando al contempo le operazioni alle sole risorse con tag ROSA. Crea, modifica ed elimina endpoint VPC con restrizioni basate su tag, permettendo a ROSA di creare e gestire endpoint VPC per la connettività privata in ambienti VPC condivisi. Servizi AWS Applica i tag agli endpoint VPC e ai gruppi di sicurezza appena creati durante la creazione per una corretta identificazione e gestione delle risorse.

Per visualizzare maggiori dettagli sulla policy, inclusa l'ultima versione del documento sulla policy JSON, consulta Policy nella AWS Managed ROSASharedVPCEndpointPolicy Reference Guide.

ROSA con politiche degli operatori HCP

Questa sezione fornisce dettagli sulle politiche degli operatori necessarie per ROSA con piani di controllo ospitati (HCP). È possibile allegare queste politiche AWS gestite ai ruoli di operatore necessari per utilizzare ROSA con HCP. Le autorizzazioni sono necessarie per consentire agli OpenShift operatori di gestire ROSA con i nodi del cluster HCP.

> **Note**
>
> AWS le politiche gestite sono destinate all'uso da parte di ROSA con piani di controllo ospitati (HCP). I cluster classici ROSA utilizzano politiche IAM gestite dal cliente. Per ulteriori informazioni sulle politiche ROSA classic, consulta the section called "Politiche relative all'account ROSA classic" ethe section called "POLICY ROSA classic per gli operatori".

AWS politica gestita: ROSAAmazon EBSCSIDriver OperatorPolicy

Puoi collegarti `ROSAAmazonEBSCSIDriverOperatorPolicy` alle tue IAM entità. È necessario collegare questa policy a un ruolo di operatore IAM 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 di operatore per ogni cluster.

Questa politica concede le autorizzazioni necessarie al Amazon EBS CSI Driver Operator per installare e gestire il driver Amazon EBS CSI su un cluster. ROSA Per ulteriori informazioni sull'operatore, consulta aws-ebs-csi-driver l'operatore nella documentazione. OpenShift GitHub

Dettagli delle autorizzazioni

Questa politica include le seguenti autorizzazioni che consentono all'operatore del Amazon EBS conducente di completare le seguenti attività:

- `ec2`— Creare, modificare, allegare, scollegare ed eliminare i Amazon EBS volumi collegati alle Amazon EC2 istanze. Crea ed elimina istantanee di Amazon EBS volume ed elenca Amazon EC2 istanze, volumi e istantanee.

Per visualizzare il documento completo sulla policy JSON, consulta la AWS Managed Policy ROSAAmazonEBSCSIDriverOperatorPolicyReference Guide.

AWS politica gestita: ROSAIngress OperatorPolicy

Puoi collegarti `ROSAIngressOperatorPolicy` alle tue IAM entità. È necessario collegare questa policy a un ruolo di operatore IAM 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 di 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 DNS per i cluster. ROSA La policy consente l'accesso in lettura ai valori dei tag. L'operatore filtra quindi i valori dei tag per Route 53 le risorse per scoprire le zone ospitate. Per ulteriori informazioni sull'operatore, consulta OpenShift Ingress Operator nella OpenShift GitHub documentazione.

Dettagli delle autorizzazioni

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`— Elenca le zone Route 53 ospitate e modifica i record che gestiscono il DNS controllato dal cluster ROSA.
- `tag`— Gestisci le risorse contrassegnate utilizzando l'`tag:GetResources`autorizzazione.

Per visualizzare il documento completo sulla policy JSON, consulta ROSAIngressOperatorPolicyla AWS Managed Policy Reference Guide.

AWS politica gestita: ROSAImage RegistryOperatorPolicy

Puoi collegarti `ROSAImageRegistryOperatorPolicy` alle tue IAM entità. È necessario collegare questa policy a un ruolo di operatore IAM 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 di operatore per ogni cluster.

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

Dettagli delle autorizzazioni

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

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

Per visualizzare il documento completo sulla policy JSON, consulta la AWS Managed Policy ROSAImageRegistryOperatorPolicyReference Guide.

AWS politica gestita: ROSACloud NetworkConfigOperatorPolicy

Puoi collegarti `ROSACloudNetworkConfigOperatorPolicy` alle tue IAM entità. È necessario collegare questa policy a un ruolo di operatore IAM 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 di 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 l'overlay di rete del ROSA cluster. L'operatore utilizza queste autorizzazioni per gestire gli indirizzi IP privati per le Amazon EC2 istanze come parte del cluster. ROSA Per ulteriori informazioni sull'operatore, vedere C loud-network-config-controller nella OpenShift GitHub documentazione.

Dettagli delle autorizzazioni

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 connettere Amazon EC2 istanze, Amazon VPC sottoreti e interfacce di rete elastiche in un cluster. ROSA

Per visualizzare il documento completo sulla policy JSON, consulta la Managed Policy Reference Guide ROSACloudNetworkConfigOperatorPolicy. AWS

AWS politica gestita: ROSAKube ControllerPolicy

Puoi collegarti `ROSAKubeControllerPolicy` alle tue IAM entità. È necessario collegare questa policy a un ruolo di operatore IAM 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 di operatore per ogni cluster.

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

Dettagli delle autorizzazioni

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

- `ec2`— Creare, eliminare e aggiungere tag ai gruppi di sicurezza delle Amazon EC2 istanze. Aggiungi regole in entrata ai gruppi di sicurezza. Descrivi le zone di disponibilità, Amazon EC2 le istanze, le tabelle di routing VPCs, i gruppi di sicurezza e le sottoreti.
- `elasticloadbalancing`— Crea e gestisci sistemi di bilanciamento del carico e le relative politiche. Crea e gestisci i listener di load balancer. Registra e annulla la registrazione degli obiettivi

con i gruppi target e gestisci i gruppi target. Registra e annulla la registrazione Amazon EC2 delle istanze con un sistema di bilanciamento del carico e aggiungi tag ai sistemi di bilanciamento del carico.

- `kms`— Recupera informazioni dettagliate su una chiave. AWS KMS 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 completo sulla policy JSON, consulta ROSAKubeControllerPolicyla AWS Managed Policy Reference Guide.

AWS politica gestita: ROSANode PoolManagementPolicy

Puoi collegarti `ROSANodePoolManagementPolicy` alle tue IAM entità. È necessario collegare questa policy a un ruolo di operatore IAM per consentire a un cluster ROSA con piani di controllo ospitati di effettuare chiamate ad altri AWS servizi. È richiesto un set unico di ruoli di operatore per ogni cluster.

Questa politica concede le autorizzazioni necessarie al NodePool controller per descrivere, eseguire e terminare Amazon EC2 le istanze gestite come nodi di lavoro. Questa policy concede inoltre le autorizzazioni per consentire la crittografia del disco del volume root del nodo di lavoro mediante AWS KMS chiavi, per etichettare l'interfaccia elastica di rete collegata al nodo di lavoro e per accedere alle prenotazioni di capacità di Amazon EC2. Per ulteriori informazioni su questo controller, consulta l'architettura del controller nella documentazione. OpenShift

Dettagli delle autorizzazioni

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

- `ec2`— Esegui Amazon EC2 istanze utilizzando un AMIs server ospitato in Account AWS proprietà e gestito da Red Hat. Gestisci i cicli di vita EC2 nel cluster. ROSA Crea e integra dinamicamente nodi di lavoro con Elastic Load Balancing,,, Amazon VPC e. Route 53 Amazon EBS Amazon EC2 Accedi e descrivi le prenotazioni di capacità per supportare la funzionalità di prenotazione della capacità in ROSA.
- `iam`— Utilizzo Elastic Load Balancing tramite il ruolo collegato al servizio denominato. `AWSServiceRoleForElasticLoadBalancing` Assegna ruoli ai profili di istanza Amazon EC2 .
- `kms`— Leggi una AWS KMS chiave, crea e gestisci le sovvenzioni e restituisci una chiave dati simmetrica unica da utilizzare all'esterno di. Amazon EC2 AWS KMS Ciò è necessario per consentire la crittografia del disco del volume principale del nodo di lavoro.

Per visualizzare il documento completo sulla policy JSON, consulta ROSANodePoolManagementPolicyla AWS Managed Policy Reference Guide.

AWS politica gestita: ROSAKMSProvider politica

Puoi collegarti `ROSAKMSProviderPolicy` alle tue IAM entità. È necessario collegare questa policy a un ruolo di operatore IAM 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 di operatore per ogni cluster.

Questa politica concede le autorizzazioni necessarie all' AWS Encryption Provider integrato per gestire AWS KMS le chiavi che supportano la crittografia `etcd` dei dati. Questa politica consente di Amazon EC2 utilizzare le chiavi KMS fornite dall' AWS Encryption Provider per crittografare e decrittografare i dati. `etcd` Per ulteriori informazioni su questo provider, consulta AWS Encryption Provider nella documentazione di Kubernetes. GitHub

Dettagli delle autorizzazioni

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

- `kms`— Crittografa, decrittografa e recupera qualsiasi chiave. AWS KMS 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 completo sulla policy JSON, consulta ROSAKMSProviderPolicy nella AWS Managed Policy Reference Guide.

AWS politica gestita: ROSAControl PlaneOperatorPolicy

Puoi collegarti `ROSAControlPlaneOperatorPolicy` alle tue IAM entità. È necessario collegare questa policy a un ruolo di operatore IAM 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 di operatore per ogni cluster.

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

Dettagli delle autorizzazioni

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

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

Per visualizzare il documento completo sulla policy JSON, consulta ROSAControlPlaneOperatorPolicyla AWS Managed Policy Reference Guide.

ROSA aggiornamenti alle politiche AWS gestite

Visualizza i dettagli sugli aggiornamenti delle politiche AWS gestite ROSA da quando questo servizio ha iniziato a tenere traccia di queste modifiche. Per gli avvisi automatici sulle modifiche apportate alla pagina, iscriviti al feed RSS alla pagina Cronologia dei documenti.

Modifica	Descrizione	Data
ROSANodePoolManagementPolicy — Politica aggiornata	ROSA ha aggiornato la policy per aggiungere l'accesso alle risorse per le prenotazioni di capacità di Amazon EC2. Questa modifica consente al NodePool controller di accedere e descrivere Capacity Reservations per una migliore gestione delle risorse. Per ulteriori informazioni, consulta the section called "AWS politica gestita: ROSANode PoolManagementPolicy".	3 settembre 2025
ROSASharedVPCEndpointPolitica: aggiunta una nuova politica	ROSA ha aggiunto una nuova policy per consentire all' ROSA installatore di configurare endpoint VPC e gruppi di sicurezza in ambienti	7 agosto 2025

Modifica	Descrizione	Data
	VPC condivisi. Questa policy fornisce un sottoinsieme di autorizzazioni EC2 su misura per casi d'uso VPC condivisi . Per ulteriori informazi oni, consulta the section called "AWS politica gestita: ROSAShared VPCEndpoint politica".	
ROSASharedVPCRoute 53Politica: è stata aggiunta una nuova politica	ROSA ha aggiunto una nuova policy per consentir e all' ROSA installatore di configurare i record Route 53 in ambienti VPC condivisi . Questa policy fornisce un sottoinsieme di autorizza zioni Route 53 su misura per casi d'uso VPC condivisi. Per ulteriori informazioni, consulta the section called "AWS politica gestita: ROSAShared VPCRoute53 politica".	7 agosto 2025

Modifica	Descrizione	Data
ROSAInstallerPolicy: policy aggiornata	ROSA ha aggiornato la policy per consentire all' ROSA installatore di ispeziona re Amazon EC2 Capacity Reservations per supportar e la nuova funzionalità Capacity Reservations in ROSA. Questo aggiornam ento consente inoltre all'insta llatore di eliminare i tag sulle sottoreti utilizzando chiavi di tag corrispondenti `"kubernet es.io/cluster/*"` per una migliore gestione dei tag del cluster Kubernetes. Per ulteriori informazioni, consulta the section called "AWS politica gestita: ROSAInstaller politica".	7 agosto 2025
ROSAImageRegistryO peratorPolicy — Politica aggiornata	ROSA ha aggiornato la policy in modo che le autorizza zioni siano limitate al livello di risorsa del bucket S3. Questa modifica soddisfa i requisiti di archiviazione ROSA sia per le aree commerciali che per quelle regionali. AWS GovCloud Per ulteriori informazioni, consulta the section called "AWS politica gestita: ROSAImage RegistryOperatorPolicy".	19 maggio 2025

Modifica	Descrizione	Data
ROSANodePoolManagementPolicy — Politica aggiornata	ROSA ha aggiornato la policy per consentire il tagging dell'interfaccia elastica di rete collegata al nodo di lavoro. Per ulteriori informazioni, consulta the section called "AWS politica gestita: ROSANode PoolManagementPolicy".	5 maggio 2025
ROSAImageRegistryOperatorPolicy — Politica aggiornata	ROSA ha aggiornato la policy per consentire a Red Hat OpenShift Image Registry Operator di effettuare il provisioning e gestire i bucket e gli oggetti Amazon S3 nelle AWS GovCloud regioni per l'utilizzo da parte del registro di immagini ROSA in-cluster. Questa modifica soddisfa i requisiti di storage ROSA per le regioni. AWS GovCloud Per ulteriori informazioni, consulta the section called "AWS politica gestita: ROSAImageRegistryOperatorPolicy".	16 aprile 2025

Modifica	Descrizione	Data
ROSAWorkerInstancePolicy — Politica aggiornata	ROSA ha aggiornato la policy per consentire ai nodi di lavoro di valutare e ottenere immagini dai repository ECR gestiti da ROSA necessarie per l'installazione del cluster e la gestione del ciclo di vita dei nodi di lavoro. Per ulteriori informazioni, consulta the section called "AWS politica gestita: ROSAWorker InstancePolicy".	3 marzo 2025
ROSANodePoolManage mentPolicy — Politica aggiornata	ROSA ha aggiornato la policy per consentire alle interfacc e di rete elastiche di essere etichettate in modo simile alle istanze EC2 solo durante le RunInstances chiamate ec2: quando la richiesta include il tag. `red-hat-managed: true` Queste autorizzazioni sono necessarie per supportar e ROSA con i cluster HCP 4.17. Per ulteriori informazi oni, consulta the section called "AWS politica gestita: ROSANode PoolManag ementPolicy".	24 febbraio 2025

Modifica	Descrizione	Data
ROSAAmazonEBSCSIDriverOperatorPolicy — Politica aggiornata	ROSA ha aggiornato la policy per supportare la nuova API di autorizzazione delle Amazon EBS istantanee. Per ulteriori informazioni, consulta the section called "AWS politica gestita: ROSAAmazon EBSCSIDriver OperatorPolicy".	17 gennaio 2025
ROSANodePoolManagementPolicy — Politica aggiornata	ROSA ha aggiornato la policy per consentire al gestore del pool di ROSA nodi di descrivere i set di opzioni DHCP al fine di impostare i nomi DNS privati appropriati. Per ulteriori informazioni, consulta the section called "AWS politica gestita: ROSANodePoolManagementPolicy".	2 maggio 2024
ROSAInstallerPolitica: politica aggiornata	ROSA ha aggiornato la politica per consentire all' ROSA installatore di aggiungere tag alle sottoreti utilizzando le chiavi dei tag corrispondenti. `"kubernetes.io/cluster/*"` Per ulteriori informazioni, consulta the section called "AWS politica gestita: ROSAInstaller politica" .	24 aprile 2024

Modifica	Descrizione	Data
ROSASRESupportPolitica: politica aggiornata	ROSA ha aggiornato la policy per consentire al ruolo SRE di recuperare informazioni sui profili di istanza che sono stati contrassegnati da ROSA as. `red-hat-managed` Per ulteriori informazioni, consulta the section called "AWS politica gestita: ROSASRESupport politica".	10 aprile 2024
ROSAInstallerPolitica: politica aggiornata	ROSA ha aggiornato la politica per consentire all' ROSA installatore di verificare che le politiche AWS gestite per ROSA siano associate ai IAM ruoli utilizzati da. ROSA Questo aggiornamento consente inoltre all'installatore di identificare se le politiche gestite dal cliente sono state associate ai ruoli. ROSA Per ulteriori informazioni, consulta the section called "AWS politica gestita: ROSAInstaller politica".	10 aprile 2024

Modifica	Descrizione	Data
ROSAInstallerPolitica: politica aggiornata	ROSA ha aggiornato la policy per consentire al servizio di fornire messaggi di avviso all'installatore quando l'install azione del cluster non riesce a causa della mancanza di un provider OIDC del cluster specificato dal cliente. Questo aggiornamento consente inoltre al servizio di recuperar e i name server DNS esistenti in modo che le operazion i di provisioning del cluster siano idempotenti. Per ulteriori informazioni, consulta the section called "AWS politica gestita: ROSAInstaller politica" .	26 gennaio 2024
ROSASRESupportPolitica: politica aggiornata	ROSA ha aggiornato la policy per consentire al servizio di eseguire operazioni di lettura sui gruppi di sicurezza utilizzando l' DescribeS ecurityGroups API. Per ulteriori informazioni, consulta the section called "AWS politica gestita: ROSASRESu pport politica".	22 gennaio 2024

Modifica	Descrizione	Data
ROSAImageRegistryOperatorPolicy — Politica aggiornata	ROSA ha aggiornato la politica per consentire all'Image Registry Operator di intraprendere azioni sui Amazon S3 bucket nelle regioni con nomi di 14 caratteri. Per ulteriori informazioni, consulta the section called "AWS politica gestita: ROSAImage RegistryOperatorPolicy".	12 dicembre 2023
ROSAKubeControllerPolicy — Politica aggiornata	ROSA ha aggiornato la politica per consentire di kube-controller-manager descrivere zone di disponibilità, Amazon EC2 istanze, tabelle di routing VPCs, gruppi di sicurezza e sottoreti. Per ulteriori informazioni, consulta the section called "AWS politica gestita: ROSAKube ControllerPolicy".	16 ottobre 2023
ROSAManageAbbonamento: politica aggiornata	ROSA ha aggiornato la politica per aggiungere il ROSA con piani di controllo ospitati ProductId. Per ulteriori informazioni, consulta the section called "AWS politica gestita: ROSAManage abbonamento".	1° agosto 2023

Modifica	Descrizione	Data
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
ROSANodePoolManagementPolicy — Aggiunta una nuova politica	ROSA ha aggiunto una nuova policy per consentire al NodePool controller di descrivere, eseguire e terminare Amazon EC2 le istanze gestite come nodi di lavoro. Questa politica consente inoltre la crittografia del disco del volume root del nodo di lavoro utilizzando AWS KMS le chiavi. Per ulteriori informazioni, consulta the section called "AWS politica gestita: ROSANodePoolManagementPolicy".	8 giugno 2023

Modifica	Descrizione	Data
ROSAInstallerPolicy: è stata aggiunta una nuova politica	ROSA ha aggiunto una nuova politica per consentire all'installatore di gestire AWS le risorse che supportano l'installazione del cluster. Per ulteriori informazioni, consulta the section called "AWS politica gestita: ROSAInstaller politica".	6 giugno 2023
ROSASRESupportPolitica: è stata aggiunta una nuova politica	ROSA ha aggiunto una nuova policy per consentire SREs a Red Hat di osservare, diagnosticare e supportare direttamente AWS le risorse associate ai ROSA cluster, inclusa la possibilità di modificare lo stato dei nodi del ROSA cluster. Per ulteriori informazioni, consulta the section called "AWS politica gestita: ROSASRESupport politica".	1 giugno 2023
ROSAKMSProviderPolicy — È stata aggiunta una nuova policy	ROSA ha aggiunto una nuova politica per consentire all' AWS Encryption Provider integrato di gestire AWS KMS le chiavi per supportare la crittografia dei dati etcd. Per ulteriori informazioni, consulta the section called "AWS politica gestita: ROSAKMSProvider politica".	27 aprile 2023

Modifica	Descrizione	Data
ROSAKubeControllerPolicy — Aggiunta una nuova politica	ROSA ha aggiunto una nuova policy per consentire al controller kube di gestire e gestire Amazon EC2 le Elastic Load Balancing AWS KMS risorse relative ai cluster ROSA con piani di controllo ospitati. Per ulteriori informazioni, consulta the section called "AWS politica gestita: ROSAKube ControllerPolicy".	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 il registro delle immagini ROSA interno al cluster e i servizi dipendenti, incluso S3. Per ulteriori informazioni, consulta the section called "AWS politica gestita: ROSAImage RegistryOperatorPolicy".	27 aprile 2023

Modifica	Descrizione	Data
ROSAControlPlaneOperatorPolicy — Aggiunta una nuova politica	ROSA ha aggiunto una nuova politica per consentire all'operatore del piano di controllo di gestire Amazon EC2 le Route 53 risorse relative ROSA ai cluster di piani di controllo ospitati. Per ulteriori informazioni, consulta the section called "AWS politica gestita: ROSAControlPlaneOperatorPolicy".	24 aprile 2023
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 l'overlay di rete del ROSA 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 DNS per i cluster. ROSA Per ulteriori informazioni, consulta the section called "AWS politica gestita: ROSAIngressOperatorPolicy".	20 aprile 2023

Modifica	Descrizione	Data
ROSAAmazonEBSCSIDriverOperatorPolicy — Aggiunta una nuova politica	ROSA ha aggiunto una nuova politica per consentire a Amazon EBS CSI Driver Operator di installare e gestire il driver Amazon EBS CSI su un ROSA cluster. Per ulteriori informazioni, consulta the section called "AWS politica gestita: ROSAAmazon EBSCSIDriver OperatorPolicy".	20 aprile 2023
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: ROSAWorker InstancePolicy".	20 aprile 2023
ROSAManageAbbonamento: è stata aggiunta una nuova politica	ROSA ha aggiunto una nuova politica per concedere le Marketplace AWS autorizzazioni necessarie per gestire l' ROSA abbonamento. Per ulteriori informazioni, consulta the section called "AWS politica gestita: ROSAManage abbonamento".	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 tenere traccia delle modifiche per le sue politiche AWS gestite.	2 marzo 2022

Risoluzione dei problemi di ROSA identità e accesso

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

AWS Organizations la politica di controllo del servizio nega le autorizzazioni richieste Marketplace AWS

Se la policy AWS Organizations di controllo del servizio (SCP) non consente le autorizzazioni di Marketplace AWS abbonamento richieste quando si tenta di abilitare ROSA, si verifica il seguente errore della 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 ricevi questo errore, devi 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 per consentire `aws-marketplace:Subscribe` e `aws-marketplace:Unsubscribe` `aws-marketplace:ViewSubscriptions` autorizzazioni. Per ulteriori informazioni, vedere Aggiornamento di un SCP nella Guida per l' AWS Organizations utente.
2. Abilita ROSA nell'account di gestione dell'organizzazione.
3. Condividi l' ROSA abbonamento con gli account dei membri che richiedono l'accesso all'interno dell'organizzazione. Per ulteriori informazioni, consulta Condivisione degli abbonamenti in un'organizzazione nella Guida all' Marketplace AWS acquisto.

L'utente o il ruolo non dispone delle autorizzazioni richieste Marketplace AWS

Se il IAM responsabile non dispone delle autorizzazioni di Marketplace AWS abbonamento richieste 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 alla IAM console e collega la policy AWS gestita `ROSAManageSubscription` alla tua identità IAM. Per ulteriori informazioni, consulta ROSAManageSubscription nella AWS Managed Policy Reference Guide.
2. Segui la procedura riportata in the section called "Abilita ROSA e configura i AWS prerequisiti".

Se non disponi dell'autorizzazione per visualizzare o aggiornare l'autorizzazione impostata IAM o ricevi un errore, devi contattare l'amministratore per ricevere assistenza. Chiedi a quella persona di `ROSAManageSubscription` allegare la tua IAM identità e segui la procedura riportata inthe section called "Abilita ROSA e configura i AWS prerequisiti". Quando un amministratore esegue questa azione, lo abilita ROSA aggiornando il set di autorizzazioni per tutte IAM le identità in. Account AWS

Marketplace AWS Autorizzazioni richieste bloccate da un amministratore

Se l'amministratore dell'account ha bloccato le autorizzazioni di Marketplace AWS abbonamento richieste, durante il tentativo di attivazione si verifica il seguente errore della console. 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 ricevi questo errore, devi contattare l'amministratore per ricevere assistenza. Chiedi a quella persona di fare quanto segue:

1. Vai alla ROSA console e collega la policy AWS gestita `ROSAManageSubscription` alla tua identità IAM. Per ulteriori informazioni, consulta ROSAManageSubscription nella AWS Managed Policy Reference Guide.
2. Segui la procedura illustrata the section called "Abilita ROSA e configura i AWS prerequisiti" per abilitare ROSA. Questa procedura consente ROSA l'aggiornamento del set di autorizzazioni per tutte IAM le identità in. 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 tenti di creare un ruolo 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 `AWSServiceRoleForElasticLoadBalancing` ruolo è assegnato al tuo account.

   ```
   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 Guida per l' Elastic Load Balancing utente.

Resilienza in ROSA

AWS resilienza dell'infrastruttura globale

L'infrastruttura AWS globale è costruita attorno a zone Regioni AWS 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 è possibile 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 una singola 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 sulle zone Regioni AWS di disponibilità, vedere AWS Global Infrastructure.

ROSA resilienza del cluster

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

Il piano ROSA dati è costituito da almeno due nodi di OpenShift infrastruttura e due OpenShift nodi di lavoro. I nodi dell'infrastruttura eseguono pod che supportano i 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 in SREs modo proattivo il ROSA cluster e si occupa della sostituzione di eventuali nodi del piano di controllo e nodi dell'infrastruttura guasti. Per ulteriori informazioni, consulta the section called "Responsabilità".

> **Important**
>
> ROSA Trattandosi di un servizio gestito, Red Hat è responsabile della gestione dell' AWS infrastruttura sottostante che ROSA utilizza. I clienti non devono tentare di chiudere manualmente le Amazon EC2 istanze ROSA utilizzate dalla 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 a quando il nodo guasto non viene ripristinato o sostituito. 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 fornisca 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, consultate About availability ROSA nella documentazione di Red Hat.

Sicurezza dell'infrastruttura in ROSA

In quanto servizio gestito, Servizio Red Hat OpenShift su AWS è protetto dalla sicurezza di rete AWS globale. Per informazioni sui servizi AWS di sicurezza e su come AWS protegge l'infrastruttura, consulta AWS Cloud Security. Per progettare il tuo AWS ambiente utilizzando le migliori pratiche per la sicurezza dell'infrastruttura, vedi Infrastructure Protection in Security Pillar — AWS Well-Architected Framework.

Utilizzi chiamate API AWS pubblicate per accedere ROSA attraverso la rete. AWS I client devono supportare quanto segue:

- Transport Layer Security (TLS). È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Suite di cifratura con Perfect Forward Secrecy (PFS), ad esempio Ephemeral Diffie-Hellman (DHE) o 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. In alternativa è possibile utilizzare AWS Security Token Service (AWS STS) per generare credenziali di sicurezza temporanee per sottoscrivere 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, consultathe section called "Responsabilità".

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

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

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

Se crei un ROSA cluster in un VPC esistente, specifichi le sottoreti VPC e le zone di disponibilità da utilizzare per il cluster. È inoltre possibile definire gli intervalli CIDR da utilizzare per la rete di cluster

e abbinare questi intervalli CIDR alle sottoreti VPC. Per ulteriori informazioni, consultate le definizioni degli intervalli CIDR nella documentazione di Red Hat.

Per i cluster che utilizzano l'endpoint API pubblico, è ROSA necessario che il 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'endpoint API privato, sono necessarie solo sottoreti private.

Se utilizzi un VPC esistente, puoi configurare i ROSA cluster in modo che utilizzino un server proxy HTTP o HTTPS durante o dopo la creazione del cluster per crittografare il traffico web del cluster, aggiungendo un altro livello di sicurezza per i tuoi dati. Quando abiliti 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 ROSA cluster.

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. ROSA classic 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 per i pagamenti, la fatturazione, Marketplace AWS gli abbonamenti e gli acquisti contrattuali.

Terminologia

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

Amazon Machine Image (AMI)

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

Abbonamento AMI

: Nel Marketplace AWS, i prodotti software basati su AMI come ROSA classic utilizzano 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 tipo di istanza. Amazon EC2

Abbonamento SaaS

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

Offerta pubblica

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

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. Per impostazione predefinita, le tariffe del servizio ROSA con HCP vengono addebitate su richiesta, a una tariffa oraria fissa basata sul numero di cluster in esecuzione e worker node v in CPUs esecuzione in tali cluster. I costi del servizio ROSA classic vengono calcolati su richiesta in base al numero di worker node v. CPUs ROSA classic 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' Gestione dei costi e fatturazione AWS 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 Account AWS , sei abbonato agli elenchi ROSA classic e ROSA with HCP attivi. 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 classic 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 con HCP e 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

È possibile acquistare contratti di offerta pubblica di 12 mesi per ROSA classic e ROSA with HCP dalla console. ROSA

> **Note**
>
> ROSA classic 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 classic di 12 mesi

Quando acquisti un contratto ROSA classic di 12 mesi, effettui un pagamento anticipato per un periodo annuale e non paghi alcuna tariffa oraria 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, consultare Servizio Red Hat OpenShift su AWS Prezzi.

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**
>
> I contratti ROSA classic di 12 mesi non si rinnovano automaticamente.

Per acquistare un contratto di 12 mesi per ROSA classic

> **Note**
>
> Se si utilizza la ROSA console in una regione che non supporta ancora ROSA con HCP, questo flusso di lavoro non è ancora disponibile. Per un elenco delle regioni che supportano ROSA con HCP, consulta. the section called "Confronto tra ROSA e HCP e ROSA classic"

Per acquistare i contratti ROSA classic nelle regioni senza ROSA con supporto HCP, 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 Contracts for ROSA classic.
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 Supporto Centro e apri una richiesta di assistenza.

Acquisto di un contratto ROSA con HCP di 12 mesi

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

Quando acquisti un contratto ROSA con HCP di 12 mesi, effettui un pagamento anticipato per un periodo annuale e non paghi alcuna tariffa oraria di utilizzo per i 12 mesi successivi per il worker node v e i piani di controllo coperti. CPUs Il costo del contratto si basa sul numero di worknode v CPUs e di piani di controllo selezionati. Il contratto copre solo il nodo di lavoro v CPUs 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, consultare Servizio Red Hat OpenShift su AWS Prezzi.

Quota di utilizzo mensile

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

- Nodo di lavoro vCPUs: numero di v CPUs 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 work-node v CPUs e 8 piani di controllo verrebbe convertito in una quota mensile di 2.920.000 ore di vCPU del nodo di lavoro e 5.840 ore di piano di controllo consumabili al mese.

Per acquistare un contratto ROSA con HCP di 12 mesi

> **Note**
>
> Se si utilizza la Servizio Red Hat OpenShift su AWS console in una regione che non supporta ancora ROSA con piani di controllo ospitati, questo flusso di lavoro non è ancora disponibile. Per un elenco delle regioni che supportano ROSA con HCP, consultathe section called "Confronto tra ROSA e HCP e ROSA classic".

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 v CPUs 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 Supporto Centro e apri una richiesta di assistenza.

Aggiornamento di un contratto ROSA con HCP di 12 mesi

È possibile aggiornare il contratto ROSA attivo con HCP di 12 mesi in qualsiasi momento con worker node v e piani di controllo aggiuntivi. CPUs Quando aggiorni il tuo contratto ROSA con HCP di 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 v CPUs 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 v CPUs e control aggiunti vengono convertiti in una quota di utilizzo mensile utilizzando le stesse formule del contratto di acquisto originale. Per l'utilizzo della vCPU e del piano di controllo che supera la quota mensile si applicano le tariffe orarie di utilizzo on demand. Per ulteriori informazioni, consulta the section called "Quota di utilizzo mensile".

Per aggiornare un contratto di 12 mesi con ROSA con 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 v CPUs 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**
>
> I contratti ROSA classic di 12 mesi non possono essere aggiornati. I contratti ROSA classic 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 o ROSA classic per ricevere i prezzi dei prodotti e i termini del contratto di licenza con l'utente finale (EULA) negoziati con Red Hat. Per ulteriori informazioni, consulta la sezione Offerte private nella Guida all'acquisto. Marketplace AWS

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 classic 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 avere effettuato l'accesso all'account corretto, verrà visualizzato l'errore Pagina non trovata (404).

4. Esamina 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 debug della ROSA CLI forniscono dettagli sui messaggi di errore che vengono prodotti quando una cluster non riesce a creare.

Per visualizzare le informazioni di cluster debug, esegui il seguente comando ROSA CLI. Nel comando, sostituisci `<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 accesso offline scaduti della ROSA CLI

Se utilizzi la 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 API di OpenShift Cluster Manager 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 si utilizza il metodo non STS per il provisioning dei cluster ROSA . Per evitare questo problema, esegui il provisioning dei cluster utilizzando ROSA . AWS STS Per ulteriori informazioni, consulta the section called "Crea un cluster ROSA classic - 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
   ```

Fasi successive

- Consulta la documentazione. OpenShift
- Apri una Supporto 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 di supporto di ROSA, vederethe section called "Ottenere supporto".

Ottenere ROSA assistenza

Con ROSA, puoi ricevere supporto da Supporto 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 Supporto

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 utilizza l' Supporto API per aprire casi per i 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 Supporto piani, consulta. Supporto

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

Per informazioni sulla creazione di un Supporto 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, è possibile iscriversi a un feed RSS.

Modifica	Descrizione	Data
Aggiornato ROSAKubeController Policy	È stata aggiornata la policy AWS gestita ROSAKube ControllerPolicy per chiarire le autorizzazioni di Elastic Load Balancing per la registrazione e l'annullamento della registrazione dei target presso i gruppi target. Per ulteriori informazioni, consulta gli aggiornamenti alle politiche gestite.ROSAAWS	5 marzo 2026
Aggiornato ROSANodePoolManagementPolicy	ROSA ha aggiornato la politica gestita `ROSANodePoolManagementPolicy` per aggiungere l'accesso alle risorse per le prenotazioni di capacità al fine di supportare la funzionalità di prenotazione delle capacità. Per informazioni, consulta ROSA gli aggiornamenti delle politiche AWS gestite.	3 settembre 2025
Politica aggiornata ROSAInstaller	È stata aggiornata la ROSAInstaller policy AWS gestita per supportare la nuova funzionalità di prenotazione delle capacità in ROSA e migliorare la gestione dei tag	7 agosto 2025

	del cluster Kubernetes. Per informazioni, consulta ROSA gli aggiornamenti alle AWS politiche gestite.	
Nuova ROSAShared VPCRoute53 politica	ROSA ha rilasciato una nuova policy gestita `ROSASharedVPCRoute53Policy` per consentire all'installatore ROSA di configurare i record Route 53 in ambienti VPC condivisi. Per informazioni, consulta ROSA gli aggiornamenti alle politiche AWS gestite.	7 agosto 2025
Nuova ROSAShared VPCEndpoint politica	ROSA ha rilasciato una nuova policy gestita `ROSASharedVPCEndpointPolicy` per consentire all'installatore ROSA di configurare endpoint e gruppi di sicurezza VPC in ambienti VPC condivisi . Questa policy fornisce un sottoinsieme di autorizzazioni EC2 su misura per casi d'uso VPC condivisi. Per informazioni, consulta ROSA gli aggiornamenti alle politiche gestite. AWS	7 agosto 2025
Aggiornato ROSAImageRegistryOperatorPolicy	È stata aggiornata la politica AWS gestita ROSAImageRegistryOperatorPolicy.	19 maggio 2025
Aggiornato ROSANodePoolManagementPolicy	È stata aggiornata la politica AWS gestita ROSANodePoolManagementPolicy .	5 maggio 2025

Aggiornato ROSAImage RegistryOperatorPolicy	È stata aggiornata la politica AWS gestita ROSAImage RegistryOperatorPolicy.	16 aprile 2025
Aggiornato ROSAWorke rInstancePolicy	È stata aggiornata la politica AWS gestita ROSAWorke rInstancePolicy.	3 marzo 2025
Aggiornato ROSANodeP oolManagementPolicy	È stata aggiornata la politica AWS gestita ROSANodeP oolManagementPolicy.	24 febbraio 2025
Aggiornato ROSAAmazo nEBSCSIDriverOperatorPolicy	Aggiornata la politica AWS ROSAAmazon EBSCSIDriver OperatorPolicy gestita.	17 gennaio 2025
ROSA con espansione HCP Regione AWS	ROSA con piani di controllo ospitati (HCP) è ora disponibi le in Medio Oriente (Emirati Arabi Uniti). Regione AWS	13 maggio 2024
ROSA con espansione HCP Regione AWS	ROSA con piani di controllo ospitati (HCP) è ora disponibi le in Europa (Parigi). Regione AWS	6 maggio 2024
Aggiornato ROSANodeP oolManagementPolicy	È stata aggiornata la politica AWS ROSANode PoolManag ementPolicy gestita.	2 maggio 2024
ROSA con espansione HCP Regione AWS	ROSA con piani di controllo ospitati (HCP) è ora disponibi le in Europa (Spagna). Regione AWS	29 aprile 2024
Politica aggiornata ROSAInsta ller	Aggiornamento della ROSAInstaller politica AWS gestita.	24 aprile 2024

ROSA con espansione HCP Regione AWS	ROSA con piani di controllo ospitati (HCP) è ora disponibi le in Europa (Zurigo). Regione AWS	19 aprile 2024
ROSA con espansione HCP Regione AWS	ROSA con piani di controllo ospitati (HCP) è ora disponibi le nella regione Asia-Pacifico (Osaka). Regione AWS	17 aprile 2024
ROSAInstallerPolitica e ROSASRESupport politica aggiornate	Aggiornate la ROSAInstaller politica e ROSASRESupport la politica delle politiche AWS gestite.	10 aprile 2024
ROSA con espansione HCP Regione AWS	ROSA con piani di controllo ospitati (HCP) è ora disponibi le nella regione Asia-Pacifico (Hong Kong) Regione AWS.	8 aprile 2024
ROSA con espansione HCP Regione AWS	ROSA con piani di controllo ospitati (HCP) è ora disponibi le in Sud America (San Paolo). Regione AWS	1 aprile 2024
ROSA con espansione HCP Regione AWS	ROSA con piani di controllo ospitati (HCP) è ora disponibi le in Medio Oriente (Regione AWS Bahrein).	25 marzo 2024
ROSA con espansione HCP Regione AWS	ROSA con piani di controllo ospitati (HCP) è ora disponibi le nella regione Asia-Pacifico (Seoul). Regione AWS	14 marzo 2024

ROSA con espansione HCP Regione AWS	ROSA con piani di controllo ospitati (HCP) è ora disponibile in Africa (Città del Capo). Regione AWS	5 marzo 2024
Politica aggiornata ROSAInstaller	Aggiornamento della ROSAInstaller politica AWS gestita.	26 gennaio 2024
ROSASRESupportPolitica aggiornata	Aggiornamento della ROSASRESupport politica AWS gestita.	22 gennaio 2024
Aggiornato ROSAImage RegistryOperatorPolicy	È stata aggiornata la politica AWS gestita ROSAImage RegistryOperatorPolicy.	12 dicembre 2023
Aggiornato ROSAKubeC ontrollerPolicy	È stata aggiornata la politica AWS gestita ROSAKubeC ontrollerPolicy.	16 ottobre 2023
ROSAManageAbbonamento aggiornato	È stato aggiornato l' ROSAManageabbonamento alla politica AWS gestita.	1° agosto 2023
Aggiornato ROSAKubeC ontrollerPolicy	È stata aggiornata la politica AWS gestita ROSAKubeC ontrollerPolicy.	13 luglio 2023
Sono state aggiunte pagine di sicurezza ROSA	Sono state aggiunte la resilienza in ROSA, la sicurezza dell'infrastruttura in ROSA e la protezione dei dati nelle pagine ROSA.	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 politica AWS gestita ROSANode PoolManagementPolicy	È ROSANode PoolManagementPolicy stata aggiunta una nuova politica AWS gestita.	8 giugno 2023
È stata aggiunta una nuova ROSAInstaller politica AWS gestita	È stata aggiunta una nuova ROSAInstaller politica AWS gestita.	6 giugno 2023
È stata aggiunta una nuova ROSASRESupport politica AWS gestita	È stata aggiunta una nuova ROSASRESupport politica AWS gestita.	1 giugno 2023
È stata aggiunta una panoramica delle responsabilità di ROSA	È stata aggiunta una panoramica delle responsabilità per la pagina ROSA.	26 maggio 2023
Aggiornato Che cos'è Servizio Red Hat OpenShift su AWS?	Aggiornata la Servizio Red Hat OpenShift su AWS pagina Cos'è.	24 maggio 2023
Sono state aggiunte nuove politiche AWS gestite per i ruoli di operatore ROSA	Sono state aggiunte nuove politiche AWS ROSAImage RegistryOperatorPolicy gestite e ROSAKMSProvider politiche . ROSAKube ControllerPolicy	27 aprile 2023
È stata aggiunta una nuova politica AWS gestita ROSAControl PlaneOperatorPolicy	È ROSAControl PlaneOperatorPolicy stata aggiunta una nuova politica AWS gestita.	24 aprile 2023
Sono state aggiunte nuove politiche AWS gestite per i ruoli degli account ROSA	Sono state aggiunte nuove pagine di policy AWS gestite per l'account ROSA e la pagina dei ruoli dell'operatore.	20 aprile 2023

È stata aggiunta la pagina delle quote del servizio ROSA	È stata aggiunta la pagina delle quote del servizio ROSA.	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
Aggiunta una nuova polizza AWS gestita (ROSAManageabbonamento)	È stato aggiunto un nuovo ROSAManage abbonamento alla politica AWS gestita.	11 aprile 2022
Versione iniziale	La versione iniziale della Guida per l' Servizio Red Hat OpenShift su AWS 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.