Guida per l'utente

Servizio Red Hat OpenShift su AWS

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

Table of Contents

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 ROSAsemplifica lo spostamento dei OpenShift carichi di lavoro Red Hat locali verso e offre una stretta integrazione con altri. AWS Servizi AWS

Funzionalità

ROSAè 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 Support for ROSA.

ROSAoffre inoltre le seguenti funzionalità:

- Installazione del cluster, manutenzione e aggiornamenti del cluster supportati da Red Hat SRE.
- Servizio AWSIe 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'AWSelevata disponibilità.
- Gestisci i cluster utilizzando OpenShift API e strumenti di produttività per sviluppatori, tra cui Service Mesh, CodeReady Workspaces e Serverless.

ROSAmodelli di distribuzione dei cluster

ROSAoffre due modelli di implementazione del cluster: ROSA con piani di controllo ospitati (ROSA con HCP) e ROSA classic. Con ROSA con HCP, ogni cluster dispone di un piano di controllo dedicato isolato all'interno di Red Hat Account AWS e gestito da Red Hat. Con ROSA classic, l'infrastruttura del piano di controllo del cluster è ospitata presso il clienteAccount 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. Per ulteriori informazioni su ROSA with HCP e ROSA classic, vedere Opzioni di distribuzione.

> **Note**
>
> ROSA con piani di controllo ospitati non offre al momento certificazioni di conformità o Federal Information Processing Standards (FIPS). Per ulteriori informazioni, consulta Compliance nella documentazione di Red Hat.

Accesso a ROSA

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

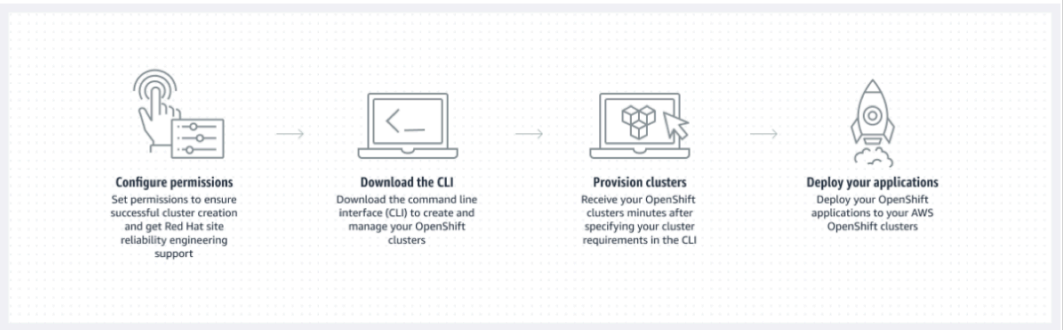
AWS

- ROSAconsole: fornisce un'interfaccia web per abilitare l'ROSAabbonamento 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
- ROSACLI (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 di 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.

Nozioni di base su ROSA



Di seguito viene riepilogato il processo introduttivo di. ROSA Per istruzioni introduttive dettagliate, consulta Guida introduttiva ROSA.

AWS Management Console/AWS CLI

1. Configura le autorizzazioni su Servizi AWS cui ROSA si basa l'erogazione delle funzionalità del servizio. Per ulteriori informazioni, consulta Prerequisiti.
2. Installa e configura lo strumento più recenteAWS CLI. Per ulteriori informazioni, consulta Installazione dell'aggiornamento della versione più recente di AWS CLI nella Guida per l'AWS CLIutente.
3. Abilita ROSA nella ROSAconsole.

ROSAConsole/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.

ROSAcosti 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 supportateAWS. Oltre al costo del servizio worker node, i cluster ROSA con piani di controllo ospitati (HCP) prevedono una tariffa oraria per il cluster.

ROSAoffre 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 i contratti. ROSA

AWStariffe per l'infrastruttura

AWSle 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. AWSle tariffe per l'infrastruttura variano in baseRegione AWS.

Panoramica delle responsabilità per Servizio Red Hat OpenShift su AWS

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 di ROSA servizio e i Red Hat Site Reliability Engineer (SRE) vi accedono in remoto 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

La tabella seguente fornisce una panoramica delle responsabilità di AWSRed 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).

Resource (Risorsa)	Gestione degli incidenti e delle operazioni	Gestione delle modifiche	Autorizzazione dell'accesso e dell'identità	Sicurezza e conformità alle normative	Ripristino di emergenza
Dati dei clienti	Customer	Customer	Customer	Customer	Customer
Applicazioni per i clienti	Customer	Customer	Customer	Customer	Customer
Servizi per sviluppatori	Customer	Customer	Customer	Customer	Customer

Resource (Risorsa)	Gestione degli incidenti e delle operazioni	Gestione delle modifiche	Autorizzazione dell'accesso e dell'identità	Sicurezza e conformità alle normative	Ripristino di emergenza
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, infrastruttura e nodi di lavoro)	Red Hat	Red Hat	Red Hat	Red Hat	Red Hat
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

Resource (Risorsa)	Gestione degli incidenti e delle operazioni	Gestione delle modifiche	Autorizzazione dell'accesso e dell'identità	Sicurezza e conformità alle normative	Ripristino di emergenza
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/ infrastrutturaglobaleAWS	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.

Resource (Risorsa)	Responsabilità di servizio	Responsabilità del cliente
Rete delle applicazioni	Red Hat	Cliente

Resource (Risorsa)	Responsabilità di servizio	Responsabilità del cliente
	• Monitora OpenShift il servizio router nativo e rispondi agli avvisi.	• 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 bilanciamento del AWS carico. • Monitora il traffico di rete configurato opzionalm ente tramite connessione Amazon VPC-to-VPC, AWS VPN connessione o AWS 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 chiave per la Amazon EBS crittografia.

Resource (Risorsa)	Responsabilità di servizio	Responsabilità del cliente
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 globaleAWS	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 AWSRed 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.

Resource (Risorsa)	Responsabilità del servizio	Responsabilità del cliente
Registrazione di log	Red Hat • Aggrega e monitora centralmente i log di controllo della piattaforma.	Cliente • Installa l'operatore di registrazione delle applicazi

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

Resource (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 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.

Resource (Risorsa)	Responsabilità del servizio	Responsabilità del cliente
Rete in cluster	Red Hat • Configura i component i di gestione del cluster, come gli endpoint dei servizi pubblici o privati e l'integra zione necessaria con Amazon VPCi 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'endpoin t del servizio API sia reso pubblico o privato al momento della creazione del cluster o dopo la creazione del cluster tramite Cluster Manager. OpenShift

Resource (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 AWS VPN connettività con risorse locali, connettività Amazon VPCa VPC e, se necessari o, tramite AWS 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, AWS VPN connessione o. AWS Direct Connect • Richiedi e configura eventuali bilanciatori di carico aggiuntivi per servizi specifici.

Resource (Risorsa)	Responsabilità del servizio	Responsabilità del cliente
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.
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.

Resource (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. Consulta le risorse aggiuntiv e per ulteriori informazioni sui pool di computer. • 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.

Resource (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.

Resource (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:
	  • AWS VPN
	  • AWS Direct Connect
	  • AWS PrivateLink
		Cliente
		
		• Firma le richieste utilizzan do un ID chiave di accesso e una chiave di accesso segreta associati a 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

Resource (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.

Resource (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

Resource (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 • Configura 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.

Resource (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 • Configura 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.

Resource (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.

Resource (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 S3Fornisce, 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

Resource (Risorsa)	Responsabilità di servizio	Responsabilità del cliente
Hardware/infrastruttura globaleAWS	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:

Resource (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

Resource (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.

Resource (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.

Resource (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.	

Resource (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'infr astruttura Amazon EC2nella 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 EC2nella Guida per l' Amazon EC2 utente. • Provide AWS KMS, che ROSA consente di crittogra fare i volumi del piano di controllo, dell'infrastruttur a e dei nodi di lavoro e i volumi persistenti. Per ulteriori informazioni, vedere la Amazon EBS crittografia	Cliente • Garantisci che vengano seguite le migliori pratiche di sicurezza e il principio del privilegio minimo per proteggere i dati sull' Amazon EC2 istanza. Per ulteriori informazioni, consulta Sicurezza dell'infr astruttura in Amazon EC2 e Protezione dei dati in Amazon EC2. • Monitora i componenti di rete virtuali configura ti opzionali per individua re potenziali problemi e minacce alla sicurezza. • Configura le regole firewall o le protezioni del data center del cliente necessarie in base alle esigenze. • Crea una 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 informazi oni, consultare il AWS Shared Responsibility Model

Resource (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).

Resource (Risorsa)	Responsabilità di servizio	Responsabilità del cliente
Hardware/infrastruttura globaleAWS	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.

Resource (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.

Resource (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.

Resource (Risorsa)	Responsabilità di servizio	Responsabilità del cliente
AWS software (AWS servizi pubblici)	AWS Calcolo • Fornisci Amazon EC2 funzionalità che supportan o la resilienza dei dati come Amazon EBS istantanee e. Amazon EC2 Auto ScalingPe r ulteriori informazioni, consulta Resilience Amazon EC2nella 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	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

Resource (Risorsa)	Responsabilità di servizio	Responsabilità del cliente
	e Amazon Virtual Private Cloudnella Guida per l'utente. Amazon VPC	
Hardware/infrastruttura globaleAWS	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 AWSTuttavia, AWS Red Hat fornisce vari strumenti per aiutare il cliente a gestire i dati e le applicazioni sulla piattaforma.

Resource (Risorsa)	Come 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

Resource (Risorsa)	Come 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 tali dati.

Resource (Risorsa)	Come AWS e Red Hat aiuta	Responsabilità del cliente
Applicazioni per i clienti	Red Hat • Esegui il provisioning dei cluster con OpenShift componenti installat i in modo che i clienti possano accedere alle API Kubernetes OpenShift e implementare e gestire applicazioni 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 l'accesso alle OpenShift API 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 cliente, servire estername

Resource (Risorsa)	Come 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.	nte, salvare, eseguire il backup e ripristinare i dati e gestire in altro modo i carichi di lavoro ad alta disponibilità e resilienza. • Mantieni la 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.

Opzioni di implementazione

ROSA offre due modelli di implementazione del cluster: ROSA con piani di controllo ospitati (ROSA con HCP) e ROSA classic. Con ROSA con HCP, ogni cluster dispone di un piano di controllo dedicato isolato all'interno di Red Hat Account AWS e gestito da Red Hat. Con ROSA classic, l'infrastruttura del piano di controllo del cluster è ospitata 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. Entrambi i modelli di implementazione del cluster possono essere abilitati nella AWS ROSA console. Puoi scegliere il modello di implementazione che desideri utilizzare quando esegui il provisioning dei ROSA cluster utilizzando la ROSA CLI.

> **Note**
>
> Al momento, ROSA con piani di controllo ospitati non offre certificazioni di conformità o Federal Information Processing Standards (FIPS). Per ulteriori informazioni, consulta Compliance nella documentazione di Red Hat.

Differenze tra ROSA con HCP e ROSA classic

Esistono diverse differenze tecniche tra ROSA con HCP e ROSA classic.

	ROSA con HCP	ROSA classica
Hosting di infrastrutture cluster	• I componenti del piano di controllo, come etcd, API server e oauth, sono ospitati su piattaforme di proprietà e gestite da Red Hat. Account AWS L'infrastruttura del nodo di lavoro è ospitata presso il cliente. Account AWS	• I componenti del piano di controllo sono ospitati sul cliente Account AWS, insieme all'infrastruttura e ai nodi di lavoro.
Durata del provisioning	• Circa 10 minuti.	• Circa 40 minuti.
Architettura	• L'infrastruttura Control Plane è completamente gestita da Red Hat. L'infrastruttura Control Plane non è direttamente disponibile per i clienti finali, tranne che attraverso endpoint dedicati ed esplicitamente esposti. • I nodi di lavoro sono ospitati presso il cliente. Account AWS	• L'infrastruttura del piano di controllo è ospitata presso il cliente Account AWS. • I nodi di lavoro sono ospitati presso il cliente Account AWS.
Amazon EC2 Ingombro minimo	• Un cluster richiede un minimo di due nodi ospitati sul sito del cliente Account AWS.	• Un cluster richiede un minimo di sette nodi ospitati presso il cliente Account AWS.
Fornitura di cluster	• Esegui il provisioning dei cluster utilizzando la CLI ROSA.	• Esegui il provisioning dei cluster utilizzando la CLI

	ROSA con HCP	ROSA classica
	• I clienti forniscono cluster che implementano i componenti del piano di controllo in Red Hat. Account AWS • I clienti forniscono pool di macchine che installano nodi di lavoro all'interno del cliente. Account AWS	ROSA o l'interfaccia utente Web. • Il piano di controllo del cluster, i nodi di lavoro e i nodi dell'infrastruttura vengono forniti al cliente. Account AWS
Aggiornamenti	• Aggiorna il piano di controllo e i pool di macchine separatamente.	• L'intero cluster deve essere aggiornato contempor aneamente.

	ROSA con HCP	ROSA classica
Regioni AWS	• Stati Uniti orientali (Virginia settentrionale) (us-east-1) • Stati Uniti orientali (Ohio) (us-east-2) • Stati Uniti occidentali (Oregon) (us-west-2) • Africa (Città del Capo) (af-south-1) • Asia Pacifico (Hyderabad) (ap-south-2) • Asia Pacific (Giacarta) (ap-southeast-3) • Asia Pacifico (Melbourne) (ap-southeast-4) • Asia Pacifico (Mumbai) (ap-south-1) • Asia Pacifico (Seoul) (ap-northeast-2) • Asia Pacifico (Singapore) (ap-southeast-1) • Asia Pacifico (Sydney) (ap-southeast-2) • Asia Pacifico (Tokyo) (ap-northeast-1) • Canada (Centrale) (ca-central-1) • Europa (Francoforte) (eu-central-1) • Europa (Irlanda) (eu-west-1) • Europa (Londra) (eu-west-2)	• Per Regione AWS la disponibilità, consulta gli Servizio Red Hat OpenShift su AWS endpoint e le quote nella Guida generale di riferimento. AWS

	ROSA con HCP	ROSA classica
	• Europa (Milano) (eu-south-1) • Europa (Stoccolma) (eu-north-1) • Medio Oriente (Bahrein) (me-south-1) • Sud America (San Paolo) (sa-east-1)	
Conformità	• Certificazioni di conformità e FIPS non ancora disponibili.	• Per informazioni sulla conformità, consulta Compliance nella documentazione di Red Hat.

Nozioni di base su 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

ROSAmodelli di implementazione dei cluster

ROSAsupporta due modelli di implementazione del cluster: ROSA con piani di controllo ospitati (ROSA con HCP) e ROSA classic. ROSA con HCP offre un'architettura del piano di controllo più efficiente che riduce i costi di AWS infrastruttura ROSA e consente tempi di creazione dei cluster più rapidi. Per ulteriori informazioni su ROSA with HCP e ROSA classic, consulta Opzioni di distribuzione.

> **Note**
>
> ROSA con piani di controllo ospitati non offre al momento certificazioni di conformità o FIPS. Per ulteriori informazioni, consulta la sezione Compliance nella documentazione di Red Hat.

Guide introduttive

Sono disponibili quattro guide introduttive per la distribuzione di un'applicazione in un ROSA cluster appena creato. Ogni tutorial tratta quanto segue:

- Abilitazione del ROSA servizio e configurazione dei AWS prerequisiti
- Creazione dei IAM ruoli e delle politiche necessari
- Creazione del ROSA cluster
- Creazione di un amministratore del cluster per un accesso rapido al cluster
- Configurazione di un provider di identità
- Concessione dell'accesso degli utenti al cluster
- Distribuire un'applicazione nel cluster
- Eliminazione del cluster e delle risorse del cluster

Guida introduttiva a ROSA con HCP

Con ROSA with HCP, è possibile utilizzare AWS STS la ROSA CLI per creare un cluster con i ruoli e le politiche IAM necessari collegati. Per ulteriori informazioni sulle IAM politiche per ROSA con HCP, consulta le politiche AWSgestite IAM per. ROSA

Una volta creato il cluster, è possibile distribuire carichi di lavoro di applicazioni pubbliche nel cluster utilizzando la Red Hat Hybrid Cloud Console o la CLI OpenShift . Per i passaggi per distribuire un'applicazione su un cluster ROSA con HCP appena creato, vedere Guida introduttiva a ROSA con HCP utilizzando la CLI ROSA in modalità auto.

Guida introduttiva a ROSA classic

Con ROSA classic, è possibile utilizzare AWS STS la ROSA CLI per creare un cluster con i IAM ruoli e le politiche necessari allegati. Una volta creato il cluster, è possibile distribuire carichi di lavoro di applicazioni pubbliche nel cluster utilizzando la Red Hat Hybrid Cloud Console o la CLI OpenShift . Per i passaggi per iniziare a utilizzare la modalità di creazione automatica del cluster (`auto`) della CLI ROSA, vedere Guida introduttiva a ROSA classic utilizzando la ROSA CLI in modalità auto. Per i passaggi per iniziare a utilizzare la modalità di creazione manuale del cluster (`manual`) della CLI ROSA, vedere Guida introduttiva a ROSA classic all'uso della ROSA CLI in modalità manuale.

Se desideri che i carichi di lavoro del cluster e delle applicazioni ROSA classic siano privati, consulta Guida introduttiva all'utilizzo di ROSA classic. AWS PrivateLink

Guida introduttiva a ROSA con HCP utilizzando la ROSA CLI in modalità auto

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 ulteriori informazioni su ROSA con HCP, vedere Opzioni di distribuzione.

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 altre opzioni per iniziare, consulta Guida introduttiva. ROSA

Argomenti

Prerequisiti

Prima di iniziare, assicurati di aver completato queste azioni:

- Installa e configura la versione più recenteAWS 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.
- Service Quotasdeve avere le quote di servizio richieste impostate per Amazon EC2Amazon VPC,Amazon EBS, e Elastic Load Balancing necessarie per creare ed eseguire un ROSA cluster. AWSoppure Red Hat può richiedere aumenti delle quote di servizio per vostro conto, se necessario per la risoluzione dei problemi. Per visualizzare le quote richieste, consulta Servizio Red Hat OpenShift su AWSendpoint e quote nel AWS Riferimento generale.
- Per ricevere AWS supporto perROSA, 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 Support for ROSA. Per abilitareAWS Support, consulta la AWS Supportpagina.

- 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 la documentazione sulla risoluzione dei problemi di ROSASCP. Per ulteriori informazioni sugli SCP, vedere Service control policies (SCP).
- 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 incluse nel comando Account AWS seguente.

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

  Per ulteriori informazioni sull'abilitazione delle regioni, consulta Managing Regioni AWS in AWS General Reference.

Fase 1: abilitare ROSA e configurare i prerequisiti

Per creare un ROSAcluster, devi prima 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 Inizia.
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

Fase 2: Creare Amazon VPC un'architettura per ROSA con cluster HCP

Per creare un ROSA con HCPcluster, è necessario innanzitutto configurare la propria Amazon VPC architettura in cui implementare la soluzione. ROSA with HCP richiede che i clienti configurino

almeno una sottorete pubblica e privata per ogni zona di disponibilità utilizzata per creare i cluster. Per i cluster Single-AZ, viene utilizzata solo la zona di disponibilità. Per i cluster Multi-AZ, sono necessarie tre zone di disponibilità.

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

La procedura seguente utilizza la AWS CLI per creare una sottorete pubblica e privata in un'unica zona di disponibilità per un cluster Single-AZ. Tutte le cluster risorse si trovano nella sottorete privata. La sottorete pubblica indirizza il traffico in uscita utilizzando un gateway NAT verso Internet.

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).

1. Imposta una variabile di ambiente per il cluster nome eseguendo il comando seguente.

   ```
   ROSA_CLUSTER_NAME=rosa-hcp
   ```

2. 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 del nuovo VPC. Di seguito è riportato un esempio di output.

   ```
   vpc-0410832ee325aafea
   ```

3. Utilizzando l'ID VPC del passaggio precedente, tagga il VPC utilizzando la variabile. `ROSA_CLUSTER_NAME`

   ```
   aws ec2 create-tags --resources <VPC_ID_VALUE> --tags Key=Name,Value=
   $ROSA_CLUSTER_NAME
   ```

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

   ```
   aws ec2 modify-vpc-attribute --vpc-id <VPC_ID_VALUE> --enable-dns-hostnames
   ```

5. Crea una sottorete pubblica nel VPC con `10.0.1.0/24` un blocco CIDR, specificando la zona di disponibilità in cui deve essere creata la risorsa.

> **Important**
>
> Durante la creazione di sottoreti, assicurati che le sottoreti vengano create in una zona di disponibilità con tipi di istanze disponibili. ROSA Se non scegli una zona di disponibilità specifica, la sottorete viene creata in una qualsiasi delle zone di disponibilità specificate. Regione AWS
>
> Per specificare una zona di disponibilità specifica, utilizzate l'`--availability zone`argomento nel `create-subnet` comando. È possibile utilizzare il `rosa list instance-types` comando per elencare tutti i tipi di ROSA istanze disponibili. Per verificare se un tipo di istanza è disponibile per una determinata zona di disponibilità, utilizzate il comando seguente.
>
> ```
> aws ec2 describe-instance-type-offerings --location-type availability-zone --
> filters Name=location,Values=<availability_zone> --region <region> --output
>  text | egrep "<instance_type>"
> ```

> **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 i cluster Single-AZ, è necessaria una sola zona di disponibilità. Per i cluster Multi-AZ, sono necessarie tre zone di disponibilità. Se questi requisiti non vengono soddisfatti, la creazione del cluster non riesce.

```
aws ec2 create-subnet --vpc-id <VPC_ID_VALUE> --cidr-block 10.0.1.0/24 --
availability-zone <AZ_NAME> --query Subnet.SubnetId --output text
```

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

```
subnet-0b6a7e8cbc8b75920
```

6. Utilizzando l'ID di sottorete del passaggio precedente, etichettate la sottorete utilizzando la variabile. `ROSA_CLUSTER_NAME-public`

```
aws ec2 create-tags --resources <PUBLIC_SUBNET_ID> --tags Key=Name,Value=
$ROSA_CLUSTER_NAME-public
```

7. Crea una sottorete privata nel VPC con `10.0.0.0/24` un blocco CIDR, specificando la stessa zona di disponibilità in cui è stata distribuita la sottorete pubblica.

   ```
   aws ec2 create-subnet --vpc-id <VPC_ID_VALUE> --cidr-block 10.0.0.0/24 --
   availability-zone <AZ_NAME> --query Subnet.SubnetId --output text
   ```

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

   ```
   subnet-0b6a7e8cbc8b75920
   ```

8. Utilizzando l'ID di sottorete del passaggio precedente, etichettate la sottorete utilizzando la variabile. `ROSA_CLUSTER_NAME-private`

   ```
   aws ec2 create-tags --resources <PRIVATE_SUBNET_ID> --tags Key=Name,Value=
   $ROSA_CLUSTER_NAME-private
   ```

9. Crea un gateway Internet per il traffico in uscita e collegalo al VPC.

   ```
   aws ec2 create-internet-gateway --query InternetGateway.InternetGatewayId --output
    text

   aws ec2 attach-internet-gateway --vpc-id <VPC_ID_VALUE> --internet-gateway-id
    <IG_ID_VALUE>
   ```

10. Etichetta il gateway Internet con la `ROSA_CLUSTER_NAME` variabile.

    ```
    aws ec2 create-tags --resources <IG_ID_VALUE> --tags Key=Name,Value=
    $ROSA_CLUSTER_NAME
    ```

11. Crea una tabella di routing per il traffico in uscita, associala alla sottorete pubblica e configura il traffico da indirizzare verso il gateway Internet.

    ```
    aws ec2 create-route-table --vpc-id <VPC_ID_VALUE> --query RouteTable.RouteTableId --
    output text
    ```

```
aws ec2 associate-route-table --subnet-id <PUBLIC_SUBNET_ID> --route-table-id
 <PUBLIC_RT_ID>

aws ec2 create-route --route-table-id <PUBLIC_RT_ID> --destination-cidr-block
 0.0.0.0/0 --gateway-id <IG_ID_VALUE>
```

12. Etichetta la tabella delle rotte pubbliche con la `ROSA_CLUSTER_NAME` variabile e verifica che la tabella delle rotte sia stata configurata correttamente.

```
aws ec2 create-tags --resources <PUBLIC_RT_ID> --tags Key=Name,Value=
$ROSA_CLUSTER_NAME

aws ec2 describe-route-tables --route-table-id <PUBLIC_RT_ID>
```

13. Crea un gateway NAT nella sottorete pubblica con un indirizzo IP elastico per abilitare il traffico verso la sottorete privata.

```
aws ec2 allocate-address --domain vpc --query AllocationId --output text

aws ec2 create-nat-gateway --subnet-id <PUBLIC_SUBNET_ID> --allocation-id
 <EIP_ADDRESS>  --query NatGateway.NatGatewayId --output text
```

14. Etichetta il gateway NAT e l'indirizzo IP elastico con la variabile. `$ROSA_CLUSTER_NAME`

```
aws ec2 create-tags --resources <EIP_ADDRESS>  --resources <NAT_GATEWAY_ID> --tags
 Key=Name,Value=$ROSA_CLUSTER_NAME
```

15. Crea una tabella di routing per il traffico di sottorete privato, associala alla sottorete privata e configura il traffico per il routing verso il gateway NAT.

```
aws ec2 create-route-table --vpc-id <VPC_ID_VALUE> --query RouteTable.RouteTableId --
output text

aws ec2 associate-route-table --subnet-id <PRIVATE_SUBNET_ID> --route-table-id
 <PRIVATE_RT_ID>

aws ec2 create-route --route-table-id <PRIVATE_RT_ID> --destination-cidr-block
 0.0.0.0/0 --gateway-id <NAT_GATEWAY_ID>
```

16. Assegna un tag alla tabella di routing privata e all'indirizzo IP elastico con la variabile. `$ROSA_CLUSTER_NAME-private`

```
aws ec2 create-tags --resources <PRIVATE_RT_ID> <EIP_ADDRESS> --tags Key=Name,Value=
$ROSA_CLUSTER_NAME-private
```

Fase 3: 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, consulta le politiche gestite per. AWSIAMROSA

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'IAMaccount richiesti.

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

   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.

   > **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 Risolvere i 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
```

Fase 4: Creare un cluster ROSA con HCP AWS STS e la modalità ROSA CLI `auto`

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-AZcluster, specificate `multi-az` nel comando e gli ID di sottorete privati 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 gli ID di sottorete pubblici e privati.

```
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 gli ID di sottorete privati.

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

2. clusterControlla 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, consulta Risolvere i problemi di creazione ROSA del cluster.
> Per contattare il AWS Support nostro supporto Red Hat per ricevere assistenza, consulta Support for ROSA.

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

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

Fase 5: Configurare un provider di identità e concedere l'accesso cluster

ROSAinclude un server OAuth integrato. Dopo aver creato cluster il tuo, devi configurare OAuth per utilizzare un provider di identità. Puoi quindi aggiungere utenti al tuo provider di identità configurato per concedere loro l'accesso al tuo. cluster Puoi concedere a questi utenti `cluster-admin` o `dedicated-admin` autorizzazioni come richiesto.

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

> **Important**
>
> Il provider di identità HTPasswd è incluso solo per consentire la creazione di un singolo utente amministratore statico. HTPassWD non è supportato come provider di identità di uso generale 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'clusteraccesso 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 applicazione OAuth nella tua GitHub organizzazione.
7. Utilizza le informazioni della pagina GitHub OAuth 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 OAuth. GitHub

```
...
? 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 pod OAuth ridistribuirsi con la configurazione aggiornata.

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

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

Passaggio 6: concedere 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.

Passaggio 7: concedere le autorizzazioni di amministratore a un utente

Dopo aver aggiunto un utente al provider di identità configurato, puoi concedere all'utente `cluster-admin` o le `dedicated-admin` autorizzazioni per il tuo. cluster

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

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

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

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

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

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

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

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

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

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

Fase 8: 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. Sostituisci `<CLUSTER_NAME>` con il nome del 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.

Fase 9: Implementazione di un'applicazione dal Catalogo per sviluppatori

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

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

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

10. Nella sezione Git, scegli Try Sample.
11. Nel campo Nome, aggiungi un nome univoco.
12. Seleziona 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.

Passo 10: 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 daROSA, puoi utilizzare la console. IAM

> **Important**
>
> IAMi 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 tuocluster.

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

> **Important**
>
> È necessario attendere l'clustereliminazione 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 predefinito`ManagedOpenShift`.

```
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 percluster.

Guida introduttiva a ROSA classic utilizzando la ROSA CLI in modalità auto

Le seguenti sezioni descrivono come iniziare a usare ROSA classic utilizzando AWS STS e la ROSA CLI. Per ulteriori informazioni su ROSA classic, consulta Opzioni di distribuzione.

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.

Le procedure in questo documento utilizzano la `auto` modalità ROSA CLI per creare le IAM risorse richieste per ROSA classic. Per ulteriori opzioni per iniziare, consulta Guida introduttiva ROSA.

Argomenti

Prerequisiti

Prima di iniziare, assicurati di aver completato queste azioni:

- Installa e configura la versione più recenteAWS 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.
- Service Quotasdeve avere le quote di servizio richieste impostate per Amazon EC2Amazon VPC,Amazon EBS, e Elastic Load Balancing necessarie per creare ed eseguire un ROSA cluster. AWSoppure Red Hat può richiedere aumenti delle quote di servizio per vostro conto, se necessario per la risoluzione dei problemi. Per visualizzare le quote richieste, consulta Servizio Red Hat OpenShift su AWSendpoint e quote nel AWS Riferimento generale.

- Per ricevere AWS supporto perROSA, 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 Support for ROSA. Per abilitareAWS Support, consulta la AWS Supportpagina.
- 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 la documentazione sulla risoluzione dei problemi di ROSASCP. Per ulteriori informazioni sugli SCP, vedere Service control policies (SCP).
- 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 incluse nel comando Account AWS seguente.

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

  Per ulteriori informazioni sull'abilitazione delle regioni, consulta Managing Regioni AWS in AWS General Reference.

Fase 1: abilitare ROSA e configurare i prerequisiti

Per creare un ROSAcluster, è necessario innanzitutto abilitare il ROSA servizio nella AWS ROSA console e verificare che i AWS prerequisiti siano stati soddisfatti. 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. Scegliere Inizia.
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 di terminale per creare il tuo primo ROSA classic utilizzando la CLI. cluster ROSA

Fase 2: Creare un cluster ROSA classic con AWS STS e la modalità ROSA`auto` CLI

È possibile creare un classico ROSA cluster utilizzando AWS Security Token Service (AWS STS) e la `auto` modalità fornita nella ROSA CLI.

1. Crea i ruoli e le politiche IAM dell'account richiesti.

```
rosa create account-roles --mode auto
```

> **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 Risolvere i token di accesso offline scaduti della ROSA CLI.

2. Crea un cluster with AWS STS utilizzando le impostazioni predefinite nella modalità CLI. ROSA `auto` Quando si utilizzano le impostazioni predefinite, viene installata l'ultima versione stabile. OpenShift

```
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.

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, consulta Risolvere i problemi di provisioning ROSA del cluster.

Per contattare il AWS Support nostro supporto Red Hat per ricevere assistenza, consulta Support for ROSA.

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

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

Fase 3: Configurare un provider di identità e concedere l'accesso cluster

ROSAinclude un server OAuth integrato. Dopo aver creato cluster il tuo, devi configurare OAuth per utilizzare un provider di identità. Puoi quindi aggiungere utenti al tuo provider di identità configurato per concedere loro l'accesso al tuo. cluster Puoi concedere a questi utenti `cluster-admin` o `dedicated-admin` autorizzazioni come richiesto.

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

Important

Il provider di identità HTPasswd è incluso solo per consentire la creazione di un singolo utente amministratore statico. HTPassWD non è supportato come provider di identità di uso generale 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'clusteraccesso 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 applicazione OAuth nella tua GitHub organizzazione.
7. Utilizza le informazioni della pagina GitHub OAuth 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 OAuth. GitHub

```
...
? 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 pod OAuth ridistribuirsi con la configurazione aggiornata.

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

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

Passaggio 4: concedere 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.

Passaggio 5: concedere le autorizzazioni di amministratore a un utente

Dopo aver aggiunto un utente al provider di identità configurato, puoi concedere all'utente `cluster-admin` o le `dedicated-admin` autorizzazioni per il tuo. cluster

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

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

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

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

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

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

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

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

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

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

Passaggio 6: Accedere a cluster tramite la console Web

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. Sostituisci `<CLUSTER_NAME>` con il nome del 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 tuocluster, scegli il nome del provider di identità nella finestra di dialogo Accedi con... e completa tutte le richieste di autorizzazione presentate dal tuo provider.

Fase 7: Implementazione di un'applicazione dal Catalogo per sviluppatori

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

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

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

10. Nella sezione Git, scegli Try Sample.
11. Nel campo Nome, aggiungi un nome univoco.
12. Seleziona 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.

Passaggio 8: Revoca le autorizzazioni di amministratore e l'accesso degli utenti

È possibile revocare `dedicated-admin` le `cluster-admin` autorizzazioni a un utente utilizzando la CLI. ROSA

Per revocare l'accesso a un utente, è necessario rimuovere l'utente dal provider di identità configurato.

Revoca le autorizzazioni **`cluster-admin`** di 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.

Fase 9: 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 daROSA, puoi utilizzare la console. IAM

> **Important**
>
> IAMi 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 tuocluster.

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

> **Important**
>
> È necessario attendere l'clustereliminazione 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 dall'installatore. 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 percluster.

Guida introduttiva a ROSA classic utilizzando la ROSA CLI in modalità manuale

Le seguenti sezioni descrivono come iniziare a usare ROSA classic utilizzando AWS STS e la ROSA CLI. Per ulteriori informazioni su ROSA classic, consulta Opzioni di distribuzione.

La ROSA CLI utilizza la `auto` modalità o la `manual` modalità per creare IAM le risorse necessarie per il provisioning di 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. È inoltre possibile utilizzare `manual` per passare i comandi a un altro amministratore o gruppo dell'organizzazione in modo che possa creare le risorse.

Le procedure in questo documento utilizzano la `manual` modalità ROSA CLI per creare le IAM risorse richieste per ROSA classic. Per ulteriori opzioni per iniziare, consulta Guida introduttiva ROSA.

Argomenti

- Prerequisiti
- Fase 1: abilitare ROSA e configurare i prerequisiti
- Fase 2: Creare un cluster ROSA classic con AWS STS e la modalità ROSAmanual CLI

- Fase 3: Configurare un provider di identità e concedere l'accesso cluster
- Passaggio 4: concedere all'utente l'accesso a un cluster
- Passaggio 5: concedere le autorizzazioni di amministratore a un utente
- Passaggio 6: Accedere a cluster tramite la console Web
- Fase 7: Distribuire un'applicazione dal Catalogo per sviluppatori
- Passaggio 8: Revoca le autorizzazioni di amministratore e l'accesso degli utenti
- Fase 9: Eliminare un cluster e AWS STS delle risorse

Prerequisiti

Prima di iniziare, assicurati di aver completato queste azioni:

- Installa e configura la versione più recenteAWS 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.
- Service Quotasdeve avere le quote di servizio richieste impostate per Amazon EC2Amazon VPC,Amazon EBS, e Elastic Load Balancing necessarie per creare ed eseguire un ROSA cluster. AWSoppure Red Hat può richiedere aumenti delle quote di servizio per vostro conto, se necessario per la risoluzione dei problemi. Per visualizzare le quote richieste, consulta Servizio Red Hat OpenShift su AWSendpoint e quote nel AWS Riferimento generale.
- Per ricevere AWS supporto perROSA, 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 Support for ROSA. Per abilitareAWS Support, consulta la AWS Supportpagina.
- 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 la documentazione sulla risoluzione dei problemi di ROSASCP. Per ulteriori informazioni sugli SCP, vedere Service control policies (SCP).
- 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 incluse nel comando Account AWS seguente.

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

Per ulteriori informazioni sull'abilitazione delle regioni, consulta Managing Regioni AWS in AWS General Reference.

Fase 1: abilitare ROSA e configurare i prerequisiti

Per creare un ROSAcluster, devi prima 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. Scegliere Inizia.
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

Fase 2: Creare un cluster ROSA classic con AWS STS e la modalità ROSA`manual` CLI

È possibile creare un classico ROSA cluster utilizzando AWS Security Token Service (AWS STS) e la `manual` modalità fornita nella ROSA CLI.

Quando si crea uncluster, è possibile `rosa create cluster --interactive` eseguire la personalizzazione della distribuzione con una serie di istruzioni interattive. Per ulteriori informazioni, consultate Interactive Cluster Creation Mode Reference nella documentazione di Red Hat.

Dopo il provisioning, cluster viene fornito un singolo comando nell'output. Esegui questo comando per distribuire altri cluster che utilizzano la stessa identica configurazione personalizzata.

> **Note**
>
> AWSI VPC condivisi non sono attualmente supportati per le installazioni. ROSA

1. Crea i ruoli e le politiche IAM dell'account richiesti.

```
rosa create account-roles --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 Risolvere i token di accesso offline scaduti della ROSA CLI.

2. Esegui i AWS CLI comandi generati nell'output per creare i ruoli e le politiche.
3. Crea una `--interactive` modalità cluster with AWS STS in per specificare eventuali impostazioni personalizzate.

```
rosa create cluster --interactive --sts
```

> **Important**
>
> Dopo aver abilitato la crittografia etcd per i valori delle chiavi in etcd, si verifica un sovraccarico di prestazioni di circa il 20%. L'overhead è il risultato dell'introduzione di questo secondo livello di crittografia, in aggiunta alla Amazon EBS crittografia predefinita che crittografa i volumi etcd.

4. Per creare i IAM ruoli operatore specifici del cluster, genera i file JSON delle politiche dell'operatore nella directory di lavoro corrente e invia i comandi per la revisione. AWS CLI

```
rosa create operator-roles --mode manual --cluster <CLUSTER_NAME|CLUSTER_ID>
```

5. Esegui i AWS CLI comandi dall'output.
6. Crea il provider OpenID Connect (OIDC) che cluster gli operatori utilizzano per l'autenticazione.

```
rosa create oidc-provider --mode auto --cluster <CLUSTER_NAME|CLUSTER_ID>
```

7. Controlla lo stato del tuo. cluster

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

> **Note**
>
> Se il processo di creazione fallisce o il `State` campo non diventa pronto dopo 40 minuti, consulta Risolvere i problemi di creazione ROSA del cluster.
> Per contattare il AWS Support nostro supporto Red Hat per ricevere assistenza, consulta Support for ROSA.

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

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

Fase 3: Configurare un provider di identità e concedere l'accesso cluster

ROSAinclude un server OAuth integrato. Dopo aver creato cluster il tuo, devi configurare OAuth per utilizzare un provider di identità. Puoi quindi aggiungere utenti al tuo provider di identità configurato per concedere loro l'accesso al tuo. cluster Puoi concedere a questi utenti `cluster-admin` o `dedicated-admin` autorizzazioni come richiesto.

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

> **Important**
>
> Il provider di identità HTPasswd 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 tuo cluster.

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

4. Segui le istruzioni di configurazione nell'output per limitare l'clusteraccesso 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 con il seguente comando. Sostituiscilo <GITHUB_ORG_NAME> con il nome della tua GitHub organizzazione.
6. Nella pagina GitHub Web, scegli Registra applicazione per registrare una nuova applicazione OAuth nella tua GitHub organizzazione.

7. Utilizza le informazioni della pagina GitHub OAuth per compilare i prompt `rosa create idp` interattivi rimanenti utilizzando il comando seguente. Sostituisci `<GITHUB_CLIENT_ID>` e `<GITHUB_CLIENT_SECRET>` con le credenziali dell'applicazione OAuth. GitHub

```
...
? 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 pod OAuth ridistribuirsi con la configurazione aggiornata.

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

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

Passaggio 4: concedere 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 a. 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 documentazione su Github.

Passaggio 5: concedere le autorizzazioni di amministratore a un utente

Dopo aver aggiunto un utente al provider di identità configurato, puoi concedere all'utente `cluster-admin` o le `dedicated-admin` autorizzazioni per il tuo. cluster

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

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

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

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

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

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

1. Concedi le `dedicated-admin` autorizzazioni utilizzando 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>
```

Passaggio 6: Accedere a cluster tramite la console Web

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 cluster utilizzando il seguente comando. Sostituisci `<CLUSTER_NAME>` con il nome del cluster.

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

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

Fase 7: Distribuire un'applicazione dal Catalogo per sviluppatori

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

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

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

10. Nella sezione Git, scegli Try Sample.

11. Nel campo Nome, aggiungi un nome univoco.
12. Seleziona 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.

Passaggio 8: Revoca le autorizzazioni di amministratore e l'accesso degli utenti

È possibile revocare `dedicated-admin` le `cluster-admin` autorizzazioni a un utente utilizzando la CLI. ROSA

Per revocare l'accesso a un utente, è necessario rimuovere l'utente dal provider di identità configurato.

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

1. Revoca l'`cluster-admin`autorizzazione 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 l'`dedicated-admin`autorizzazione 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.

Fase 9: 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 daROSA, puoi utilizzare la console. IAM

> **Important**
>
> IAMi 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 tuocluster.

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

> **Important**
>
> È necessario attendere l'clustereliminazione 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 predefinito`ManagedOpenShift`.

```
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 percluster.

Guida introduttiva all'utilizzo di ROSA classic 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, consulta Opzioni di distribuzione. 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 PrivateLinkè 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. ConAWS 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 Che cos'è AWS PrivateLink.

Argomenti

Prerequisiti

Prima di iniziare, assicurati di aver completato queste azioni:

- Installa e configura la versione più recenteAWS 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.
- Service Quotasdeve avere le quote di servizio richieste impostate per Amazon EC2Amazon VPC,Amazon EBS, e Elastic Load Balancing necessarie per creare ed eseguire un ROSA cluster. AWSoppure Red Hat può richiedere aumenti delle quote di servizio per vostro conto, se necessario per la risoluzione dei problemi. Per visualizzare le quote richieste, consulta Servizio Red Hat OpenShift su AWSendpoint e quote nel AWS Riferimento generale.
- Per ricevere AWS supporto perROSA, 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 Support for ROSA. Per abilitareAWS Support, consulta la AWS Supportpagina.
- 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 la documentazione sulla risoluzione dei problemi di ROSASCP. Per ulteriori informazioni sugli SCP, vedere Service control policies (SCP).
- 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 incluse nel comando Account AWS seguente.

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

  Per ulteriori informazioni sull'abilitazione delle regioni, consulta Managing Regioni AWS in AWS General Reference.

Fase 1: abilitare ROSA e configurare i prerequisiti

Per creare un ROSAcluster, devi prima 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 Inizia.
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

Fase 2: Creare l'architettura per il cluster Amazon VPC

Per creare un'architettura ROSA cluster che utilizziAWS PrivateLink, devi prima configurare la tua Amazon VPC architettura in cui implementare la soluzione. ROSArichiede che i clienti configurino almeno una sottorete pubblica e privata per ogni zona di disponibilità utilizzata per creare i cluster. Per i cluster Single-AZ, viene utilizzata solo la zona di disponibilità. Per i cluster Multi-AZ, sono necessarie tre zone di disponibilità.

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

La procedura seguente utilizza la AWS CLI per creare una sottorete pubblica e privata in un'unica zona di disponibilità per un cluster Single-AZ. Tutte le cluster risorse si trovano nella sottorete privata. La sottorete pubblica indirizza il traffico in uscita utilizzando un gateway NAT verso Internet.

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).

1. Imposta una variabile di ambiente per il cluster nome eseguendo il comando seguente.

```
ROSA_CLUSTER_NAME=rosa-privatelink
```

2. 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 del nuovo VPC. Di seguito è riportato un esempio di output.

```
vpc-0410832ee325aafea
```

3. Utilizzando l'ID VPC del passaggio precedente, tagga il VPC utilizzando la variabile. `ROSA_CLUSTER_NAME`

```
aws ec2 create-tags --resources <VPC_ID_VALUE> --tags Key=Name,Value=
$ROSA_CLUSTER_NAME
```

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

```
aws ec2 modify-vpc-attribute --vpc-id <VPC_ID_VALUE> --enable-dns-hostnames
```

5. Crea una sottorete pubblica nel VPC con `10.0.1.0/24` un blocco CIDR, specificando la zona di disponibilità in cui deve essere creata la risorsa.

> **Important**
>
> Durante la creazione di sottoreti, assicurati che le sottoreti vengano create in una zona di disponibilità con tipi di istanze disponibili. ROSA Se non scegli una zona di disponibilità specifica, la sottorete viene creata in una qualsiasi delle zone di disponibilità specificate. Regione AWS
> Per specificare una zona di disponibilità specifica, utilizzate l'`--availability zone`argomento nel `create-subnet` comando. È possibile utilizzare il `rosa list instance-types` comando per elencare tutti i tipi di ROSA istanze disponibili. Per verificare se un tipo di istanza è disponibile per una determinata zona di disponibilità, utilizzate il comando seguente.
>
> ```
> aws ec2 describe-instance-type-offerings --location-type availability-zone --
> filters Name=location,Values=<availability_zone> --region <region> --output
>  text | egrep "<instance_type>"
> ```

> **Important**
>
> ROSArichiede che i clienti configurino almeno una sottorete pubblica e privata per ogni zona di disponibilità utilizzata per creare i cluster. Per i cluster Single-AZ, è necessaria una

sola zona di disponibilità. Per i cluster Multi-AZ, sono necessarie tre zone di disponibilità. Se questi requisiti non vengono soddisfatti, la creazione del cluster non riesce.

```
aws ec2 create-subnet --vpc-id <VPC_ID_VALUE> --cidr-block 10.0.1.0/24 --
availability-zone <AZ_NAME> --query Subnet.SubnetId --output text
```

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

```
subnet-0b6a7e8cbc8b75920
```

6. Utilizzando l'ID di sottorete del passaggio precedente, etichettate la sottorete utilizzando la variabile. `ROSA_CLUSTER_NAME-public`

```
aws ec2 create-tags --resources <PUBLIC_SUBNET_ID> --tags Key=Name,Value=
$ROSA_CLUSTER_NAME-public
```

7. Crea una sottorete privata nel VPC con `10.0.0.0/24` un blocco CIDR, specificando la stessa zona di disponibilità in cui è stata distribuita la sottorete pubblica.

```
aws ec2 create-subnet --vpc-id <VPC_ID_VALUE> --cidr-block 10.0.0.0/24 --
availability-zone <AZ_NAME> --query Subnet.SubnetId --output text
```

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

```
subnet-0b6a7e8cbc8b75920
```

8. Utilizzando l'ID di sottorete del passaggio precedente, etichettate la sottorete utilizzando la variabile. `ROSA_CLUSTER_NAME-private`

```
aws ec2 create-tags --resources <PRIVATE_SUBNET_ID> --tags Key=Name,Value=
$ROSA_CLUSTER_NAME-private
```

9. Crea un gateway Internet per il traffico in uscita e collegalo al VPC.

```
aws ec2 create-internet-gateway --query InternetGateway.InternetGatewayId --output
 text
```

```
aws ec2 attach-internet-gateway --vpc-id <VPC_ID_VALUE> --internet-gateway-id
 <IG_ID_VALUE>
```

10. Etichetta il gateway Internet con la ROSA_CLUSTER_NAME variabile.

```
aws ec2 create-tags --resources <IG_ID_VALUE> --tags Key=Name,Value=
$ROSA_CLUSTER_NAME
```

11. Crea una tabella di routing per il traffico in uscita, associala alla sottorete pubblica e configura il traffico da indirizzare verso il gateway Internet.

```
aws ec2 create-route-table --vpc-id <VPC_ID_VALUE> --query RouteTable.RouteTableId --
output text

aws ec2 associate-route-table --subnet-id <PUBLIC_SUBNET_ID> --route-table-id
 <PUBLIC_RT_ID>

aws ec2 create-route --route-table-id <PUBLIC_RT_ID> --destination-cidr-block
 0.0.0.0/0 --gateway-id <IG_ID_VALUE>
```

12. Etichetta la tabella delle rotte pubbliche con la ROSA_CLUSTER_NAME variabile e verifica che la tabella delle rotte sia stata configurata correttamente.

```
aws ec2 create-tags --resources <PUBLIC_RT_ID> --tags Key=Name,Value=
$ROSA_CLUSTER_NAME

aws ec2 describe-route-tables --route-table-id <PUBLIC_RT_ID>
```

13. Crea un gateway NAT nella sottorete pubblica con un indirizzo IP elastico per abilitare il traffico verso la sottorete privata.

```
aws ec2 allocate-address --domain vpc --query AllocationId --output text

aws ec2 create-nat-gateway --subnet-id <PUBLIC_SUBNET_ID> --allocation-id
 <EIP_ADDRESS>  --query NatGateway.NatGatewayId --output text
```

14. Etichetta il gateway NAT e l'indirizzo IP elastico con la variabile. $ROSA_CLUSTER_NAME

```
aws ec2 create-tags --resources <EIP_ADDRESS>  --resources <NAT_GATEWAY_ID> --tags
 Key=Name,Value=$ROSA_CLUSTER_NAME
```

15. Crea una tabella di routing per il traffico di sottorete privato, associala alla sottorete privata e configura il traffico per il routing verso il gateway NAT.

```
aws ec2 create-route-table --vpc-id <VPC_ID_VALUE> --query RouteTable.RouteTableId --
output text

aws ec2 associate-route-table --subnet-id <PRIVATE_SUBNET_ID> --route-table-id
 <PRIVATE_RT_ID>

aws ec2 create-route --route-table-id <PRIVATE_RT_ID> --destination-cidr-block
 0.0.0.0/0 --gateway-id <NAT_GATEWAY_ID>
```

16. Etichetta la tabella di routing privata e l'indirizzo IP elastico con la variabile. `$ROSA_CLUSTER_NAME-private`

```
aws ec2 create-tags --resources <PRIVATE_RT_ID> <EIP_ADDRESS> --tags Key=Name,Value=
$ROSA_CLUSTER_NAME-private
```

Fase 3: Creare un cluster con AWS PrivateLink

È possibile utilizzare AWS PrivateLink e la ROSA CLI per creare una cluster 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` comando per creare un Single-AZ. ROSA cluster Per creare una Multi-AZcluster, specificate `multi-az` nel comando e gli ID di sottorete privati per ogni sottorete privata in cui desiderate effettuare la distribuzione.

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

1. Create un Single-AZ cluster eseguendo il seguente comando.

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

> **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`

2. Crea i IAM ruoli dell'clusteroperatore seguendo le istruzioni interattive.

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

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

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

4. Controlla lo stato del tuo. cluster

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

   Example

> **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, vedi Risolvere i problemi di provisioning ROSA del cluster.

   Per contattare il AWS Support nostro supporto Red Hat per ricevere assistenza, consulta Support for ROSA.

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

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

Fase 4: Configurare AWS PrivateLink l'inoltro 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

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>`

1. Aprire la console Route 53.
2. Nel riquadro di navigazione sotto Resolver, scegli Endpoint in entrata.
3. Scegli Configura endpoint.
4. In alto a destra, usa il Regione AWS selettore per scegliere Regione AWS quello che contiene il VPC usato per il cluster.
5. In Configurazione di base, scegli Solo in entrata, quindi scegli Avanti.
6. Nella pagina Configura l'endpoint in entrata, completa la sezione Impostazioni generali per l'endpoint in entrata. In Gruppo di sicurezza per questo endpoint, scegli un gruppo di sicurezza che consenta il traffico UDP e TCP in entrata dalla rete remota sulla porta di destinazione 53.
7. Nella sezione Indirizzo IP, scegli le zone di disponibilità e le sottoreti private utilizzate durante la creazione del cluster e scegli Avanti.
8. (Facoltativo) Completa la sezione Tag.
9. Scegli Submit (Invia).

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.

Fase 5: Configurare un provider di identità e concedere l'accesso cluster

ROSAinclude un server OAuth integrato. Dopo aver creato ROSA cluster il tuo, devi configurare OAuth per utilizzare un provider di identità. Puoi quindi aggiungere utenti al tuo provider di identità configurato per concedere loro l'accesso al tuo. cluster Puoi concedere a questi utenti `cluster-admin` o `dedicated-admin` autorizzazioni come richiesto.

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

> **Important**
>
> Il provider di identità HTPasswd è incluso solo per consentire la creazione di un singolo utente amministratore statico. HTPassWD non è supportato come provider di identità di uso generale 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'clusteraccesso 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 applicazione OAuth nella tua GitHub organizzazione.
7. Utilizza le informazioni della pagina GitHub OAuth per compilare i prompt `rosa create idp` interattivi rimanenti, sostituendo <GITHUB_CLIENT_ID> e <GITHUB_CLIENT_SECRET> con le credenziali dell'applicazione OAuth. GitHub

```
...
? 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 pod OAuth ridistribuirsi con la configurazione aggiornata.

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

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

Passaggio 6: concedere 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.

Passaggio 7: concedere le autorizzazioni di amministratore a un utente

Dopo aver aggiunto un utente al provider di identità configurato, puoi concedere all'utente `cluster-admin` o le `dedicated-admin` autorizzazioni per il tuo. cluster

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

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

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

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

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

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

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

Fase 8: Accedere a cluster tramite la console web

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. Sostituisci `<CLUSTER_NAME>` con il nome del 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 tuocluster, scegli il nome del provider di identità nella finestra di dialogo Accedi con... e completa tutte le richieste di autorizzazione presentate dal tuo provider.

Fase 9: Implementazione di un'applicazione dal catalogo per sviluppatori

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

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

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

10. Nella sezione Git, scegli Try Sample.
11. Nel campo Nome, aggiungi un nome univoco.
12. Seleziona 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.

Passo 10: Revoca le autorizzazioni di amministratore e l'accesso degli utenti

È possibile revocare `dedicated-admin` le `cluster-admin` autorizzazioni a un utente utilizzando la CLI. ROSA

Per revocare l'accesso a un utente, è necessario rimuovere l'utente dal provider di identità configurato.

Revoca le autorizzazioni **`cluster-admin`** di 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.

Fase 11: 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 daROSA, puoi utilizzare la console. IAM

> **Important**
>
> IAMi 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 tuocluster.

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

> **Important**
>
> È necessario attendere l'clustereliminazione 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 predefinito`ManagedOpenShift`.

```
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 percluster.

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. Sei anche responsabile di altri fattori, tra cui la riservatezza dei dati, i requisiti della tua azienda e le leggi e normative vigenti.

Questa documentazione aiuta a capire come applicare il modello di responsabilità condivisa durante l'utilizzo ROSA. Ti mostra come configurare 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.

Argomenti

- Protezione dei dati in ROSA
- AWSIAM politiche gestite per ROSA
- Resilienza in ROSA
- Sicurezza dell'infrastruttura in ROSA

Protezione dei dati in ROSA

La panoramica delle responsabilità per la ROSA 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 questo modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere il proprio lavoro. Ti suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- Utilizza SSL/TLS per comunicare con le risorse. AWS È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Configura l'API e la registrazione delle attività degli utenti con. AWS CloudTrail
- Utilizza soluzioni di AWS crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno Servizi AWS.
- Utilizza 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 o Servizi AWS utilizzi la console, l'API ROSA o gli SDK. AWS CLI AWS 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
- Riservatezza del traffico Internet

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 gli ID di gruppo secondari del punto di accesso. Amazon EFS sostituisce gli ID utente e di gruppo sui file con gli ID utente e di gruppo sul punto di accesso e ignora gli ID client NFS. Di conseguenza, ignora Amazon EFS silenziosamente le impostazioni. `fsGroup` ROSA non è in grado di sostituire i GID dei 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 Crittografia dei dati tramite KMS.

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.

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. ROSA I cluster appena creati sono configurati per utilizzare la classe di storage 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 key Per ulteriori informazioni sulla creazione di chiavi, consulta Creazione di chiavi KMS di crittografia simmetrica nella AWS KMS Developer Guide.

Puoi anche 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.

Quando si crittografano volumi persistenti utilizzando i propri, è necessario considerare i seguenti punti: 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.

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, vedere Sicurezza dell'infrastruttura in. ROSA

AWSIAM 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 Consigliamo

pertanto di ridurre ulteriormente le autorizzazioni definendo policy gestite dal cliente specifiche per i tuoi casi d'uso.

Non è possibile modificare le autorizzazioni definite nelle 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: ROSA ManageSubscription

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

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

Dettagli dell'autorizzazione

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 ROSA ManageSubscription nella AWS Managed Policy Reference Guide.

AWS politiche gestite per ROSA con ruoli di account HCP

È possibile allegare queste politiche AWS gestite ai ruoli di account necessari per utilizzare ROSA con piani di controllo ospitati (HCP). Le autorizzazioni sono necessarie per il supporto del Red Hat Site Reliability Engineering (SRE) sul cluster, la creazione del cluster e la funzionalità di calcolo.

Sono richieste le seguenti policy gestite:

- ROSA WorkerInstancePolicy: consente al ROSA servizio di gestire i cicli di vita delle Amazon EC2 istanze in un cluster. ROSA
- ROSASRE SupportPolicy — Concede le autorizzazioni necessarie ai Red Hat Site Reliability Engineer (SRE) per osservare, diagnosticare e supportare direttamente le AWS risorse associate ai cluster, inclusa la possibilità di modificare lo stato dei nodi del ROSA cluster. ROSA
- ROSA InstallerPolicy — Concede le autorizzazioni necessarie all'installatore per gestire le risorse che supportano l'installazione del cluster. AWS

AWS politiche gestite per ROSA con ruoli di operatore HCP

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

Sono richieste le seguenti politiche gestite:

- RosaAmazoneBSCSI DriverOperatorPolicy: concede le autorizzazioni necessarie al CSI Driver Operator per installare e Amazon EBS gestire il driver CSI su un cluster. Amazon EBS ROSA
- ROSA IngressOperatorPolicy — 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.
- ROSA ImageRegistryOperatorPolicy: concede le autorizzazioni necessarie all'Image Registry Operator per fornire e gestire le risorse per il registro delle immagini ROSA interno al cluster e i servizi dipendenti, incluso S3.
- ROSA CloudNetworkConfigOperatorPolicy — 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.
- ROSA KubeControllerPolicy — Concede le autorizzazioni necessarie a kube controller per la gestione Amazon EC2 e le AWS KMS risorse per un cluster con Elastic Load Balancing piani di controllo ospitati. ROSA
- ROSA NodePoolManagementPolicy — Concede le autorizzazioni necessarie al NodePool controller per 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 le chiavi. AWS KMS

- ROSAKMS ProviderPolicy — Concede le autorizzazioni necessarie all' AWS Encryption Provider integrato per gestire le AWS KMS chiavi che supportano la crittografia dei dati etcd. Questa politica consente di Amazon EC2 crittografare e decrittografare i `etcd` dati utilizzando le chiavi KMS fornite dall'Encryption Provider. AWS
- ROSA ControlPlaneOperatorPolicy — Concede le autorizzazioni necessarie all'operatore del Control Plane per la gestione Amazon EC2 e le Route 53 risorse necessarie ai cluster dei Control Plane Hosted Control Plane. ROSA

Per visualizzare le autorizzazioni relative alle policy gestite, consulta le policy gestite nella AWS Managed Policy Reference AWS 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 ricevere avvisi automatici sulle modifiche a questa pagina, iscriviti al feed RSS nella pagina della cronologia dei ROSA documenti.

Modifica	Descrizione	Data
ROSA InstallerPolicy — Politica aggiornata	ROSA ha aggiornato la politica 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. Questa politica è stata inoltre aggiornata con autorizzazioni che consentono al servizio di recuperare i name server DNS esistenti in modo che le operazioni di provisioning del cluster siano idempotenti. Per	26 gennaio 2024

Modifica	Descrizione	Data
	ulteriori informazioni, consulta ROSA. InstallerPolicy	
ROSASRE SupportPolicy — Informativa 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, vedere ROSASRE SupportPolicy.	22 gennaio 2024
ROSA ImageRegistryOpera torPolicy — Politica aggiornata	ROSA ha aggiornato la politica per consentire all'Image Registry Operator di intrapren dere azioni sui Amazon S3 bucket nelle regioni con nomi di 14 caratteri. Per saperne di più, consulta ROSA. ImageRegistryOperatorPolicy	12 dicembre 2023
ROSA KubeControllerPolicy — Politica aggiornata	ROSA ha aggiornato la policy per consentire di kube-cont roller-manager descrivere zone di disponibilità, Amazon EC2 istanze, tabelle di routing, gruppi di sicurezza, VPC e sottoreti. Per saperne di più, consulta ROSA. KubeContr ollerPolicy	16 ottobre 2023

Modifica	Descrizione	Data
ROSA ManageSubscription — Politica aggiornata	ROSA ha aggiornato la politica per aggiungere il ROSA con piani di controllo ospitati ProductId. Per saperne di più, consulta ROSA ManageSubscription.	1° agosto 2023
ROSA KubeControllerPolicy — Politica aggiornata	ROSA ha aggiornato la policy 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 saperne di più, consulta ROSA. KubeControllerPolicy	13 luglio 2023
ROSA NodePoolManagement Policy — 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, vedere ROSA NodePoolManagement Policy.	8 giugno 2023

Modifica	Descrizione	Data
ROSA InstallerPolicy — 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 saperne di più, consulta ROSA InstallerPolicy.	6 giugno 2023
ROSASRE SupportPolicy — Aggiunta una nuova politica	ROSA ha aggiunto una nuova policy per consentire agli SRE Red Hat di osservare , diagnosticare e supportar e direttamente AWS le risorse associate ai ROSA cluster, inclusa la possibilità di modificare lo stato dei nodi del cluster. ROSA Per saperne di più, consulta ROSASRE. SupportPolicy	1 giugno 2023
ROSAMS ProviderPolicy — Aggiunta una nuova politica	ROSA ha aggiunto una nuova politica per consentire all' AWS Encryption Provider integrato di gestire AWS KMS le chiavi per supportar e la crittografia dei dati etcd. Per saperne di più, consulta ProviderPolicyROSAKMS.	27 aprile 2023

Modifica	Descrizione	Data
ROSA KubeControllerPolicy — 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 saperne di più, consulta ROSA. KubeControllerPolicy	27 aprile 2023
ROSA ImageRegistryOperatorPolicy — 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 saperne di più, consulta ROSA. ImageRegistryOperatorPolicy	27 aprile 2023
ROSA ControlPlaneOperatorPolicy — Aggiunta una nuova politica	ROSA ha aggiunto una nuova politica per consentire al Control Plane Operator di gestire Amazon EC2 le Route 53 risorse relative ROSA ai cluster di piani di controllo ospitati. Per saperne di più, consulta ROSA ControlPlaneOperatorPolicy.	24 aprile 2023

Modifica	Descrizione	Data
ROSA CloudNetworkConfig OperatorPolicy — 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 saperne di più, consulta ROSA. CloudNetworkConfig OperatorPolicy	20 aprile 2023
ROSA IngressOperatorPolicy — Aggiunta una nuova politica	ROSA ha aggiunto una nuova politica per consentire a Ingress Operator di fornire e gestire i bilanciatori di carico e le configurazioni DNS per i cluster. ROSA Per saperne di più, consulta ROSA. IngressOperatorPolicy	20 aprile 2023
RosaAmazone.BSCSI: aggiunta una nuova DriverOperatorPolicy politica	ROSA ha aggiunto una nuova politica per consentire a Amazon EBS CSI Driver Operator di installare e gestire il driver CSI su un cluster. Amazon EBS ROSA Per ulteriori informazioni, consulta RosaAmazoneBSCSI. DriverOperatorPolicy	20 aprile 2023
ROSA — Aggiunta una nuova politica WorkerInstancePolicy	ROSA ha aggiunto una nuova politica per consentire al servizio di gestire le risorse del cluster. Per ulteriori informazioni, consulta ROSA WorkerInstancePolicy.	20 aprile 2023

Modifica	Descrizione	Data
ROSA ManageSubscription — Aggiunta una nuova politica	ROSA ha aggiunto una nuova politica per concedere le Marketplace AWS autorizza zioni necessarie per gestire l' ROSA abbonamento. Per saperne di più, consulta ROSA ManageSubscription.	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

AWS politiche gestite per ROSA con ruoli di account HCP

> **Note**
>
> Queste politiche AWS gestite sono destinate all'uso da parte di ROSA con piani di controllo ospitati, un aggiornamento del servizio imminente. ROSA i cluster creati con l'architettura esistente continueranno a utilizzare le politiche IAM gestite dal cliente. Per ulteriori informazioni sulle politiche IAM gestite dai clienti utilizzate da ROSA, consulta Informazioni sulle risorse IAM per ROSA i cluster che utilizzano. AWS STS

Queste politiche AWS gestite aggiungono le autorizzazioni utilizzate dai ruoli ROSA IAM. Le autorizzazioni sono necessarie per il supporto di Red Hat Site Reliability Engineering (SRE) sul cluster, la creazione del cluster e la funzionalità di calcolo.

Argomenti

- AWS politica gestita: ROSA WorkerInstancePolicy
- AWS politica gestita: ROSASRE SupportPolicy
- AWS politica gestita: ROSA InstallerPolicy

AWS politica gestita: ROSA WorkerInstancePolicy

Puoi collegarti `ROSAWorkerInstancePolicy` alle tue IAM entità. Prima di creare un cluster ROSA con piani di controllo ospitati, è necessario collegare questa policy a un ruolo IAM di lavoro.

Dettagli dell'autorizzazione

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

- `ec2`— Revisione dei dettagli Regione AWS e delle Amazon EC2 istanze nell'ambito della gestione del ciclo di vita dei nodi di lavoro in un cluster. ROSA

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

AWS politica gestita: ROSASRE SupportPolicy

È possibile allegare `ROSASRESupportPolicy` alle entità IAM.

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

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni che consentono a Red Hat SRE di 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 ROSASRE SupportPolicy nella Managed Policy Reference Guide. AWS

AWS politica gestita: ROSA InstallerPolicy

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 dell'autorizzazione

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

- `ec2`— Esegui Amazon EC2 istanze utilizzando AMI ospitate in siti di Account AWS proprietà e gestiti da Red Hat. Amazon EC2 Descrivi le istanze, i volumi e le risorse di rete associate ai nodi. Amazon EC2 Ciò è necessario affinché il piano di controllo di Kubernetes possa unire le istanze a un cluster. Ciò è necessario anche per consentire al cluster di valutarne la presenza all'interno. Amazon VPC
- `elasticloadbalancing`— Aggiungere sistemi di bilanciamento del carico ai nodi di destinazione di un cluster. Rimuove 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 ROSA InstallerPolicy nella Managed Policy Reference Guide. AWS

AWS politiche gestite per ROSA con ruoli di operatore HCP

> **Note**
>
> Queste politiche AWS gestite sono destinate all'uso da parte di ROSA con i piani di controllo ospitati (HCP), un aggiornamento del servizio imminente. ROSA i cluster creati con l'architettura esistente continueranno a utilizzare le politiche IAM gestite dal cliente. Per ulteriori informazioni sulle politiche IAM gestite dai clienti utilizzate da ROSA, consulta Informazioni sulle risorse IAM per ROSA i cluster che utilizzano. AWS STS

Queste politiche AWS gestite aggiungono le autorizzazioni utilizzate dai ruoli ROSA IAM. Le autorizzazioni sono necessarie OpenShift agli operatori del cluster ROSA with HCP per gestire i nodi del cluster.

Argomenti

- AWS politica gestita: rosaAmazoneBSCSI DriverOperatorPolicy
- AWS politica gestita: ROSA IngressOperatorPolicy
- AWS politica gestita: ROSA ImageRegistryOperatorPolicy
- AWS politica gestita: ROSA CloudNetworkConfigOperatorPolicy
- AWS politica gestita: ROSA KubeControllerPolicy
- AWS politica gestita: ROSA NodePoolManagementPolicy
- AWS politica gestita: ROSAMS ProviderPolicy

- AWS politica gestita: ROSA ControlPlaneOperatorPolicy

AWS politica gestita: rosaAmazoneBSCSI DriverOperatorPolicy

Puoi collegarti alle tue entità. `ROSAAmazonEBSCSIDriverOperatorPolicy` IAM 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 dell'autorizzazione

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 DriverOperatorPolicyRosaAmazoneBSCSI nella Managed Policy Reference Guide. AWS

AWS politica gestita: ROSA IngressOperatorPolicy

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 dell'autorizzazione

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

- `elasticloadbalancing`— Descrivere lo stato dei sistemi di bilanciamento del carico predisposti.
- `route53`— 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 ROSA IngressOperatorPolicy nella AWS Managed Policy Reference Guide.

AWS politica gestita: ROSA ImageRegistryOperatorPolicy

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 dell'autorizzazione

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

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

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

AWS politica gestita: ROSA CloudNetworkConfigOperatorPolicy

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 dell'autorizzazione

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

- `ec2`— Leggere, assegnare e descrivere le configurazioni per 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 ROSA CloudNetworkConfigOperatorPolicy nella Managed Policy Reference Guide. AWS

AWS politica gestita: ROSA KubeControllerPolicy

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 dell'autorizzazione

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 zone di disponibilità, Amazon EC2 istanze, tabelle di routing, gruppi di sicurezza, VPC e sottoreti.

- `elasticloadbalancing`— Crea e gestisci i sistemi di bilanciamento del carico e le relative politiche, crea e gestisci i listener di load balancer, registra gli obiettivi con i gruppi target e gestisci i gruppi target, registra e annulla la registrazione delle Amazon EC2 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 ROSA KubeControllerPolicy nella AWS Managed Policy Reference Guide.

AWS politica gestita: ROSA NodePoolManagementPolicy

Puoi collegarti `ROSANodePoolManagementPolicy` 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`. 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 politica concede inoltre le autorizzazioni per consentire la crittografia del disco del volume radice del nodo di lavoro utilizzando le chiavi. AWS KMS Per ulteriori informazioni su questo controller, consulta l'architettura del controller nella OpenShift documentazione.

Dettagli dell'autorizzazione

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

- `ec2`— Esegui Amazon EC2 istanze utilizzando AMI ospitate presso Red Hat di Account AWS proprietà e gestite 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
- `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 ROSA NodePoolManagementPolicy nella AWS Managed Policy Reference Guide.

AWS politica gestita: ROSAMS ProviderPolicy

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 dell'autorizzazione

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 ROSAKMS ProviderPolicy nella AWS Managed Policy Reference Guide.

AWS politica gestita: ROSA ControlPlaneOperatorPolicy

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 dell'autorizzazione

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

- `ec2`— Creare e gestire 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 ROSA ControlPlaneOperatorPolicy nella AWS Managed Policy Reference Guide.

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, puoi progettare e gestire applicazioni e database che eseguono automaticamente il failover tra zone di disponibilità senza interruzioni. Le zone di disponibilità sono più disponibili, tolleranti ai guasti e scalabili rispetto alle infrastrutture a data center singolo o multiplo tradizionali.

ROSA offre ai clienti la possibilità di eseguire il piano di controllo e il piano dati di Kubernetes in 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 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 Red Hat Site Reliability Engineer (SRE) gestiscono completamente il piano di controllo e i nodi dell'infrastruttura. Gli SRE Red Hat monitorano in modo proattivo il ROSA cluster e sono responsabili della sostituzione di eventuali nodi del piano di controllo e nodi dell'infrastruttura guasti. Per ulteriori informazioni, consulta Panoramica delle responsabilità per. ROSA

> **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 della 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. O puoi utilizzare AWS Security Token Service (AWS STS) per generare credenziali di sicurezza temporanee per sottoscrivere le richieste.

Isolamento della rete di cluster

I Red Hat Site Reliability Engineer (SRE) 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 ROSA, consulta Panoramica delle responsabilità per ROSA.

Quando si crea un nuovo cluster, ROSA offre la possibilità di creare un endpoint server e percorsi applicativi pubblici dell'API Kubernetes o un endpoint e percorsi applicativi privati dell'API Kubernetes. 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. Per maggiori informazioni, consultate la policy di rete nella documentazione di Red Hat.

Quote di servizio di ROSA

Servizio Red Hat OpenShift su AWS(ROSA) utilizza le quote di servizio perAmazon EC2, Amazon Virtual Private Cloud (Amazon VPC), Amazon Elastic Block Store (Amazon EBS) e Elastic Load Balancing (ELB) per fornire cluster.

Quote minime richieste per ROSA

Per quanto segue Amazon EC2 e per le Amazon EBS quote, ROSA richiede una quota superiore a quella fornita dal servizio predefinito. Per l'utilizzoROSA, potrebbe essere necessario richiedere un aumento di tali quote. Per ulteriori informazioni, consulta Richiesta di un aumento di quota nella Guida per l'Service Quotasutente.

Important

Per Amazon EC2 istanze on demand standard (A, C, D, H, I, M, R, T, Z), il valore predefinito di 5 vCPUs non è sufficiente per creare cluster. ROSA ROSAPer la creazione di cluster, richiede 100 o più vCPUs. Per aumentare la quota, apri la Service Quotasconsole e richiedi un aumento.

Note

Puoi controllare le tue quote utilizzando gli AWS SDK, ma il calcolo dell'SDK non include le risorse esistenti. ROSA Il controllo delle quote nell'SDK potrebbe essere superato e la ROSA cluster creazione potrebbe fallire. Per risolvere il problema, apri la Service Quotasconsole e richiedi un aumento.

Nome	Codice del servizio	Impostazione predefinita	Minimo richiesto	Regolabile	Descrizione
Esecuzione di istanze on demand standard (A,	ec2	5	100	Sì	Numero massimo di vCPUs assegnate

Nome	Codice del servizio	Impostazione predefinita	Minimo richiesto	Regolabile	Descrizione
C, D, H, I, M, R, T, Z)					alle istanze (A, C, D, H, I, M, R, T, Z) standard on demand in esecuzione. Il valore predefinito di 5 vCPUs non è sufficiente per creare ROSA cluster. ROSAPer la creazione di cluster, richiede 100 vCPUs.

Nome	Codice del servizio	Impostazione predefinita	Minimo richiesto	Regolabile	Descrizione
Archiviazione per volumi SSD a scopo generico (gp3) in TiB	ebs	50	300	Sì	La quantità massima aggregata di archiviazione, in TiB, di cui è possibile eseguire il provisioning su volumi SSD (gp3) a scopo generico in questa regione. Sono necessari 300 TiB di spazio di archiviazione per prestazioni ottimali.

Nome	Codice del servizio	Impostazione predefinita	Minimo richiesto	Regolabile	Descrizione
Archiviazione per volumi SSD a scopo generico (gp2) in TiB	ebs	50	300	Sì	La quantità massima aggregata di archiviazione, in TiB, di cui è possibile eseguire il provisioning su volumi SSD (gp2) a scopo generico in questa regione. Sono necessari 300 TiB di spazio di archiviazione per prestazioni ottimali.

Nome	Codice del servizio	Impostazione predefinita	Minimo richiesto	Regolabile	Descrizione
Archiviazione per volumi SSD IOPS con provisioning (io1) in TiB	ebs	50	300	Sì	La quantità massima aggregata di archiviazione, in TiB, di cui è possibile eseguire il provisioning su volumi SSD (io1) con capacità di IOPS allocata in questa regione. Sono necessari 300 TiB di spazio di archiviazione per prestazioni ottimali.

> **Note**
>
> I valori predefiniti sono le quote iniziali impostate da AWS, che sono separate dal valore effettivo della quota applicata e dalla quota di servizio massima possibile. Per ulteriori informazioni, vedere Terminologia Service Quotas nella Guida per l'Service Quotasutente.

Quote predefinite per ROSA

ROSAutilizza le seguenti quote predefinite perAmazon EC2, Amazon VPCAmazon EBS, eElastic Load Balancing. Per informazioni sull'aumento delle quote, vedere Richiesta di aumento delle quote nella Guida per l'Service Quotasutente.

Amazon EC2

- IP elastici EC2-VPC

Amazon VPC

- VPC per regione
- Interfacce di rete per regione
- Gateway Internet per regione

Amazon EBS

- Snapshot per regione
- IOPS per volumi SSD (io1) con capacità di IOPS allocata

Elastic Load Balancing

- Application Load Balancersper regione
- Classic Load Balancersper regione

Servizi AWS integrati con ROSA

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

Argomenti

- Come ROSA funziona con Marketplace AWS

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 monitora il tuo utilizzo e paghi solo per quello che usi.

Offerta pubblica

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

Offerta privata

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

ROSA costi di servizio

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

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 Red Hat Site Reliability Engineer (SRE). ROSA i costi di servizio sono uniformi in tutte le regioni AWS standard supportate. Le tariffe del servizio ROSA con HCP vengono addebitate su richiesta per impostazione predefinita a una tariffa oraria fissa basata sul numero di cluster in esecuzione e di vCPU dei nodi di lavoro in esecuzione in tali cluster. I costi del servizio ROSA classic vengono calcolati su richiesta in base al numero di vCPU dei nodi di lavoro. ROSA classic non addebita costi di servizio per il piano di controllo o i nodi di infrastruttura richiesti.

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

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

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

Iscrizione alle inserzioni ROSA del Marketplace tramite la console

Quando lo attivi ROSA nella ROSA console 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.

ROSA contratti

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, consulta la sezione Prezzi di Servizio Red Hat OpenShift su AWS.

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

> **Note**
>
> 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, vedi Differenze tra ROSA con HCP e ROSA classic.

Per acquistare 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 istanza EC2 e il numero di istanze di cui hai bisogno.
6. Scegli Rivedi il contratto.
7. Controlla i dettagli del contratto e scegli Contratto di acquisto.

Note

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

Acquisto di un contratto ROSA con HCP 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 si sceglie di acquistare un contratto ROSA con HCP per risparmiare sui costi di servizio del nodo di lavoro, il contratto iniziale viene modificato per coprire i costi di utilizzo delle vCPU e dei piani di controllo del nodo di lavoro specificati.

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

Quota di utilizzo mensile

Al momento dell'acquisto, le vCPU e i piani di controllo 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:

- vCPU del nodo di lavoro: numero di vCPU 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 vCPU di nodi di lavoro e 8 piani di controllo verrebbe convertito in una quota mensile di 2.920.000 ore di vCPU dei nodi di lavoro e 5.840 ore di vCPU del 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, vedi Differenze tra ROSA con 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 vCPU da acquistare. Specificare in multipli di 4.
6. Inserire il numero di piani di controllo da acquistare.
7. Scegli Rivedi contratto.
8. Controlla i dettagli del contratto e scegli Contratto di acquisto.

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

Aggiornamento di un contratto ROSA con HCP di 12 mesi

È possibile aggiornare il contratto ROSA attivo con HCP di 12 mesi in qualsiasi momento con vCPU e piani di controllo aggiuntivi per nodi di lavoro. Quando effettui l'upgrade di ROSA con un contratto 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 le vCPU e i piani di controllo del nodo di lavoro specificati durante la creazione del contratto. Gli aggiornamenti contrattuali non influiscono sulle tariffe addebitate per l'infrastruttura. AWS

Al momento dell'aggiornamento, le vCPU e i piani di controllo 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 Quota di utilizzo mensile.

Per aggiornare un contratto ROSA con HCP di 12 mesi

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. Immettere il numero di vCPU 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 accedere all'account corretto, verrà visualizzato l'errore Page note found (404).

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

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

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

Marketplace privato

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

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

Risoluzione dei problemi

La seguente documentazione illustra come risolvere i problemi che potrebbero verificarsi durante l'attivazione e il provisioning dei cluster. ROSA ROSA

Argomenti

Support per ROSA

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

AWS Support

Per aprire casi ROSA tecnici è necessario un piano AWS Developer Support, ma si consiglia un piano AWS Business o Enterprise On-Ramp Support per un accesso continuo al supporto ROSA tecnico e alla guida architetturale. Red Hat utilizza l' AWS Support API per aprire casi per i clienti quando necessario. AWS Business Support ed AWS Enterprise On-Ramp consentono l'accesso continuo al telefono, al Web e alla chat ai tecnici dell'assistenza. Per ulteriori informazioni sui AWS Support piani, consulta. AWS Support

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

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

Supporto Red Hat

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.

Risolvi gli errori ROSA di abilitazione nella console ROSA

ROSAvengono utilizzati Marketplace AWS per facilitare la gestione degli abbonamenti, la fatturazione e la misurazione. Quando l'opzione è ROSA abilitata, la pagina della AWS ROSA console sottoscrive un ROSA elenco su. Marketplace AWS Se al tuo IAM principale mancano le autorizzazioni di `aws-marketplace` abbonamento richieste quando abiliti ROSA nella ROSA console, la console genera un messaggio di errore.

Questa sezione illustra come risolvere i problemi di autorizzazione all'Marketplace AWSabbonamento che potresti riscontrare quando scegli Abilita ROSA nella console. ROSA

ConROSA, puoi anche ricevere supporto per la risoluzione dei problemi dai team AWS Support di supporto di Red Hat. Per ulteriori informazioni, consulta Support for ROSA.

Argomenti

AWS Organizationsla politica di controllo del servizio (SCP) sta negando le autorizzazioni richieste Marketplace AWS

Descrizione

Se la tua policy di controllo del AWS Organizations servizio (SCP) non è configurata per consentire l'`aws-marketplace:Subscribe`autorizzazione richiesta quando scegli Abilita ROSA, la ROSA console genera il seguente messaggio di errore: `An error occurred while enabling Servizio Red Hat OpenShift su AWS (ROSA), because an AWS Organizations Service Control Policy (SCP) is denying required permissions. Contact your AWS Organizations management account administrator, and consult the documentation for troubleshooting.`

Soluzione

L'amministratore dell'account di gestione dell'organizzazione può abilitare ROSA l'account di gestione dell'organizzazione. Una volta ROSA abilitati, possono utilizzarli AWS License Manager

per distribuire il diritto alla Marketplace AWS licenza tra gli account membri ROSA all'interno dell'organizzazione.

Contatta l'amministratore del tuo account e richiedi che distribuisca e attivi l'ROSAautorizzazione per il tuo account.

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

Descrizione

Se il IAM responsabile non dispone dell'`aws-marketplace:Subscribe`autorizzazione richiesta quando si sceglie Abilita ROSA, la ROSA console genera il seguente messaggio di errore: `An error occurred while enabling Servizio Red Hat OpenShift su AWS (ROSA), because your user or role does not have the required permissions.`

Soluzione

1. Vai alla ROSAconsole e collega la policy AWS gestita `ROSAManageSubscription` alla tua IAM identità. Per ulteriori informazioni in meritoROSAManageSubscription, consulta la policy AWS gestita: ROSA ManageSubscription.
2. Scegli Inizia.
3. Nella pagina Verifica i ROSA prerequisiti, seleziona Accetto di condividere le mie informazioni di contatto con Red Hat.
4. Scegli Abilita. ROSA

Se non disponi dell'autorizzazione per visualizzare o aggiornare il tuo set di autorizzazioniIAM, contatta Account AWS l'amministratore e chiedigli di attivarlo ROSA per il tuo account.

Marketplace AWSAutorizzazioni richieste bloccate da un amministratore

Descrizione

Se l'amministratore dell'account ha bloccato l'`aws-marketplace:Subscribe`autorizzazione richiesta, la ROSA console genera il seguente messaggio di errore quando scegli Abilita ROSA: `An error occurred while enabling Servizio Red Hat OpenShift su AWS (ROSA), because required permissions have been blocked by an administrator.`

```
ROSAManageSubscription, an AWS managed policy, includes the permissions
required to enable ROSA. Consult the documentation and try again.
```

Soluzione

Contatta Account AWS l'amministratore e chiedigli di intraprendere le seguenti azioni:

1. Passare alla console ROSA.
2. Scegli Inizia.
3. Nella pagina Verifica i ROSA prerequisiti, seleziona Accetto di condividere le mie informazioni di contatto con Red Hat.
4. Scegli Abilita. ROSA Questa azione abilita tutte ROSA le IAM identità incluse in. Account AWS

Risoluzione dei problemiROSAproblemi di creazione di cluster

Questa sezione contiene le soluzioni ai problemi che potresti riscontrare durante la creazioneROSAgrappoli.

ConROSA, puoi anche ricevere assistenza per la risoluzione dei problemi daAWS Supporte i team di supporto Red Hat. Per ulteriori informazioni, vedereSupporto perROSA.

Argomenti

- AccessoROSAregistri di debug del cluster
- Elastic Load BalancingIl ruolo (ELB) non esiste
- ROSAil cluster fallisceAWScontrollo della quota di servizio duranteclustercreazione
- Risoluzione dei problemiROSAToken di accesso offline scaduti della CLI

AccessoROSAregistri di debug del cluster

Per iniziare a risolvere i problemi con la tua applicazione, consulta innanzitutto i registri di debug. LaROSAI registri di debug CLI forniscono dettagli sui messaggi di errore che vengono prodotti quando unclusternon riesce a creare.

Da visualizzareclusterinformazioni di debug, esegui quanto segueROSAComando CLI. Nel comando, sostituisci`<cluster_name>`con il nome del tuocluster.

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

Elastic Load BalancingIl ruolo (ELB) non esiste

Descrizione

Se non hai creato un sistema di bilanciamento del carico nel tuoAccount AWS, il`AWSServiceRoleForElasticLoadBalacing`il ruolo potrebbe non essere stato creato. Se non configuri ilElastic Load Balancingruolo corretto e tentativo di creare unROSA cluster, viene restituito il seguente messaggio di errore:`Error creating network Load Balancer: AccessDenied`.

Soluzione

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

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

2. Se non disponi di questo ruolo, crealo eseguendo il comando seguente.

```
aws iam get-role --role-name "AWSServiceRoleForElasticLoadBalancing" || aws iam
 create-service-linked-role --aws-service-name "elasticloadbalancing.amazonaws.com"
```

ROSAil cluster fallisceAWScontrollo della quota di servizio duranteclustercreazione

Descrizione

Da usareROSA, potrebbe essere necessario aumentare le quote di servizio per il tuo account. Per ulteriori informazioni, consulta Quote di servizio di ROSA.

Soluzione

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

```
rosa verify quota
```

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

2. Se devi aumentare la tua quota, vai allaService Quotasplancia.
3. Nel riquadro di navigazione, scegli AWSservizi.
4. Scegli il servizio che richiede un aumento della quota.
5. Seleziona la quota che deve essere aumentata e scegliRichiedi un aumento della quota.
6. PerRichiedi un aumento della quota, inserisci l'importo totale che desideri assegnare alla quota e scegliRichiesta.

Risoluzione dei problemiROSAToken di accesso offline scaduti della CLI

Descrizione

Se si utilizza ilROSACLI e la tuaapi.openshift.comil token di accesso offline scade, viene visualizzato un messaggio di errore. Questo accade quandosso.redhat.cominvalida il token.

Soluzione

1. Accedere allaOpenShiftPagina dei token API di Cluster Managere scegliToken di caricamento.
2. Copia e incolla il seguente comando di autenticazione nel terminale.

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

Risoluzione dei problemi relativi aiROSA cluster non STS

Questa sezione spiega come risolvere i problemi che potrebbero verificarsi durante il provisioning diROSA cluster non STS.

Si consiglia di effettuare il provisioningROSA dei cluster utilizzando credenziali di breve durataAWS Security Token Service (STS) per una migliore protezione della sicurezza. Per ulteriori informazioni sul provisioning dei clusterROSA STS, vedere Guida introduttiva all'ROSAutilizzoAWS STS in modalità auto.

ConROSA, puoi anche ricevere supporto per la risoluzione dei problemi daiAWS Support o dai team di supporto Red Hat. Per ulteriori informazioni, consulta Support perROSA.

Impossibile creare un filecluster con un osdCcsAdmin errore

> **Note**
>
> Questo errore si verifica solo quando si utilizza il metodo non STS per il provisioning deiROSA cluster. Per evitare questo problema, esegui il provisioningROSA dei cluster utilizzandoAWS STS. Per ulteriori informazioni, vedere Guida introduttiva all'ROSAusoAWS STS in modalità auto.

Descrizione

Secluster non riesci a creazione di, 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.
```

Soluzione

1. Eliminare lo stack.

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

2. Reazione di nell'account.

   ```
   rosa init
   ```

Cronologia dei documenti per la Guida per ROSA l'utente

La tabella seguente riporta tutti gli aggiornamenti della documentazione per ROSA.

Modifica	Descrizione	Data
ROSA con espansione HCP Regione AWS	ROSA con piani di controllo ospitati (HCP) è ora disponibile 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 disponibile in Medio Oriente (Bahrain). Regione AWS	25 marzo 2024
ROSA con espansione HCP Regione AWS	ROSA con piani di controllo ospitati (HCP) è ora disponibile 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
ROSA aggiornato Installer Policy	Aggiornamento della policy gestita AWS ROSAInstallerPolicy.	26 gennaio 2024
ROSASRE aggiornato SupportPolicy	Aggiornata la policy gestita di AWS ROSASRESupportPolicy.	22 gennaio 2024
ROSA aggiornato ImageRegistryOperatorPolicy	Aggiornamento della policy gestita AWS ROSAImageRegistryOperatorPolicy.	12 dicembre 2023

ROSA aggiornato KubeControllerPolicy	Aggiornamento della policy gestita AWS ROSAKubeControllerPolicy.	16 ottobre 2023
ROSA aggiornato ManageSubscription	Aggiornamento della policy gestita AWS ROSAManageSubscription.	1° agosto 2023
ROSA aggiornato KubeControllerPolicy	Aggiornamento della policy gestita AWS ROSAKubeControllerPolicy.	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
Aggiunta la nuova policy gestita AWS ROSA NodePoolManagementPolicy	È stata aggiunta la nuova policy gestita da AWS ROSANodePoolManagementPolicy .	8 giugno 2023
Aggiunta la nuova policy gestita AWS ROSA Installer Policy	È stata aggiunta la nuova policy gestita da AWS ROSAInstallerPolicy .	6 giugno 2023
Aggiunta nuova policy gestita da AWS ROSASRESupportPolicy	È stata aggiunta la nuova policy gestita da AWS ROSASRESupportPolicy .	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 Cos'è Red Hat OpenShift Service on AWS?	È stata aggiornata la pagina What is Red Hat OpenShift Service on AWS.	24 maggio 2023
Aggiunte nuove policy gestite da AWS per i ruoli di operatore ROSA	ProviderPolicy Sono state aggiunte nuove policy gestite da AWS ROSA ImageRegistryOperatorPolicy KubeControllerPolicy, ROSA e ROSAKMS.	27 aprile 2023
Aggiunta la nuova policy gestita AWS ROSA ControlPlaneOperatorPolicy	È stata aggiunta la nuova policy gestita da AWS ROSAControlPlaneOperatorPolicy .	24 aprile 2023
Aggiunte nuove policy gestite da AWS per i ruoli degli account ROSA	Sono state aggiunte nuove pagine di policy gestite da AWS per l'account ROSA e la pagina dei ruoli degli operatori.	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 di risoluzione dei problemi	1 novembre 2022
Sono state aggiunte pagine introduttive	Sono state aggiunte pagine introduttive	12 agosto 2022
Aggiunta la nuova policy gestita AWS ROSA ManageSubscription	È stata aggiunta la nuova policy gestita da AWS ROSAManageSubscription .	11 aprile 2022
Versione iniziale	La versione iniziale della Red Hat OpenShift Service on AWS User Guide	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.