Panduan Pengguna

Layanan OpenShift Red Hat di AWS

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Layanan OpenShift Red Hat di AWS: Panduan Pengguna

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Merek dagang dan tampilan dagang Amazon tidak boleh digunakan sehubungan dengan produk atau layanan apa pun yang bukan milik Amazon, dengan cara apa pun yang dapat menyebabkan kebingungan di antara pelanggan, atau dengan cara apa pun yang menghina atau mendiskreditkan Amazon. Semua merek dagang lain yang tidak dimiliki oleh Amazon adalah milik dari pemiliknya masing-masing, yang mungkin berafiliasi atau mungkin tidak berafiliasi dengan, atau disponsori oleh Amazon.

Table of Contents

Apa itu Layanan OpenShift Red Hat di AWS?

Layanan OpenShift Red Hat di AWS (ROSA) adalah layanan terkelola yang dapat Anda gunakan untuk membangun, menskalakan, dan menyebarkan aplikasi kontainer dengan platform Red Hat OpenShift Enterprise Kubernetes. AWS ROSA merampingkan pemindahan OpenShift beban kerja Red Hat lokal AWS, dan menawarkan integrasi yang ketat dengan yang lain. Layanan AWS

Fitur

ROSA Didukung dan dioperasikan bersama oleh Red AWS Hat. Setiap ROSA cluster dilengkapi dengan dukungan insinyur keandalan situs (SRE) Red Hat 24 jam untuk manajemen klaster, didukung oleh perjanjian tingkat layanan uptime (SLA) 99,95% dari Red Hat. Untuk informasi selengkapnya tentang model dukungan layanan, lihatthe section called “Mendapatkan Dukungan”.

ROSA juga menyediakan fitur-fitur berikut:

- Red Hat SRE mendukung instalasi klaster, pemeliharaan klaster, dan peningkatan klaster.
- Layanan AWS Integrasi meliputi AWS komputasi, database, analitik, pembelajaran mesin, jaringan, dan seluler.
- Jalankan dan skalakan bidang kontrol Kubernetes di beberapa AWS Availability Zone untuk memastikan ketersediaan yang tinggi.
- Mengoperasikan cluster menggunakan OpenShift APIs dan mengembangkan alat produktivitas, termasuk Service Mesh, CodeReady Workspaces, dan Serverless.

Mengakses ROSA

Anda dapat menentukan dan mengonfigurasi penerapan ROSA layanan Anda menggunakan antarmuka berikut.

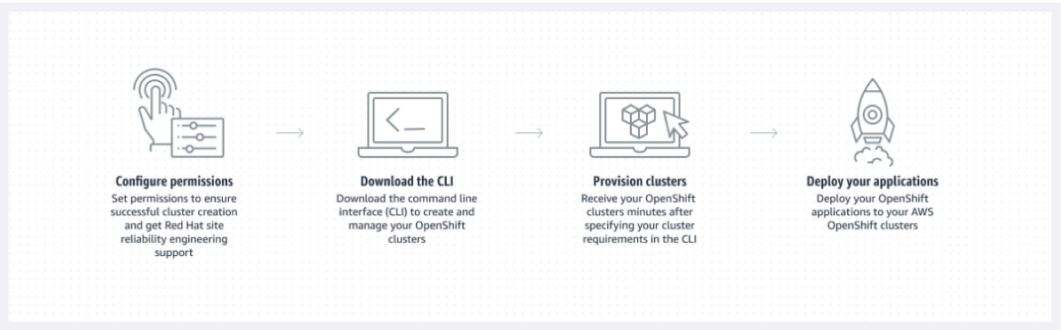
AWS

- ROSA konsol — Menyediakan antarmuka web untuk memungkinkan ROSA berlangganan dan membeli kontrak ROSA perangkat lunak.
- AWS Command Line Interface (AWS CLI) — Menyediakan perintah untuk serangkaian luas Layanan AWS dan didukung pada Windows, macOS, dan Linux. Untuk informasi selengkapnya, lihat AWS Command Line Interface.

Topi Merah OpenShift

- Red Hat Hybrid Cloud Console — Menyediakan antarmuka web untuk membuat, memperbarui, dan mengelola ROSA cluster, menginstal add-on cluster, dan membuat dan menyebarkan aplikasi ke cluster. ROSA
- ROSA CLI (rosa) — Menyediakan perintah untuk membuat, memperbarui, dan mengelola cluster. ROSA
- OpenShift CLI (oc) - Menyediakan perintah untuk membuat aplikasi dan mengelola proyek Platform OpenShift Kontainer.
- Knative CLI (kn) - Menyediakan perintah yang dapat digunakan untuk berinteraksi OpenShift dengan komponen Tanpa Server, seperti Knative Serving dan Eventing.
- Pipelines CLI (tkn) - Menyediakan perintah untuk berinteraksi OpenShift dengan Pipelines menggunakan terminal.
- opm CLI - Menyediakan perintah yang membantu pengembang Operator dan administrator cluster membuat dan OpenShift memelihara katalog Operator dari terminal.
- Operator SDK CLI - Menyediakan perintah yang dapat digunakan pengembang Operator untuk membangun, menguji, dan menyebarkan OpenShift operator.

Bagaimana untuk memulai dengan ROSA



Berikut ini merangkum proses memulai untuk ROSA. Untuk instruksi memulai yang terperinci, lihatMemulai dengan ROSA .

AWS Management Console/AWS CLI

1. Konfigurasikan izin untuk Layanan AWS itu ROSA bergantung pada untuk memberikan fungsionalitas layanan. Untuk informasi selengkapnya, lihat the section called “Prasyarat”.

2. Instal dan konfigurasikan AWS CLI alat terbaru. Untuk informasi selengkapnya, lihat Menginstal pembaruan versi terbaru kami AWS CLI di Panduan AWS CLI Pengguna.
3. Aktifkan ROSA di ROSA konsol.

Konsol Awan Hibrida Red Hibrida/CLI ROSA

1. Unduh versi terbaru CLI dan ROSA OpenShift CLI dari Red Hat Hybrid Cloud Console. Untuk informasi selengkapnya, lihat Memulai ROSA CLI di dokumentasi Red Hat.
2. Buat ROSA cluster di Red Hat Hybrid Cloud Console atau dengan ROSA CLI.
3. Saat klaster Anda siap, konfigurasikan penyedia identitas untuk memberikan akses pengguna ke klaster.
4. Terapkan dan kelola beban kerja di ROSA klaster Anda dengan cara yang sama seperti yang Anda lakukan dengan lingkungan lain OpenShift .

Harga

Total biaya ROSA terdiri dari dua komponen: biaya ROSA layanan dan biaya AWS infrastruktur. Untuk informasi lebih lanjut tentang harga, lihat Layanan OpenShift Red Hat di AWS Harga.

ROSA biaya layanan

Secara default, biaya ROSA layanan bertambah sesuai permintaan dengan tarif per jam per 4 vCPU yang digunakan oleh node pekerja. Biaya layanan seragam di semua Wilayah AWS standar yang didukung. Selain biaya layanan node pekerja, ROSA dengan cluster pesawat kontrol yang dihosting (HCP) dikenakan biaya cluster per jam.

ROSA menawarkan kontrak biaya layanan 1 tahun dan 3 tahun yang dapat Anda beli untuk penghematan biaya layanan sesuai permintaan untuk node pekerja. Untuk informasi selengkapnya, lihat the section called “Membeli ROSA kontrak”.

AWS biaya infrastruktur

AWS Biaya infrastruktur berlaku untuk node pekerja yang mendasarinya, node infrastruktur, node bidang kontrol, penyimpanan, dan sumber daya jaringan yang dihosting di infrastruktur AWS global. AWS Biaya infrastruktur berbeda-beda Wilayah AWS.

Ikhtisar tanggung jawab untuk ROSA

Dokumentasi ini menguraikan tanggung jawab Amazon Web Services (AWS), Red Hat, dan pelanggan untuk Layanan OpenShift Red Hat di AWS (ROSA) layanan yang dikelola. Untuk informasi selengkapnya tentang ROSA dan komponennya, lihat Kebijakan dan definisi layanan dalam dokumentasi Red Hat.

Model tanggung jawab AWS bersama mendefinisikan AWS tanggung jawab untuk melindungi infrastruktur yang menjalankan semua layanan yang ditawarkan di AWS Cloud, termasuk ROSA. AWS Infrastruktur meliputi perangkat keras, perangkat lunak, jaringan, dan fasilitas yang menjalankan AWS Cloud layanan. AWS Tanggung jawab ini sering disebut sebagai “keamanan cloud”. Untuk beroperasi ROSA sebagai layanan yang dikelola sepenuhnya, Red Hat dan pelanggan bertanggung jawab atas elemen-elemen layanan yang didefinisikan oleh model AWS tanggung jawab sebagai “keamanan di cloud”.

Red Hat bertanggung jawab atas manajemen dan keamanan infrastruktur ROSA cluster yang sedang berlangsung, platform aplikasi yang mendasarinya, dan sistem operasi. Sementara ROSA cluster di-host pada AWS sumber daya di pelanggan Akun AWS, mereka diakses dari jarak jauh oleh komponen ROSA layanan dan insinyur keandalan situs Red Hat (SREs) melalui IAM peran yang dibuat pelanggan. Red Hat menggunakan akses ini untuk mengelola penyebaran dan kapasitas semua bidang kontrol dan node infrastruktur di cluster, dan memelihara versi untuk node bidang kontrol, node infrastruktur, dan node pekerja.

Red Hat dan pelanggan berbagi tanggung jawab untuk manajemen ROSA jaringan, pencatatan klaster, pembuatan versi klaster, dan manajemen kapasitas. Sementara Red Hat mengelola ROSA layanan, pelanggan bertanggung jawab penuh untuk mengelola dan mengamankan aplikasi, beban kerja, dan data apa pun yang digunakan. ROSA

Gambaran Umum

Tabel berikut memberikan gambaran umum tentang AWS, Red Hat, dan tanggung jawab pelanggan untuk Layanan OpenShift Red Hat di AWS.

> **Note**
>
> Jika `cluster-admin` peran ditambahkan ke pengguna, lihat tanggung jawab dan catatan pengecualian di Lampiran 4 Perjanjian Perusahaan Red Hat (Layanan Berlangganan Online).

Sumber Daya	Manajemen insiden dan operasi	Manajemen perubahan	Akses dan otorisasi identitas	Kepatuhan keamanan dan regulasi	Pemulihan bencana
Data pelanggan	Pelanggan	Pelanggan	Pelanggan	Pelanggan	Pelanggan
Aplikasi pelanggan	Pelanggan	Pelanggan	Pelanggan	Pelanggan	Pelanggan
Layanan pengembang	Pelanggan	Pelanggan	Pelanggan	Pelanggan	Pelanggan
Pemantauan platform	Topi Merah	Topi Merah	Topi Merah	Topi Merah	Topi Merah
Pencatatan log	Topi Merah	Red Hat dan pelanggan	Red Hat dan pelanggan	Red Hat dan pelanggan	Topi Merah
Jaringan aplikasi	Red Hat dan pelanggan	Red Hat dan pelanggan	Red Hat dan pelanggan	Topi Merah	Topi Merah
Jaringan cluster	Topi Merah	Red Hat dan pelanggan	Red Hat dan pelanggan	Topi Merah	Topi Merah
Manajemen jaringan virtual	Red Hat dan pelanggan	Red Hat dan pelanggan	Red Hat dan pelanggan	Red Hat dan pelanggan	Red Hat dan pelanggan
Manajemen komputasi virtual (bidang kontrol, infrastruktur, dan node pekerja)	Topi Merah	Topi Merah	Topi Merah	Topi Merah	Topi Merah

Sumber Daya	Manajemen insiden dan operasi	Manajemen perubahan	Akses dan otorisasi identitas	Kepatuhan keamanan dan regulasi	Pemulihan bencana
Versi cluster	Topi Merah	Red Hat dan pelanggan	Topi Merah	Topi Merah	Topi Merah
Manajemen kapasitas	Topi Merah	Red Hat dan pelanggan	Topi Merah	Topi Merah	Topi Merah
Manajemen penyimpanan virtual	Topi Merah	Topi Merah	Topi Merah	Topi Merah	Topi Merah
AWS perangkat lunak (publik Layanan AWS)	AWS	AWS	AWS	AWS	AWS
Perangkat keras/infrastruktur global AWS	AWS	AWS	AWS	AWS	AWS

Tugas untuk tanggung jawab bersama berdasarkan area

AWS, Red Hat, dan pelanggan berbagi tanggung jawab untuk pemantauan dan pemeliharaan ROSA komponen. Dokumentasi ini mendefinisikan tanggung jawab ROSA layanan berdasarkan area dan tugas.

Manajemen insiden dan operasi

AWS bertanggung jawab untuk melindungi infrastruktur perangkat keras yang menjalankan semua layanan yang ditawarkan di AWS Cloud. Red Hat bertanggung jawab untuk mengelola komponen layanan yang diperlukan untuk jaringan platform default. Pelanggan bertanggung jawab atas insiden dan manajemen operasi data aplikasi pelanggan dan jaringan khusus apa pun yang mungkin telah dikonfigurasi pelanggan.

Sumber Daya	Tanggung jawab layanan	Tanggung jawab pelanggan
Jaringan aplikasi	Topi Merah • Pantau layanan OpenShift router asli, dan tanggapi peringatan.	Pelanggan • Pantau kesehatan rute aplikasi, dan titik akhir di belakangnya. • Laporkan pemadaman ke AWS dan Red Hat.
Manajemen jaringan virtual	Topi Merah • Memantau penyeimbang AWS beban, Amazon VPC subnet, dan Layanan AWS komponen yang diperluka n untuk jaringan platform default. Menanggapi peringatan.	Pelanggan • Pantau kesehatan titik akhir penyeimbang AWS beban. • Pantau lalu lintas jaringan yang secara opsional dikonfigurasi melalui koneksi Amazon VPC ke-VPC, AWS VPN koneksi, atau AWS Direct Connect untuk potensi masalah atau ancaman keamanan.
Manajemen penyimpanan virtual	Topi Merah • Monitor Amazon EBS volume yang digunakan untuk node cluster, dan Amazon S3 bucket yang digunakan untuk registri gambar kontainer bawaan ROSA layanan. Menanggap i peringatan.	Pelanggan • Memantau kesehatan data aplikasi. • Jika dikelola pelanggan AWS KMS keys digunakan , buat dan kendalikan siklus hidup kunci dan kebijakan kunci untuk Amazon EBS enkripsi.
AWS perangkat lunak (publik Layanan AWS)	AWS • Untuk informasi tentang AWS insiden dan	Pelanggan

Sumber Daya	Tanggung jawab layanan	Tanggung jawab pelanggan
	manajemen operasi, lihat Bagaimana AWS menjaga ketahanan operasional dan kontinuitas layanan di whitepaper. AWS	• Pantau kesehatan AWS sumber daya di akun pelanggan. • Gunakan IAM alat untuk menerapkan izin yang sesuai ke AWS sumber daya di akun pelanggan.
Perangkat keras/infrastruktur global AWS	AWS • Untuk informasi tentang AWS insiden dan manajemen operasi, lihat Bagaimana AWS menjaga ketahanan operasional dan kontinuitas layanan di whitepaper. AWS	Pelanggan • Mengkonfigurasi, mengelola , dan memantau aplikasi dan data pelanggan untuk memastikan aplikasi dan kontrol keamanan data ditegakkan dengan benar.

Manajemen perubahan

AWS bertanggung jawab untuk melindungi infrastruktur perangkat keras yang menjalankan semua layanan yang ditawarkan di AWS Cloud. Red Hat bertanggung jawab untuk memungkinkan perubahan pada infrastruktur dan layanan cluster yang akan dikendalikan pelanggan, serta mempertahankan versi untuk node bidang kontrol, node infrastruktur, dan node pekerja. Pelanggan bertanggung jawab untuk memulai perubahan infrastruktur. Pelanggan juga bertanggung jawab untuk menginstal dan memelihara layanan opsional, konfigurasi jaringan pada cluster, dan perubahan data dan aplikasi pelanggan.

Sumber Daya	Tanggung jawab layanan	Tanggung jawab pelanggan
Pencatatan log	Topi Merah • Mengagregat dan memantau log audit platform secara terpusat.	Pelanggan • Instal operator logging aplikasi default opsional di cluster.

Sumber Daya	Tanggung jawab layanan	Tanggung jawab pelanggan
	• Menyediakan dan memelihara Operator logging untuk memungkinkan pelanggan menerapkan tumpukan logging untuk pencatatan aplikasi default. • Berikan log audit atas permintaan pelanggan.	• Instal, konfigurasikan, dan pertahankan solusi pencatatan aplikasi opsional apa pun, seperti pencatatan kontainer sespan atau aplikasi logging pihak ketiga. • Menyetel ukuran dan frekuensi log aplikasi yang diproduksi oleh aplikasi pelanggan jika mereka mempengaruhi stabilitas tumpukan logging atau cluster. • Minta log audit platform melalui kasus dukungan untuk meneliti insiden tertentu.

Sumber Daya	Tanggung jawab layanan	Tanggung jawab pelanggan
Jaringan aplikasi	Topi Merah • Siapkan penyeimbang beban publik. Memberikan kemampuan untuk mengatur penyeimbang beban pribadi dan hingga satu penyeimbang beban tambahan bila diperlukan. • Siapkan layanan OpenShift router asli. Berikan kemampuan untuk mengatur router sebagai pribadi dan menambahkan hingga satu pecahan router tambahan. • Instal, konfigurasi, dan pertahankan komponen OpenShift SDN untuk lalu lintas pod internal default. • Memberikan kemampuan bagi pelanggan untuk mengelola `NetworkPolicy` dan `EgressNetworkPolicy` (firewall) objek.	Pelanggan • Konfigurasikan izin jaringan pod non-default untuk jaringan project dan pod, pod ingress, dan pod egress menggunakan objek. `NetworkPolicy` • Gunakan OpenShift Cluster Manager untuk meminta penyeimbang beban pribadi untuk rute aplikasi default. • Gunakan OpenShift Cluster Manager untuk mengonfigurasi hingga satu pecahan router publik atau pribadi tambahan dan penyeimbang beban yang sesuai. • Minta dan konfigurasikan penyeimbang beban layanan tambahan untuk layanan tertentu. • Konfigurasikan aturan penerusan DNS yang diperlukan.

Sumber Daya	Tanggung jawab layanan	Tanggung jawab pelanggan
Jaringan cluster	Topi Merah • Siapkan komponen manajemen klaster, seperti titik akhir layanan publik atau pribadi dan integrasi yang diperlukan dengan Amazon VPC komponen. • Menyiapkan komponen jaringan internal yang diperlukan untuk komunikasi klaster internal antara pekerja, infrastruktur, dan node bidang kontrol.	Pelanggan • Berikan rentang alamat IP non-default opsional untuk CIDR mesin, CIDR layanan, dan pod CIDR jika diperlukan melalui OpenShift Cluster Manager saat cluster disediakan. • Minta endpoint layanan API dibuat publik atau pribadi pada pembuatan klaster atau setelah pembuatan klaster melalui OpenShift Cluster Manager.

Sumber Daya	Tanggung jawab layanan	Tanggung jawab pelanggan
Manajemen jaringan virtual	Topi Merah • Siapkan dan konfigurasikan Amazon VPC komponen yang diperlukan untuk menyediakan klaster, seperti subnet, penyeimba ng beban, gateway internet, dan gateway NAT. • Memberikan kemampuan bagi pelanggan untuk mengelola AWS VPN konektivitas dengan sumber daya lokal, konektivitas Amazon VPC ke VPC, dan AWS Direct Connect sesuai kebutuhan melalui OpenShift Cluster Manager. • Memungkinkan pelanggan untuk membuat dan menerapkan penyeimba ng AWS beban untuk digunakan dengan penyeimbang beban layanan.	Pelanggan • Siapkan dan pertahankan Amazon VPC komponen opsional, seperti koneksi Amazon VPC ke-VPC, AWS VPN koneksi, atau. AWS Direct Connect • Minta dan konfigurasikan penyeimbang beban tambahan untuk layanan tertentu.

Sumber Daya	Tanggung jawab layanan	Tanggung jawab pelanggan
Manajemen komputasi virtual	Topi Merah • Siapkan dan konfigura sikan bidang ROSA kontrol dan bidang data untuk menggunakan Amazon EC2 instance untuk komputasi cluster. • Memantau dan mengelola penyebaran bidang Amazon EC2 kontrol dan node infrastruktur pada cluster.	Pelanggan • Pantau dan kelola node Amazon EC2 pekerja dengan membuat kumpulan mesin menggunakan OpenShift Cluster Manager atau ROSA CLI. • Kelola perubahan pada aplikasi dan data aplikasi yang digunakan pelanggan.
Versi cluster	Topi Merah • Aktifkan proses penjadwal an peningkatan. • Pantau kemajuan peningkat an dan perbaiki masalah apa pun yang dihadapi. • Publikasikan log perubahan dan catatan rilis untuk peningkatan minor dan pemeliharaan.	Pelanggan • Jadwal upgrade versi pemeliharaan baik segera, untuk masa depan, atau memiliki upgrade otomatis. • Mengakui dan menjadwal kan upgrade versi minor. • Pastikan versi cluster tetap pada versi minor yang didukung. • Uji aplikasi pelanggan pada versi minor dan pemelihar aan untuk memastikan kompatibilitas.

Sumber Daya	Tanggung jawab layanan	Tanggung jawab pelanggan
Manajemen kapasitas	Topi Merah • Pantau penggunaan bidang kontrol. Bidang kontrol termasuk node bidang kontrol dan node infrastru ktur. • Skala dan ubah ukuran node bidang kontrol untuk menjaga kualitas layanan.	Pelanggan • Pantau pemanfaatan node pekerja dan, jika sesuai, aktifkan fitur penskalaan otomatis. • Tentukan strategi penskalaa n cluster. • Gunakan kontrol OpenShift Cluster Manager yang disediaka n untuk menambah atau menghapus node pekerja tambahan sesuai kebutuhan . • Menanggapi pemberita huan Red Hat mengenai persyaratan sumber daya klaster.

Sumber Daya	Tanggung jawab layanan	Tanggung jawab pelanggan
Manajemen penyimpanan virtual	Topi Merah • Siapkan dan konfigura sikan Amazon EBS untuk menyediakan penyimpanan node lokal dan penyimpan an volume persisten untuk cluster. • Siapkan dan konfigura sikan registri gambar bawaan untuk menggunak an penyimpanan Amazon S3 bucket. • Pangkas sumber daya registri gambar secara teratur Amazon S3 untuk mengoptimalkan Amazon S3 penggunaan dan kinerja cluster.	Pelanggan • Secara opsional konfigura sikan driver Amazon EBS CSI atau driver Amazon EFS CSI untuk menyediak an volume persisten pada cluster.

Sumber Daya	Tanggung jawab layanan	Tanggung jawab pelanggan

AWS perangkat lunak (AWS layanan publik)	AWS
	
	Hitung
	
	• Menyediakan Amazon EC2 layanan, digunakan untuk bidang ROSA kontrol, infrastruktur, dan node pekerja.
	
	Penyimpanan
	
	• Menyediakan Amazon EBS untuk memungkinkan ROSA layanan menyediak an penyimpanan node lokal dan penyimpanan volume persisten untuk cluster.
	
	Jaringan
	
	• Menyediakan AWS Cloud layanan berikut untuk memenuhi kebutuhan infrastruktur jaringan ROSA virtual:
	  • Amazon VPC
	  • Elastic Load Balancing
	  • IAM
	• Berikan Layanan AWS integrasi opsional berikut untuk ROSA:
	  • AWS VPN
	  • AWS Direct Connect
		Pelanggan
		
		• Menandatangani permintaa n menggunakan ID kunci akses dan kunci akses rahasia yang terkait dengan kredensi keamanan IAM utama atau AWS STS sementara.
		• Tentukan subnet VPC untuk cluster yang akan digunakan selama pembuatan klaster.
		• Konfigurasikan VPC yang dikelola pelanggan secara opsional untuk digunakan dengan cluster. ROSA

Sumber Daya	Tanggung jawab layanan	Tanggung jawab pelanggan
	• AWS PrivateLink • AWS Transit Gateway	
Perangkat keras/infrastruktur global AWS	AWS • Untuk informasi tentang kontrol manajemen untuk pusat AWS data, lihat Kontrol Kami di halaman AWS Cloud Keamanan. • Untuk informasi tentang praktik terbaik manajemen perubahan, lihat Panduan untuk Manajemen Perubahan AWS di Perpustakaan AWS Solusi.	Pelanggan • Menerapkan praktik terbaik manajemen perubahan untuk aplikasi pelanggan dan data yang dihosting di AWS Cloud.

Akses dan otorisasi identitas

Akses dan otorisasi identitas mencakup tanggung jawab untuk mengelola akses resmi ke cluster, aplikasi, dan sumber daya infrastruktur. Ini termasuk tugas-tugas seperti menyediakan mekanisme kontrol akses, otentikasi, otorisasi, dan mengelola akses ke sumber daya.

Sumber Daya	Tanggung jawab layanan	Tanggung jawab pelanggan
Pencatatan log	Topi Merah • Patuhi proses akses internal berjenjang berbasis standar industri untuk log audit platform. • Memberikan kemampuan OpenShift RBAC asli.	Pelanggan • Konfigurasikan OpenShift RBAC untuk mengontro l akses ke proyek dan dengan ekstensi log aplikasi proyek. • Untuk solusi pencatata n aplikasi pihak ketiga atau kustom, pelanggan

Sumber Daya	Tanggung jawab layanan	Tanggung jawab pelanggan
		bertanggung jawab atas manajemen akses.
Jaringan aplikasi	Topi Merah • Menyediakan OpenShift RBAC asli dan `dedicated-admin` kemampuan.	Pelanggan • Konfigurasikan OpenShift `dedicated-admin` dan RBAC untuk mengontrol akses ke konfigurasi rute sesuai kebutuhan. • Kelola administrator organisasi Red Hat untuk Red Hat untuk memberikan akses ke Manajer OpenShift Cluster. Manajer cluster digunakan untuk mengkonfigurasi opsi router dan menyediakan kuota penyeimbang beban layanan.
Jaringan cluster	Topi Merah • Menyediakan kontrol akses pelanggan melalui OpenShift Cluster Manager. Menyediakan OpenShift RBAC asli dan `dedicated-admin` kemampuan.	Pelanggan • Konfigurasikan OpenShift `dedicated-admin` dan RBAC untuk mengontrol akses ke konfigurasi rute sesuai kebutuhan. • Kelola keanggotaan organisasi Red Hat dari akun Red Hat. • Kelola administrator organisasi untuk Red Hat untuk memberikan akses ke Manajer OpenShift Cluster.

Sumber Daya	Tanggung jawab layanan	Tanggung jawab pelanggan
Manajemen jaringan virtual	Topi Merah • Menyediakan kontrol akses pelanggan melalui OpenShift Cluster Manager.	Pelanggan • Kelola akses pengguna opsional ke AWS komponen melalui OpenShift Cluster Manager.
Manajemen komputasi virtual	Topi Merah • Menyediakan kontrol akses pelanggan melalui OpenShift Cluster Manager.	Pelanggan • Kelola akses pengguna opsional ke AWS komponen melalui OpenShift Cluster Manager. • Buat IAM peran dan kebijakan terlampir yang diperlukan untuk mengaktif kan akses ROSA layanan.
Manajemen penyimpanan virtual	Topi Merah • Menyediakan kontrol akses pelanggan melalui OpenShift Cluster Manager.	Pelanggan • Kelola akses pengguna opsional ke AWS komponen melalui OpenShift Cluster Manager. • Buat IAM peran dan kebijakan terlampir yang diperlukan untuk mengaktif kan akses ROSA layanan.

Sumber Daya	Tanggung jawab layanan	Tanggung jawab pelanggan
AWS perangkat lunak (AWS layanan publik)	AWS Hitung • Menyediakan Amazon EC2 layanan, digunakan untuk bidang ROSA kontrol, infrastruktur, dan node pekerja. Penyimpanan • Menyediakan Amazon EBS, digunakan ROSA untuk memungkinkan penyediaa n penyimpanan node lokal dan penyimpanan volume persisten untuk cluster. • Menyediakan Amazon S3, digunakan untuk registri gambar bawaan layanan. Jaringan • Menyediakan AWS Identity and Access Managemen t (IAM), digunakan oleh pelanggan untuk mengontro l akses ke ROSA sumber daya yang berjalan di akun pelanggan.	Pelanggan • Buat IAM peran dan kebijakan terlampir yang diperlukan untuk mengaktif kan akses ROSA layanan. • Gunakan IAM alat untuk menerapkan izin yang sesuai ke AWS sumber daya di akun pelanggan. • Untuk mengaktifkan ROSA di seluruh AWS organisasi Anda, pelanggan bertanggung jawab untuk mengelola AWS Organizat ions administrator. • Untuk mengaktifkan ROSA di seluruh AWS organisasi Anda, pelanggan bertanggu ng jawab untuk mendistri busikan hibah ROSA hak menggunakan. AWS License Manager

Sumber Daya	Tanggung jawab layanan	Tanggung jawab pelanggan
Perangkat keras/infrastruktur global AWS	AWS • Untuk informasi tentang kontrol akses fisik untuk pusat AWS data, lihat Kontrol Kami di halaman AWS Cloud Keamanan.	Pelanggan • Pelanggan tidak bertanggung jawab atas infrastruktur AWS global.

Kepatuhan keamanan dan regulasi

Berikut ini adalah tanggung jawab dan kontrol yang terkait dengan kepatuhan:

Sumber Daya	Tanggung jawab layanan	Tanggung jawab pelanggan
Pencatatan log	Topi Merah • Kirim log audit klaster ke Red Hat SIEM untuk menganalisis peristiwa keamanan. Menyimpan log audit untuk jangka waktu tertentu untuk mendukung analisis forensik.	Pelanggan • Analisis log aplikasi untuk acara keamanan. • Kirim log aplikasi ke titik akhir eksternal melalui pencatatan kontainer sidecar atau aplikasi logging pihak ketiga jika diperlukan retensi yang lebih lama daripada yang ditawarkan oleh tumpukan logging default.
Manajemen jaringan virtual	Topi Merah • Memantau komponen jaringan virtual untuk potensi masalah dan ancaman keamanan.	Pelanggan • Pantau komponen jaringan virtual opsional yang dikonfigurasi untuk potensi masalah dan ancaman keamanan.

Sumber Daya	Tanggung jawab layanan	Tanggung jawab pelanggan
	• Gunakan AWS alat publik untuk pemantauan dan perlindungan tambahan.	• Konfigurasikan aturan firewall yang diperlukan atau perlindungan pusat data pelanggan sesuai kebutuhan.
Manajemen komputasi virtual	Topi Merah • Pantau komponen komputasi virtual untuk potensi masalah dan ancaman keamanan. • Gunakan AWS alat publik untuk pemantauan dan perlindungan tambahan.	Pelanggan • Pantau komponen jaringan virtual opsional yang dikonfigurasi untuk potensi masalah dan ancaman keamanan. • Konfigurasikan aturan firewall yang diperlukan atau perlindungan pusat data pelanggan sesuai kebutuhan.

Sumber Daya	Tanggung jawab layanan	Tanggung jawab pelanggan
Manajemen penyimpanan virtual	Topi Merah • Pantau komponen penyimpanan virtual untuk potensi masalah dan ancaman keamanan. • Gunakan AWS alat publik untuk pemantauan dan perlindungan tambahan. • Konfigurasikan ROSA layanan untuk mengenkripsi data volume control plane, infrastruktur, dan worker node secara default menggunakan kunci KMS AWS terkelola yang Amazon EBS menyediakan. • Konfigurasikan ROSA layanan untuk mengenkripsi volume persisten pelanggan yang menggunakan kelas penyimpanan default dengan kunci KMS AWS terkelola yang Amazon EBS menyediakan. • Memberikan kemampuan bagi pelanggan untuk menggunakan pelanggan yang KMS key berhasil mengenkripsi volume persisten. • Konfigurasikan registri gambar kontainer untuk mengenkripsi data registri	Pelanggan • Amazon EBS Volume ketentuan. • Kelola penyimpanan Amazon EBS volume untuk memastikan penyimpanan yang cukup tersedia untuk dipasang sebagai volume masuk ROSA. • Buat klaim volume persisten dan hasilkan volume persisten melalui OpenShift Cluster Manager.

Sumber Daya	Tanggung jawab layanan	Tanggung jawab pelanggan
	gambar saat istirahat menggunakan enkripsi sisi server dengan kunci Amazon S3 terkelola (SSE-3). • Memberikan kemampuan bagi pelanggan untuk membuat registri Amazon S3 gambar publik atau pribadi untuk melindungi gambar kontainer mereka dari akses pengguna yang tidak sah.	

Sumber Daya	Tanggung jawab layanan	Tanggung jawab pelanggan
AWS perangkat lunak (AWS layanan publik)	AWS Hitung • Menyediakan Amazon EC2, digunakan untuk bidang ROSA kontrol, infrastruktur, dan node pekerja. Untuk informasi selengkapnya, lihat Keamanan infrastruktur Amazon EC2 di Panduan Amazon EC2 Pengguna. Penyimpanan • Menyediakan Amazon EBS, digunakan untuk bidang ROSA kontrol, infrastru ktur, dan volume node pekerja, serta volume persisten Kubernetes. Untuk informasi selengkapnya, lihat Perlindungan data Amazon EC2 di Panduan Amazon EC2 Pengguna. • Menyediakan AWS KMS, yang ROSA digunakan untuk mengenkripsi bidang kontrol, infrastruktur, dan volume node pekerja dan volume persisten. Untuk informasi selengkapnya, lihat Amazon EBS enkripsi di Panduan Amazon EC2 Pengguna.	Pelanggan • Pastikan praktik terbaik keamanan dan prinsip hak istimewa paling sedikit diikuti untuk melindungi data pada Amazon EC2 instance. Untuk informasi selengkap nya, lihat Keamanan infrastruktur Amazon EC2 dan Perlindungan data di Amazon EC2. • Pantau komponen jaringan virtual opsional yang dikonfigurasi untuk potensi masalah dan ancaman keamanan. • Konfigurasikan aturan firewall yang diperlukan atau perlindungan pusat data pelanggan sesuai kebutuhan. • Buat kunci KMS terkelola pelanggan opsional dan enkripsi volume Amazon EBS persisten menggunak an kunci KMS. • Pantau data pelanggan dalam penyimpanan virtual untuk potensi masalah dan ancaman keamanan. Untuk informasi selengkap nya, lihat Model Tanggung Jawab AWS Bersama.

Sumber Daya	Tanggung jawab layanan	Tanggung jawab pelanggan
	• Menyediakan Amazon S3, digunakan untuk registri gambar kontainer bawaan layanan ROSA. Untuk informasi selengkapnya, lihat Amazon S3 keamanan di Panduan Amazon S3 Pengguna. Jaringan • Menyediakan kemampuan dan layanan keamanan untuk meningkatkan privasi dan kontrol akses jaringan pada infrastruktur AWS global, termasuk firewall jaringan bawaan Amazon VPC, koneksi jaringan pribadi atau khusus, dan enkripsi otomatis semua lalu lintas di jaringan AWS global dan regional antara fasilitas AWS aman. Untuk informasi selengkapnya, lihat Model Tanggung Jawab AWS Bersama dan keamanan Infrastruktur di whitepaper Pengantar AWS Keamanan.	

Sumber Daya	Tanggung jawab layanan	Tanggung jawab pelanggan
Perangkat keras/infrastruktur global AWS	AWS • Menyediakan infrastruktur AWS global yang ROSA digunakan untuk memberikan fungsionalitas layanan. Untuk informasi selengkapnya tentang kontrol AWS keamanan, lihat Keamanan AWS Infrastruktur di AWS whitepaper. • Menyediakan dokumentasi bagi pelanggan untuk mengelola kebutuhan kepatuhan dan memeriksa status keamanan mereka dalam AWS menggunakan alat seperti AWS Artifact dan AWS Security Hub.	Pelanggan • Mengkonfigurasi, mengelola, dan memantau aplikasi dan data pelanggan untuk memastikan aplikasi dan kontrol keamanan data ditegakkan dengan benar. • Gunakan IAM alat untuk menerapkan izin yang sesuai ke AWS sumber daya di akun pelanggan.

Pemulihan bencana

Pemulihan bencana meliputi cadangan data dan konfigurasi, replikasi data dan konfigurasi lingkungan pemulihan bencana, dan failover pada peristiwa bencana.

Sumber Daya	Tanggung jawab layanan	Tanggung jawab pelanggan
Manajemen jaringan virtual	Topi Merah • Kembalikan atau buat ulang komponen jaringan virtual yang terpengaruh yang diperlukan agar platform berfungsi.	Pelanggan • Konfigurasikan koneksi jaringan virtual dengan lebih dari satu terowongan jika memungkinkan untuk perlindungan terhadap pemadaman.

Sumber Daya	Tanggung jawab layanan	Tanggung jawab pelanggan
		• Pertahankan DNS failover dan load balancing jika menggunakan penyeimba ng beban global dengan beberapa cluster.
Manajemen komputasi virtual	Topi Merah • Pantau cluster dan ganti bidang Amazon EC2 kontrol atau node infrastruktur yang gagal. • Memberikan kemampuan bagi pelanggan untuk secara manual atau otomatis mengganti node pekerja yang gagal.	Pelanggan • Ganti node Amazon EC2 pekerja yang gagal dengan mengedit konfigurasi kumpulan mesin melalui OpenShift Cluster Manager atau ROSA CLI.
Manajemen penyimpanan virtual	Topi Merah • Untuk ROSA cluster yang dibuat dengan kredenal AWS IAM pengguna, buat cadangan semua objek Kubernetes di cluster melalui snapshot volume per jam, harian, dan mingguan.	Pelanggan • Cadangkan aplikasi pelanggan dan data aplikasi.

Sumber Daya	Tanggung jawab layanan	Tanggung jawab pelanggan
AWS perangkat lunak (AWS layanan publik)	AWS Hitung • Menyediakan Amazon EC2 fitur yang mendukung ketahanan data seperti Amazon EBS snapshot dan. Amazon EC2 Auto Scaling Untuk informasi selengkap nya, lihat Ketahanan Amazon EC2 di Amazon EC2 Panduan Pengguna. Penyimpanan • Memberikan kemampuan bagi ROSA layanan dan pelanggan untuk mencadangkan Amazon EBS volume pada cluster melalui snapshot Amazon EBS volume. • Untuk informasi tentang Amazon S3 fitur yang mendukung ketahanan data, lihat Ketahanan di. Amazon S3 Jaringan • Untuk informasi tentang Amazon VPC fitur yang mendukung ketahanan data, lihat Ketahanan Amazon	Pelanggan • Konfigurasikan cluster ROSA multi-AZ untuk meningkatkan toleransi kesalahan dan ketersediaan cluster. • Menyediakan volume persisten menggunak an driver Amazon EBS CSI untuk mengaktifkan snapshot volume. • Buat snapshot volume CSI dari volume Amazon EBS persisten.

Sumber Daya	Tanggung jawab layanan	Tanggung jawab pelanggan
	Virtual Private Cloud dalam Panduan Pengguna. Amazon VPC	
Perangkat keras/infrastruktur global AWS	AWS • Menyediakan infrastruktur AWS global yang memungkinkan ROSA untuk menskalakan bidang kontrol, infrastruktur, dan node pekerja di seluruh Availability Zone. Fungsi ini memungkinkan ROSA untuk mengatur failover otomatis antar zona tanpa gangguan. • Untuk informasi selengkapnya tentang praktik terbaik pemulihan bencana, lihat Opsi pemulihan bencana di cloud di AWS Well-Architected Framework.	Pelanggan • Konfigurasikan cluster ROSA multi-AZ untuk meningkatkan toleransi kesalahan dan ketersediaan cluster.

Tanggung jawab pelanggan untuk data dan aplikasi

Pelanggan bertanggung jawab atas aplikasi, beban kerja, dan data yang mereka gunakan. Layanan OpenShift Red Hat di AWS Namun, AWS Red Hat menyediakan berbagai alat untuk membantu pelanggan mengelola data dan aplikasi di platform.

Sumber Daya	Bagaimana AWS dan Red Hat membantu	Tanggung jawab pelanggan
Data pelanggan	Topi Merah	Pelanggan

Sumber Daya	Bagaimana AWS dan Red Hat membantu	Tanggung jawab pelanggan
	• Mempertahankan standar tingkat platform untuk enkripsi data sebagaimana didefinisikan oleh standar keamanan dan kepatuhan industri. • Menyediakan OpenShift komponen untuk membantu mengelola data aplikasi, seperti rahasia. • Aktifkan integrasi dengan layanan data seperti Amazon RDS untuk menyimpan dan mengelola data di luar cluster dan/atau AWS AWS • Menyediakan Amazon RDS untuk memungkin kan pelanggan menyimpan dan mengelola data di luar cluster.	• Menjaga tanggung jawab atas semua data pelanggan yang disimpan di platform dan bagaimana aplikasi pelanggan mengkonsumsi dan mengekspos data ini.

Sumber Daya	Bagaimana AWS dan Red Hat membantu	Tanggung jawab pelanggan
Aplikasi pelanggan	Topi Merah • Menyediakan klaster dengan OpenShift komponen yang terpasang sehingga pelanggan dapat mengakses OpenShift dan Kubernetes APIs untuk menyebarkan dan mengelola aplikasi kontainer . • Buat cluster dengan rahasia tarik gambar sehingga penerapan pelanggan dapat menarik gambar dari registri Katalog Red Hat Container. • Menyediakan akses ke OpenShift APIs yang dapat digunakan pelanggan untuk mengatur Operator untuk menambahkan layanan komunitas, pihak ketiga AWS, dan Red Hat ke cluster. • Menyediakan kelas penyimpanan dan plugin untuk mendukung volume persisten untuk digunakan dengan aplikasi pelanggan. • Menyediakan registri gambar kontainer sehingga pelanggan dapat menyimpan	Pelanggan • Menjaga tanggung jawab untuk aplikasi pelanggan dan pihak ketiga, data, dan siklus hidup aplikasi yang lengkap. • Jika pelanggan menambahk an Red Hat, komunitas , pihak ketiga, layanan mereka sendiri, atau layanan lain ke klaster dengan menggunakan Operator atau gambar eksternal, pelanggan bertanggung jawab atas layanan ini dan untuk bekerja dengan penyedia yang sesuai (termasuk Red Hat) untuk memecahkan masalah apa pun. • Gunakan alat dan fitur yang disediakan untuk mengonfig urasi dan menerapkan; tetap up to date; mengatur permintaan dan batasan sumber daya; ukuran cluster untuk memiliki sumber daya yang cukup untuk menjalank an aplikasi; mengatur izin; mengintegrasikan dengan layanan lain; mengelola aliran gambar atau templat

Sumber Daya	Bagaimana AWS dan Red Hat membantu	Tanggung jawab pelanggan
	gambar kontainer aplikasi dengan aman di cluster untuk menyebarkan dan mengelola aplikasi. AWS • Menyediakan Amazon EBS untuk mendukung volume persisten untuk digunakan dengan aplikasi pelanggan. • Menyediakan Amazon S3 untuk mendukung penyediaan Red Hat dari registri gambar kontainer.	apa pun yang digunakan pelanggan; melayani secara eksternal; menyimpan , mencadangkan, dan memulihkan data; dan sebaliknya kelola beban kerjanya yang sangat tersedia dan tangguh. • Pertahankan tanggung jawab untuk memantau aplikasi yang dijalankan Layanan OpenShift Red Hat di AWS, termasuk menginstal dan mengopera sikan perangkat lunak untuk mengumpulkan metrik, membuat peringatan, dan melindungi rahasia dalam aplikasi.

ROSA arsitektur

Layanan OpenShift Red Hat di AWS (ROSA) memiliki topologi cluster berikut:

- Hosted control plane (HCP) - Pesawat kontrol dihosting di dalam Red Hat Akun AWS dan dikelola oleh Red Hat. Node pekerja dikerahkan di pelanggan. Akun AWS
- Klasik — Pesawat kontrol dan node pekerja dikerahkan di pelanggan. Akun AWS

ROSA dengan HCP menawarkan arsitektur bidang kontrol yang lebih efisien yang membantu mengurangi biaya AWS infrastruktur yang dikeluarkan saat berjalan ROSA dan memungkinkan waktu pembuatan cluster lebih cepat. Baik ROSA dengan HCP dan ROSA classic dapat diaktifkan di konsol. AWS ROSA Anda memiliki pilihan untuk memilih arsitektur mana yang ingin Anda gunakan saat Anda menyediakan ROSA cluster menggunakan ROSA CLI.

> **Note**
>
> ROSA dengan pesawat kontrol yang dihosting (HCP) tidak menawarkan sertifikasi kepatuhan FedRAMP High dan HIPAA Qualified. Untuk informasi selengkapnya, lihat Kepatuhan dalam dokumentasi Red Hat.

> **Note**
>
> ROSA dengan pesawat kontrol yang dihosting (HCP) tidak menawarkan titik akhir Federal Information Processing Standard (FIPS).

Membandingkan ROSA dengan HCP dan ROSA klasik

Tabel berikut membandingkan ROSA dengan model arsitektur klasik HCP dan ROSA.

	ROSA dengan HCP	ROSA klasik
Hosting infrastruktur cluster	Komponen bidang kontrol, seperti etcd, server API, dan oauth, di-host di Red Hat milik. Akun AWS	Komponen bidang kontrol, seperti etcd, server API, dan oauth, dihosting di milik pelanggan. Akun AWS
Amazon VPC	Node pekerja berkomunikasi dengan bidang kontrol di atas AWS PrivateLink.	Node pekerja dan node bidang kontrol digunakan di VPC pelanggan.
AWS Identity and Access Management	Menggunakan kebijakan AWS terkelola.	Menggunakan kebijakan yang dikelola pelanggan yang ditentukan oleh layanan.
Penyebaran multi-zona	Pesawat kontrol dikerahkan di beberapa Availability Zones (AZs).	Pesawat kontrol dapat digunakan dalam satu AZ atau beberapa AZs.
Node infrastruktur	Tidak menggunakan node infrastruktur khusus.	Menggunakan dua single-AZ atau tiga node khusus

	ROSA dengan HCP	ROSA klasik
	Komponen platform dikerahkan ke node pekerja.	multi-AZ untuk meng-host komponen platform.
OpenShift kemampuan	Pemantauan platform, registri gambar, dan pengontrol ingress digunakan di node pekerja.	Pemantauan platform, registri gambar, dan pengontrol ingress digunakan di node infrastruktur khusus.
Upgrade cluster	Bidang kontrol dan setiap kolam mesin dapat ditingkatkan secara terpisah.	Seluruh cluster harus ditingkatkan pada saat yang sama.
Amazon EC2 Jejak minimum	Dua Amazon EC2 contoh diperlukan untuk membuat cluster.	Tujuh Amazon EC2 instans Single-AZ atau sembilan multi-AZ diperlukan untuk membuat cluster.
Wilayah AWS	Untuk Wilayah AWS ketersediaan, lihat Layanan OpenShift Red Hat di AWS titik akhir dan kuota di Panduan Referensi AWS Umum.	Untuk Wilayah AWS ketersediaan, lihat Layanan OpenShift Red Hat di AWS titik akhir dan kuota di Panduan Referensi AWS Umum.

Memulai dengan ROSA

Layanan OpenShift Red Hat di AWS (ROSA) adalah layanan terkelola yang dapat Anda gunakan untuk membangun, menskalakan, dan menyebarkan aplikasi kontainer dengan platform Red Hat OpenShift Enterprise Kubernetes. AWS

Anda dapat menggunakan panduan berikut untuk membuat ROSA klaster pertama Anda, memberikan akses pengguna, menerapkan aplikasi pertama Anda, dan mempelajari cara mencabut akses pengguna dan menghapus klaster Anda.

- the section called “Buat cluster ROSA HCP - CLI”- Buat ROSA pertama Anda dengan menggunakan cluster HCP AWS STS dan CLI ROSA .
- the section called “Buat cluster klasik ROSA - AWS PrivateLink ”- Buat cluster klasik ROSA pertama Anda menggunakan AWS PrivateLink.
- the section called “Buat cluster klasik ROSA - CLI”- Buat cluster klasik ROSA pertama Anda menggunakan AWS STS dan ROSA CLI.

Siapkan untuk digunakan ROSA

Untuk mempersiapkan lingkungan Anda untuk membuat ROSA cluster, Anda harus menyelesaikan tindakan berikut.

Prasyarat

Prasyarat berikut harus dipenuhi untuk mengaktifkan pembuatan cluster. ROSA

- Instal dan konfigurasikan yang terbaru AWS CLI. Untuk informasi selengkapnya, lihat Menginstal atau memperbarui versi terbaru AWS CLI.
- Instal dan konfigurasikan ROSA CLI terbaru dan OpenShift Container Platform CLI. Untuk informasi selengkapnya, lihat Memulai ROSA CLI.
- Anda harus memiliki kuota layanan yang diperlukan untuk Amazon EC2,, Amazon VPC Amazon EBS, dan Elastic Load Balancing. AWS atau Red Hat dapat meminta peningkatan kuota layanan atas nama Anda sebagaimana diperlukan untuk penyelesaian masalah. Untuk melihat kuota layanan yang diperlukan ROSA, lihat Layanan OpenShift Red Hat di AWS titik akhir dan kuota di Referensi Umum. AWS

- Untuk menerima AWS dukungan ROSA, Anda harus mengaktifkan paket dukungan AWS Bisnis, Enterprise On-Ramp, atau Enterprise. Red Hat dapat meminta AWS dukungan atas nama Anda sebagaimana diperlukan untuk penyelesaian masalah. Untuk informasi selengkapnya, lihat the section called “Mendapatkan Dukungan”. Untuk mengaktifkan Dukungan, lihat Dukungan halaman.
- Jika Anda menggunakan AWS Organizations untuk mengelola host ROSA layanan tersebut, kebijakan kontrol layanan organisasi (SCP) harus dikonfigurasi agar Red Hat dapat melakukan tindakan kebijakan yang tercantum dalam SCP tanpa batasan. Akun AWS Untuk informasi selengkapnya, lihat the section called “AWS Organizations kebijakan kontrol layanan menolak izin yang diperlukan AWS Marketplace”. Untuk informasi selengkapnya SCPs, lihat Kebijakan kontrol layanan (SCPs).
- Jika menerapkan ROSA klaster with AWS STS ke diaktifkan Wilayah AWS yang dinonaktifkan secara default, Anda harus memperbarui token keamanan ke versi 2 untuk semua Wilayah Akun AWS dengan perintah berikut.

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

  Untuk informasi selengkapnya tentang mengaktifkan Wilayah, lihat tautan: accounts/latest/reference/manage

Aktifkan ROSA dan konfigurasikan AWS prasyarat

Untuk membuat ROSA klaster, Anda harus mengaktifkan ROSA layanan di AWS ROSA konsol. AWS ROSA Konsol memverifikasi apakah Anda Akun AWS memiliki AWS Marketplace izin yang diperlukan, kuota layanan, dan peran terkait layanan Elastic Load Balancing (ELB) bernama. `AWSServiceRoleForElasticLoadBalancing` Jika salah satu prasyarat ini hilang, konsol memberikan panduan tentang cara mengonfigurasi akun Anda untuk memenuhi prasyarat.

1. Navigasikan ke konsol ROSA tersebut.
2. Pilih Mulai.
3. Pada halaman Verifikasi ROSA prasyarat, pilih Saya setuju untuk membagikan informasi kontak saya dengan Red Hat.
4. Pilih Aktifkan ROSA .
5. Setelah halaman memverifikasi kuota layanan Anda memenuhi ROSA prasyarat dan peran terkait layanan ELB dibuat, buka sesi terminal baru untuk membuat yang pertama menggunakan CLI. ROSA klaster ROSA

Buat ROSA dengan cluster HCP menggunakan CLI ROSA

Bagian berikut menjelaskan cara memulai dengan ROSA dengan pesawat kontrol yang dihosting (ROSA dengan HCP) menggunakan AWS STS dan CLI. ROSA Untuk langkah-langkah membuat ROSA dengan cluster HCP menggunakan Terraform, lihat dokumentasi Red Hat. Untuk mempelajari lebih lanjut tentang penyedia Terraform untuk membuat ROSA cluster, lihat dokumentasi Terraform.

ROSA CLI menggunakan `auto` mode atau `manual` mode untuk membuat IAM sumber daya dan konfigurasi OpenID Connect (OIDC) yang diperlukan untuk membuat file. ROSA klaster`auto`mode secara otomatis membuat IAM peran dan kebijakan yang diperlukan dan penyedia OIDC. `manual`mode output AWS CLI perintah yang diperlukan untuk membuat IAM sumber daya secara manual. Dengan menggunakan `manual` mode, Anda dapat meninjau AWS CLI perintah yang dihasilkan sebelum menjalankannya secara manual. Dengan `manual` mode, Anda juga dapat meneruskan perintah ke administrator atau grup lain di organisasi Anda sehingga mereka dapat membuat sumber daya.

Prosedur dalam dokumen ini menggunakan `auto` mode ROSA CLI untuk membuat IAM sumber daya yang diperlukan dan konfigurasi OIDC untuk ROSA dengan HCP. Untuk opsi lainnya untuk memulai, lihatMemulai dengan ROSA .

Topik

Prasyarat

Lengkapi tindakan prasyarat yang tercantum dalam. the section called “Penyiapan”

Buat Amazon VPC arsitektur

Prosedur berikut menciptakan Amazon VPC arsitektur yang dapat digunakan untuk meng-host cluster. Semua klaster sumber daya di-host di subnet pribadi. Subnet publik mengarahkan lalu lintas keluar dari subnet pribadi melalui gateway NAT ke internet publik. Contoh ini menggunakan blok CIDR `10.0.0.0/16` untuk file. Amazon VPC Namun, Anda dapat memilih blok CIDR yang berbeda. Untuk informasi selengkapnya, lihat Pengukuran VPC.

> **Important**
>
> Jika Amazon VPC persyaratan tidak terpenuhi, pembuatan cluster gagal.

Example

Terraform

1. Instal CLI Terraform. Untuk informasi selengkapnya, lihat petunjuk pemasangan di dokumentasi Terraform.
2. Buka sesi terminal dan kloning repositori VPC Terraform.

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

3. Arahkan ke direktori yang dibuat.

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

4. Memulai file Terraform.

   ```
   terraform init
   ```

   Setelah selesai, CLI mengembalikan pesan bahwa Terraform telah berhasil diinisialisasi.
5. Untuk membuat rencana Terraform berdasarkan template yang ada, jalankan perintah berikut. Wilayah AWS Harus ditentukan. Secara opsional, Anda dapat memilih untuk menentukan nama cluster.

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

Setelah perintah berjalan, `rosa.tfplan` file ditambahkan ke `hypershift-tf` direktori. Untuk opsi yang lebih detail, lihat file README repositori VPC Terraform.

6. Terapkan file rencana untuk membangun VPC.

```
terraform apply rosa.tfplan
```

Setelah selesai, CLI mengembalikan pesan sukses yang memverifikasi sumber daya yang ditambahkan.

a. (Opsional) Buat variabel lingkungan untuk subnet pribadi, publik, dan machinepool yang disediakan Terraform IDs untuk digunakan saat membuat ROSA Anda dengan cluster HCP.

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

b. (Opsional) Verifikasi bahwa variabel lingkungan disetel dengan benar.

```
echo $SUBNET_IDS
```

Amazon VPC console

1. Buka konsol Amazon VPC.
2. Di dasbor VPC, pilih Buat VPC.
3. Agar Sumber Daya dapat dibuat, pilih VPC dan lainnya.
4. Biarkan pembuatan otomatis tag Nama dipilih untuk membuat tag Nama untuk sumber daya VPC, atau hapus untuk menyediakan tag Nama Anda sendiri untuk sumber daya VPC.
5. Untuk blok IPv4 CIDR, masukkan rentang IPv4 alamat untuk VPC. VPC harus memiliki rentang IPv4 alamat.
6. (Opsional) Untuk mendukung IPv6 lalu lintas, pilih blok IPv6 CIDR, blok CIDR yang disediakan Amazon IPv6 .
7. Tinggalkan Tenancy sebagai`Default`.
8. Untuk Jumlah Availability Zones (AZs), pilih nomor yang Anda butuhkan. Untuk penerapan Multi-AZ, ROSA membutuhkan tiga Availability Zone. Untuk memilih subnet Anda, perluas Kustomisasi AZs. AZs

> **Note**
>
> Beberapa jenis ROSA instance hanya tersedia di Availability Zones tertentu. Anda dapat menggunakan perintah ROSA CLI `rosa list instance-types` perintah untuk daftar semua jenis ROSA instance yang tersedia. Untuk memeriksa apakah jenis instance tersedia untuk Availability Zone tertentu, gunakan AWS CLI perintah`aws ec2 describe-instance-type-offerings --location-type availability-zone --filters Name=location,Values=<availability_zone> --region <region> --output text | egrep "<instance_type>"`.

9. Untuk mengkonfigurasi subnet Anda, pilih nilai untuk Jumlah subnet publik dan Jumlah subnet pribadi. Untuk memilih rentang alamat IP untuk subnet Anda, perluas Sesuaikan subnet blok CIDR.

> **Note**
>
> ROSA dengan HCP mengharuskan pelanggan mengonfigurasi setidaknya satu subnet publik dan pribadi per Availability Zone yang digunakan untuk membuat cluster.

10. Untuk memberikan sumber daya di subnet pribadi akses ke internet publik melalui IPv4, untuk gateway NAT, pilih jumlah AZs di mana untuk membuat gateway NAT. Dalam produksi, kami menyarankan Anda menerapkan gateway NAT di setiap AZ dengan sumber daya yang memerlukan akses ke internet publik.
11. (Opsional) Jika Anda perlu mengakses Amazon S3 langsung dari VPC Anda, pilih titik akhir VPC, S3 Gateway.
12. Biarkan opsi DNS default dipilih. ROSA membutuhkan dukungan nama host DNS pada VPC.
13. Perluas Tag tambahan, pilih Tambahkan tag baru, dan tambahkan kunci tag berikut. ROSA menggunakan pemeriksaan preflight otomatis yang memverifikasi bahwa tag ini digunakan.
    - Kunci: `kubernetes.io/role/elb`
    - Kunci: `kubernetes.io/role/internal-elb`
14. Pilih Buat VPC.

AWS CLI

1. Buat VPC dengan Blok CIDR `10.0.0.0/16`.

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

Perintah sebelumnya mengembalikan ID VPC. Berikut ini adalah output contoh.

```
vpc-1234567890abcdef0
```

2. Simpan ID VPC dalam variabel lingkungan.

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

3. Buat `Name` tag untuk VPC, menggunakan variabel `VPC_ID` lingkungan.

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

4. Aktifkan dukungan nama host DNS di VPC.

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

5. Buat subnet publik dan pribadi di VPC, tentukan Availability Zones tempat sumber daya harus dibuat.

> **Important**
>
> ROSA dengan HCP mengharuskan pelanggan mengonfigurasi setidaknya satu subnet publik dan pribadi per Availability Zone yang digunakan untuk membuat cluster. Untuk penerapan Multi-AZ, diperlukan tiga Availability Zone. Jika persyaratan ini tidak terpenuhi, pembuatan cluster gagal.

> **Note**
>
> Beberapa jenis ROSA instance hanya tersedia di Availability Zones tertentu. Anda dapat menggunakan perintah ROSA CLI `rosa list instance-types` perintah untuk daftar semua jenis ROSA instance yang tersedia. Untuk memeriksa apakah jenis

instance tersedia untuk Availability Zone tertentu, gunakan AWS CLI perintah`aws ec2 describe-instance-type-offerings --location-type availability-zone --filters Name=location,Values=<availability_zone> --region <region> --output text | egrep "<instance_type>"`.

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

6. Simpan subnet publik dan pribadi IDs dalam variabel lingkungan.

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

7. Buat tag berikut untuk subnet VPC Anda. ROSA menggunakan pemeriksaan preflight otomatis yang memverifikasi bahwa tag ini digunakan.

> **Note**
>
> Anda harus menandai setidaknya satu subnet pribadi dan, jika berlaku, satu subnet publik.

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

8. Buat gateway internet dan tabel rute untuk lalu lintas keluar. Buat tabel rute dan alamat IP elastis untuk lalu lintas pribadi.

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

9. Menyimpan variabel IDs dalam lingkungan.

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

10. Lampirkan gateway internet ke VPC.

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

11. Kaitkan tabel rute publik ke subnet publik, dan konfigurasikan lalu lintas untuk rute ke gateway internet.

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

12. Buat gateway NAT dan kaitkan dengan alamat IP elastis untuk mengaktifkan lalu lintas ke subnet pribadi.

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

13. Kaitkan tabel rute pribadi ke subnet pribadi, dan konfigurasikan lalu lintas untuk merutekan ke gateway NAT.

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

14. (Opsional) Untuk penerapan Multi-AZ, ulangi langkah-langkah di atas untuk mengonfigurasi dua Zona Ketersediaan lainnya dengan subnet publik dan pribadi.

Buat IAM peran yang diperlukan dan konfigurasi OpenID Connect

Sebelum membuat ROSA dengan cluster HCP, Anda harus membuat IAM peran dan kebijakan yang diperlukan dan konfigurasi OpenID Connect (OIDC). Untuk informasi selengkapnya tentang IAM peran dan kebijakan ROSA dengan HCP, lihat. the section called “ AWS Kebijakan yang dikelola”

Prosedur ini menggunakan `auto` mode ROSA CLI untuk secara otomatis membuat konfigurasi OIDC yang diperlukan untuk membuat ROSA dengan cluster HCP.

1. Buat peran dan kebijakan IAM akun yang diperlukan. `--force-policy-creation`Parameter memperbarui peran dan kebijakan yang ada. Jika tidak ada peran dan kebijakan yang ada, perintah akan membuat sumber daya ini sebagai gantinya.

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

> **Note**
>
> Jika token akses offline Anda telah kedaluwarsa, ROSA CLI mengeluarkan pesan kesalahan yang menyatakan bahwa token otorisasi Anda perlu diperbarui. Untuk langkah-

langkah untuk memecahkan masalah, lihat. the section called “Memecahkan masalah ROSA CLI token akses offline kedaluwarsa”

2. Buat konfigurasi OpenID Connect (OIDC) yang memungkinkan otentikasi pengguna ke cluster. Konfigurasi ini terdaftar untuk digunakan dengan OpenShift Cluster Manager (OCM).

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

3. Salin ID konfigurasi OIDC yang disediakan dalam output CLI ROSA . ID konfigurasi OIDC perlu disediakan nanti untuk membuat ROSA dengan cluster HCP.
4. Untuk memverifikasi konfigurasi OIDC yang tersedia untuk cluster yang terkait dengan organisasi pengguna Anda, jalankan perintah berikut.

```
rosa list oidc-config
```

5. Buat peran IAM operator yang diperlukan, ganti `<OIDC_CONFIG_ID>` dengan ID konfigurasi OIDC yang disalin sebelumnya.

   Example

   Important

   Anda harus memberikan awalan `<PREFIX_NAME>` saat membuat peran Operator. Gagal melakukannya menghasilkan kesalahan.

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

6. Untuk memverifikasi peran IAM operator dibuat, jalankan perintah berikut:

```
rosa list operator-roles
```

Buat ROSA dengan cluster HCP menggunakan CLI ROSA dan AWS STS

Anda dapat membuat ROSA dengan HCP klaster menggunakan AWS Security Token Service (AWS STS) dan `auto` mode yang disediakan di CLI ROSA . Anda memiliki opsi untuk membuat cluster dengan API publik dan Ingress atau API pribadi dan Ingress.

Anda dapat membuat klaster dengan Availability Zone tunggal (Single-AZ) atau beberapa Availability Zone (Multi-AZ). Dalam kedua kasus tersebut, nilai CIDR mesin Anda harus sesuai dengan nilai CIDR VPC Anda.

Prosedur berikut menggunakan `rosa create cluster --hosted-cp` perintah untuk membuat ROSA Single-AZ dengan HCP. klaster Untuk membuat Multi-AZ klaster, tentukan `multi-az` dalam perintah dan subnet pribadi IDs untuk setiap subnet pribadi yang ingin Anda gunakan.

1. Buat ROSA dengan cluster HCP dengan salah satu perintah berikut.
   - Buat ROSA dengan klaster HCP dengan API publik dan Ingress, tentukan nama cluster, awalan peran operator, ID konfigurasi OIDC, dan subnet publik dan pribadi. IDs

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

   - Buat ROSA dengan cluster HCP dengan API pribadi dan Ingress, tentukan nama cluster, awalan peran operator, ID konfigurasi OIDC, dan subnet pribadi. IDs

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

2. Periksa status Anda klaster.

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

   > **Note**
   >
   > Jika proses pembuatan gagal atau `State` bidang tidak berubah menjadi status siap setelah 10 menit, lihatPemecahan Masalah.
   > Untuk menghubungi Dukungan atau dukungan Red Hat untuk bantuan, lihatthe section called “Mendapatkan Dukungan”.

3. Lacak kemajuan klaster pembuatan dengan menonton log OpenShift penginstal.

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

Konfigurasikan penyedia identitas dan berikan klaster akses

ROSA termasuk OAuth server bawaan. Setelah klaster dibuat, Anda harus mengonfigurasi OAuth untuk menggunakan penyedia identitas. Anda kemudian dapat menambahkan pengguna ke penyedia identitas yang dikonfigurasi untuk memberi mereka akses ke layanan Anda klaster. Anda dapat memberikan pengguna `cluster-admin` atau `dedicated-admin` izin ini sesuai kebutuhan.

Anda dapat mengonfigurasi berbagai jenis penyedia identitas untuk Anda ROSA klaster. Jenis yang didukung termasuk GitHub, GitHub Enterprise, GitLab, Google, LDAP, OpenID Connect HTPasswd , dan penyedia identitas.

> **Important**
>
> Penyedia HTPasswd identitas disertakan hanya untuk memungkinkan satu pengguna administrator statis dibuat. HTPasswd tidak didukung sebagai penyedia identitas penggunaan umum untuk. ROSA

Prosedur berikut mengkonfigurasi penyedia GitHub identitas sebagai contoh. Untuk petunjuk tentang cara mengonfigurasi setiap jenis penyedia identitas yang didukung, lihat Mengonfigurasi penyedia identitas untuk AWS STS.

1. Arahkan ke github.com dan masuk ke akun Anda. GitHub
2. Jika Anda tidak memiliki GitHub organisasi untuk digunakan untuk penyediaan identitas untuk Anda klaster, buat satu. Untuk informasi selengkapnya, lihat langkah-langkah dalam GitHub dokumentasi.
3. Menggunakan mode interaktif ROSA CLI, konfigurasikan penyedia identitas untuk klaster Anda.

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

4. Ikuti petunjuk konfigurasi di output untuk membatasi klaster akses ke anggota organisasi Anda 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. Buka URL di output, ganti `<GITHUB_ORG_NAME>` dengan nama GitHub organisasi Anda.
6. Di halaman GitHub web, pilih Daftarkan aplikasi untuk mendaftarkan OAuth aplikasi baru di GitHub organisasi Anda.
7. Gunakan informasi dari GitHub OAuth halaman untuk mengisi prompt `rosa create idp` interaktif yang tersisa dengan menjalankan perintah berikut. Ganti `<GITHUB_CLIENT_ID>` dan `<GITHUB_CLIENT_SECRET>` dengan kredensi dari aplikasi Anda GitHub OAuth .

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

> **Note**
>
> Mungkin diperlukan waktu sekitar dua menit agar konfigurasi penyedia identitas menjadi aktif. Jika Anda mengonfigurasi `cluster-admin` pengguna, Anda dapat menjalankan `oc get pods -n openshift-authentication --watch` untuk melihat OAuth pod di-deploy ulang dengan konfigurasi yang diperbarui.

8. Verifikasi bahwa penyedia identitas dikonfigurasi dengan benar.

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

Memberikan akses pengguna ke klaster

Anda dapat memberikan akses pengguna ke Anda klaster dengan menambahkannya ke penyedia identitas yang dikonfigurasi.

Prosedur berikut menambahkan pengguna ke GitHub organisasi yang dikonfigurasi untuk penyediaan identitas ke cluster.

1. Arahkan ke github.com dan masuk ke akun Anda. GitHub
2. Undang pengguna yang memerlukan klaster akses ke GitHub organisasi Anda. Untuk informasi selengkapnya, lihat Mengundang pengguna untuk bergabung dengan organisasi Anda dalam GitHub dokumentasi.

Konfigurasikan **`cluster-admin`** izin

1. Berikan `cluster-admin` izin dengan menjalankan perintah berikut. Ganti `<IDP_USER_NAME>` dan `<CLUSTER_NAME>` dengan nama pengguna dan cluster Anda.

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

2. Verifikasi bahwa pengguna terdaftar sebagai anggota `cluster-admins` grup.

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

Konfigurasikan **`dedicated-admin`** izin

1. Berikan `dedicated-admin` izin dengan menggunakan perintah berikut. Ganti `<IDP_USER_NAME>` dan `<CLUSTER_NAME>` dengan pengguna dan klaster nama Anda dengan menjalankan perintah berikut.

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

2. Verifikasi bahwa pengguna terdaftar sebagai anggota `cluster-admins` grup.

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

Akses klaster melalui Red Hat Hybrid Cloud Console

Masuk ke Anda klaster melalui Red Hat Hybrid Cloud Console.

1. Dapatkan URL konsol untuk Anda klaster menggunakan perintah berikut. Ganti <CLUSTER_NAME> dengan nama Anda klaster.

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

2. Arahkan ke URL konsol di output dan masuk.

   Dalam dialog Masuk dengan..., pilih nama penyedia identitas dan lengkapi permintaan otorisasi yang disajikan oleh penyedia Anda.

Menyebarkan aplikasi dari Katalog Pengembang

Dari Red Hat Hybrid Cloud Console, Anda dapat menerapkan aplikasi pengujian Katalog Pengembang dan mengeksposnya dengan rute.

1. Arahkan ke Red Hat Hybrid Cloud Console dan pilih cluster tempat Anda ingin menerapkan aplikasi.
2. Pada halaman cluster, pilih Open console.
3. Dalam perspektif Administrator, pilih Home > Projects > Create Project.
4. Masukkan nama untuk proyek Anda dan secara opsional tambahkan Nama Tampilan dan Deskripsi.
5. Pilih Buat untuk membuat proyek.
6. Beralih ke perspektif Pengembang dan pilih +Tambah. Pastikan bahwa proyek yang dipilih adalah yang baru saja dibuat.
7. Dalam dialog Katalog Pengembang, pilih Semua layanan.
8. Di halaman Katalog Pengembang, pilih Bahasa > JavaScriptdari menu.
9. Pilih Node.js, lalu pilih Create Application untuk membuka halaman Create Source-to-Image Application.

> **Note**
>
> Anda mungkin perlu memilih Hapus Semua Filter untuk menampilkan opsi Node.js.

10. Di bagian Git, pilih Coba Sampel.
11. Di bidang Nama, tambahkan nama unik.
12. Pilih Buat.

> **Note**
>
> Aplikasi baru membutuhkan waktu beberapa menit untuk digunakan.

13. Saat penerapan selesai, pilih URL rute untuk aplikasi.

    Tab baru di browser terbuka dengan pesan yang mirip dengan berikut ini.

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

14. (Opsional) Hapus aplikasi dan bersihkan sumber daya:
    a. Dalam perspektif Administrator, pilih Home > Projects.
    b. Buka menu tindakan untuk proyek Anda dan pilih Hapus Proyek.

Mencabut **`cluster-admin`** izin dari pengguna

1. Cabut `cluster-admin` izin menggunakan perintah berikut. Ganti <IDP_USER_NAME> dan <CLUSTER_NAME> dengan pengguna dan klaster nama Anda.

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

2. Verifikasi bahwa pengguna tidak terdaftar sebagai anggota `cluster-admins` grup.

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

Mencabut **dedicated-admin** izin dari pengguna

1. Cabut `dedicated-admin` izin dengan menggunakan perintah berikut. Ganti `<IDP_USER_NAME>` dan `<CLUSTER_NAME>` dengan pengguna dan klaster nama Anda.

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

2. Verifikasi bahwa pengguna tidak terdaftar sebagai anggota `dedicated-admins` grup.

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

Mencabut akses pengguna ke klaster

Anda dapat mencabut klaster akses untuk pengguna penyedia identitas dengan menghapusnya dari penyedia identitas yang dikonfigurasi.

Anda dapat mengonfigurasi berbagai jenis penyedia identitas untuk Anda klaster. Prosedur berikut mencabut klaster akses untuk anggota GitHub organisasi.

1. Arahkan ke github.com dan masuk ke akun Anda. GitHub
2. Hapus pengguna dari GitHub organisasi Anda. Untuk informasi selengkapnya, lihat Menghapus anggota dari organisasi Anda di GitHub dokumentasi.

Hapus cluster dan AWS STS sumber daya

Anda dapat menggunakan ROSA CLI untuk menghapus klaster yang menggunakan AWS Security Token Service ()AWS STS. Anda juga dapat menggunakan ROSA CLI untuk menghapus IAM peran dan penyedia OIDC yang dibuat oleh. ROSA Untuk menghapus IAM kebijakan yang dibuat oleh ROSA, Anda dapat menggunakan IAM konsol.

> **Note**
>
> IAM peran dan kebijakan yang dibuat oleh ROSA mungkin digunakan oleh ROSA cluster lain di akun yang sama.

1. Hapus klaster dan perhatikan log. Ganti `<CLUSTER_NAME>` dengan nama atau ID Anda klaster.

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

> **Important**
>
> Anda harus menunggu penghapusan sepenuhnya sebelum menghapus IAM peran, kebijakan, dan penyedia OIDC. klaster Peran IAM akun diperlukan untuk menghapus sumber daya yang dibuat oleh penginstal. Peran IAM operator diperlukan untuk membersihkan sumber daya yang dibuat oleh OpenShift operator. Operator menggunakan penyedia OIDC untuk mengautentikasi.

2. Hapus penyedia OIDC yang digunakan klaster operator untuk mengautentikasi dengan menjalankan perintah berikut.

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

3. Hapus peran operator khusus cluster. IAM

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

4. Hapus peran IAM akun menggunakan perintah berikut. Ganti `<PREFIX>` dengan awalan peran IAM akun yang akan dihapus. Jika Anda menetapkan awalan kustom saat membuat peran IAM akun, tentukan awalan default`ManagedOpenShift`.

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

5. Hapus IAM kebijakan yang dibuat oleh ROSA.
   a. Masuk ke IAM konsol.
   b. Di menu sebelah kiri di bawah Manajemen akses, pilih Kebijakan.
   c. Pilih kebijakan yang ingin Anda hapus dan pilih Tindakan > Hapus.
   d. Masukkan nama kebijakan dan pilih Hapus.
   e. Ulangi langkah ini untuk menghapus setiap kebijakan IAM untuk. klaster

Buat cluster klasik ROSA menggunakan CLI ROSA

Bagian berikut menjelaskan cara memulai menggunakan ROSA klasik AWS STS dan ROSA CLI. Untuk langkah-langkah membuat klaster klasik ROSA menggunakan Terraform, lihat dokumentasi

Red Hat. Untuk mempelajari lebih lanjut tentang penyedia Terraform untuk membuat ROSA cluster, lihat dokumentasi Terraform.

ROSA CLI menggunakan `auto` mode atau `manual` mode untuk membuat IAM sumber daya yang diperlukan untuk menyediakan a. ROSA klaster`auto`mode segera membuat IAM peran dan kebijakan yang diperlukan dan penyedia OpenID Connect (OIDC). `manual`mode output AWS CLI perintah yang diperlukan untuk membuat IAM sumber daya. Dengan menggunakan `manual` mode, Anda dapat meninjau AWS CLI perintah yang dihasilkan sebelum menjalankannya secara manual. Dengan `manual` mode, Anda juga dapat meneruskan perintah ke administrator atau grup lain di organisasi Anda sehingga mereka dapat membuat sumber daya.

Untuk opsi lainnya untuk memulai, lihatMemulai dengan ROSA .

Topik

Prasyarat

Lengkapi tindakan prasyarat yang tercantum dalam. the section called “Penyiapan”

Buat cluster klasik ROSA menggunakan ROSA CLI dan AWS STS

Anda dapat membuat ROSA klasik klaster menggunakan ROSA AWS STS CLI dan.

1. Buat peran dan kebijakan IAM akun yang diperlukan menggunakan `--mode auto` atau`--mode manual`.

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

     > **Note**
     >
     > Jika token akses offline Anda telah kedaluwarsa, ROSA CLI mengeluarkan pesan kesalahan yang menyatakan bahwa token otorisasi Anda perlu diperbarui. Untuk langkah-langkah untuk memecahkan masalah, lihat. the section called “Memecahkan masalah ROSA CLI token akses offline kedaluwarsa”

2. Buat klaster menggunakan `--mode auto` atau`--mode manual`. `auto`mode memungkinkan Anda untuk membuat cluster lebih cepat. `manual`modus meminta Anda untuk menentukan pengaturan kustom untuk cluster Anda.

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

     > **Note**
     >
     > Saat Anda menentukan`--mode auto`, `rosa create cluster` perintah akan membuat IAM peran operator khusus cluster dan penyedia OIDC secara otomatis. Operator menggunakan penyedia OIDC untuk mengautentikasi.

     > **Note**
     >
     > Saat menggunakan `--mode auto` default, OpenShift versi stabil terbaru diinstal.

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

> **Important**
>
> Jika Anda mengaktifkan enkripsi etcd dalam `manual` mode, Anda akan dikenakan overhead kinerja sekitar 20%. Overhead adalah hasil dari memperkenalkan lapisan enkripsi kedua ini, selain enkripsi Amazon EBS default yang mengenkripsi volume etcd.

> **Note**
>
> Setelah menjalankan `manual` mode untuk membuat cluster, Anda perlu membuat peran IAM operator khusus cluster secara manual dan penyedia OpenID Connect yang digunakan operator klaster untuk mengautentikasi.

3. Periksa status Anda klaster.

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

> **Note**
>
> Jika proses penyediaan gagal atau `State` bidang tidak berubah menjadi status siap setelah 40 menit, lihat. Pemecahan Masalah Untuk menghubungi Dukungan atau dukungan Red Hat untuk bantuan, lihatthe section called “Mendapatkan Dukungan”.

4. Lacak kemajuan klaster pembuatan dengan menonton log OpenShift penginstal.

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

Konfigurasikan penyedia identitas dan berikan klaster akses

ROSA termasuk OAuth server bawaan. Setelah klaster dibuat, Anda harus mengonfigurasi OAuth untuk menggunakan penyedia identitas. Anda kemudian dapat menambahkan pengguna ke penyedia identitas yang dikonfigurasi untuk memberi mereka akses ke layanan Anda klaster. Anda dapat memberikan pengguna `cluster-admin` atau `dedicated-admin` izin ini sesuai kebutuhan.

Anda dapat mengonfigurasi berbagai jenis penyedia identitas untuk Anda ROSA klaster. Jenis yang didukung termasuk GitHub, GitHub Enterprise, GitLab, Google, LDAP, OpenID Connect HTPasswd , dan penyedia identitas.

> **Important**
>
> Penyedia HTPasswd identitas disertakan hanya untuk memungkinkan satu pengguna administrator statis dibuat. HTPasswd tidak didukung sebagai penyedia identitas penggunaan umum untuk. ROSA

Prosedur berikut mengkonfigurasi penyedia GitHub identitas sebagai contoh. Untuk petunjuk tentang cara mengonfigurasi setiap jenis penyedia identitas yang didukung, lihat Mengonfigurasi penyedia identitas untuk AWS STS.

1. Arahkan ke github.com dan masuk ke akun Anda. GitHub
2. Jika Anda tidak memiliki GitHub organisasi untuk digunakan untuk penyediaan identitas untuk Anda klaster, buat satu. Untuk informasi selengkapnya, lihat langkah-langkah dalam GitHub dokumentasi.
3. Menggunakan mode interaktif ROSA CLI, konfigurasikan penyedia identitas untuk klaster Anda.

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

4. Ikuti petunjuk konfigurasi di output untuk membatasi klaster akses ke anggota organisasi Anda 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. Buka URL di output, ganti <GITHUB_ORG_NAME> dengan nama GitHub organisasi Anda.
6. Di halaman GitHub web, pilih Daftarkan aplikasi untuk mendaftarkan OAuth aplikasi baru di GitHub organisasi Anda.
7. Gunakan informasi dari GitHub OAuth halaman untuk mengisi prompt `rosa create idp` interaktif yang tersisa dengan menjalankan perintah berikut. Ganti <GITHUB_CLIENT_ID> dan <GITHUB_CLIENT_SECRET> dengan kredensi dari aplikasi Anda GitHub OAuth .

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

> **Note**
>
> Mungkin diperlukan waktu sekitar dua menit agar konfigurasi penyedia identitas menjadi aktif. Jika Anda mengonfigurasi `cluster-admin` pengguna, Anda dapat menjalankan `oc get pods -n openshift-authentication --watch` untuk melihat OAuth pod di-deploy ulang dengan konfigurasi yang diperbarui.

8. Verifikasi bahwa penyedia identitas dikonfigurasi dengan benar.

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

Memberikan akses pengguna ke klaster

Anda dapat memberikan akses pengguna ke Anda klaster dengan menambahkannya ke penyedia identitas yang dikonfigurasi.

Prosedur berikut menambahkan pengguna ke GitHub organisasi yang dikonfigurasi untuk penyediaan identitas ke cluster.

1. Arahkan ke github.com dan masuk ke akun Anda. GitHub
2. Undang pengguna yang memerlukan klaster akses ke GitHub organisasi Anda. Untuk informasi selengkapnya, lihat Mengundang pengguna untuk bergabung dengan organisasi Anda dalam GitHub dokumentasi.

Konfigurasikan **`cluster-admin`** izin

1. Berikan `cluster-admin` izin dengan menjalankan perintah berikut. Ganti `<IDP_USER_NAME>` dan `<CLUSTER_NAME>` dengan nama pengguna dan cluster Anda.

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

2. Verifikasi bahwa pengguna terdaftar sebagai anggota `cluster-admins` grup.

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

Konfigurasikan **`dedicated-admin`** izin

1. Berikan `dedicated-admin` izin dengan menggunakan perintah berikut. Ganti `<IDP_USER_NAME>` dan `<CLUSTER_NAME>` dengan pengguna dan klaster nama Anda dengan menjalankan perintah berikut.

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

2. Verifikasi bahwa pengguna terdaftar sebagai anggota `cluster-admins` grup.

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

Akses klaster melalui Red Hat Hybrid Cloud Console

Setelah membuat pengguna klaster administrator atau menambahkan pengguna ke penyedia identitas yang dikonfigurasi, Anda dapat masuk klaster melalui Red Hat Hybrid Cloud Console.

1. Dapatkan URL konsol untuk Anda klaster menggunakan perintah berikut. Ganti <CLUSTER_NAME> dengan nama Anda klaster.

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

2. Arahkan ke URL konsol di output dan masuk.
   - Jika Anda membuat `cluster-admin` pengguna, masuk menggunakan kredensi yang disediakan.
   - Jika Anda mengonfigurasi penyedia identitas untuk Anda klaster, pilih nama penyedia identitas di dialog Masuk dengan... dan lengkapi permintaan otorisasi apa pun yang disajikan oleh penyedia Anda.

Menyebarkan aplikasi dari Katalog Pengembang

Dari Red Hat Hybrid Cloud Console, Anda dapat menerapkan aplikasi pengujian Katalog Pengembang dan mengeksposnya dengan rute.

1. Arahkan ke Red Hat Hybrid Cloud Console dan pilih cluster tempat Anda ingin menerapkan aplikasi.
2. Pada halaman cluster, pilih Open console.
3. Dalam perspektif Administrator, pilih Home > Projects > Create Project.
4. Masukkan nama untuk proyek Anda dan secara opsional tambahkan Nama Tampilan dan Deskripsi.
5. Pilih Buat untuk membuat proyek.
6. Beralih ke perspektif Pengembang dan pilih +Tambah. Pastikan bahwa proyek yang dipilih adalah yang baru saja dibuat.
7. Dalam dialog Katalog Pengembang, pilih Semua layanan.
8. Di halaman Katalog Pengembang, pilih Bahasa > JavaScriptdari menu.
9. Pilih Node.js, lalu pilih Create Application untuk membuka halaman Create Source-to-Image Application.

> **Note**
>
> Anda mungkin perlu memilih Hapus Semua Filter untuk menampilkan opsi Node.js.

10. Di bagian Git, pilih Coba Sampel.
11. Di bidang Nama, tambahkan nama unik.
12. Pilih Buat.

> **Note**
>
> Aplikasi baru membutuhkan waktu beberapa menit untuk digunakan.

13. Saat penerapan selesai, pilih URL rute untuk aplikasi.

    Tab baru di browser terbuka dengan pesan yang mirip dengan berikut ini.

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

14. (Opsional) Hapus aplikasi dan bersihkan sumber daya:
    a. Dalam perspektif Administrator, pilih Home > Projects.
    b. Buka menu tindakan untuk proyek Anda dan pilih Hapus Proyek.

Mencabut **`cluster-admin`** izin dari pengguna

1. Cabut `cluster-admin` izin menggunakan perintah berikut. Ganti <IDP_USER_NAME> dan <CLUSTER_NAME> dengan pengguna dan klaster nama Anda.

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

2. Verifikasi bahwa pengguna tidak terdaftar sebagai anggota `cluster-admins` grup.

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

Mencabut **`dedicated-admin`** izin dari pengguna

1. Cabut `dedicated-admin` izin dengan menggunakan perintah berikut. Ganti <IDP_USER_NAME> dan <CLUSTER_NAME> dengan pengguna dan klaster nama Anda.

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

2. Verifikasi bahwa pengguna tidak terdaftar sebagai anggota `dedicated-admins` grup.

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

Mencabut akses pengguna ke klaster

Anda dapat mencabut klaster akses untuk pengguna penyedia identitas dengan menghapusnya dari penyedia identitas yang dikonfigurasi.

Anda dapat mengonfigurasi berbagai jenis penyedia identitas untuk Anda klaster. Prosedur berikut mencabut klaster akses untuk anggota GitHub organisasi.

1. Arahkan ke github.com dan masuk ke akun Anda. GitHub
2. Hapus pengguna dari GitHub organisasi Anda. Untuk informasi selengkapnya, lihat Menghapus anggota dari organisasi Anda di GitHub dokumentasi.

Hapus klaster dan AWS STS sumber daya

Anda dapat menggunakan ROSA CLI untuk menghapus klaster yang menggunakan AWS Security Token Service ()AWS STS. Anda juga dapat menggunakan ROSA CLI untuk menghapus IAM peran dan penyedia OIDC yang dibuat oleh. ROSA Untuk menghapus IAM kebijakan yang dibuat oleh ROSA, Anda dapat menggunakan IAM konsol.

> **Important**
>
> IAM peran dan kebijakan yang dibuat oleh ROSA mungkin digunakan oleh ROSA cluster lain di akun yang sama.

1. Hapus klaster dan perhatikan log. Ganti <CLUSTER_NAME> dengan nama atau ID Anda klaster.

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

> **Important**
>
> Anda harus menunggu penghapusan sepenuhnya sebelum menghapus IAM peran, kebijakan, dan penyedia OIDC. klaster Peran IAM akun diperlukan untuk menghapus sumber daya yang dibuat oleh penginstal. Peran IAM operator diperlukan untuk

membersihkan sumber daya yang dibuat oleh OpenShift operator. Operator menggunakan penyedia OIDC untuk mengautentikasi.

2. Hapus penyedia OIDC yang digunakan klaster operator untuk mengautentikasi dengan menjalankan perintah berikut.

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

3. Hapus peran operator khusus cluster. IAM

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

4. Hapus peran IAM akun menggunakan perintah berikut. Ganti <PREFIX> dengan awalan peran IAM akun yang akan dihapus. Jika Anda menetapkan awalan kustom saat membuat peran IAM akun, tentukan awalan default`ManagedOpenShift`.

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

5. Hapus IAM kebijakan yang dibuat oleh ROSA.
   a. Masuk ke IAM konsol.
   b. Di menu sebelah kiri di bawah Manajemen akses, pilih Kebijakan.
   c. Pilih kebijakan yang ingin Anda hapus dan pilih Tindakan > Hapus.
   d. Masukkan nama kebijakan dan pilih Hapus.
   e. Ulangi langkah ini untuk menghapus setiap kebijakan IAM untuk. klaster

Buat klaster klasik ROSA yang menggunakan AWS PrivateLink

Cluster klasik ROSA dapat digunakan dalam beberapa cara berbeda: publik, pribadi, atau pribadi dengan. AWS PrivateLink Untuk informasi lebih lanjut tentang ROSA klasik, lihatthe section called “Arsitektur”. Untuk klaster konfigurasi publik dan pribadi, OpenShift klaster memiliki akses ke internet, dan privasi diatur pada beban kerja aplikasi di lapisan aplikasi.

Jika Anda memerlukan beban kerja aplikasi klaster dan aplikasi bersifat pribadi, Anda dapat mengonfigurasi AWS PrivateLink dengan ROSA classic. AWS PrivateLink adalah teknologi yang sangat tersedia dan dapat diskalakan yang ROSA digunakan untuk membuat koneksi pribadi antara ROSA layanan dan sumber daya cluster di akun AWS pelanggan. Dengan AWS PrivateLink, tim rekayasa keandalan situs Red Hat (SRE) dapat mengakses cluster untuk tujuan dukungan

dan remediasi dengan menggunakan subnet pribadi yang terhubung ke titik akhir cluster. AWS PrivateLink

Untuk informasi lebih lanjut tentang AWS PrivateLink, lihat Apa itu AWS PrivateLink?

Topik

Prasyarat

Lengkapi tindakan prasyarat yang tercantum dalam. the section called “Penyiapan”

Buat Amazon VPC arsitektur

Prosedur berikut menciptakan Amazon VPC arsitektur yang dapat digunakan untuk meng-host cluster. Semua klaster sumber daya di-host di subnet pribadi. Subnet publik mengarahkan lalu lintas keluar dari subnet pribadi melalui gateway NAT ke internet publik. Contoh ini menggunakan blok CIDR `10.0.0.0/16` untuk file. Amazon VPC Namun, Anda dapat memilih blok CIDR yang berbeda. Untuk informasi selengkapnya, lihat Pengukuran VPC.

> **Important**
>
> Jika Amazon VPC persyaratan tidak terpenuhi, pembuatan cluster gagal.

Example

Amazon VPC console

1. Buka konsol Amazon VPC.
2. Di dasbor VPC, pilih Buat VPC.
3. Agar Sumber Daya dapat dibuat, pilih VPC dan lainnya.
4. Biarkan pembuatan otomatis tag Nama dipilih untuk membuat tag Nama untuk sumber daya VPC, atau hapus untuk menyediakan tag Nama Anda sendiri untuk sumber daya VPC.
5. Untuk blok IPv4 CIDR, masukkan rentang IPv4 alamat untuk VPC. VPC harus memiliki rentang IPv4 alamat.
6. (Opsional) Untuk mendukung IPv6 lalu lintas, pilih blok IPv6 CIDR, blok CIDR yang disediakan Amazon IPv6 .
7. Tinggalkan Tenancy sebagai`Default`.
8. Untuk Jumlah Availability Zones (AZs), pilih nomor yang Anda butuhkan. Untuk penerapan Multi-AZ, ROSA membutuhkan tiga Availability Zone. Untuk memilih subnet Anda, perluas Kustomisasi AZs. AZs

   > **Note**
   >
   > Beberapa jenis ROSA instance hanya tersedia di Availability Zones tertentu. Anda dapat menggunakan perintah ROSA CLI `rosa list instance-types` perintah untuk daftar semua jenis ROSA instance yang tersedia. Untuk memeriksa apakah jenis instance tersedia untuk Availability Zone tertentu, gunakan AWS CLI perintah`aws ec2 describe-instance-type-offerings --location-type availability-zone --filters Name=location,Values=<availability_zone> --region <region> --output text | egrep "<instance_type>"`.
9. Untuk mengkonfigurasi subnet Anda, pilih nilai untuk Jumlah subnet publik dan Jumlah subnet pribadi. Untuk memilih rentang alamat IP untuk subnet Anda, perluas Sesuaikan subnet blok CIDR.

> **Note**
>
> ROSA mengharuskan pelanggan mengonfigurasi setidaknya satu subnet pribadi per Availability Zone yang digunakan untuk membuat cluster.

10. Untuk memberikan sumber daya di subnet pribadi akses ke internet publik melalui IPv4, untuk gateway NAT, pilih jumlah AZs di mana untuk membuat gateway NAT. Dalam produksi, kami menyarankan Anda menerapkan gateway NAT di setiap AZ dengan sumber daya yang memerlukan akses ke internet publik.
11. (Opsional) Jika Anda perlu mengakses Amazon S3 langsung dari VPC Anda, pilih titik akhir VPC, S3 Gateway.
12. Biarkan opsi DNS default dipilih. ROSA membutuhkan dukungan nama host DNS pada VPC.
13. Pilih Buat VPC.

AWS CLI

1. Buat VPC dengan Blok CIDR `10.0.0.0/16`.

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

Perintah sebelumnya mengembalikan ID VPC. Berikut ini adalah output contoh.

```
vpc-1234567890abcdef0
```

2. Simpan ID VPC dalam variabel lingkungan.

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

3. Buat `Name` tag untuk VPC, menggunakan variabel `VPC_ID` lingkungan.

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

4. Aktifkan dukungan nama host DNS di VPC.

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

5. Buat subnet publik dan pribadi di VPC, tentukan Availability Zones tempat sumber daya harus dibuat.

> **Important**
>
> ROSA mengharuskan pelanggan mengonfigurasi setidaknya satu subnet pribadi per Availability Zone yang digunakan untuk membuat cluster. Untuk penerapan Multi-AZ, diperlukan tiga Availability Zone. Jika persyaratan ini tidak terpenuhi, pembuatan cluster gagal.

> **Note**
>
> Beberapa jenis ROSA instance hanya tersedia di Availability Zones tertentu. Anda dapat menggunakan perintah ROSA CLI `rosa list instance-types` perintah untuk daftar semua jenis ROSA instance yang tersedia. Untuk memeriksa apakah jenis instance tersedia untuk Availability Zone tertentu, gunakan AWS CLI perintah`aws ec2 describe-instance-type-offerings --location-type availability-zone --filters Name=location,Values=<availability_zone> --region <region> --output text | egrep "<instance_type>"`.

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

6. Simpan subnet publik dan pribadi IDs dalam variabel lingkungan.

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

7. Buat gateway internet dan tabel rute untuk lalu lintas keluar. Buat tabel rute dan alamat IP elastis untuk lalu lintas pribadi.

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

8. Simpan variabel IDs dalam lingkungan.

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

9. Lampirkan gateway internet ke VPC.

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

10. Kaitkan tabel rute publik ke subnet publik, dan konfigurasikan lalu lintas untuk rute ke gateway internet.

```
aws ec2 associate-route-table \
    --subnet-id $PUBLIC_SUB \
```

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

11. Buat gateway NAT dan kaitkan dengan alamat IP elastis untuk mengaktifkan lalu lintas ke subnet pribadi.

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

12. Kaitkan tabel rute pribadi ke subnet pribadi, dan konfigurasikan lalu lintas untuk merutekan ke gateway NAT.

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

13. (Opsional) Untuk penerapan Multi-AZ, ulangi langkah-langkah di atas untuk mengonfigurasi dua Zona Ketersediaan lainnya dengan subnet publik dan pribadi.

Buat cluster klasik ROSA menggunakan ROSA CLI dan AWS PrivateLink

Anda dapat menggunakan ROSA CLI dan AWS PrivateLink membuat klaster dengan Availability Zone tunggal (Single-AZ) atau beberapa Availability Zone (Multi-AZ). Dalam kedua kasus tersebut, nilai CIDR mesin Anda harus sesuai dengan nilai CIDR VPC Anda.

Prosedur berikut menggunakan `rosa create cluster` perintah untuk membuat ROSA klasik klaster. Untuk membuat Multi-AZ klaster, tentukan `--multi-az` dalam perintah, lalu pilih subnet pribadi IDs yang ingin Anda gunakan saat diminta.

> **Note**
>
> Jika Anda menggunakan firewall, Anda harus mengkonfigurasinya sehingga ROSA dapat mengakses situs yang diperlukan untuk berfungsi.
> Untuk informasi selengkapnya, lihat prasyarat AWS firewall di dokumentasi Red Hat. OpenShift

1. Buat peran dan kebijakan IAM akun yang diperlukan menggunakan `--mode auto` atau`--mode manual`.

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

     > **Note**
     >
     > Jika token akses offline Anda telah kedaluwarsa, ROSA CLI mengeluarkan pesan kesalahan yang menyatakan bahwa token otorisasi Anda perlu diperbarui. Untuk langkah-langkah untuk memecahkan masalah, lihat. the section called “Memecahkan masalah ROSA CLI token akses offline kedaluwarsa”

2. Buat klaster dengan menjalankan salah satu perintah berikut.

   - AZ Tunggal

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

   - Multi-AZ

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

> **Note**
>
> Untuk membuat klaster yang menggunakan kredensial AWS PrivateLink dengan AWS Security Token Service (AWS STS) berumur pendek, tambahkan `--sts --mode auto` atau `--sts --mode manual` ke akhir perintah. `rosa create cluster`

3. Buat IAM peran klaster operator dengan mengikuti petunjuk interaktif.

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

4. Buat penyedia OpenID Connect (OIDC) yang digunakan klaster operator untuk mengautentikasi.

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

5. Periksa status Anda klaster.

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

> **Note**
>
> Mungkin diperlukan waktu hingga 40 menit bagi klaster `State` lapangan untuk menunjukkan `ready` status. Jika penyediaan gagal atau tidak ditampilkan `ready` setelah 40 menit, lihat. Pemecahan Masalah Untuk menghubungi Dukungan atau dukungan Red Hat untuk bantuan, lihatthe section called “Mendapatkan Dukungan”.

6. Lacak kemajuan klaster pembuatan dengan menonton log OpenShift penginstal.

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

Konfigurasikan AWS PrivateLink penerusan DNS

Cluster yang menggunakan AWS PrivateLink membuat zona yang dihosting publik dan zona host pribadi di Route 53. Catatan dalam zona host Route 53 pribadi hanya dapat diselesaikan dari dalam VPC tempat ia ditugaskan.

Validasi Let's Encrypt DNS-01 memerlukan zona publik sehingga sertifikat yang valid dan dipercaya publik dapat dikeluarkan untuk domain tersebut. Catatan validasi dihapus setelah validasi Let's

Encrypt selesai. Zona ini masih diperlukan untuk menerbitkan dan memperbarui sertifikat ini, yang biasanya diperlukan setiap 60 hari. Meskipun zona ini biasanya tampak kosong, zona publik memainkan peran penting dalam proses validasi.

Untuk informasi selengkapnya tentang zona yang dihosting AWS pribadi, lihat Bekerja dengan zona pribadi. Untuk informasi selengkapnya tentang zona yang dihosting publik, lihat Bekerja dengan zona yang dihosting publik.

Konfigurasikan Route 53 Resolver titik akhir masuk

1. Untuk memungkinkan catatan seperti `api.<cluster_domain>` dan `*.apps.<cluster_domain>` untuk menyelesaikan di luar VPC, konfigurasikan titik akhir Route 53 Resolver masuk.

   > **Note**
   >
   > Saat Anda mengonfigurasi titik akhir masuk, Anda diminta untuk menentukan minimal dua alamat IP untuk redundansi. Kami menyarankan Anda menentukan alamat IP di setidaknya dua Availability Zone. Secara opsional Anda dapat menentukan alamat IP tambahan di Availability Zone tersebut atau lainnya.

2. Saat Anda mengonfigurasi titik akhir masuk, pilih VPC dan subnet pribadi yang digunakan saat Anda membuat cluster.

Konfigurasikan penerusan DNS untuk cluster

Setelah endpoint Route 53 Resolver internal dikaitkan dan operasional, konfigurasikan penerusan DNS sehingga kueri DNS dapat ditangani oleh server yang ditunjuk di jaringan Anda.

1. Konfigurasikan jaringan perusahaan Anda untuk meneruskan kueri DNS ke alamat IP tersebut untuk domain tingkat atas, seperti. `drow-pl-01.htno.p1.openshiftapps.com`
2. Jika Anda meneruskan kueri DNS dari satu VPC ke VPC lain, ikuti petunjuk di Mengelola aturan penerusan.
3. Jika Anda mengonfigurasi server DNS jaringan jarak jauh, lihat dokumentasi server DNS spesifik Anda untuk mengonfigurasi penerusan DNS selektif untuk domain cluster yang diinstal.

Konfigurasikan penyedia identitas dan berikan klaster akses

ROSA termasuk OAuth server bawaan. Setelah ROSA klaster dibuat, Anda harus mengonfigurasi OAuth untuk menggunakan penyedia identitas. Anda kemudian dapat menambahkan pengguna ke penyedia identitas yang dikonfigurasi untuk memberi mereka akses ke layanan Anda klaster. Anda dapat memberikan pengguna `cluster-admin` atau `dedicated-admin` izin ini sesuai kebutuhan.

Anda dapat mengonfigurasi berbagai jenis penyedia identitas untuk Anda klaster. Jenis yang didukung termasuk GitHub, GitHub Enterprise,, Google GitLab, LDAP, OpenID Connect HTPasswd , dan penyedia identitas.

> **Important**
>
> Penyedia HTPasswd identitas disertakan hanya untuk memungkinkan satu pengguna administrator statis dibuat. HTPasswd tidak didukung sebagai penyedia identitas penggunaan umum untuk. ROSA

Prosedur berikut mengkonfigurasi penyedia GitHub identitas sebagai contoh. Untuk petunjuk tentang cara mengonfigurasi setiap jenis penyedia identitas yang didukung, lihat Mengonfigurasi penyedia identitas untuk AWS STS.

1. Arahkan ke github.com dan masuk ke akun Anda. GitHub
2. Jika Anda tidak memiliki GitHub organisasi untuk digunakan untuk penyediaan identitas untuk Anda ROSA klaster, buat satu. Untuk informasi selengkapnya, lihat langkah-langkah dalam GitHub dokumentasi.
3. Menggunakan mode interaktif ROSA CLI, konfigurasikan penyedia identitas untuk cluster Anda dengan menjalankan perintah berikut.

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

4. Ikuti petunjuk konfigurasi di output untuk membatasi klaster akses ke anggota organisasi Anda 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. Buka URL di output, ganti <GITHUB_ORG_NAME> dengan nama GitHub organisasi Anda.
6. Di halaman GitHub web, pilih Daftarkan aplikasi untuk mendaftarkan OAuth aplikasi baru di GitHub organisasi Anda.
7. Gunakan informasi dari GitHub OAuth halaman untuk mengisi permintaan `rosa create idp` interaktif yang tersisa, mengganti <GITHUB_CLIENT_ID> dan <GITHUB_CLIENT_SECRET> dengan kredensi dari aplikasi Anda. GitHub OAuth

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

> **Note**
>
> Mungkin diperlukan waktu sekitar dua menit agar konfigurasi penyedia identitas menjadi aktif. Jika Anda mengonfigurasi `cluster-admin` pengguna, Anda dapat menjalankan `oc get pods -n openshift-authentication --watch` perintah untuk melihat OAuth pod di-deploy ulang dengan konfigurasi yang diperbarui.

8. Verifikasi penyedia identitas telah dikonfigurasi dengan benar.

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

Memberikan akses pengguna ke klaster

Anda dapat memberikan akses pengguna ke Anda klaster dengan menambahkannya ke penyedia identitas yang dikonfigurasi.

Prosedur berikut menambahkan pengguna ke GitHub organisasi yang dikonfigurasi untuk penyediaan identitas ke cluster.

1. Arahkan ke github.com dan masuk ke akun Anda. GitHub
2. Undang pengguna yang memerlukan klaster akses ke GitHub organisasi Anda. Untuk informasi selengkapnya, lihat Mengundang pengguna untuk bergabung dengan organisasi Anda dalam GitHub dokumentasi.

Konfigurasikan **`cluster-admin`** izin

1. Berikan `cluster-admin` izin menggunakan perintah berikut. Ganti `<IDP_USER_NAME>` dan `<CLUSTER_NAME>` dengan nama pengguna dan cluster Anda.

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

2. Verifikasi bahwa pengguna terdaftar sebagai anggota `cluster-admins` grup.

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

Konfigurasikan **`dedicated-admin`** izin

1. Berikan `dedicated-admin` izin dengan perintah berikut. Ganti `<IDP_USER_NAME>` dan `<CLUSTER_NAME>` dengan pengguna dan klaster nama Anda.

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

2. Verifikasi bahwa pengguna terdaftar sebagai anggota `cluster-admins` grup.

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

Akses klaster melalui Red Hat Hybrid Cloud Console

Setelah membuat pengguna klaster administrator atau menambahkan pengguna ke penyedia identitas yang dikonfigurasi, Anda dapat masuk klaster melalui Red Hat Hybrid Cloud Console.

1. Dapatkan URL konsol untuk Anda klaster menggunakan perintah berikut. Ganti `<CLUSTER_NAME>` dengan nama Anda klaster.

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

2. Arahkan ke URL konsol di output dan masuk.
   - Jika Anda membuat `cluster-admin` pengguna, masuk menggunakan kredensi yang disediakan.
   - Jika Anda mengonfigurasi penyedia identitas untuk Anda klaster, pilih nama penyedia identitas di dialog Masuk dengan... dan lengkapi permintaan otorisasi apa pun yang disajikan oleh penyedia Anda.

Menyebarkan aplikasi dari Katalog Pengembang

Dari Red Hat Hybrid Cloud Console, Anda dapat menerapkan aplikasi pengujian Katalog Pengembang dan mengeksposnya dengan rute.

1. Arahkan ke Red Hat Hybrid Cloud Console dan pilih cluster tempat Anda ingin menerapkan aplikasi.
2. Pada halaman cluster, pilih Open console.
3. Dalam perspektif Administrator, pilih Home > Projects > Create Project.
4. Masukkan nama untuk proyek Anda dan secara opsional tambahkan Nama Tampilan dan Deskripsi.
5. Pilih Buat untuk membuat proyek.
6. Beralih ke perspektif Pengembang dan pilih +Tambah. Pastikan bahwa proyek yang dipilih adalah yang baru saja dibuat.
7. Dalam dialog Katalog Pengembang, pilih Semua layanan.

8. Di halaman Katalog Pengembang, pilih Bahasa > JavaScriptdari menu.
9. Pilih Node.js, lalu pilih Create Application untuk membuka halaman Create Source-to-Image Application.

> **Note**
>
> Anda mungkin perlu memilih Hapus Semua Filter untuk menampilkan opsi Node.js.

10. Di bagian Git, pilih Coba Sampel.
11. Di bidang Nama, tambahkan nama unik.
12. Pilih Buat.

> **Note**
>
> Aplikasi baru membutuhkan waktu beberapa menit untuk digunakan.

13. Saat penerapan selesai, pilih URL rute untuk aplikasi.

    Tab baru di browser terbuka dengan pesan yang mirip dengan berikut ini.

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

14. (Opsional) Hapus aplikasi dan bersihkan sumber daya.
    a. Dalam perspektif Administrator, pilih Home > Projects.
    b. Buka menu tindakan untuk proyek Anda dan pilih Hapus Proyek.

Mencabut **`cluster-admin`** izin dari pengguna

1. Cabut `cluster-admin` izin menggunakan perintah berikut. Ganti `<IDP_USER_NAME>` dan `<CLUSTER_NAME>` dengan pengguna dan klaster nama Anda.

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

2. Verifikasi bahwa pengguna tidak terdaftar sebagai anggota `cluster-admins` grup.

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

Mencabut **dedicated-admin** izin dari pengguna

1. Cabut `dedicated-admin` izin menggunakan perintah berikut. Ganti `<IDP_USER_NAME>` dan `<CLUSTER_NAME>` dengan pengguna dan klaster nama Anda.

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

2. Verifikasi bahwa pengguna tidak terdaftar sebagai anggota `dedicated-admins` grup.

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

Mencabut akses pengguna ke klaster

Anda dapat mencabut klaster akses untuk pengguna penyedia identitas dengan menghapusnya dari penyedia identitas yang dikonfigurasi.

Anda dapat mengonfigurasi berbagai jenis penyedia identitas untuk Anda klaster. Prosedur berikut mencabut klaster akses untuk anggota GitHub organisasi.

1. Arahkan ke github.com dan masuk ke akun Anda. GitHub
2. Hapus pengguna dari GitHub organisasi Anda. Untuk informasi selengkapnya, lihat Menghapus anggota dari organisasi Anda di GitHub dokumentasi.

Hapus cluster dan AWS STS sumber daya

Anda dapat menggunakan ROSA CLI untuk menghapus klaster yang menggunakan AWS Security Token Service ()AWS STS. Anda juga dapat menggunakan ROSA CLI untuk menghapus IAM peran dan penyedia OIDC yang dibuat oleh. ROSA Untuk menghapus IAM kebijakan yang dibuat oleh ROSA, Anda dapat menggunakan IAM konsol.

> **Important**
>
> IAM peran dan kebijakan yang dibuat oleh ROSA mungkin digunakan oleh ROSA cluster lain di akun yang sama.

1. Hapus klaster dan perhatikan log. Ganti `<CLUSTER_NAME>` dengan nama atau ID Anda klaster.

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

> **Important**
>
> Anda harus menunggu penghapusan sepenuhnya sebelum menghapus IAM peran, kebijakan, dan penyedia OIDC. klaster Peran IAM akun diperlukan untuk menghapus sumber daya yang dibuat oleh penginstal. Peran IAM operator diperlukan untuk membersihkan sumber daya yang dibuat oleh OpenShift operator. Operator menggunakan penyedia OIDC untuk mengautentikasi.

2. Hapus penyedia OIDC yang digunakan klaster operator untuk mengautentikasi dengan menjalankan perintah berikut.

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

3. Hapus peran operator khusus cluster. IAM

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

4. Hapus peran IAM akun menggunakan perintah berikut. Ganti <PREFIX> dengan awalan peran IAM akun yang akan dihapus. Jika Anda menetapkan awalan kustom saat membuat peran IAM akun, tentukan awalan default`ManagedOpenShift`.

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

5. Hapus IAM kebijakan yang dibuat oleh ROSA.
   a. Masuk ke IAM konsol.
   b. Di menu sebelah kiri di bawah Manajemen akses, pilih Kebijakan.
   c. Pilih kebijakan yang ingin Anda hapus dan pilih Tindakan > Hapus.
   d. Masukkan nama kebijakan dan pilih Hapus.
   e. Ulangi langkah ini untuk menghapus setiap kebijakan IAM untuk. klaster

Keamanan di ROSA

Keamanan cloud di AWS merupakan prioritas tertinggi. Sebagai AWS pelanggan, Anda mendapatkan keuntungan dari pusat data dan arsitektur jaringan yang dibangun untuk memenuhi persyaratan organisasi yang paling sensitif terhadap keamanan.

Keamanan adalah tanggung jawab bersama antara AWS dan Anda. Model tanggung jawab bersama menggambarkan hal ini sebagai keamanan cloud dan keamanan di dalam cloud:

- Keamanan cloud — AWS bertanggung jawab untuk melindungi infrastruktur yang menjalankan AWS layanan di AWS Cloud. AWS juga menyediakan layanan yang bisa Anda gunakan dengan aman. Auditor pihak ketiga secara teratur menguji dan memverifikasi keefektifan keamanan kami sebagai bagian dari program kepatuhan AWS. Untuk mempelajari program kepatuhan yang berlaku Layanan AWS di ROSA, lihat Cakupan Menurut Program Kepatuhan.
- Keamanan dalam cloud — Tanggung jawab Anda ditentukan menurut apa Layanan AWS yang Anda gunakan. Anda juga bertanggung jawab atas faktor lain, yang mencakup sensitivitas data Anda, persyaratan perusahaan Anda, serta undang-undang dan peraturan yang berlaku.

Dokumentasi ini akan membantu Anda memahami cara menerapkan model tanggung jawab bersama saat menggunakan ROSA. Topik berikut menunjukkan cara mengonfigurasi ROSA untuk memenuhi tujuan keamanan dan kepatuhan Anda. Anda juga mempelajari cara menggunakan Layanan AWS yang membantu Anda memantau dan mengamankan ROSA sumber daya Anda.

Daftar Isi

Perlindungan data di ROSA

the section called “Tanggung Jawab”Dokumentasi dan model tanggung jawab AWS bersama menentukan perlindungan data di ROSA. AWS bertanggung jawab untuk melindungi infrastruktur global yang menjalankan semua AWS Cloud. Red Hat bertanggung jawab untuk melindungi infrastruktur cluster dan platform layanan yang mendasarinya. Pelanggan bertanggung jawab

untuk menjaga kendali terhadap konten yang di-hosting pada infrastruktur ini. Konten ini mencakup konfigurasi keamanan dan tugas manajemen untuk berbagai layanan Layanan AWS yang Anda gunakan. Untuk informasi selengkapnya tentang privasi data, silakan lihat Pertanyaan Umum Privasi Data. Untuk informasi tentang perlindungan data di Eropa, lihat postingan blog Model Tanggung Jawab AWS Bersama dan Peraturan Perlindungan Data Umum (GDPR) di Blog AWS Keamanan.

Untuk tujuan perlindungan data, kami merekomendasikan agar Anda melindungi Akun AWS kredenal dan menyiapkan pengguna individu dengan AWS Identity and Access Management ()IAM. Dengan cara itu, setiap pengguna hanya diberi izin yang diperlukan untuk memenuhi tanggung jawab tugasnya. Kami juga menyarankan supaya Anda mengamankan data dengan cara-cara berikut:

- Gunakan autentikasi multi-faktor (MFA) pada setiap akun.
- Gunakan SSL/TLS untuk berkomunikasi dengan sumber daya. AWS Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Atur API dan pencatatan aktivitas pengguna dengan AWS CloudTrail.
- Gunakan solusi AWS enkripsi, bersama semua kontrol keamanan default di dalamnya Layanan AWS.
- Gunakan layanan keamanan terkelola lanjutan seperti Amazon Macie, yang membantu menemukan dan mengamankan data sensitif yang disimpan di. Amazon S3
- Jika Anda memerlukan modul kriptografi yang divalidasi FIPS 140-2 ketika mengakses AWS melalui antarmuka baris perintah atau API, gunakan titik akhir FIPS. Untuk informasi lebih lanjut tentang titik akhir FIPS yang tersedia, lihat Standar Pemrosesan Informasi Federal (FIPS) 140-2.

Kami sangat merekomendasikan agar Anda tidak memasukkan informasi identifikasi sensitif apapun, seperti nomor rekening pelanggan Anda, ke dalam kolom isian teks bebas seperti kolom Nama. Ini termasuk saat Anda bekerja dengan ROSA atau lainnya Layanan AWS menggunakan konsol, API AWS CLI, atau AWS SDKs. Data apa pun yang Anda masukkan ke ROSA atau layanan lain mungkin akan diambil untuk dimasukkan dalam catatan diagnostik. Saat Anda memberikan URL ke server eksternal, jangan menyertakan informasi kredenal di URL untuk memvalidasi permintaan Anda ke server tersebut.

Topik

- Melindungi data dengan menggunakan enkripsi

Melindungi data dengan menggunakan enkripsi

Perlindungan data mengacu pada perlindungan data saat transit (saat melakukan perjalanan ke dan dari ROSA) dan saat diam (sementara data disimpan di dalam disk di pusat AWS data).

Layanan OpenShift Red Hat di AWS menyediakan akses aman ke Amazon Elastic Block Store (Amazon EBS) volume penyimpanan yang dilampirkan ke Amazon EC2 instance untuk ROSA control plane, infrastruktur, dan node pekerja, serta volume persisten Kubernetes untuk penyimpanan persisten. ROSA mengenkripsi data volume saat istirahat dan dalam perjalanan, dan menggunakan AWS Key Management Service (AWS KMS) untuk membantu melindungi data terenkripsi Anda. Layanan ini digunakan Amazon S3 untuk penyimpanan registri gambar kontainer, yang dienkripsi saat istirahat secara default.

> **Important**
>
> Karena ROSA merupakan layanan yang dikelola, AWS dan Red Hat mengelola infrastruktur yang ROSA digunakan. Pelanggan tidak boleh mencoba mematikan Amazon EC2 instance yang ROSA digunakan secara manual dari AWS konsol atau CLI. Tindakan ini dapat menyebabkan hilangnya data pelanggan.

Enkripsi data untuk Amazon EBS volume penyimpanan yang didukung

Layanan OpenShift Red Hat di AWS menggunakan kerangka kerja persisten volume (PV) Kubernetes untuk memungkinkan administrator klaster menyediakan penyimpanan persisten pada klaster. Volume persisten, serta bidang kontrol, infrastruktur, dan node pekerja, didukung oleh Amazon Elastic Block Store (Amazon EBS) volume penyimpanan yang dilampirkan ke Amazon EC2 instance.

Untuk ROSA volume dan node yang didukung oleh Amazon EBS, operasi enkripsi terjadi di server yang menghosting EC2 instans, memastikan keamanan data saat diam dan data dalam transit antara instans dan penyimpanan yang terpasang. Untuk informasi selengkapnya, lihat Amazon EBS enkripsi di Panduan Amazon EC2 Pengguna.

Enkripsi data untuk driver Amazon EBS CSI dan driver Amazon EFS CSI

ROSA default menggunakan driver Amazon EBS CSI untuk menyediakan penyimpanan. Amazon EBS Driver Amazon EBS CSI dan Operator Driver Amazon EBS CSI diinstal pada cluster secara

default di namespace. `openshift-cluster-csi-drivers` Driver dan operator Amazon EBS CSI memungkinkan Anda menyediakan volume persisten secara dinamis dan membuat snapshot volume.

ROSA juga mampu menyediakan volume persisten menggunakan driver CSI dan Operator Driver Amazon EFS Amazon EFS CSI. Amazon EFS Driver dan operator juga memungkinkan Anda untuk berbagi data sistem file antar pod atau dengan aplikasi lain di dalam atau di luar Kubernetes.

Data volume diamankan dalam perjalanan untuk driver Amazon EBS CSI dan driver Amazon EFS CSI. Untuk informasi selengkapnya, lihat Menggunakan Container Storage Interface (CSI) di dokumentasi Red Hat.

> **Important**
>
> Saat menyediakan volume ROSA persisten secara dinamis menggunakan driver Amazon EFS CSI, Amazon EFS pertimbangkan ID pengguna, ID grup (GID), dan grup IDs sekunder titik akses saat mengevaluasi izin sistem file. Amazon EFS menggantikan pengguna dan grup IDs pada file dengan pengguna dan grup IDs pada titik akses dan mengabaikan klien NFS. IDs Akibatnya, Amazon EFS diam-diam mengabaikan pengaturan. `fsGroup` ROSA tidak dapat mengganti file dengan menggunakan`fsGroup`. GIDs Pod apa pun yang dapat mengakses titik Amazon EFS akses yang terpasang dapat mengakses file apa pun pada volume. Untuk informasi selengkapnya, lihat Bekerja dengan titik Amazon EFS akses di Panduan Amazon EFS Pengguna.

enkripsi etcd

ROSA menyediakan opsi untuk mengaktifkan enkripsi nilai-nilai `etcd` kunci dalam `etcd` volume selama pembuatan cluster, menambahkan lapisan enkripsi tambahan. Setelah `etcd` dienkripsi, Anda akan dikenakan sekitar 20% overhead kinerja tambahan. Kami merekomendasikan agar Anda mengaktifkan `etcd` enkripsi hanya jika Anda secara khusus memerlukannya untuk kasus penggunaan Anda. Untuk informasi selengkapnya, lihat enkripsi etcd dalam definisi ROSA layanan.

Manajemen kunci

ROSA digunakan KMS keys untuk mengelola bidang kontrol, infrastruktur, dan volume data pekerja dengan aman dan volume persisten untuk aplikasi pelanggan. Selama pembuatan klaster, Anda memiliki pilihan untuk menggunakan default yang AWS dikelola oleh KMS key Amazon EBS, atau menentukan kunci terkelola pelanggan Anda sendiri. Untuk informasi selengkapnya, lihat the section called “Manajemen kunci”.

Enkripsi data untuk registri gambar bawaan

ROSA menyediakan registri gambar kontainer bawaan untuk menyimpan, mengambil, dan berbagi gambar kontainer melalui penyimpanan Amazon S3 ember. Registri dikonfigurasi dan dikelola oleh OpenShift Image Registry Operator. Ini memberikan out-of-the-box solusi bagi pengguna untuk mengelola gambar yang menjalankan beban kerja mereka, dan berjalan di atas infrastruktur cluster yang ada. Untuk informasi selengkapnya, lihat Registri di dokumentasi Red Hat.

ROSA menawarkan pendaftar gambar publik dan pribadi. Untuk aplikasi perusahaan, sebaiknya gunakan registri pribadi untuk melindungi gambar Anda agar tidak digunakan oleh pengguna yang tidak sah. Untuk melindungi data registri Anda saat istirahat, ROSA gunakan enkripsi sisi-server secara default dengan kunci Amazon S3 terkelola (SSE-S3). Pengategorian ini tidak memerlukan tindakan apa pun dari bagian Anda, dan ditawarkan tanpa biaya tambahan. Untuk informasi selengkapnya, lihat Melindungi Data Menggunakan Enkripsi Sisi Server dengan Kunci Enkripsi Amazon S3 Terkelola (SSE-S3) di Panduan Pengguna. Amazon S3

ROSA menggunakan protokol Transport Layer Security (TLS) untuk mengamankan data dalam transit ke dan dari registri gambar. Untuk informasi selengkapnya, lihat Registri di dokumentasi Red Hat.

Privasi lalu lintas antarjaringan

Layanan OpenShift Red Hat di AWS menggunakan Amazon Virtual Private Cloud (Amazon VPC) untuk membuat batasan antara sumber daya di ROSA klaster Anda dan mengontrol lalu lintas antara mereka, jaringan on-premise Anda, dan internet. Untuk informasi selengkapnya tentang Amazon VPC keamanan, lihat Privasi lalu lintas Internetwork Amazon VPC di Amazon VPC Panduan Pengguna.

Di dalam VPC, Anda dapat mengonfigurasi ROSA cluster Anda untuk menggunakan server proxy HTTP atau HTTPS untuk menolak akses internet langsung. Jika Anda adalah administrator klaster, Anda juga dapat menentukan kebijakan jaringan di tingkat pod yang membatasi lalu lintas internetwork ke pod di klaster Anda. ROSA Untuk informasi selengkapnya, lihat the section called “Keamanan infrastruktur”.

Enkripsi data menggunakan KMS

ROSA digunakan AWS KMS untuk mengelola kunci dengan aman untuk data terenkripsi. Bidang kontrol, infrastruktur, dan volume node pekerja dienkripsi secara default menggunakan AWS managed yang KMS key disediakan oleh. Amazon EBS Ini KMS key memiliki alias`aws/ebs`. Volume persisten yang menggunakan kelas penyimpanan gp3 default juga dienkripsi secara default menggunakan ini. KMS key

ROSA Cluster yang baru dibuat dikonfigurasi untuk menggunakan kelas penyimpanan gp3 default untuk mengenkripsi volume persisten. Volume persisten yang dibuat dengan menggunakan kelas penyimpanan lain hanya dienkripsi jika kelas penyimpanan dikonfigurasi untuk dienkripsi. Untuk informasi selengkapnya tentang kelas penyimpanan ROSA bawaan, lihat Mengonfigurasi penyimpanan persisten dalam dokumentasi Red Hat.

Selama pembuatan klaster, Anda dapat memilih untuk mengenkripsi volume persisten di klaster menggunakan kunci Amazon EBS-provided default, atau menentukan simetris yang dikelola pelanggan Anda sendiri. KMS key Untuk informasi selengkapnya tentang pembuatan kunci, lihat Membuat Kunci KMS enkripsi simetris di Panduan AWS KMS Developer.

Anda juga dapat mengenkripsi volume persisten untuk kontainer individual dalam klaster dengan mendefinisikan file. KMS key Pengategorian ini berguna saat Anda memiliki kepatuhan eksplisit dan pedoman keamanan saat menerapkan ke. AWS Untuk informasi selengkapnya, lihat Mengenkripsi volume persisten kontainer AWS dengan dokumentasi KMS key dalam Red Hat.

Poin-poin berikut harus dipertimbangkan saat mengenkripsi volume persisten menggunakan volume Anda sendiri: KMS keys

- Saat Anda menggunakan enkripsi KMS dengan Anda sendiri KMS key, kunci harus ada sama Wilayah AWS seperti klaster Anda.
- Ada biaya yang terkait dengan pembuatan dan penggunaan Anda sendiri KMS keys. Untuk informasi selengkapnya, lihat harga AWS Key Management Service.

Identity and access management untuk ROSA

AWS Identity and Access Management (IAM) Layanan AWS adalah administrator dalam mengendalikan akses ke AWS sumber daya dengan aman. IAM administrator mengontrol siapa yang dapat terautentikasi (masuk) dan diotorisasi (mendapatkan izin) untuk menggunakan sumber daya. ROSA IAM adalah solusi Layanan AWS yang dapat Anda gunakan tanpa biaya tambahan.

Topik

- Audiens
- Mengautentikasi dengan identitas
- Mengelola akses menggunakan kebijakan
- ROSA Contoh kebijakan berbasis identitas

- AWS kebijakan terkelola untuk ROSA
- Pemecahan masalah ROSA identitas dan akses

Audiens

Cara menggunakan AWS Identity and Access Management (IAM) berbeda-beda, tergantung pada pekerjaan yang Anda lakukan di ROSA.

Pengguna layanan - Jika Anda menggunakan ROSA layanan untuk melakukan tugas Anda, administrator Anda akan memberikan kredenal dan izin yang Anda butuhkan. Saat Anda menggunakan lebih banyak ROSA fitur untuk melakukan pekerjaan, Anda mungkin memerlukan izin tambahan. Memahami cara akses dikelola dapat membantu Anda meminta izin yang tepat dari administrator Anda. Jika Anda tidak dapat mengakses fitur di ROSA, lihatthe section called “Pemecahan Masalah”.

Administrator layanan — Jika Anda bertanggung jawab atas ROSA sumber daya di perusahaan Anda, Anda mungkin memiliki akses penuh ke ROSA. Tugas Anda adalah menentukan ROSA fitur dan sumber daya mana yang dapat diakses pengguna layanan Anda. Anda kemudian harus mengirimkan permintaan ke IAM administrator untuk mengubah izin pengguna layanan Anda. Tinjau informasi di halaman ini untuk memahami konsep dasar IAM.

IAM administrator - Jika Anda adalah IAM administrator, Anda mungkin ingin mempelajari detail tentang kebijakan yang digunakan untuk mengelola akses ke ROSA. Untuk melihat contoh kebijakan ROSA berbasis identitas yang dapat Anda gunakan, lihat. IAMthe section called “ ROSA Contoh kebijakan berbasis identitas”

Mengautentikasi dengan identitas

Autentikasi adalah cara Anda untuk masuk ke AWS menggunakan kredenal identitas Anda. Anda harus terautentikasi (masuk ke AWS) sebagai pengguna Akun AWS root Pengguna IAM, atau dengan mengasumsikan peran IAM .

Anda dapat masuk AWS sebagai identitas federasi dengan menggunakan kredensil yang disediakan melalui sumber identitas. AWS IAM Identity Center (IAM Identity Center) pengguna, autentikasi masuk tunggal perusahaan Anda, dan kredensi Google atau Facebook Anda adalah contoh identitas gabungan. Saat Anda masuk sebagai identitas gabungan, administrator Anda sebelumnya menyiapkan federasi identitas menggunakan IAM peran. Ketika Anda mengakses AWS dengan menggunakan federasi, Anda secara tidak langsung mengambil peran.

Bergantung pada jenis pengguna Anda, Anda dapat masuk ke AWS Management Console atau portal AWS akses. Untuk informasi selengkapnya tentang masuk AWS, lihat Cara Akun AWS masuk ke Panduan Pengguna AWS Masuk.

Jika Anda mengakses AWS secara terprogram, AWS sediakan kit pengembangan perangkat lunak (SDK) dan antarmuka baris perintah (CLI) untuk menandatangani permintaan Anda secara kriptografis menggunakan kredensil Anda. Jika Anda tidak menggunakan AWS alat, Anda harus menandatangani permintaan sendiri. Untuk informasi selengkapnya tentang menggunakan metode yang disarankan untuk menandatangani permintaan sendiri, lihat Menandatangani permintaan AWS API di Panduan IAM Pengguna.

Terlepas dari metode autentikasi yang Anda gunakan, Anda mungkin juga diminta untuk menyediakan informasi keamanan tambahan. Misalnya, AWS menyarankan agar Anda menggunakan autentikasi multi-faktor (MFA) untuk meningkatkan keamanan akun Anda. Untuk mempelajari lebih lanjut, lihat Autentikasi multi-faktor di Panduan Pengguna Pusat AWS Identitas IAM (penerus AWS Single Sign-On) dan Menggunakan otentikasi multi-faktor (MFA) di Panduan Pengguna IAM. AWS

Akun AWS Pengguna root

Saat Anda membuat akun Akun AWS, Anda memulai dengan identitas masuk tunggal yang memiliki akses penuh ke semua sumber Layanan AWS daya dalam akun tersebut. Identitas ini disebut pengguna Akun AWS akar dan diakses dengan cara masuk menggunakan alamat email dan kata sandi yang Anda gunakan untuk membuat akun. Kami sangat menyarankan agar Anda tidak menggunakan pengguna root untuk tugas sehari-hari. Lindungi kredenal pengguna root Anda dan gunakan kredenal pengguna root Anda dan gunakan untuk melakukan tugas yang hanya dapat dilakukan oleh pengguna root. Untuk daftar lengkap tugas yang mengharuskan Anda masuk sebagai pengguna root, lihat Tugas yang memerlukan kredenal pengguna root di IAM Panduan Pengguna.

Identitas gabungan

Sebagai praktik terbaik, mewajibkan pengguna manusia, termasuk pengguna yang memerlukan akses administrator, untuk menggunakan federasi dengan penyedia identitas untuk mengakses Layanan AWS dengan menggunakan kredensi sementara.

Identitas federasi adalah pengguna dari direktori pengguna perusahaan Anda, penyedia identitas web, direktori Pusat Identitas AWS Directory Service, atau pengguna mana pun yang mengakses Layanan AWS dengan menggunakan kredensil yang disediakan melalui sumber identitas. Ketika

identitas federasi mengakses Akun AWS, mereka mengambil peran, dan peran memberikan kredensi sementara.

Untuk manajemen akses terpusat, kami sarankan Anda menggunakan AWS IAM Identity Center. Anda dapat membuat pengguna dan grup di Pusat Identitas IAM, atau Anda dapat menghubungkan dan menyinkronkan ke sekumpulan pengguna dan grup di sumber identitas Anda sendiri untuk digunakan di semua aplikasi Akun AWS dan aplikasi Anda. Untuk informasi tentang Pusat Identitas IAM, lihat Apa itu Pusat Identitas IAM? di Panduan Pengguna Pusat AWS Identitas IAM (penerus AWS Single Sign-On).

Pengguna IAM dan kelompok

An Pengguna IAMadalah identitas dalam akun Anda Akun AWS yang memiliki izin khusus untuk satu orang atau aplikasi. Jika memungkinkan, kami sarankan untuk mengandalkan kredensi sementara daripada membuat Pengguna IAM yang memiliki kredensi jangka panjang seperti kata sandi dan kunci akses. Namun, jika Anda memiliki kasus penggunaan khusus yang memerlukan kredensyal jangka panjang Pengguna IAM, kami sarankan Anda memutar kunci akses. Untuk informasi selengkapnya, lihat Merotasi kunci akses secara teratur untuk kasus penggunaan yang memerlukan kredensial jangka panjang dalam Panduan Pengguna IAM.

IAM Grup adalah identitas yang menentukan kumpulan. Pengguna IAM Anda tidak dapat masuk sebagai grup. Anda dapat menggunakan grup untuk menentukan izin bagi beberapa pengguna sekaligus. Grup mempermudah manajemen izin untuk sejumlah besar pengguna sekaligus. Misalnya, Anda dapat memiliki grup yang memiliki nama IAMAdminsdan memberikan izin kepada grup tersebut untuk mengelola sumber daya IAM .

Pengguna berbeda dari peran. Pengguna secara unik terkait dengan satu orang atau aplikasi, tetapi peran dimaksudkan untuk dapat digunakan oleh siapa pun yang membutuhkannya. Pengguna memiliki kredensial jangka panjang permanen, tetapi peran memberikan kredensial sementara. Untuk mempelajari lebih lanjut, lihat Kapan membuat Pengguna IAM (bukan peran) di Panduan Pengguna IAM.

IAM peran

IAM Peran adalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus. Peran ini mirip dengan Pengguna IAM, tetapi tidak terkait dengan orang tertentu. Anda dapat menjalankan IAM peran sementara di AWS Management Console dengan beralih peran. Anda dapat mengambil peran dengan memanggil operasi AWS API AWS CLI atau menggunakan URL kustom. Untuk informasi

selengkapnya tentang metode menggunakan peran, lihat Menggunakan IAM peran dalam Panduan Pengguna IAM.

IAM peran dengan kredensi sementara berguna dalam situasi-situasi berikut:

- Akses pengguna gabungan - Untuk menetapkan izin ke identitas gabungan, Anda membuat peran dan menentukan izin untuk peran tersebut. Ketika identitas terfederasi mengautentikasi, identitas tersebut terhubung dengan peran dan diberi izin yang ditentukan oleh peran. Untuk informasi tentang peran untuk federasi, lihat Membuat peran untuk Penyedia Identitas pihak ketiga dalam Panduan Pengguna IAM. Jika menggunakan Pusat Identitas IAM, Anda harus mengonfigurasi set izin. Untuk mengontrol apa yang dapat diakses identitas Anda setelah diautentikasi, IAM Identity Center mengkorelasikan izin yang disetel ke peran. IAM Untuk informasi tentang set izin, lihat Set izin di Panduan Pengguna Pusat Identitas AWS IAM (penerus AWS Single Sign-On).
- Pengguna IAM Izin sementara — Seorang Pengguna IAM dapat mengambil IAM peran sementara untuk mengambil izin yang berbeda untuk tugas tertentu.
- Akses lintas akun — Anda dapat menggunakan IAM peran untuk mengizinkan seseorang (prinsipal terpercaya) di akun yang berbeda untuk mengakses sumber daya di akun Anda. Peran adalah cara utama untuk memberikan akses lintas akun. Namun, pada beberapa hal Layanan AWS, Anda dapat melampirkan kebijakan langsung ke sumber daya (alih-alih menggunakan peran sebagai proksi). Untuk mempelajari perbedaan kebijakan peran dan berbasis sumber daya untuk akses lintas akun, lihat Perbedaan IAM peran dari kebijakan berbasis sumber daya dalam Panduan Pengguna IAM.
- Akses lintas layanan - Beberapa Layanan AWS menggunakan fitur di lainnya Layanan AWS. Misalnya, saat Anda melakukan panggilan di layanan, merupakan hal yang biasa bagi layanan tersebut untuk menjalankan aplikasi di Amazon EC2 atau menyimpan objek di Amazon S3. Layanan mungkin melakukan hal ini dengan menggunakan izin prinsipal yang melakukan panggilan, menggunakan peran layanan, atau menggunakan peran tertaut-layanan.
  - Forward Access session (FAS) — Saat Anda menggunakan peran Pengguna IAM atau untuk melakukan tindakan di AWS, Anda dianggap sebagai prinsipal. Ketika Anda menggunakan beberapa layanan, Anda mungkin melakukan sebuah tindakan yang kemudian menginisiasi tindakan lain di layanan yang berbeda. FAS menggunakan izin dari pemanggilan utama Layanan AWS, dikombinasikan dengan permintaan Layanan AWS untuk membuat permintaan ke layanan hilir. Permintaan FAS hanya dibuat ketika layanan menerima permintaan yang memerlukan interaksi dengan orang lain Layanan AWS atau sumber daya untuk menyelesaikannya. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan ketika mengajukan permintaan FAS, lihat Sesi akses maju.

  - Peran layanan — Peran layanan adalah IAM peran yang dimiliki layanan untuk melakukan tindakan atas nama Anda. IAM Administrator dapat membuat, memodifikasi, dan menghapus peran layanan dari dalam IAM. Untuk informasi selengkapnya, lihat Membuat sebuah peran untuk mendelegasikan izin ke Layanan AWS dalam Panduan pengguna IAM.
  - Peran tertaut-layanan — Peran tertaut-layanan adalah jenis peran layanan yang tertaut dengan. Layanan AWS Layanan tersebut dapat menjalankan peran untuk melakukan tindakan atas nama Anda. Peran terkait layanan muncul di IAM akun Anda dan dimiliki oleh layanan tersebut. IAM Administrator dapat melihat, tetapi tidak dapat mengedit izin untuk peran yang ditautkan dengan layanan.
- Aplikasi yang berjalan Amazon EC2 — Anda dapat menggunakan IAM peran untuk mengelola kredenal sementara untuk aplikasi yang berjalan pada Amazon EC2 instans dan membuat permintaan AWS CLI atau AWS API. Ini lebih disukai daripada menyimpan kunci akses di dalam Amazon EC2 instans. Untuk menetapkan AWS peran ke Amazon EC2 instans dan membuatnya tersedia untuk semua aplikasinya, Anda membuat profil instans yang terlampir ke instans. Profil instans berisi peran dan memungkinkan program yang berjalan di Amazon EC2 contoh untuk mendapatkan kredenal sementara. Untuk informasi selengkapnya, lihat Menggunakan IAM peran untuk memberikan izin ke aplikasi yang berjalan pada Amazon EC2 instance di Panduan Pengguna IAM.

Untuk mempelajari kapan saatnya menggunakan IAM peran atau IAM pengguna, lihat Kapan membuat IAM peran (alih-alih pengguna) di Panduan Pengguna IAM.

Mengelola akses menggunakan kebijakan

Anda mengontrol akses di AWS dengan membuat kebijakan dan melampirkannya ke AWS identitas atau sumber daya. Kebijakan adalah objek di, AWS yang saat terkait dengan sebuah identitas atau sumber daya, mendefinisikan izin yang dimilikinya. AWS mengevaluasi kebijakan ini saat penanggung jawab (pengguna, pengguna root, atau sesi peran) mengajukan permintaan. Izin dalam kebijakan menentukan apakah permintaan diizinkan atau ditolak. Sebagian besar kebijakan disimpan dalam AWS dokumen JSON. Untuk informasi selengkapnya tentang struktur dan isi dokumen kebijakan JSON, lihat Gambaran umum kebijakan JSON dalam Panduan Pengguna IAM.

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke hal apa. Artinya, prinsipal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan kondisi apa.

Secara default, pengguna dan peran tidak memiliki izin. Untuk memberi pengguna izin untuk melakukan tindakan pada sumber daya yang mereka butuhkan, IAM administrator dapat membuat IAM kebijakan. Administrator kemudian dapat menambahkan IAM kebijakan ke peran, dan pengguna dapat mengambil peran.

IAM Kebijakan mendefinisikan izin untuk suatu tindakan terlepas dari metode yang Anda gunakan untuk melakukan operasi. Misalnya, anggaplah Anda memiliki kebijakan yang mengizinkan tindakan `iam:GetRole`. Pengguna dengan kebijakan tersebut dapat memperoleh informasi peran dari AWS Management Console, AWS CLI, atau AWS API.

Kebijakan berbasis identitas

Kebijakan berbasis identitas adalah dokumen kebijakan izin JSON yang dapat diterapkan ke sebuah identitas, seperti peran Pengguna IAM, atau grup. Kebijakan ini mengontrol jenis tindakan yang dapat dilakukan oleh pengguna dan peran, di sumber daya mana, dan berdasarkan kondisi seperti apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat Membuat IAM kebijakan di Panduan Pengguna IAM.

Kebijakan berbasis identitas dapat dikategorikan lebih lanjut sebagai kebijakan inline atau kebijakan yang dikelola. Kebijakan inline disematkan langsung ke satu pengguna, grup, atau peran. Kebijakan terkelola adalah kebijakan mandiri yang dapat diterapkan ke beberapa pengguna, grup, dan peran dalam akun Anda Akun AWS. Kebijakan yang dikelola meliputi kebijakan yang AWS dikelola dan kebijakan yang dikelola pelanggan. Untuk mempelajari cara memilih antara kebijakan yang dikelola atau kebijakan inline, lihat Memilih antara kebijakan yang dikelola dan kebijakan inline dalam Panduan Pengguna IAM.

Kebijakan berbasis sumber daya

Kebijakan berbasis sumber daya adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah kebijakan kepercayaan IAM peran dan kebijakan bucket. Amazon S3 Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Untuk sumber daya tempat kebijakan dilampirkan, kebijakan menentukan tindakan apa yang dapat dilakukan oleh prinsipal tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus menentukan prinsipal dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau. Layanan AWS

Kebijakan berbasis sumber daya merupakan kebijakan inline yang terletak di layanan tersebut. Anda tidak dapat menggunakan kebijakan yang AWS dikelola dari IAM kebijakan berbasis sumber daya.

Daftar kontrol akses (ACLs)

Access control list (ACLs) mengontrol pelaku utama mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACLs serupa dengan kebijakan berbasis sumber daya, meskipun tidak menggunakan format dokumen kebijakan JSON.

Amazon S3, AWS WAF, dan Amazon VPC merupakan contoh layanan yang mendukung ACLs. Untuk mempelajari selengkapnya ACLs, lihat Gambaran umum Daftar Kontrol Akses (ACL) di Panduan Pengguna Amazon Simple Storage Service.

Jenis-jenis kebijakan lain

AWS mendukung jenis kebijakan tambahan yang kurang lazim. Jenis-jenis kebijakan ini dapat mengatur izin maksimum yang diberikan kepada Anda oleh jenis kebijakan yang lebih umum.

- Batas izin - Batas izin adalah fitur lanjutan di mana Anda mengatur izin maksimum yang dapat diberikan oleh kebijakan berbasis identitas ke entitas (atau peran). IAM Pengguna IAM Anda dapat menetapkan batasan izin untuk suatu entitas. Izin yang dihasilkan adalah titik pertemuan antara kebijakan berbasis identitas dan batasan izinnya. Kebijakan berbasis sumber daya yang menentukan pengguna atau peran dalam bidang `Principal` tidak dibatasi oleh batasan izin. Penolakan eksplisit dalam salah satu kebijakan ini akan menggantikan pemberian izin. Untuk informasi selengkapnya tentang batas izin, lihat Batas izin untuk IAM entitas di Panduan Pengguna IAM.
- Kebijakan kontrol layanan (SCPs) - SCPs adalah kebijakan JSON yang menentukan izin maksimum untuk sebuah organisasi atau unit organisasional (OU) di. AWS Organizations AWS Organizations adalah layanan untuk mengelompokkan dan secara terpusat mengelola beberapa Akun AWS bisnis Anda. Jika Anda mengaktifkan semua fitur di suatu organisasi, maka Anda dapat menerapkan kebijakan kontrol layanan (SCPs) ke setiap atau semua akun Anda. SCP membatasi izin untuk entitas dalam akun anggota, termasuk setiap pengguna Akun AWS root. Untuk informasi selengkapnya tentang Organizations dan SCPs, lihat Kebijakan kontrol layanan (SCPs) di Panduan AWS Organizations Pengguna.
- Kebijakan sesi - Kebijakan sesi adalah kebijakan lanjutan yang Anda jalani sebagai parameter saat Anda secara terprogram membuat sesi sementara untuk peran atau pengguna federasi. Izin sesi yang dihasilkan adalah titik pertemuan antara kebijakan berbasis identitas pengguna atau peran dan kebijakan sesi. Izin juga bisa datang dari kebijakan berbasis sumber daya. Penolakan eksplisit dalam salah satu kebijakan ini akan menggantikan pemberian izin. Untuk informasi selengkapnya, lihat Kebijakan sesi dalam Panduan Pengguna IAM.

Berbagai jenis kebijakan

Ketika beberapa jenis kebijakan berlaku pada suatu permintaan, izin yang dihasilkan lebih rumit untuk dipahami. Untuk mempelajari cara AWS menentukan apakah akan mengizinkan permintaan jika beberapa jenis kebijakan dilibatkan, lihat Logika evaluasi kebijakan dalam Panduan Pengguna IAM.

ROSA Contoh kebijakan berbasis identitas

Secara default, Pengguna IAM dan role tidak memiliki izin untuk membuat atau memodifikasi AWS sumber daya. Mereka juga tidak dapat melakukan tugas menggunakan AWS Management Console, AWS CLI, atau AWS API. IAM Administrator harus membuat IAM kebijakan yang memberi izin kepada pengguna dan peran untuk melakukan operasi API tertentu pada sumber daya yang diperlukan. Administrator kemudian harus melampirkan kebijakan tersebut ke Pengguna IAM atau grup yang memerlukan izin tersebut.

Untuk mempelajari cara membuat kebijakan IAM berbasis identitas menggunakan contoh dokumen kebijakan JSON ini, lihat Membuat kebijakan di tab JSON di Panduan Pengguna IAM.

Menggunakan ROSA konsol

Untuk berlangganan ROSA dari konsol, kepala sekolah IAM Anda harus memiliki AWS Marketplace izin yang diperlukan. Izin memungkinkan kepala sekolah untuk berlangganan dan berhenti berlangganan daftar ROSA produk AWS Marketplace dan melihat AWS Marketplace langganan. Untuk menambahkan izin yang diperlukan, buka ROSA konsol dan lampirkan kebijakan AWS terkelola `ROSAManageSubscription` ke kepala IAM Anda. Untuk informasi selengkapnya tentang `ROSAManageSubscription`, lihat the section called “AWS kebijakan terkelola: ROSAManage Berlangganan”.

Otorisasi ROSA dengan HCP untuk mengelola sumber daya AWS

ROSA dengan pesawat kontrol yang dihosting (HCP) menggunakan kebijakan AWS terkelola dengan izin yang diperlukan untuk operasi dan dukungan layanan. Anda menggunakan ROSA CLI atau IAM konsol untuk melampirkan kebijakan ini ke peran layanan di Anda. Akun AWS

Untuk informasi selengkapnya, lihat the section called “ AWS Kebijakan yang dikelola”.

Mengotorisasi ROSA classic untuk mengelola sumber daya AWS

ROSA classic menggunakan kebijakan IAM yang dikelola pelanggan dengan izin yang telah ditentukan sebelumnya oleh layanan. Anda menggunakan ROSA CLI untuk membuat kebijakan ini

dan melampirkannya ke peran layanan di Anda. Akun AWS ROSA mensyaratkan bahwa kebijakan ini dikonfigurasi sebagaimana didefinisikan oleh layanan untuk memastikan operasi berkelanjutan dan dukungan layanan.

> **Note**
>
> Anda tidak boleh mengubah kebijakan klasik ROSA tanpa terlebih dahulu berkonsultasi dengan Red Hat. Melakukan hal itu dapat membatalkan perjanjian tingkat layanan uptime klaster Red Hat 99,95%. ROSA dengan pesawat kontrol yang di-host menggunakan kebijakan AWS terkelola dengan serangkaian izin yang lebih terbatas. Untuk informasi selengkapnya, lihat the section called “ AWS Kebijakan yang dikelola”.

Ada dua jenis kebijakan yang dikelola pelanggan untuk ROSA: kebijakan akun dan kebijakan operator. Kebijakan akun dilampirkan pada IAM peran yang digunakan layanan untuk membangun hubungan kepercayaan dengan Red Hat untuk dukungan insinyur keandalan situs (SRE), pembuatan klaster, dan fungsionalitas komputasi. Kebijakan operator dilampirkan ke IAM peran yang digunakan OpenShift operator untuk operasi klaster yang terkait dengan ingress, storage, image registry, dan node management. Kebijakan akun dibuat satu kali per Akun AWS, sedangkan kebijakan operator dibuat satu kali per klaster.

Untuk informasi selengkapnya, lihat the section called “Kebijakan akun ROSA classic” dan the section called “Kebijakan operator ROSA classic”.

Mengizinkan pengguna melihat izin mereka sendiri

Contoh ini menunjukkan bagaimana Anda dapat membuat kebijakan yang memungkinkan Pengguna IAM untuk melihat kebijakan inline dan kebijakan terkelola yang terlampir pada identitas pengguna mereka. Kebijakan ini mencakup izin untuk menyelesaikan tindakan ini di konsol tersebut atau secara terprogram menggunakan. AWS CLI

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
```

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

Kebijakan akun ROSA classic

Bagian ini memberikan rincian tentang kebijakan akun yang diperlukan untuk ROSA classic. Izin ini diperlukan untuk ROSA classic untuk mengelola AWS sumber daya yang dijalankan cluster dan memungkinkan dukungan insinyur keandalan situs Red Hat untuk cluster. Anda dapat menetapkan awalan khusus untuk nama kebijakan, tetapi kebijakan ini harus diberi nama seperti yang ditentukan pada halaman ini (misalnya,`ManagedOpenShift-Installer-Role-Policy`).

Kebijakan akun khusus untuk versi rilis OpenShift minor dan kompatibel ke belakang. Sebelum membuat atau memutakhirkan klaster, Anda harus memverifikasi bahwa versi kebijakan dan versi klaster sama dengan `rosa list account-roles` menjalankannya. Jika versi kebijakan kurang dari versi klaster, jalankan `rosa upgrade account-roles` untuk memutakhirkan peran dan kebijakan terlampir. Anda dapat menggunakan kebijakan dan peran akun yang sama untuk beberapa cluster dari versi rilis minor yang sama.

[Awalan] -Installer-Role-Policy

Anda dapat melampirkan `[Prefix]-Installer-Role-Policy` ke entitas IAM Anda. Sebelum Anda dapat membuat klaster klasik ROSA, Anda harus terlebih dahulu melampirkan kebijakan ini ke peran IAM. `[Prefix]-Installer-Role` Kebijakan ini memberikan izin yang diperlukan yang memungkinkan ROSA penginstal mengelola AWS sumber daya yang diperlukan untuk pembuatan klaster.

Kebijakan izin

Izin yang ditentukan dalam dokumen kebijakan ini menentukan tindakan mana yang diizinkan atau ditolak.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "autoscaling:DescribeAutoScalingGroups",
                "ec2:AllocateAddress",
                "ec2:AssociateAddress",
                "ec2:AssociateDhcpOptions",
                "ec2:AssociateRouteTable",
                "ec2:AttachInternetGateway",
                "ec2:AttachNetworkInterface",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CopyImage",
                "ec2:CreateDhcpOptions",
                "ec2:CreateInternetGateway",
                "ec2:CreateNatGateway",
                "ec2:CreateNetworkInterface",
                "ec2:CreateRoute",
                "ec2:CreateRouteTable",
                "ec2:CreateSecurityGroup",
                "ec2:CreateSubnet",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:CreateVpc",
                "ec2:CreateVpcEndpoint",
                "ec2:DeleteDhcpOptions",
                "ec2:DeleteInternetGateway",
                "ec2:DeleteNatGateway",
```

```
                "ec2:DeleteNetworkInterface",
                "ec2:DeleteRoute",
                "ec2:DeleteRouteTable",
                "ec2:DeleteSecurityGroup",
                "ec2:DeleteSnapshot",
                "ec2:DeleteSubnet",
                "ec2:DeleteTags",
                "ec2:DeleteVolume",
                "ec2:DeleteVpc",
                "ec2:DeleteVpcEndpoints",
                "ec2:DeregisterImage",
                "ec2:DescribeAccountAttributes",
                "ec2:DescribeAddresses",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeDhcpOptions",
                "ec2:DescribeImages",
                "ec2:DescribeInstanceAttribute",
                "ec2:DescribeInstanceCreditSpecifications",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:DescribeInstanceTypeOfferings",
                "ec2:DescribeInstanceTypes",
                "ec2:DescribeInternetGateways",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeNatGateways",
                "ec2:DescribeNetworkAcls",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribePrefixLists",
                "ec2:DescribeRegions",
                "ec2:DescribeReservedInstancesOfferings",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSecurityGroupRules",
                "ec2:DescribeSubnets",
                "ec2:DescribeTags",
                "ec2:DescribeVolumes",
                "ec2:DescribeVpcAttribute",
                "ec2:DescribeVpcClassicLink",
                "ec2:DescribeVpcClassicLinkDnsSupport",
                "ec2:DescribeVpcEndpoints",
                "ec2:DescribeVpcs",
                "ec2:DetachInternetGateway",
                "ec2:DisassociateRouteTable",
                "ec2:GetConsoleOutput",
```

```
                "ec2:GetEbsDefaultKmsKeyId",
                "ec2:ModifyInstanceAttribute",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:ModifySubnetAttribute",
                "ec2:ModifyVpcAttribute",
                "ec2:ReleaseAddress",
                "ec2:ReplaceRouteTableAssociation",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:RunInstances",
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances",
                "elasticloadbalancing:AddTags",
                "elasticloadbalancing:ApplySecurityGroupsToLoadBalancer",
                "elasticloadbalancing:AttachLoadBalancerToSubnets",
                "elasticloadbalancing:ConfigureHealthCheck",
                "elasticloadbalancing:CreateListener",
                "elasticloadbalancing:CreateLoadBalancer",
                "elasticloadbalancing:CreateLoadBalancerListeners",
                "elasticloadbalancing:CreateTargetGroup",
                "elasticloadbalancing:DeleteLoadBalancer",
                "elasticloadbalancing:DeleteTargetGroup",
                "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
                "elasticloadbalancing:DeregisterTargets",
                "elasticloadbalancing:DescribeAccountLimits",
                "elasticloadbalancing:DescribeInstanceHealth",
                "elasticloadbalancing:DescribeListeners",
                "elasticloadbalancing:DescribeLoadBalancerAttributes",
                "elasticloadbalancing:DescribeLoadBalancers",
                "elasticloadbalancing:DescribeTags",
                "elasticloadbalancing:DescribeTargetGroupAttributes",
                "elasticloadbalancing:DescribeTargetGroups",
                "elasticloadbalancing:DescribeTargetHealth",
                "elasticloadbalancing:ModifyLoadBalancerAttributes",
                "elasticloadbalancing:ModifyTargetGroup",
                "elasticloadbalancing:ModifyTargetGroupAttributes",
                "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
                "elasticloadbalancing:RegisterTargets",
                "elasticloadbalancing:SetLoadBalancerPoliciesOfListener",
                "iam:AddRoleToInstanceProfile",
                "iam:CreateInstanceProfile",
                "iam:DeleteInstanceProfile",
                "iam:GetInstanceProfile",
```

```
                "iam:TagInstanceProfile",
                "iam:GetRole",
                "iam:GetRolePolicy",
                "iam:GetUser",
                "iam:ListAttachedRolePolicies",
                "iam:ListInstanceProfiles",
                "iam:ListInstanceProfilesForRole",
                "iam:ListRolePolicies",
                "iam:ListRoles",
                "iam:ListUserPolicies",
                "iam:ListUsers",
                "iam:RemoveRoleFromInstanceProfile",
                "iam:SimulatePrincipalPolicy",
                "iam:TagRole",
                "iam:UntagRole",
                "route53:ChangeResourceRecordSets",
                "route53:ChangeTagsForResource",
                "route53:CreateHostedZone",
                "route53:DeleteHostedZone",
                "route53:GetAccountLimit",
                "route53:GetChange",
                "route53:GetHostedZone",
                "route53:ListHostedZones",
                "route53:ListHostedZonesByName",
                "route53:ListResourceRecordSets",
                "route53:ListTagsForResource",
                "route53:UpdateHostedZoneComment",
                "s3:CreateBucket",
                "s3:DeleteBucket",
                "s3:DeleteObject",
                "s3:DeleteObjectVersion",
                "s3:GetAccelerateConfiguration",
                "s3:GetBucketAcl",
                "s3:GetBucketCORS",
                "s3:GetBucketLocation",
                "s3:GetBucketLogging",
                "s3:GetBucketObjectLockConfiguration",
                "s3:GetBucketPolicy",
                "s3:GetBucketReplication",
                "s3:GetBucketRequestPayment",
                "s3:GetBucketTagging",
                "s3:GetBucketVersioning",
                "s3:GetBucketWebsite",
                "s3:GetEncryptionConfiguration",
```

```
                "s3:GetLifecycleConfiguration",
                "s3:GetObject",
                "s3:GetObjectAcl",
                "s3:GetObjectTagging",
                "s3:GetObjectVersion",
                "s3:GetReplicationConfiguration",
                "s3:ListBucket",
                "s3:ListBucketVersions",
                "s3:PutBucketAcl",
                "s3:PutBucketTagging",
                "s3:PutBucketVersioning",
                "s3:PutEncryptionConfiguration",
                "s3:PutObject",
                "s3:PutObjectAcl",
                "s3:PutObjectTagging",
                "servicequotas:GetServiceQuota",
                "servicequotas:ListAWSDefaultServiceQuotas",
                "sts:AssumeRole",
                "sts:AssumeRoleWithWebIdentity",
                "sts:GetCallerIdentity",
                "tag:GetResources",
                "tag:UntagResources",
                "ec2:CreateVpcEndpointServiceConfiguration",
                "ec2:DeleteVpcEndpointServiceConfigurations",
                "ec2:DescribeVpcEndpointServiceConfigurations",
                "ec2:DescribeVpcEndpointServicePermissions",
                "ec2:DescribeVpcEndpointServices",
                "ec2:ModifyVpcEndpointServicePermissions",
                "kms:DescribeKey",
                "cloudwatch:GetMetricData"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "secretsmanager:GetSecretValue"
            ],
            "Effect": "Allow",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/red-hat-managed": "true"
                }
```

```
            }
        }
    ]
}
```

[Awalan] - ControlPlane -Peran-Kebijakan

Anda dapat melampirkan `[Prefix]-ControlPlane-Role-Policy` ke entitas IAM Anda. Sebelum Anda dapat membuat klaster klasik ROSA, Anda harus terlebih dahulu melampirkan kebijakan ini ke peran IAM. `[Prefix]-ControlPlane-Role` Kebijakan ini memberikan izin yang diperlukan kepada ROSA classic untuk mengelola Amazon EC2 dan Elastic Load Balancing sumber daya yang menghosting bidang ROSA kontrol, serta membaca. KMS keys

Kebijakan izin

Izin yang ditentukan dalam dokumen kebijakan ini menentukan tindakan mana yang diizinkan atau ditolak.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:AttachVolume",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateSecurityGroup",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DeleteSecurityGroup",
                "ec2:DeleteVolume",
                "ec2:Describe*",
                "ec2:DetachVolume",
                "ec2:ModifyInstanceAttribute",
                "ec2:ModifyVolume",
                "ec2:RevokeSecurityGroupIngress",
                "elasticloadbalancing:AddTags",
                "elasticloadbalancing:AttachLoadBalancerToSubnets",
                "elasticloadbalancing:ApplySecurityGroupsToLoadBalancer",
                "elasticloadbalancing:CreateListener",
                "elasticloadbalancing:CreateLoadBalancer",
                "elasticloadbalancing:CreateLoadBalancerPolicy",
                "elasticloadbalancing:CreateLoadBalancerListeners",
                "elasticloadbalancing:CreateTargetGroup",
```

```
                "elasticloadbalancing:ConfigureHealthCheck",
                "elasticloadbalancing:DeleteListener",
                "elasticloadbalancing:DeleteLoadBalancer",
                "elasticloadbalancing:DeleteLoadBalancerListeners",
                "elasticloadbalancing:DeleteTargetGroup",
                "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
                "elasticloadbalancing:DeregisterTargets",
                "elasticloadbalancing:Describe*",
                "elasticloadbalancing:DetachLoadBalancerFromSubnets",
                "elasticloadbalancing:ModifyListener",
                "elasticloadbalancing:ModifyLoadBalancerAttributes",
                "elasticloadbalancing:ModifyTargetGroup",
                "elasticloadbalancing:ModifyTargetGroupAttributes",
                "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
                "elasticloadbalancing:RegisterTargets",
                "elasticloadbalancing:SetLoadBalancerPoliciesForBackendServer",
                "elasticloadbalancing:SetLoadBalancerPoliciesOfListener",
                "kms:DescribeKey"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

[Awalan] -Pekerja-Peran-Kebijakan

Anda dapat melampirkan `[Prefix]-Worker-Role-Policy` ke entitas IAM Anda. Sebelum Anda dapat membuat klaster klasik ROSA, Anda harus terlebih dahulu melampirkan kebijakan ini ke peran IAM. `[Prefix]-Worker-Role` Kebijakan ini memberikan izin yang diperlukan ke ROSA classic untuk menjelaskan EC2 instance yang berjalan sebagai node pekerja.

Kebijakan izin

Izin yang ditentukan dalam dokumen kebijakan ini menentukan tindakan mana yang diizinkan atau ditolak.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:DescribeInstances",
```

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

[Awalan] -Dukungan-Peran-Kebijakan

Anda dapat melampirkan `[Prefix]-Support-Role-Policy` ke entitas IAM Anda. Sebelum Anda dapat membuat klaster klasik ROSA, Anda harus terlebih dahulu melampirkan kebijakan ini ke peran IAM. `[Prefix]-Support-Role` Kebijakan ini memberikan izin yang diperlukan untuk rekayasa keandalan situs Red Hat untuk mengamati, mendiagnosis, dan mendukung AWS sumber daya yang digunakan klaster klasik ROSA, termasuk kemampuan untuk mengubah status node cluster.

Kebijakan izin

Izin yang ditentukan dalam dokumen kebijakan ini menentukan tindakan mana yang diizinkan atau ditolak.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "cloudtrail:DescribeTrails",
                "cloudtrail:LookupEvents",
                "cloudwatch:GetMetricData",
                "cloudwatch:GetMetricStatistics",
                "cloudwatch:ListMetrics",
                "ec2-instance-connect:SendSerialConsoleSSHPublicKey",
                "ec2:CopySnapshot",
                "ec2:CreateNetworkInsightsPath",
                "ec2:CreateSnapshot",
                "ec2:CreateSnapshots",
                "ec2:CreateTags",
                "ec2:DeleteNetworkInsightsAnalysis",
                "ec2:DeleteNetworkInsightsPath",
                "ec2:DeleteTags",
                "ec2:DescribeAccountAttributes",
                "ec2:DescribeAddresses",
                "ec2:DescribeAddressesAttribute",
```

```
                "ec2:DescribeAggregateIdFormat",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeByoipCidrs",
                "ec2:DescribeCapacityReservations",
                "ec2:DescribeCarrierGateways",
                "ec2:DescribeClassicLinkInstances",
                "ec2:DescribeClientVpnAuthorizationRules",
                "ec2:DescribeClientVpnConnections",
                "ec2:DescribeClientVpnEndpoints",
                "ec2:DescribeClientVpnRoutes",
                "ec2:DescribeClientVpnTargetNetworks",
                "ec2:DescribeCoipPools",
                "ec2:DescribeCustomerGateways",
                "ec2:DescribeDhcpOptions",
                "ec2:DescribeEgressOnlyInternetGateways",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DescribeIdentityIdFormat",
                "ec2:DescribeIdFormat",
                "ec2:DescribeImageAttribute",
                "ec2:DescribeImages",
                "ec2:DescribeInstanceAttribute",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:DescribeInstanceTypeOfferings",
                "ec2:DescribeInstanceTypes",
                "ec2:DescribeInternetGateways",
                "ec2:DescribeIpv6Pools",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeLaunchTemplates",
                "ec2:DescribeLocalGatewayRouteTables",
                "ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations",
                "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
                "ec2:DescribeLocalGateways",
                "ec2:DescribeLocalGatewayVirtualInterfaceGroups",
                "ec2:DescribeLocalGatewayVirtualInterfaces",
                "ec2:DescribeManagedPrefixLists",
                "ec2:DescribeNatGateways",
                "ec2:DescribeNetworkAcls",
                "ec2:DescribeNetworkInsightsAnalyses",
                "ec2:DescribeNetworkInsightsPaths",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribePlacementGroups",
                "ec2:DescribePrefixLists",
                "ec2:DescribePrincipalIdFormat",
```

```
                "ec2:DescribePublicIpv4Pools",
                "ec2:DescribeRegions",
                "ec2:DescribeReservedInstances",
                "ec2:DescribeRouteTables",
                "ec2:DescribeScheduledInstances",
                "ec2:DescribeSecurityGroupReferences",
                "ec2:DescribeSecurityGroupRules",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSnapshotAttribute",
                "ec2:DescribeSnapshots",
                "ec2:DescribeSpotFleetInstances",
                "ec2:DescribeStaleSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeTags",
                "ec2:DescribeTransitGatewayAttachments",
                "ec2:DescribeTransitGatewayConnectPeers",
                "ec2:DescribeTransitGatewayConnects",
                "ec2:DescribeTransitGatewayMulticastDomains",
                "ec2:DescribeTransitGatewayPeeringAttachments",
                "ec2:DescribeTransitGatewayRouteTables",
                "ec2:DescribeTransitGateways",
                "ec2:DescribeTransitGatewayVpcAttachments",
                "ec2:DescribeVolumeAttribute",
                "ec2:DescribeVolumes",
                "ec2:DescribeVolumesModifications",
                "ec2:DescribeVolumeStatus",
                "ec2:DescribeVpcAttribute",
                "ec2:DescribeVpcClassicLink",
                "ec2:DescribeVpcClassicLinkDnsSupport",
                "ec2:DescribeVpcEndpointConnectionNotifications",
                "ec2:DescribeVpcEndpointConnections",
                "ec2:DescribeVpcEndpoints",
                "ec2:DescribeVpcEndpointServiceConfigurations",
                "ec2:DescribeVpcEndpointServicePermissions",
                "ec2:DescribeVpcEndpointServices",
                "ec2:DescribeVpcPeeringConnections",
                "ec2:DescribeVpcs",
                "ec2:DescribeVpnConnections",
                "ec2:DescribeVpnGateways",
                "ec2:GetAssociatedIpv6PoolCidrs",
                "ec2:GetConsoleOutput",
                "ec2:GetManagedPrefixListEntries",
                "ec2:GetSerialConsoleAccessStatus",
                "ec2:GetTransitGatewayAttachmentPropagations",
```

```
                "ec2:GetTransitGatewayMulticastDomainAssociations",
                "ec2:GetTransitGatewayPrefixListReferences",
                "ec2:GetTransitGatewayRouteTableAssociations",
                "ec2:GetTransitGatewayRouteTablePropagations",
                "ec2:ModifyInstanceAttribute",
                "ec2:RebootInstances",
                "ec2:RunInstances",
                "ec2:SearchLocalGatewayRoutes",
                "ec2:SearchTransitGatewayMulticastGroups",
                "ec2:SearchTransitGatewayRoutes",
                "ec2:StartInstances",
                "ec2:StartNetworkInsightsAnalysis",
                "ec2:StopInstances",
                "ec2:TerminateInstances",
                "elasticloadbalancing:ConfigureHealthCheck",
                "elasticloadbalancing:DescribeAccountLimits",
                "elasticloadbalancing:DescribeInstanceHealth",
                "elasticloadbalancing:DescribeListenerCertificates",
                "elasticloadbalancing:DescribeListeners",
                "elasticloadbalancing:DescribeLoadBalancerAttributes",
                "elasticloadbalancing:DescribeLoadBalancerPolicies",
                "elasticloadbalancing:DescribeLoadBalancerPolicyTypes",
                "elasticloadbalancing:DescribeLoadBalancers",
                "elasticloadbalancing:DescribeRules",
                "elasticloadbalancing:DescribeSSLPolicies",
                "elasticloadbalancing:DescribeTags",
                "elasticloadbalancing:DescribeTargetGroupAttributes",
                "elasticloadbalancing:DescribeTargetGroups",
                "elasticloadbalancing:DescribeTargetHealth",
                "iam:GetRole",
                "iam:ListRoles",
                "kms:CreateGrant",
                "route53:GetHostedZone",
                "route53:GetHostedZoneCount",
                "route53:ListHostedZones",
                "route53:ListHostedZonesByName",
                "route53:ListResourceRecordSets",
                "s3:GetBucketTagging",
                "s3:GetObjectAcl",
                "s3:GetObjectTagging",
                "s3:ListAllMyBuckets",
                "sts:DecodeAuthorizationMessage",
                "tiros:CreateQuery",
                "tiros:GetQueryAnswer",
```

```
                "tiros:GetQueryExplanation"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "s3:ListBucket"
            ],
            "Effect": "Allow",
            "Resource": [
                "arn:aws:s3:::managed-velero*",
                "arn:aws:s3:::*image-registry*"
            ]
        }
    ]
}
```

Kebijakan operator ROSA classic

Bagian ini memberikan rincian tentang kebijakan operator yang diperlukan untuk ROSA classic. Sebelum Anda dapat membuat klaster klasik ROSA, Anda harus terlebih dahulu melampirkan kebijakan ini ke peran operator yang relevan. Satu set peran operator yang unik diperlukan untuk setiap cluster.

Izin ini diperlukan untuk memungkinkan OpenShift operator mengelola node cluster klasik ROSA. Anda dapat menetapkan awalan kustom ke nama kebijakan untuk menyederhanakan pengelolaan kebijakan (misalnya,). `ManagedOpenShift-openshift-ingress-operator-cloud-credentials`

[Awalan] - openshift-ingress-operator-cloud -credentials

Anda dapat melampirkan `[Prefix]-openshift-ingress-operator-cloud-credentials` ke entitas IAM Anda. Kebijakan ini memberikan izin yang diperlukan kepada Operator Ingress untuk menyediakan dan mengelola penyeimbang beban dan konfigurasi DNS untuk akses klaster eksternal. Kebijakan ini juga memungkinkan Operator Ingress membaca dan memfilter nilai tag Route 53 sumber daya untuk menemukan zona yang dihosting. Untuk informasi selengkapnya tentang operator, lihat Operator OpenShift Ingress di OpenShift GitHub dokumentasi.

Kebijakan izin

Izin yang ditentukan dalam dokumen kebijakan ini menentukan tindakan mana yang diizinkan atau ditolak.

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

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

Anda dapat melampirkan `[Prefix]-openshift-cluster-csi-drivers-ebs-cloud-credentials` ke entitas IAM Anda. Kebijakan ini memberikan izin yang diperlukan kepada Operator Driver Amazon EBS CSI untuk menginstal dan memelihara driver Amazon EBS CSI pada klaster klasik ROSA. Untuk informasi selengkapnya tentang operator, lihat aws-ebs-csi-driver-operator di OpenShift GitHub dokumentasi.

Kebijakan izin

Izin yang ditentukan dalam dokumen kebijakan ini menentukan tindakan mana yang diizinkan atau ditolak.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:AttachVolume",
                "ec2:CreateSnapshot",
                "ec2:CreateTags",
```

```
                "ec2:CreateVolume",
                "ec2:DeleteSnapshot",
                "ec2:DeleteTags",
                "ec2:DeleteVolume",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeInstances",
                "ec2:DescribeSnapshots",
                "ec2:DescribeTags",
                "ec2:DescribeVolumes",
                "ec2:DescribeVolumesModifications",
                "ec2:DetachVolume",
                "ec2:EnableFastSnapshotRestores",
                "ec2:ModifyVolume"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

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

Anda dapat melampirkan `[Prefix]-openshift-machine-api-aws-cloud-credentials` ke entitas IAM Anda. Kebijakan ini memberikan izin yang diperlukan kepada Operator Machine Config untuk mendeskripsikan, menjalankan, dan menghentikan Amazon EC2 instance yang dikelola sebagai node pekerja. Kebijakan ini juga memberikan izin untuk mengizinkan enkripsi disk dari volume root node pekerja yang digunakan. AWS KMS keys Untuk informasi selengkapnya tentang operator, lihat machine-config-operatordi OpenShift GitHub dokumentasi.

Kebijakan izin

Izin yang ditentukan dalam dokumen kebijakan ini menentukan tindakan mana yang diizinkan atau ditolak.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:CreateTags",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeDhcpOptions",
                "ec2:DescribeImages",
```

```
                "ec2:DescribeInstances",
                "ec2:DescribeInternetGateways",
                "ec2:DescribeInstanceTypes",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeRegions",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:RunInstances",
                "ec2:TerminateInstances",
                "elasticloadbalancing:DescribeLoadBalancers",
                "elasticloadbalancing:DescribeTargetGroups",
                "elasticloadbalancing:DescribeTargetHealth",
                "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
                "elasticloadbalancing:RegisterTargets",
                "elasticloadbalancing:DeregisterTargets",
                "iam:CreateServiceLinkedRole"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "kms:Decrypt",
                "kms:Encrypt",
                "kms:GenerateDataKey",
                "kms:GenerateDataKeyWithoutPlainText",
                "kms:DescribeKey"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "kms:RevokeGrant",
                "kms:CreateGrant",
                "kms:ListGrants"
            ],
            "Effect": "Allow",
            "Resource": "*",
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": true
                }
            }
```

```
        }
    ]
}
```

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

Anda dapat melampirkan `[Prefix]-openshift-cloud-credential-operator-cloud-credentials` ke entitas IAM Anda. Kebijakan ini memberikan izin yang diperlukan kepada Cloud Credential Operator untuk mengambil Pengguna IAM detail, termasuk kunci akses, dokumen kebijakan sebaris yang dilampirkan IDs, tanggal pembuatan pengguna, jalur, ID pengguna, dan Nama Sumber Daya Amazon (ARN). Untuk informasi selengkapnya tentang operator, lihat cloud-credential-operatordi OpenShift GitHub dokumentasi.

Kebijakan izin

Izin yang ditentukan dalam dokumen kebijakan ini menentukan tindakan mana yang diizinkan atau ditolak.

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

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

Anda dapat melampirkan `[Prefix]-openshift-image-registry-installer-cloud-credentials` ke entitas IAM Anda. Kebijakan ini memberikan izin yang diperlukan kepada Operator Registri Gambar untuk menyediakan dan mengelola sumber daya untuk registri gambar dalam klaster ROSA classic dan layanan dependen, termasuk. Amazon S3 Ini diperlukan agar operator dapat menginstal dan memelihara registri internal cluster klasik ROSA. Untuk informasi selengkapnya tentang operator, lihat Image Registry Operator dalam OpenShift GitHub dokumentasi.

Kebijakan izin

Izin yang ditentukan dalam dokumen kebijakan ini menentukan tindakan mana yang diizinkan atau ditolak.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:CreateBucket",
                "s3:DeleteBucket",
                "s3:PutBucketTagging",
                "s3:GetBucketTagging",
                "s3:PutBucketPublicAccessBlock",
                "s3:GetBucketPublicAccessBlock",
                "s3:PutEncryptionConfiguration",
                "s3:GetEncryptionConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:GetLifecycleConfiguration",
                "s3:GetBucketLocation",
                "s3:ListBucket",
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject",
                "s3:ListBucketMultipartUploads",
                "s3:AbortMultipartUpload",
                "s3:ListMultipartUploadParts"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

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

Anda dapat melampirkan `[Prefix]-openshift-cloud-network-config-controller-cloud-cr` ke entitas IAM Anda. Kebijakan ini memberikan izin yang diperlukan kepada Operator Pengontrol Konfigurasi Jaringan Cloud untuk menyediakan dan mengelola sumber daya jaringan untuk digunakan oleh overlay jaringan klaster klasik ROSA. Operator menggunakan izin ini untuk mengelola alamat IP pribadi untuk Amazon EC2 instance sebagai bagian dari cluster klasik ROSA.

Untuk informasi selengkapnya tentang operator, lihat C loud-network-config-controller di OpenShift GitHub dokumentasi.

Kebijakan izin

Izin yang ditentukan dalam dokumen kebijakan ini menentukan tindakan mana yang diizinkan atau ditolak.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:DescribeInstanceTypes",
                "ec2:UnassignPrivateIpAddresses",
                "ec2:AssignPrivateIpAddresses",
                "ec2:UnassignIpv6Addresses",
                "ec2:AssignIpv6Addresses",
                "ec2:DescribeSubnets",
                "ec2:DescribeNetworkInterfaces"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

AWS kebijakan terkelola untuk ROSA

Kebijakan AWS terkelola adalah kebijakan mandiri yang dibuat dan dikelola oleh AWS. AWS Kebijakan terkelola dirancang untuk memberikan izin bagi banyak kasus penggunaan umum sehingga Anda dapat mulai menetapkan izin ke pengguna, grup, dan peran.

Perlu diingat bahwa kebijakan AWS terkelola mungkin tidak memberikan izin hak istimewa paling sedikit untuk kasus penggunaan spesifik Anda karena tersedia untuk digunakan semua pelanggan. AWS Kami menyarankan Anda untuk mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola pelanggan yang khusus untuk kasus penggunaan Anda.

Anda tidak dapat mengubah izin yang ditentukan dalam kebijakan AWS terkelola. Jika AWS memperbarui izin yang ditentukan dalam kebijakan AWS terkelola, pembaruan memengaruhi

semua identitas prinsipal (pengguna, grup, dan peran) yang terkait dengan kebijakan tersebut. AWS kemungkinan besar akan memperbarui kebijakan AWS terkelola saat baru Layanan AWS diluncurkan atau operasi API baru tersedia untuk layanan yang sudah ada. Untuk informasi selengkapnya, lihat kebijakan AWS terkelola di Panduan IAM Pengguna.

AWS kebijakan terkelola: ROSAManage Berlangganan

Anda dapat melampirkan `ROSAManageSubscription` kebijakan ke IAM entitas Anda. Sebelum mengaktifkan ROSA di AWS ROSA konsol, Anda harus terlebih dahulu melampirkan kebijakan ini ke peran konsol.

Kebijakan ini memberikan AWS Marketplace izin yang diperlukan bagi Anda untuk mengelola langganan. ROSA

Detail izin

Kebijakan ini mencakup izin berikut.

- `aws-marketplace:Subscribe`- Memberikan izin untuk berlangganan AWS Marketplace produk untuk ROSA.
- `aws-marketplace:Unsubscribe`- Memungkinkan kepala sekolah untuk menghapus langganan produk. AWS Marketplace
- `aws-marketplace:ViewSubscriptions`- Memungkinkan kepala sekolah untuk melihat langganan dari. AWS Marketplace Pengategorian ini diperlukan agar IAM utama dapat melihat AWS Marketplace langganan yang tersedia.

Untuk melihat dokumen kebijakan JSON lengkap, lihat ROSAManageBerlangganan di Panduan Referensi Kebijakan AWS Terkelola.

ROSA dengan kebijakan akun HCP

Bagian ini memberikan rincian tentang kebijakan akun yang diperlukan untuk ROSA dengan pesawat kontrol yang dihosting (HCP). Kebijakan AWS terkelola ini menambahkan izin yang digunakan oleh ROSA dengan peran IAM HCP. Izin diperlukan untuk dukungan teknis rekayasa keandalan situs Red Hat (SRE), instalasi cluster, dan bidang kontrol dan fungsionalitas komputasi.

> **Note**
>
> AWS kebijakan terkelola dimaksudkan untuk digunakan oleh ROSA dengan pesawat kontrol yang dihosting (HCP). Kluster klasik ROSA menggunakan kebijakan IAM yang dikelola pelanggan. Untuk informasi selengkapnya tentang kebijakan klasik ROSA, lihat the section called “Kebijakan akun ROSA classic” danthe section called “Kebijakan operator ROSA classic”.

AWS kebijakan terkelola: ROSAWorker InstancePolicy

Anda dapat melampirkan `ROSAWorkerInstancePolicy` ke IAM entitas Anda. Sebelum membuat klaster, Anda harus memiliki peran IAM pekerja ROSA dengan kebijakan terlampir ini. Layanan ROSA melakukan panggilan ke orang lain Layanan AWS atas nama Anda. Mereka melakukan ini untuk mengelola sumber daya yang Anda gunakan dengan setiap cluster.

Detail izin

Kebijakan ini mencakup izin berikut yang memungkinkan node pekerja ROSA untuk menyelesaikan tugas berikut:

- `ec2`— Evaluasi Wilayah AWS dan detail Amazon EC2 instance sebagai bagian dari manajemen siklus hidup node pekerja cluster ROSA.
- `ecr`- Evaluasi dan dapatkan gambar dari repositori ECR yang dikelola ROSA yang diperlukan untuk instalasi cluster dan manajemen siklus hidup node pekerja.

Untuk melihat dokumen kebijakan JSON lengkap, lihat ROSAWorkerInstancePolicydi Panduan Referensi Kebijakan AWS Terkelola.

AWS kebijakan terkelola: ROSASRESupport Kebijakan

Anda dapat melampirkan `ROSASRESupportPolicy` ke entitas IAM Anda.

Sebelum membuat ROSA dengan cluster control plane yang dihosting, Anda harus terlebih dahulu melampirkan kebijakan ini ke peran IAM dukungan. Kebijakan ini memberikan izin yang diperlukan kepada teknisi keandalan situs Red Hat (SREs) untuk secara langsung mengamati, mendiagnosis, dan mendukung AWS sumber daya yang terkait dengan ROSA kluster, termasuk kemampuan untuk mengubah status node ROSA cluster.

Detail izin

Kebijakan ini mencakup izin berikut yang memungkinkan Red Hat SREs untuk menyelesaikan tugas-tugas berikut:

- `cloudtrail`— Baca AWS CloudTrail acara dan jejak yang relevan dengan cluster.
- `cloudwatch`— Baca Amazon CloudWatch metrik yang relevan dengan cluster.
- `ec2`Baca, jelaskan, dan tinjau Amazon EC2 komponen yang terkait dengan kesehatan klaster seperti grup keamanan, koneksi titik akhir VPC, dan status volume. Luncurkan, hentikan, reboot, dan akhiri Amazon EC2 instance.
- `elasticloadbalancing`— Baca, jelaskan, dan tinjau Elastic Load Balancing parameter yang terkait dengan kesehatan cluster.
- `iam`— Mengevaluasi IAM peran yang berhubungan dengan kesehatan cluster.
- `route53`— Tinjau pengaturan DNS yang terkait dengan kesehatan cluster.
- `sts`— `DecodeAuthorizationMessage` — Baca IAM pesan untuk tujuan debugging.

Untuk melihat dokumen kebijakan JSON lengkap, lihat ROSASRESupportKebijakan dalam Panduan Referensi Kebijakan AWS Terkelola.

AWS kebijakan terkelola: ROSAInstaller Kebijakan

Anda dapat melampirkan `ROSAInstallerPolicy` ke IAM entitas Anda.

Sebelum membuat ROSA dengan cluster control plane yang dihosting, Anda harus terlebih dahulu melampirkan kebijakan ini ke peran IAM yang diberi nama. `[Prefix]-ROSA-Worker-Role` Kebijakan ini memungkinkan entitas untuk menambahkan peran apa pun yang mengikuti `[Prefix]-ROSA-Worker-Role` pola ke profil instance. Kebijakan ini memberikan izin yang diperlukan kepada penginstal untuk mengelola AWS sumber daya yang mendukung ROSA penginstalan klaster.

Detail izin

Kebijakan ini mencakup izin berikut yang memungkinkan penginstal untuk menyelesaikan tugas berikut:

- `ec2`— Jalankan Amazon EC2 instance menggunakan AMIs host yang Akun AWS dimiliki dan dikelola oleh Red Hat. Jelaskan Amazon EC2 contoh, volume, dan sumber daya jaringan yang terkait dengan Amazon EC2 node. Izin ini diperlukan agar bidang kendali Kubernetes dapat menggabungkan instans ke klaster, dan klaster dapat mengevaluasi keberadaannya di dalamnya.

Amazon VPC Tandai subnet menggunakan pencocokan `"kubernetes.io/cluster/*"` tombol tag. Hal ini diperlukan untuk memastikan bahwa penyeimbang beban yang digunakan untuk masuknya cluster hanya dibuat di subnet yang berlaku.

- `elasticloadbalancing`— Tambahkan penyeimbang beban ke node target pada cluster. Hapus penyeimbang beban dari node target pada cluster. Izin ini diperlukan agar bidang kendali Kubernetes dapat secara dinamis menyediakan penyeimbang beban yang diminta oleh layanan dan layanan aplikasi Kubernetes. OpenShift
- `kms`— Baca AWS KMS kunci, buat dan kelola hibah Amazon EC2, dan kembalikan kunci data simetris unik untuk digunakan di luar. AWS KMS Ini diperlukan untuk penggunaan `etcd` data terenkripsi saat `etcd` enkripsi diaktifkan pada pembuatan cluster.
- `iam`— Memvalidasi peran dan kebijakan IAM. Menyediakan dan mengelola profil Amazon EC2 instans yang relevan dengan cluster secara dinamis. Tambahkan tag ke profil instans IAM dengan menggunakan `iam:TagInstanceProfile` izin. Berikan pesan kesalahan penginstal saat penginstalan klaster gagal karena penyedia OIDC cluster yang ditentukan pelanggan tidak ada.
- `route53`— Mengelola Route 53 sumber daya yang dibutuhkan untuk membuat cluster.
- `servicequotas`— Evaluasi kuota layanan yang diperlukan untuk membuat cluster.
- `sts`— Buat AWS STS kredensi sementara untuk ROSA komponen. Asumsikan kredensyal untuk pembuatan cluster.
- `secretsmanager`— Baca nilai rahasia untuk mengizinkan konfigurasi OIDC yang dikelola pelanggan dengan aman sebagai bagian dari penyediaan klaster.

Untuk melihat dokumen kebijakan JSON lengkap, lihat ROSAInstallerKebijakan dalam Panduan Referensi Kebijakan AWS Terkelola.

ROSA dengan kebijakan operator HCP

Bagian ini memberikan rincian tentang kebijakan operator yang diperlukan untuk ROSA dengan pesawat kontrol yang dihosting (HCP). Anda dapat melampirkan kebijakan AWS terkelola ini ke peran operator yang diperlukan untuk menggunakan ROSA dengan HCP. Izin diperlukan untuk memungkinkan OpenShift operator mengelola ROSA dengan node cluster HCP.

> **Note**
>
> AWS kebijakan terkelola dimaksudkan untuk digunakan oleh ROSA dengan pesawat kontrol yang dihosting (HCP). Kluster klasik ROSA menggunakan kebijakan IAM yang dikelola pelanggan. Untuk informasi selengkapnya tentang kebijakan klasik ROSA, lihat the section

called “Kebijakan akun ROSA classic” danthe section called “Kebijakan operator ROSA classic”.

AWS kebijakan terkelola: ROSAAmazon EBSCSIDriver OperatorPolicy

Anda dapat melampirkan `ROSAAmazonEBSCSIDriverOperatorPolicy` ke IAM entitas Anda. Anda harus melampirkan kebijakan ini ke peran IAM operator untuk mengizinkan ROSA dengan cluster pesawat kontrol yang dihosting untuk melakukan panggilan ke yang lain. Layanan AWS Satu set peran operator yang unik diperlukan untuk setiap cluster.

Kebijakan ini memberikan izin yang diperlukan kepada Operator Driver Amazon EBS CSI untuk menginstal dan memelihara driver Amazon EBS CSI di klaster. ROSA Untuk informasi selengkapnya tentang operator, lihat aws-ebs-csi-driver operator di OpenShift GitHub dokumentasi.

Detail izin

Kebijakan ini mencakup izin berikut yang memungkinkan Operator Amazon EBS Pengemudi untuk menyelesaikan tugas berikut:

- `ec2`— Membuat, memodifikasi, melampirkan, melepaskan, dan menghapus Amazon EBS volume yang dilampirkan ke Amazon EC2 instance. Buat dan hapus snapshot Amazon EBS volume dan daftar Amazon EC2 instans, volume, dan snapshot.

Untuk melihat dokumen kebijakan JSON lengkap, lihat ROSAAmazonEBSCSIDriverOperatorPolicydi Panduan Referensi Kebijakan AWS Terkelola.

AWS kebijakan terkelola: ROSAIngress OperatorPolicy

Anda dapat melampirkan `ROSAIngressOperatorPolicy` ke IAM entitas Anda. Anda harus melampirkan kebijakan ini ke peran IAM operator untuk mengizinkan ROSA dengan cluster pesawat kontrol yang dihosting untuk melakukan panggilan ke yang lain. Layanan AWS Satu set peran operator yang unik diperlukan untuk setiap cluster.

Kebijakan ini memberikan izin yang diperlukan kepada Operator Ingress untuk menyediakan dan mengelola penyeimbang beban dan konfigurasi DNS untuk klaster. ROSA Kebijakan ini memungkinkan akses baca ke nilai tag. Operator kemudian memfilter nilai tag untuk Route 53 sumber daya untuk menemukan zona yang dihosting. Untuk informasi selengkapnya tentang operator, lihat Operator OpenShift Ingress di OpenShift GitHub dokumentasi.

Detail izin

Kebijakan ini mencakup izin berikut yang memungkinkan Operator Ingress untuk menyelesaikan tugas berikut:

- `elasticloadbalancing`— Jelaskan keadaan penyeimbang beban yang disediakan.
- `route53`— Buat daftar zona yang Route 53 dihosting dan edit catatan yang mengelola DNS yang dikendalikan oleh cluster ROSA.
- `tag`— Kelola sumber daya yang ditandai dengan menggunakan `tag:GetResources` izin.

Untuk melihat dokumen kebijakan JSON lengkap, lihat ROSAIngressOperatorPolicydi Panduan Referensi Kebijakan AWS Terkelola.

AWS kebijakan terkelola: ROSAImage RegistryOperatorPolicy

Anda dapat melampirkan `ROSAImageRegistryOperatorPolicy` ke IAM entitas Anda. Anda harus melampirkan kebijakan ini ke peran IAM operator untuk mengizinkan ROSA dengan cluster pesawat kontrol yang dihosting untuk melakukan panggilan ke yang lain. Layanan AWS Satu set peran operator yang unik diperlukan untuk setiap cluster.

Kebijakan ini memberikan izin yang diperlukan kepada Operator Registri Gambar untuk menyediakan dan mengelola sumber daya untuk registri gambar ROSA dalam klaster dan layanan dependen, termasuk S3. Ini diperlukan agar operator dapat menginstal dan memelihara registri internal ROSA cluster. Untuk informasi selengkapnya tentang operator, lihat Image Registry Operator dalam OpenShift GitHub dokumentasi.

Detail izin

Kebijakan ini mencakup izin berikut yang memungkinkan Operator Registri Gambar untuk menyelesaikan tindakan berikut:

- `s3`— Kelola dan evaluasi Amazon S3 bucket sebagai penyimpanan persisten untuk konten gambar kontainer dan metadata cluster.

Untuk melihat dokumen kebijakan JSON lengkap, lihat ROSAImageRegistryOperatorPolicydi Panduan Referensi Kebijakan AWS Terkelola.

AWS kebijakan terkelola: ROSACloud NetworkConfigOperatorPolicy

Anda dapat melampirkan `ROSACloudNetworkConfigOperatorPolicy` ke IAM entitas Anda. Anda harus melampirkan kebijakan ini ke peran IAM operator untuk mengizinkan ROSA dengan cluster pesawat kontrol yang dihosting untuk melakukan panggilan ke yang lain. Layanan AWS Satu set peran operator yang unik diperlukan untuk setiap cluster.

Kebijakan ini memberikan izin yang diperlukan kepada Operator Pengontrol Konfigurasi Jaringan Cloud untuk menyediakan dan mengelola sumber daya jaringan untuk hamparan jaringan klaster. ROSA Operator menggunakan izin ini untuk mengelola alamat IP pribadi untuk Amazon EC2 instance sebagai bagian dari cluster. ROSA Untuk informasi selengkapnya tentang operator, lihat C loud-network-config-controller di OpenShift GitHub dokumentasi.

Detail izin

Kebijakan ini mencakup izin berikut yang memungkinkan Operator Konfigurasi Jaringan Cloud untuk menyelesaikan tugas berikut:

- `ec2`— Baca, tetapkan, dan jelaskan konfigurasi untuk menghubungkan Amazon EC2 instance, Amazon VPC subnet, dan antarmuka jaringan elastis dalam sebuah cluster. ROSA

Untuk melihat dokumen kebijakan JSON lengkap, lihat ROSACloudNetworkConfigOperatorPolicydi Panduan Referensi Kebijakan AWS Terkelola.

AWS kebijakan terkelola: ROSAKube ControllerPolicy

Anda dapat melampirkan `ROSAKubeControllerPolicy` ke IAM entitas Anda. Anda harus melampirkan kebijakan ini ke peran IAM operator untuk mengizinkan ROSA dengan cluster pesawat kontrol yang dihosting untuk melakukan panggilan ke yang lain. Layanan AWS Satu set peran operator yang unik diperlukan untuk setiap cluster.

Kebijakan ini memberikan izin yang diperlukan kepada pengontrol kube untuk mengelola Amazon EC2 Elastic Load Balancing, dan AWS KMS sumber daya untuk ROSA dengan cluster bidang kontrol yang dihosting. Untuk informasi selengkapnya tentang controller ini, lihat arsitektur Controller dalam OpenShift dokumentasi.

Detail izin

Kebijakan ini mencakup izin berikut yang memungkinkan pengontrol kube untuk menyelesaikan tugas-tugas berikut:

- `ec2`— Buat, hapus, dan tambahkan tag ke grup keamanan Amazon EC2 instance. Tambahkan aturan masuk ke kelompok keamanan. Jelaskan Availability Zone, Amazon EC2 instance, tabel rute, grup keamanan VPCs, dan subnet.
- `elasticloadbalancing`— Membuat dan mengelola penyeimbang beban dan kebijakan mereka. Buat dan kelola pendengar penyeimbang beban. Daftarkan target dengan kelompok sasaran dan kelola kelompok sasaran. Daftarkan dan hapus registrasi Amazon EC2 instance dengan penyeimbang beban, dan tambahkan tag ke penyeimbang beban.
- `kms`— Ambil informasi rinci tentang AWS KMS kunci. Ini diperlukan untuk penggunaan `etcd` data terenkripsi saat `etcd` enkripsi diaktifkan pada pembuatan cluster.

Untuk melihat dokumen kebijakan JSON lengkap, lihat ROSAKubeControllerPolicydi Panduan Referensi Kebijakan AWS Terkelola.

AWS kebijakan terkelola: ROSANode PoolManagementPolicy

Anda dapat melampirkan `ROSANodePoolManagementPolicy` ke IAM entitas Anda. Anda harus melampirkan kebijakan ini ke peran IAM operator untuk mengizinkan ROSA dengan cluster pesawat kontrol yang dihosting untuk melakukan panggilan ke layanan lain AWS . Satu set peran operator yang unik diperlukan untuk setiap cluster.

Kebijakan ini memberikan izin yang diperlukan kepada NodePool pengontrol untuk mendeskripsikan, menjalankan, dan menghentikan Amazon EC2 instance yang dikelola sebagai node pekerja. Kebijakan ini juga memberikan izin untuk mengizinkan enkripsi disk volume root node pekerja menggunakan AWS KMS kunci, dan untuk menandai elastic network interface yang dilampirkan ke node worker. Untuk informasi selengkapnya tentang controller ini, lihat arsitektur Controller dalam OpenShift dokumentasi.

Detail izin

Kebijakan ini mencakup izin berikut yang memungkinkan NodePool pengontrol untuk menyelesaikan tugas berikut:

- `ec2`— Jalankan Amazon EC2 instance menggunakan AMIs host yang Akun AWS dimiliki dan dikelola oleh Red Hat. Kelola EC2 siklus hidup di cluster. ROSA Secara dinamis membuat dan mengintegrasikan node pekerja dengan Elastic Load Balancing,, Amazon VPC, Route 53 Amazon EBS, dan Amazon EC2.
- `iam`— Gunakan Elastic Load Balancing melalui peran terkait layanan bernama. `AWSServiceRoleForElasticLoadBalancing` Tetapkan peran ke profil Amazon EC2 contoh.

- `kms`— Baca AWS KMS kunci, buat dan kelola hibah Amazon EC2, dan kembalikan kunci data simetris unik untuk digunakan di luar. AWS KMS Ini diperlukan untuk memungkinkan enkripsi disk volume root node pekerja.

Untuk melihat dokumen kebijakan JSON lengkap, lihat ROSANodePoolManagementPolicydi Panduan Referensi Kebijakan AWS Terkelola.

AWS kebijakan terkelola: ROSAKMSProvider Kebijakan

Anda dapat melampirkan `ROSAKMSProviderPolicy` ke IAM entitas Anda. Anda harus melampirkan kebijakan ini ke peran IAM operator untuk mengizinkan ROSA dengan cluster pesawat kontrol yang dihosting untuk melakukan panggilan ke yang lain. Layanan AWS Satu set peran operator yang unik diperlukan untuk setiap cluster.

Kebijakan ini memberikan izin yang diperlukan kepada Penyedia AWS Enkripsi bawaan untuk mengelola AWS KMS kunci yang mendukung enkripsi `etcd` data. Kebijakan ini memungkinkan Amazon EC2 untuk menggunakan kunci KMS yang disediakan Penyedia AWS Enkripsi untuk mengenkripsi dan `etcd` mendekripsi data. Untuk informasi selengkapnya tentang penyedia ini, lihat Penyedia AWS Enkripsi di dokumentasi Kubernetes GitHub .

Detail izin

Kebijakan ini mencakup izin berikut yang memungkinkan Penyedia AWS Enkripsi untuk menyelesaikan tugas berikut:

- `kms`— Enkripsi, dekripsi, dan ambil kunci. AWS KMS Ini diperlukan untuk penggunaan `etcd` data terenkripsi saat `etcd` enkripsi diaktifkan pada pembuatan cluster.

Untuk melihat dokumen kebijakan JSON lengkap, lihat ROSAKMSProviderKebijakan dalam Panduan Referensi Kebijakan AWS Terkelola.

AWS kebijakan terkelola: ROSAControl PlaneOperatorPolicy

Anda dapat melampirkan `ROSAControlPlaneOperatorPolicy` ke IAM entitas Anda. Anda harus melampirkan kebijakan ini ke peran IAM operator untuk mengizinkan ROSA dengan cluster pesawat kontrol yang dihosting untuk melakukan panggilan ke yang lain. Layanan AWS Satu set peran operator yang unik diperlukan untuk setiap cluster.

Kebijakan ini memberikan izin yang diperlukan kepada Operator Pesawat Kontrol untuk mengelola Amazon EC2 dan Route 53 sumber daya ROSA dengan klaster pesawat kontrol yang dihosting.

Untuk informasi selengkapnya tentang operator ini, lihat Arsitektur pengontrol dalam OpenShift dokumentasi.

Detail izin

Kebijakan ini mencakup izin berikut yang memungkinkan Operator Pesawat Kontrol untuk menyelesaikan tugas berikut:

- `ec2`— Buat dan kelola Amazon VPC titik akhir.
- `route53`— Daftar dan ubah set Route 53 rekaman dan daftar zona yang dihosting.

Untuk melihat dokumen kebijakan JSON lengkap, lihat ROSAControlPlaneOperatorPolicydi Panduan Referensi Kebijakan AWS Terkelola.

ROSA pembaruan kebijakan AWS terkelola

Lihat detail tentang pembaruan ke kebijakan AWS terkelola untuk ROSA karena layanan ini mulai melacak perubahan tersebut. Untuk peringatan otomatis tentang perubahan pada halaman ini, berlangganan ke umpan RSS pada halaman Riwayat dokumen.

Perubahan	Deskripsi	Tanggal
ROSAImageRegistryOperatorPolicy — Kebijakan diperbarui	ROSA memperbarui kebijakan sehingga izin dicakup ke tingkat sumber daya bucket S3. Perubahan ini memenuhi persyaratan penyimpanan ROSA untuk AWS Komersil dan GovCloud Wilayah. Untuk mempelajari selengkapnya, lihat the section called “AWS kebijakan terkelola : ROSAImage RegistryOperatorPolicy”.	19 Mei 2025
ROSANodePoolManagementPolicy — Kebijakan diperbarui	ROSA memperbarui kebijakan untuk memungkinkan penandaan dari antarmuka	5 Mei 2025

Perubahan	Deskripsi	Tanggal
	jaringan elastis yang dilampirkan ke simpul pekerja. Untuk mempelajari selengkapnya, lihat the section called “AWS kebijakan terkelola : ROSANode PoolManagementPolicy”.	
ROSAImageRegistryOperatorPolicy — Kebijakan diperbarui	ROSA memperbarui kebijakan untuk mengizinkan Operator Registri OpenShift Gambar Red Hat menyediakan dan mengelola bucket dan objek Amazon S3 AWS GovCloud di Wilayah untuk digunakan oleh registri gambar dalam cluster ROSA. Perubahan ini memenuhi persyaratan penyimpanan ROSA untuk AWS GovCloud Wilayah. Untuk mempelajari selengkapnya, lihat the section called “AWS kebijakan terkelola : ROSAImage RegistryOperatorPolicy”.	16 April 2025

Perubahan	Deskripsi	Tanggal
ROSAWorkerInstancePolicy — Kebijakan diperbarui	ROSA memperbarui kebijakan untuk memungkinkan node pekerja mengevaluasi dan mendapatkan gambar dari repositori ECR yang dikelola ROSA yang diperlukan untuk instalasi cluster dan manajemen siklus hidup node pekerja. Untuk mempelaja ri selengkapnya, lihat the section called “AWS kebijakan terkelola: ROSAWorker InstancePolicy”.	3 Maret 2025
ROSANodePoolManage mentPolicy — Kebijakan diperbarui	ROSA memperbarui kebijakan untuk mengizinkan antarmuka jaringan elastis diberi tag mirip dengan EC2 instance hanya selama RunInstan ces panggilan ec2: saat permintaan menyertakan tag. `red-hat-managed: true` Izin ini diperlukan untuk mendukung ROSA dengan cluster HCP 4.17. Untuk mempelajari selengkap nya, lihat the section called “AWS kebijakan terkelola : ROSANode PoolManag ementPolicy”.	24 Februari 2025

Perubahan	Deskripsi	Tanggal
ROSAAmazonEBSCSIDriverOperatorPolicy — Kebijakan diperbarui	ROSA memperbarui kebijakan untuk mendukung API otorisasi Amazon EBS snapshot baru. Untuk mempelajari selengkapnya, lihat the section called “AWS kebijakan terkelola: ROSAAmazon EBSCSIDriver OperatorPolicy”.	17 Januari 2025
ROSANodePoolManagementPolicy — Kebijakan diperbarui	ROSA memperbarui kebijakan untuk memungkinkan pengelola kumpulan ROSA node mendeskripsikan kumpulan opsi DHCP untuk menyetel nama DNS pribadi yang tepat. Untuk mempelajari selengkapnya, lihat the section called “AWS kebijakan terkelola: ROSANode PoolManagementPolicy”.	2 Mei 2024
ROSAInstallerKebijakan — Kebijakan diperbarui	ROSA memperbarui kebijakan untuk memungkinkan ROSA penginstal menambahkan tag ke subnet menggunakan pencocokan kunci tag. `"kubernetes.io/cluster/*"` Untuk mempelajari selengkapnya, lihat the section called “AWS kebijakan terkelola: ROSAInstaller Kebijakan”.	24 April 2024

Perubahan	Deskripsi	Tanggal
ROSASRESupportKebijakan — Kebijakan diperbarui	ROSA memperbarui kebijakan untuk memungkinkan peran SRE mengambil informasi tentang profil instans yang telah ditandai oleh as. ROSA `red-hat-managed` Untuk mempelajari selengkap nya, lihat the section called “AWS kebijakan terkelola: ROSASRESupport Kebijakan”.	10 April 2024
ROSAInstallerKebijakan — Kebijakan diperbarui	ROSA memperbarui kebijakan untuk memungkinkan ROSA penginstal memvalidasi kebijakan AWS terkelola yang dilampirkan ke IAM peran ROSA yang digunakan oleh. ROSA Pembaruan ini juga memungkinkan penginstal untuk mengidentifikasi apakah kebijakan yang dikelola pelanggan telah dilampirk an ke ROSA peran. Untuk mempelajari selengkap nya, lihat the section called “AWS kebijakan terkelola: ROSAInstaller Kebijakan”.	10 April 2024

Perubahan	Deskripsi	Tanggal
ROSAInstallerKebijakan — Kebijakan diperbarui	ROSA memperbarui kebijakan untuk mengizinkan layanan menyediakan pesan peringatan penginstal saat penginstalan klaster gagal karena penyedia OIDC cluster yang ditentukan pelanggan tidak ada. Pembaruan ini juga memungkinkan layanan untuk mengambil server nama DNS yang ada sehingga operasi penyediaan klaster idempoten. Untuk mempelajari selengkapnya, lihat the section called “AWS kebijakan terkelola: ROSAInstaller Kebijakan”.	26 Januari 2024
ROSASRESupportKebijakan — Kebijakan diperbarui	ROSA memperbarui kebijakan agar layanan dapat melakukan operasi baca pada grup keamanan yang menggunakan DescribeSecurityGroups API. Untuk mempelajari selengkapnya, lihat the section called “AWS kebijakan terkelola: ROSASRESupport Kebijakan”.	22 Januari 2024

Perubahan	Deskripsi	Tanggal
ROSAImageRegistryOperatorPolicy — Kebijakan diperbarui	ROSA memperbarui kebijakan agar Operator Registri Gambar dapat mengambil tindakan pada Amazon S3 bucket di Wilayah dengan nama 14 karakter. Untuk mempelajari selengkapnya, lihat the section called “AWS kebijakan terkelola: ROSAImage RegistryOperatorPolicy”.	12 Desember 2023
ROSAKubeControllerPolicy — Kebijakan diperbarui	ROSA memperbarui kebijakan untuk memungkinkan menjelaskan Availability Zone, Amazon EC2 instance, tabel rute, grup keamanan VPCs, dan subnet. kube-controller-manager Untuk mempelajari selengkapnya, lihat the section called “AWS kebijakan terkelola: ROSAKube ControllerPolicy”.	16 Oktober 2023
ROSAManageBerlangganan - Kebijakan diperbarui	ROSA memperbarui kebijakan untuk menambahkan ROSA dengan pesawat ProductId kontrol yang dihosting. Untuk mempelajari selengkapnya, lihat the section called “AWS kebijakan terkelola: ROSAManage Berlangganan”.	1 Agustus 2023

Perubahan	Deskripsi	Tanggal
ROSAKubeControllerPolicy — Kebijakan diperbarui	ROSA memperbarui kebijakan untuk memungkinkan pembuatan Network Load Balancers sebagai penyeimbang beban layanan Kubernetes. kube-controller-manager Network Load Balancer memberikan kemampuan yang lebih besar untuk menangani beban kerja yang mudah berubah dan mendukung alamat IP statis untuk penyeimbang beban. Untuk mempelajari selengkapnya, lihat the section called “AWS kebijakan terkelola: ROSAKube ControllerPolicy”.	13 Juli 2023
ROSANodePoolManagementPolicy — Kebijakan baru ditambahkan	ROSA menambahkan kebijakan baru untuk memungkinkan NodePool pengontrol mendeskripsikan, menjalankan, dan menghentikan Amazon EC2 instance yang dikelola sebagai node pekerja. Kebijakan ini juga mengaktifkan enkripsi disk volume root node pekerja menggunakan AWS KMS kunci. Untuk mempelajari selengkapnya, lihat the section called “AWS kebijakan terkelola: ROSANode PoolManagementPolicy”.	8 Juni 2023

Perubahan	Deskripsi	Tanggal
ROSAInstallerKebijakan - Kebijakan baru ditambahkan	ROSA menambahkan kebijakan baru untuk memungkinkan penginstal mengelola AWS sumber daya yang mendukung penginsta lan klaster. Untuk mempelaja ri selengkapnya, lihat the section called “AWS kebijakan terkelola: ROSAInstaller Kebijakan”.	6 Juni 2023
ROSASRESupportKebijakan - Kebijakan baru ditambahkan	ROSA menambahkan kebijakan baru untuk memungkinkan Red Hat SREs secara langsung mengamati, mendiagnosis, dan mendukung AWS sumber daya yang terkait dengan ROSA cluster, termasuk kemampuan untuk mengubah status node ROSA cluster. Untuk mempelajari selengkap nya, lihat the section called “AWS kebijakan terkelola: ROSASRESupport Kebijakan”.	1 Juni 2023

Perubahan	Deskripsi	Tanggal
ROSAKMSProviderKebijakan - Kebijakan baru ditambahkan	ROSA menambahkan kebijakan baru untuk mengizinkan Penyedia AWS Enkripsi bawaan mengelola AWS KMS kunci untuk mendukung enkripsi data etcd. Untuk mempelajari selengkapnya, lihat the section called “AWS kebijakan terkelola: ROSAKMSProvider Kebijakan”.	27 April 2023
ROSAKubeControllerPolicy — Kebijakan baru ditambahkan	ROSA menambahkan kebijakan baru untuk mengizinkan pengontrol kube mengelola Amazon EC2 Elastic Load Balancing, dan AWS KMS sumber daya untuk cluster pesawat kontrol ROSA yang di-host. Untuk mempelajari selengkapnya, lihat the section called “AWS kebijakan terkelola: ROSAKube ControllerPolicy”.	27 April 2023

Perubahan	Deskripsi	Tanggal
ROSAImageRegistryOperatorPolicy — Kebijakan baru ditambahkan	ROSA menambahkan kebijakan baru untuk mengizinkan Operator Registri Gambar menyediakan dan mengelola sumber daya untuk registri gambar ROSA dalam cluster dan layanan dependen, termasuk S3. Untuk mempelajari selengkapnya, lihat the section called “AWS kebijakan terkelola : ROSAImage RegistryOperatorPolicy”.	27 April 2023
ROSAControlPlaneOperatorPolicy — Kebijakan baru ditambahkan	ROSA menambahkan kebijakan baru untuk memungkinkan Operator Pesawat Kontrol mengelola Amazon EC2 dan Route 53 sumber daya ROSA dengan cluster pesawat kontrol yang dihosting. Untuk mempelajari selengkapnya, lihat the section called “AWS kebijakan terkelola: ROSAControl PlaneOperatorPolicy”.	24 April 2023

Perubahan	Deskripsi	Tanggal
ROSACloudNetworkConfigOperatorPolicy — Kebijakan baru ditambahkan	ROSA menambahkan kebijakan baru untuk memungkinkan Operator Pengontrol Konfigurasi Jaringan Cloud menyediakan dan mengelola sumber daya jaringan untuk hamparan jaringan ROSA klaster. Untuk mempelajari selengkapnya, lihat the section called “AWS kebijakan terkelola: ROSACloud NetworkConfigOperatorPolicy”.	20 April 2023
ROSAIngressOperatorPolicy — Kebijakan baru ditambahkan	ROSA menambahkan kebijakan baru untuk memungkinkan Operator Ingress menyediakan dan mengelola penyeimbang beban dan konfigurasi DNS untuk klaster. ROSA Untuk mempelajari selengkapnya, lihat the section called “AWS kebijakan terkelola: ROSAIngress OperatorPolicy”.	20 April 2023

Perubahan	Deskripsi	Tanggal
ROSAAmazonEBSCSIDriverOperatorPolicy — Kebijakan baru ditambahkan	ROSA menambahkan kebijakan baru untuk memungkinkan Operator Driver Amazon EBS CSI menginstal dan memelihara driver Amazon EBS CSI di cluster. ROSA Untuk mempelajari selengkapnya, lihat the section called “AWS kebijakan terkelola: ROSAAmazon EBSCSIDriverOperatorPolicy”.	20 April 2023
ROSAWorkerInstancePolicy — Kebijakan baru ditambahkan	ROSA menambahkan kebijakan baru untuk memungkinkan layanan mengelola sumber daya klaster. Untuk mempelajari selengkapnya, lihat the section called “AWS kebijakan terkelola: ROSAWorkerInstancePolicy”.	20 April 2023
ROSAManageBerlangganan - Kebijakan baru ditambahkan	ROSA menambahkan kebijakan baru untuk memberikan AWS Marketplace izin yang diperlukan untuk mengelola ROSA langganan. Untuk mempelajari selengkapnya, lihat the section called “AWS kebijakan terkelola: ROSAManage Berlangganan”.	11 April 2022

Perubahan	Deskripsi	Tanggal
Layanan OpenShift Red Hat di AWS mulai melacak perubahan	Layanan OpenShift Red Hat di AWS mulai melacak perubahan untuk kebijakan AWS terkelola	2 Maret 2022

Pemecahan masalah ROSA identitas dan akses

Gunakan informasi berikut untuk membantu Anda mendiagnosis dan memperbaiki masalah umum yang mungkin Anda temukan saat bekerja dengan ROSA dan IAM.

AWS Organizations kebijakan kontrol layanan menolak izin yang diperlukan AWS Marketplace

Jika kebijakan kontrol AWS Organizations layanan (SCP) Anda tidak mengizinkan izin AWS Marketplace berlangganan yang diperlukan saat Anda mencoba mengaktifkan ROSA, kesalahan konsol berikut akan terjadi.

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

Jika Anda menerima kesalahan ini, Anda harus menghubungi administrator untuk mendapatkan bantuan. Administrator Anda adalah orang yang mengelola akun untuk organisasi Anda. Mintalah orang tersebut untuk melakukan hal berikut:

1. Konfigurasikan SCP untuk mengizinkan`aws-marketplace:Subscribe`,`aws-marketplace:Unsubscribe`, dan `aws-marketplace:ViewSubscriptions` izin. Untuk informasi selengkapnya, lihat Memperbarui SCP di Panduan AWS Organizations Pengguna.
2. Aktifkan ROSA di akun manajemen organisasi.
3. Bagikan ROSA langganan ke akun anggota yang memerlukan akses dalam organisasi. Untuk informasi selengkapnya, lihat Berbagi langganan di organisasi di Panduan AWS Marketplace Pembeli.

Pengguna atau peran tidak memiliki AWS Marketplace izin yang diperlukan

Jika IAM kepala sekolah Anda tidak memiliki izin AWS Marketplace berlangganan yang diperlukan saat Anda mencoba mengaktifkan ROSA, kesalahan konsol berikut akan terjadi.

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

Untuk mengatasi masalah ini, ikuti langkah-langkah berikut:

1. Buka IAM konsol dan lampirkan kebijakan AWS terkelola `ROSAManageSubscription` ke identitas IAM Anda. Untuk informasi selengkapnya, lihat ROSAManageBerlangganan di Panduan Referensi Kebijakan AWS Terkelola.
2. Ikuti prosedur di the section called “Aktifkan ROSA dan konfigurasikan AWS prasyarat”.

Jika Anda tidak memiliki izin untuk melihat atau memperbarui izin yang ditetapkan IAM atau Anda menerima kesalahan, Anda harus menghubungi administrator untuk mendapatkan bantuan. Minta orang itu `ROSAManageSubscription` untuk melampirkan IAM identitas Anda dan ikuti prosedurnyathe section called “Aktifkan ROSA dan konfigurasikan AWS prasyarat”. Ketika administrator melakukan tindakan ini, ini memungkinkan ROSA dengan memperbarui izin yang ditetapkan untuk semua IAM identitas di bawah Akun AWS.

AWS Marketplace Izin yang diperlukan diblokir oleh administrator

Jika administrator akun Anda memblokir izin AWS Marketplace berlangganan yang diperlukan, kesalahan konsol berikut akan terjadi saat Anda mencoba mengaktifkan ROSA.

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

Jika Anda menerima kesalahan ini, Anda harus menghubungi administrator untuk mendapatkan bantuan. Mintalah orang tersebut untuk melakukan hal berikut:

1. Buka ROSA konsol dan lampirkan kebijakan AWS terkelola `ROSAManageSubscription` ke identitas IAM Anda. Untuk informasi selengkapnya, lihat ROSAManageBerlangganan di Panduan Referensi Kebijakan AWS Terkelola.

2. Ikuti prosedur the section called “Aktifkan ROSA dan konfigurasikan AWS prasyarat” untuk mengaktifkan ROSA. Prosedur ini memungkinkan ROSA dengan memperbarui set izin untuk semua IAM identitas di bawah. Akun AWS

Kesalahan saat membuat penyeimbang beban: AccessDenied

Jika Anda belum membuat penyeimbang beban, peran `AWSServiceRoleForElasticLoadBalacing` terkait layanan mungkin tidak ada di akun Anda. Kesalahan berikut terjadi jika Anda mencoba membuat ROSA klaster tanpa `AWSServiceRoleForElasticLoadBalacing` peran di akun Anda.

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

Untuk mengatasi masalah ini, ikuti langkah-langkah berikut:

1. Periksa apakah akun Anda memiliki `AWSServiceRoleForElasticLoadBalancing` peran.

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

2. Jika Anda tidak memiliki peran ini, ikuti petunjuk untuk membuat peran yang ditemukan di Buat peran terkait layanan di Elastic Load Balancing Panduan Pengguna.

Ketahanan di ROSA

AWS ketahanan infrastruktur global

Infrastruktur AWS global dibangun di sekitar Wilayah AWS dan Availability Zones. Wilayah AWS menyediakan beberapa Availability Zone yang terpisah secara fisik dan terisolasi, yang terhubung melalui jaringan berlatensi rendah, throughput yang tinggi, dan sangat redundan. Dengan Zona Ketersediaan, Anda dapat merancang serta mengoperasikan aplikasi dan basis data yang secara otomatis melakukan fail over di antara zona tanpa gangguan. Zona Ketersediaan memiliki ketersediaan dan toleransi kesalahan yang lebih baik, dan dapat diskalakan dibandingkan infrastruktur pusat data tunggal atau multi tradisional.

ROSA memberi pelanggan opsi untuk menjalankan bidang kontrol Kubernetes dan bidang data dalam satu AWS Availability Zone, atau di beberapa Availability Zone. Meskipun kluster AZ tunggal dapat berguna untuk eksperimen, pelanggan didorong untuk menjalankan beban kerja mereka di

lebih dari satu Availability Zone. Ini memastikan bahwa aplikasi dapat menahan bahkan kegagalan Availability Zone lengkap - peristiwa yang sangat langka dalam dirinya sendiri.

Untuk informasi selengkapnya tentang Wilayah AWS dan Availability Zone, lihat Infrastruktur AWS Global.

ROSA ketahanan cluster

Bidang ROSA kontrol terdiri dari setidaknya tiga node bidang OpenShift kontrol. Setiap node bidang kontrol terdiri dari instance server API, `etcd` instance, dan pengontrol. Jika terjadi kegagalan node bidang kontrol, semua permintaan API secara otomatis dirutekan ke node lain yang tersedia untuk memastikan ketersediaan klaster.

Bidang ROSA data terdiri dari setidaknya dua node OpenShift infrastruktur dan dua node OpenShift pekerja. Node infrastruktur menjalankan pod yang mendukung komponen infrastruktur OpenShift klaster seperti router default, OpenShift registri bawaan, dan komponen untuk metrik dan pemantauan klaster. OpenShift node pekerja menjalankan pod aplikasi pengguna akhir.

Insinyur keandalan situs Red Hat (SREs) sepenuhnya mengelola bidang kontrol dan node infrastruktur. Red Hat SREs secara proaktif memantau ROSA cluster, dan bertanggung jawab untuk mengganti node bidang kontrol dan node infrastruktur yang gagal. Untuk informasi selengkapnya, lihat the section called “Tanggung Jawab”.

> **Important**
>
> Karena ROSA merupakan layanan terkelola, Red Hat bertanggung jawab untuk mengelola AWS infrastruktur dasar yang ROSA digunakan. Pelanggan tidak boleh mencoba mematikan Amazon EC2 instance yang ROSA digunakan secara manual dari AWS konsol atau AWS CLI. Tindakan ini dapat menyebabkan hilangnya data pelanggan.

Jika node pekerja gagal pada bidang data, bidang kontrol akan memindahkan pod yang tidak terjadwal ke node pekerja yang berfungsi hingga node yang gagal dipulihkan atau diganti. Node pekerja yang gagal dapat diganti secara manual atau otomatis dengan mengaktifkan penskalaan otomatis mesin dalam sebuah cluster. Untuk informasi selengkapnya, lihat Penskalaan otomatis klaster di dokumentasi Red Hat.

Ketahanan aplikasi yang digunakan pelanggan

Meskipun ROSA menyediakan banyak perlindungan untuk memastikan ketersediaan layanan yang tinggi, pelanggan bertanggung jawab untuk membangun aplikasi yang digunakan untuk ketersediaan tinggi guna melindungi beban kerja dari waktu henti. Untuk informasi selengkapnya, lihat Tentang ketersediaan ROSA di dokumentasi Red Hat.

Keamanan infrastruktur di ROSA

Sebagai layanan terkelola, Layanan OpenShift Red Hat di AWS dilindungi oleh keamanan jaringan AWS global. Untuk informasi tentang layanan AWS keamanan dan cara AWS melindungi infrastruktur, lihat Keamanan AWS Cloud. Untuk merancang AWS lingkungan Anda menggunakan praktik terbaik untuk keamanan infrastruktur, lihat Perlindungan Infrastruktur di Pilar Keamanan — Kerangka Kerja yang Dirancang AWS dengan Baik.

Anda menggunakan panggilan API yang AWS dipublikasikan untuk mengakses ROSA melalui AWS jaringan. Klien harus mendukung hal-hal berikut:

- Keamanan Lapisan Pengangkutan (TLS). Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Sandi cocok dengan sistem kerahasiaan maju sempurna (perfect forward secrecy, PFS) seperti DHE (Ephemeral Diffie-Hellman) atau ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Sebagian besar sistem modern seperti Java 7 dan versi lebih baru mendukung mode-mode ini.

Selain itu, permintaan harus ditandatangani menggunakan ID kunci akses dan kunci akses rahasia yang terkait dengan prinsipal IAM. Atau Anda dapat menggunakan AWS Security Token Service (AWS STS) untuk menghasilkan kredensial keamanan sementara untuk menandatangani permintaan.

Isolasi jaringan cluster

Insinyur keandalan situs Red Hat (SREs) bertanggung jawab atas manajemen berkelanjutan dan keamanan jaringan cluster dan platform aplikasi yang mendasarinya. Untuk informasi lebih lanjut tentang tanggung jawab Red Hat ROSA, lihatthe section called “Tanggung Jawab”.

Saat Anda membuat klaster baru, ROSA berikan opsi untuk membuat titik akhir server API Kubernetes publik dan rute aplikasi atau titik akhir API Kubernetes pribadi dan rute aplikasi. Koneksi ini digunakan untuk berkomunikasi dengan cluster Anda (menggunakan alat OpenShift manajemen seperti ROSA CLI dan OpenShift CLI). Koneksi privat memungkinkan semua komunikasi antara

simpul Anda dan server API tetap berada di dalam VPC Anda. Jika Anda mengaktifkan akses pribadi ke server API dan rute aplikasi, Anda harus menggunakan VPC yang ada dan menghubungkan VPC AWS PrivateLink ke layanan backend. OpenShift

Akses server Kubernetes API diamankan menggunakan kombinasi AWS Identity and Access Management (IAM) dan kontrol akses berbasis peran Kubernetes (RBAC). Untuk informasi selengkapnya tentang Kubernetes RBAC, lihat Menggunakan Otorisasi RBAC dalam dokumentasi Kubernetes.

ROSA memungkinkan Anda membuat rute aplikasi aman menggunakan beberapa jenis penghentian TLS untuk melayani sertifikat kepada klien. Untuk informasi selengkapnya, lihat Rute aman di dokumentasi Red Hat.

Jika Anda membuat ROSA klaster di VPC yang ada, Anda menentukan subnet VPC dan Availability Zone untuk digunakan oleh klaster Anda. Anda juga menentukan rentang CIDR untuk jaringan cluster yang akan digunakan, dan mencocokkan rentang CIDR ini dengan subnet VPC. Untuk informasi lebih lanjut, lihat definisi rentang CIDR dalam dokumentasi Red Hat.

Untuk kluster yang menggunakan titik akhir API publik, ROSA VPC Anda harus dikonfigurasi dengan subnet publik dan pribadi untuk setiap Availability Zone yang Anda inginkan agar klaster digunakan. Untuk cluster yang menggunakan titik akhir API pribadi, hanya subnet pribadi yang diperlukan.

Jika Anda menggunakan VPC yang ada, Anda dapat mengonfigurasi ROSA cluster Anda untuk menggunakan server proxy HTTP atau HTTPS selama atau setelah pembuatan cluster untuk mengenkripsi lalu lintas web cluster, menambahkan lapisan keamanan lain untuk data Anda. Saat Anda mengaktifkan proxy, komponen cluster inti ditolak akses langsung ke internet. Proxy tidak menolak akses internet untuk beban kerja pengguna. Untuk informasi selengkapnya, lihat Mengonfigurasi proxy di seluruh klaster dalam dokumentasi Red Hat.

Isolasi jaringan pod

Jika Anda adalah administrator klaster, Anda dapat menentukan kebijakan jaringan di tingkat pod yang membatasi lalu lintas ke pod di ROSA klaster Anda.

ROSA kuota layanan

Layanan OpenShift Red Hat di AWS (ROSA) menggunakan kuota layanan untuk Amazon EC2,, Amazon Virtual Private Cloud Amazon Elastic Block Store, dan Elastic Load Balancing untuk menyediakan cluster. Untuk informasi selengkapnya, lihat Layanan OpenShift Red Hat di AWS titik akhir dan kuota di Panduan Referensi AWS Umum.

AWS layanan terintegrasi dengan ROSA

ROSA bekerja sama dengan Layanan AWS orang lain untuk memberikan solusi tambahan untuk tantangan bisnis Anda. Topik ini mengidentifikasi layanan yang digunakan ROSA untuk menambahkan fungsionalitas, atau layanan yang ROSA digunakan untuk melakukan tugas.

Topik

Bagaimana ROSA bekerja dengan AWS Marketplace

AWS Marketplace adalah katalog digital yang dikuratori yang dapat Anda gunakan untuk menemukan, membeli, menyebarkan, dan mengelola perangkat lunak, data, dan layanan pihak ketiga yang Anda butuhkan untuk membangun solusi dan menjalankan bisnis Anda. AWS Marketplace menyederhanakan lisensi dan pengadaan perangkat lunak dengan opsi harga yang fleksibel dan beberapa metode penerapan.

ROSA digunakan AWS Marketplace untuk pengukuran dan penagihan layanan. ROSA classic diukur dan ditagih melalui produk berbasis AWS Marketplace Amazon Machine Image (AMI), sedangkan ROSA dengan pesawat kontrol yang dihosting (HCP) diukur dan ditagih melalui produk berbasis perangkat lunak AWS Marketplace sebagai layanan (SaaS).

Halaman ini menjelaskan cara ROSA kerja AWS Marketplace untuk pembayaran, penagihan, langganan, dan pembelian kontrak.

Terminologi

Halaman ini menggunakan istilah-istilah berikut ketika membahas integrasi ROSA dengan. AWS Marketplace

Gambar Mesin Amazon (AMI)

Gambar server, termasuk sistem operasi dan perangkat lunak tambahan, yang berjalan AWS.

Berlangganan AMI

Di AWS Marketplace, produk perangkat lunak berbasis AMI seperti ROSA classic menggunakan model harga berlangganan tahunan per jam. Harga per jam adalah model penetapan harga

default, tetapi Anda memiliki opsi untuk membeli penggunaan satu tahun di muka untuk satu jenis Amazon EC2 instance.

Berlangganan SaaS

Di AWS Marketplace, software-as-a-service (SaaS) produk seperti ROSA dengan HCP mengadopsi model berlangganan berbasis penggunaan. Penjual perangkat lunak melacak penggunaan Anda dan Anda hanya membayar untuk apa yang Anda gunakan.

Penawaran umum

Penawaran publik memungkinkan Anda untuk membeli AWS Marketplace perangkat lunak dan layanan langsung dari AWS Management Console.

Penawaran pribadi

Penawaran pribadi adalah program pembelian yang memungkinkan penjual dan pembeli untuk menegosiasikan harga khusus dan ketentuan perjanjian lisensi pengguna akhir (EULA) untuk pembelian di. AWS Marketplace

ROSA biaya layanan

Biaya yang ROSA dikenakan untuk OpenShift perangkat lunak dan manajemen klaster oleh insinyur keandalan situs Red Hat (SREs). ROSA biaya layanan diukur AWS Marketplace dan muncul di AWS tagihan Anda.

AWS biaya infrastruktur

Biaya standar yang AWS membebankan untuk ROSA klaster Layanan AWS yang mendasarinya, termasuk Amazon EC2, Amazon EBS, Amazon S3, dan Elastic Load Balancing. Biaya diukur melalui yang Layanan AWS digunakan dan muncul di AWS tagihan Anda.

ROSA pembayaran dan penagihan

ROSA terintegrasi dengan AWS Marketplace untuk memungkinkan pengukuran dan penagihan biaya layanan. ROSA ROSA Biaya layanan mencakup akses ke OpenShift perangkat lunak dan manajemen klaster oleh teknisi keandalan situs Red Hat (SREs). ROSA biaya layanan seragam di semua Wilayah AWS standar yang didukung. ROSA dengan biaya layanan HCP bertambah sesuai permintaan secara default dengan tarif per jam tetap berdasarkan jumlah cluster yang berjalan dan node pekerja v yang berjalan di cluster tersebut. CPUs Biaya layanan klasik ROSA bertambah berdasarkan permintaan berdasarkan jumlah node pekerja v. CPUs ROSA classic tidak membebankan biaya layanan untuk pesawat kontrol atau node infrastruktur yang diperlukan.

ROSA pelanggan juga membayar biaya AWS infrastruktur standar untuk ROSA cluster yang Layanan AWS mendasarinya, termasuk Amazon EC2,, Amazon EBS Amazon S3, dan Elastic Load Balancing. AWS Biaya infrastruktur adalah item penagihan terpisah dari biaya ROSA layanan yang diukur. AWS Marketplace AWS Biaya infrastruktur bervariasi menurut Wilayah AWS dan didasarkan pada penggunaan per jam secara default. Untuk penghematan biaya AWS infrastruktur tambahan, Anda dapat membeli paket Amazon EC2 tabungan atau instans cadangan. Untuk informasi selengkapnya, lihat Compute Savings Plans dan Instans Cadangan di Panduan Pengguna Amazon EC2 .

ROSA tidak membebankan biaya sampai Anda membuat ROSA klaster, atau membeli ROSA kontrak. Untuk informasi selengkapnya, lihat harga Layanan OpenShift Red Hat di AWS.

Anda dapat melihat biaya ROSA layanan dan biaya AWS infrastruktur dan mengelola pembayaran di AWS Billing konsol. Anda juga dapat melihat biaya Anda dan memantau penggunaan menggunakan AWS Cost Explorer Service antarmuka secara gratis. Untuk informasi selengkapnya, lihat Melihat tagihan Anda di Panduan AWS Manajemen Penagihan dan Biaya Pengguna dan Menganalisis biaya Anda dengan AWS Cost Explorer Service Panduan Pengguna Manajemen AWS Biaya.

Berlangganan daftar ROSA Marketplace melalui konsol

Saat Anda mengaktifkan ROSA di ROSA konsol, Anda Akun AWS berlangganan ROSA klasik dan ROSA dengan daftar HCP aktif. AWS Marketplace Tidak ada biaya untuk mengaktifkan ROSA langganan.

Untuk AWS Organizations pengguna, ROSA memungkinkan Anda untuk berbagi langganan klasik ROSA dengan akun lain di organisasi Anda. Untuk informasi selengkapnya, lihat Berbagi langganan di organisasi di Panduan AWS Marketplace Pembeli.

Membeli ROSA kontrak

ROSA digunakan AWS Marketplace untuk menyediakan kontrak opsional untuk ROSA dengan HCP dan ROSA klasik. Kontrak memberikan penghematan pada biaya layanan node ROSA pekerja. ROSA Kontrak tidak mempengaruhi biaya yang dibebankan untuk AWS infrastruktur.

Kontrak 12 bulan

Anda dapat membeli kontrak penawaran umum 12 bulan untuk ROSA classic dan ROSA dengan HCP dari konsol. ROSA

> **Note**
>
> ROSA classic harus diaktifkan di akun Anda sebelum Anda dapat membeli kontrak 12 bulan dari konsol.

> **Note**
>
> Kontrak 12 bulan tidak dapat ditransfer ke penawaran pribadi.

Membeli kontrak 12 bulan klasik ROSA

Ketika Anda membeli kontrak 12 bulan ROSA klasik, Anda melakukan pembayaran di muka untuk jangka waktu tahunan dan tidak membayar biaya layanan per jam selama 12 bulan ke depan untuk instans yang ditanggung. Biaya kontrak didasarkan pada jenis Amazon EC2 instans dan jumlah instance yang Anda pilih. Kontrak tidak mencakup biaya AWS infrastruktur yang ROSA membebankan biaya untuk yang mendasari Layanan AWS yang digunakan. Untuk informasi selengkapnya, silakan lihat Harga Layanan OpenShift Red Hat di AWS.

Kontrak hanya mencakup jenis instance yang Anda tentukan selama pembuatan kontrak (misalnya m5.xlarge). Anda dapat membeli kontrak 12 bulan tambahan untuk penghematan biaya pada lebih dari satu jenis Amazon EC2 instans. Penggunaan di luar kontrak 12 bulan Anda menimbulkan biaya ROSA layanan dengan tarif sesuai permintaan.

> **Note**
>
> Kontrak ROSA klasik 12 bulan tidak diperpanjang secara otomatis.

Untuk membeli kontrak 12 bulan untuk ROSA classic

> **Note**
>
> Jika Anda menggunakan ROSA konsol di Wilayah yang belum mendukung ROSA dengan HCP, alur kerja ini belum tersedia. Untuk daftar Wilayah yang mendukung ROSA dengan HCP, lihat. the section called “Membandingkan ROSA dengan HCP dan ROSA klasik”

Untuk membeli kontrak klasik ROSA di Wilayah tanpa ROSA dengan dukungan HCP, buka ROSA konsol dan pilih Beli kontrak perangkat lunak dan lihat kontrak yang ada.

1. Pergi ke ROSA konsol.
2. Di panel navigasi kiri, pilih Kontrak.
3. Pilih Kontrak untuk ROSA klasik.
4. Pilih Kontrak Pembelian.
5. Pilih jenis EC2 instans dan jumlah instance yang Anda butuhkan.
6. Pilih Kontrak Tinjauan.
7. Tinjau detail kontrak dan pilih Kontrak pembelian.

Note

ROSA Kontrak 12 bulan tidak dapat diturunkan atau dibatalkan setelah pembuatan menggunakan konsol. Jika Anda perlu menurunkan versi atau membatalkan kontrak selama durasi kontrak aktif, buka Dukungan Pusat dan buka kasus dukungan.

Membeli ROSA dengan kontrak 12 bulan HCP

Saat Anda mengaktifkan ROSA dengan HCP di konsol, ROSA 12 bulan tanpa biaya dengan kontrak HCP pada awalnya dibuat di akun Anda untuk memfasilitasi penagihan sesuai permintaan. Jika Anda memilih untuk membeli ROSA dengan kontrak HCP untuk menghemat biaya layanan node pekerja, kontrak awal dimodifikasi untuk menutupi biaya penggunaan node pekerja v CPUs dan bidang kontrol yang Anda tentukan.

Saat Anda membeli ROSA dengan kontrak 12 bulan HCP, Anda melakukan pembayaran di muka untuk jangka waktu tahunan dan tidak membayar biaya penggunaan per jam selama 12 bulan ke depan untuk node pekerja v dan pesawat kontrol yang tercakup. CPUs Biaya kontrak didasarkan pada jumlah node pekerja v CPUs dan bidang kontrol yang Anda pilih. Kontrak hanya mencakup node pekerja v CPUs dan bidang kontrol yang Anda tentukan selama pembuatan kontrak. Kontrak tidak mencakup biaya AWS infrastruktur yang ROSA membebankan biaya untuk yang mendasari Layanan AWS yang digunakan. Untuk informasi selengkapnya, silakan lihat Harga Layanan OpenShift Red Hat di AWS.

Kuota pemakaian bulanan

Setelah pembelian, pesawat v CPUs dan kontrol prabayar Anda dikonversi ke kuota penggunaan bulanan. Tarif penggunaan sesuai permintaan per jam berlaku untuk penggunaan vCPU dan pesawat kontrol yang melebihi kuota bulanan. ROSA dengan HCP menggunakan rumus berikut untuk menghitung kuota bulanan yang terkait dengan kontrak:

- Node pekerja vCPUs: jumlah v CPUs x 24 jam x 365 hari/12 bulan
- Pesawat kontrol: jumlah pesawat kontrol x 24 jam x 365 hari/12 bulan

Misalnya, pembelian 4.000 node pekerja v CPUs dan 8 pesawat kontrol akan dikonversi ke kuota bulanan 2.920.000 jam vCPU node pekerja dan 5.840 jam pesawat kontrol yang dapat dikonsumsi per bulan.

Untuk membeli ROSA dengan kontrak 12 bulan HCP

> **Note**
>
> Jika Anda menggunakan Layanan OpenShift Red Hat di AWS konsol di Wilayah yang belum mendukung ROSA dengan bidang kontrol yang di-host, alur kerja ini belum tersedia. Untuk daftar Wilayah yang mendukung ROSA dengan HCP, lihat. the section called “Membandingkan ROSA dengan HCP dan ROSA klasik”

1. Pergi ke ROSA konsol.
2. Di panel navigasi kiri, pilih Kontrak.
3. Pilih Kontrak untuk ROSA dengan HCP.
4. Pilih Kontrak Pembelian.
5. Masukkan nomor v yang CPUs akan dibeli. Tentukan dalam kelipatan 4.
6. Masukkan jumlah pesawat kontrol yang akan dibeli.
7. Pilih Kontrak Tinjauan.
8. Tinjau detail kontrak dan pilih Kontrak pembelian.

> **Note**
>
> ROSA Kontrak 12 bulan tidak dapat diturunkan atau dibatalkan setelah pembuatan menggunakan konsol. Jika Anda perlu menurunkan versi atau membatalkan kontrak selama durasi kontrak aktif, buka Dukungan Pusat dan buka kasus dukungan.

Meningkatkan ROSA dengan kontrak 12 bulan HCP

Anda dapat meningkatkan ROSA aktif Anda dengan kontrak 12 bulan HCP kapan saja dengan node pekerja tambahan v CPUs dan pesawat kontrol. Saat Anda meningkatkan ROSA Anda dengan kontrak 12 bulan HCP, Anda melakukan pembayaran prorata di muka untuk sumber daya tambahan. Jumlah prorata dihitung berdasarkan jumlah hari yang tersisa pada kontrak. Kontrak hanya mencakup node pekerja v CPUs dan bidang kontrol yang Anda tentukan selama pembuatan kontrak. Peningkatan kontrak tidak memengaruhi biaya yang dikenakan untuk AWS infrastruktur.

Setelah upgrade, v yang ditambahkan CPUs dan pesawat kontrol dikonversi ke kuota penggunaan bulanan menggunakan rumus yang sama dengan pembelian kontrak asli. Tarif penggunaan sesuai permintaan per jam berlaku untuk penggunaan vCPU dan pesawat kontrol yang melebihi kuota bulanan. Untuk informasi selengkapnya, lihat the section called “Kuota pemakaian bulanan”.

Untuk meningkatkan ROSA dengan kontrak 12 bulan HCP

1. Pergi ke ROSA konsol.
2. Di panel navigasi kiri, pilih Kontrak.
3. Pilih Kontrak untuk ROSA dengan HCP.
4. Pilih Tingkatkan.
5. Masukkan jumlah v yang CPUs akan ditambahkan. Tentukan dalam kelipatan 4.
6. Masukkan jumlah pesawat kontrol untuk ditambahkan ke kontrak.
7. Pilih Tinjau upgrade.
8. Tinjau detail kontrak dan pilih peningkatan Pembelian.

> **Note**
>
> Kontrak ROSA klasik 12 bulan tidak dapat ditingkatkan. Kontrak klasik ROSA 12 bulan tambahan dapat dibeli kapan saja menggunakan konsol. ROSA

Mendapatkan penawaran pribadi

Anda dapat meminta penawaran AWS Marketplace pribadi untuk ROSA dengan HCP atau ROSA classic untuk menerima harga produk dan persyaratan perjanjian lisensi pengguna akhir (EULA) yang dinegosiasikan dengan Red Hat. Untuk informasi selengkapnya, lihat Penawaran pribadi di Panduan AWS Marketplace Pembeli.

Untuk mendapatkan penawaran ROSA pribadi

> **Note**
>
> Jika Anda adalah AWS Organizations pengguna dan menerima penawaran pribadi yang dikeluarkan untuk akun pembayar dan anggota Anda, ikuti prosedur di bawah ini untuk berlangganan ROSA langsung di setiap akun di organisasi Anda.
> Jika Anda menerima penawaran pribadi klasik ROSA yang hanya dikeluarkan ke akun AWS Organizations pembayar, Anda harus berbagi langganan dengan akun anggota di organisasi Anda. Untuk informasi selengkapnya, lihat Berbagi langganan di organisasi di Panduan AWS Marketplace Pembeli.

1. Setelah penawaran pribadi dikeluarkan, masuk ke AWS Marketplace konsol.
2. Buka email dengan tautan penawaran ROSA pribadi.
3. Ikuti tautan untuk langsung mengakses penawaran pribadi.

> **Note**
>
> Mengikuti tautan ini sebelum masuk ke akun yang benar akan menghasilkan kesalahan Catatan halaman ditemukan (404).

4. Tinjau syarat dan ketentuan.
5. Pilih Terima persyaratan.

> **Note**
>
> Jika penawaran AWS Marketplace pribadi tidak diterima, biaya ROSA layanan dari AWS Marketplace akan terus ditagih dengan tarif per jam publik.

6. Untuk memverifikasi detail penawaran, pilih Tampilkan detail di daftar produk.

7. Untuk mulai menggunakan ROSA, pilih Lanjutkan ke konfigurasi. Anda akan dialihkan ke ROSA konsol.

Marketplace Pribadi

Private Marketplace memungkinkan administrator untuk membuat katalog digital yang disesuaikan dari produk yang disetujui. AWS Marketplace Administrator dapat membuat set unik perangkat lunak diperiksa yang tersedia AWS Marketplace untuk unit AWS organisasi atau berbeda Akun AWS dalam organisasi mereka untuk dibeli.

Jika organisasi Anda menggunakan pasar pribadi, administrator harus menambahkan AWS Marketplace daftar ROSA ke pasar pribadi sebelum pengguna dapat mengaktifkan layanan. Untuk informasi selengkapnya, lihat Memulai pasar pribadi di Panduan AWS Marketplace Pembeli.

Pemecahan Masalah

Halaman berikut merinci beberapa masalah umum yang dihadapi saat membuat atau mengelola ROSA cluster.

Topik

Akses log debug ROSA klaster

Untuk mulai memecahkan masalah dengan aplikasi Anda, pertama-tama tinjau log debug. Log debug ROSA CLI memberikan rincian tentang pesan kesalahan yang dihasilkan ketika klaster gagal untuk membuat.

Untuk menampilkan informasi klaster debug, jalankan perintah ROSA CLI berikut. Dalam perintah, ganti `<cluster_name>` dengan nama Anda klaster.

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

ROSA cluster gagal pemeriksaan kuota AWS layanan selama pembuatan klaster

Untuk menggunakannya ROSA, kuota layanan untuk akun Anda mungkin perlu ditingkatkan. Untuk informasi lebih lanjut, lihat Layanan OpenShift Red Hat di AWS kuota dan titik akhir.

1. Jalankan perintah berikut untuk mengidentifikasi kuota akun Anda.

```
rosa verify quota
```

> **Note**
>
> Kuota berbeda dalam hal yang berbeda Wilayah AWS. Pastikan untuk memverifikasi setiap kuota untuk Wilayah Anda.

2. Jika Anda perlu menambah kuota, navigasikan ke Service Quotas konsol.
3. Pada panel navigasi, pilih AWS layanan.
4. Pilih layanan yang membutuhkan peningkatan kuota.
5. Pilih kuota yang perlu ditingkatkan dan pilih Permintaan kenaikan kuota.
6. Untuk peningkatan kuota Permintaan, masukkan jumlah total kuota yang Anda inginkan dan pilih Permintaan.

Memecahkan masalah ROSA CLI token akses offline kedaluwarsa

Jika Anda menggunakan ROSA CLI dan token akses offline api.openshift.com Anda kedaluwarsa, pesan kesalahan akan muncul. Ini terjadi ketika sso.redhat.com membatalkan token.

1. Arahkan ke halaman Token API Manajer OpenShift Cluster dan pilih Load Token.
2. Salin dan tempel perintah otentikasi berikut di terminal.

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

Gagal membuat klaster dengan osdCcsAdmin kesalahan

> **Note**
>
> Kesalahan ini hanya terjadi ketika Anda menggunakan metode non-STS untuk menyediakan kluster. ROSA Untuk menghindari masalah ini, sediakan ROSA cluster Anda menggunakan AWS STS. Untuk informasi selengkapnya, lihat the section called “Buat cluster klasik ROSA - CLI”.

Jika klaster gagal membuat, Anda mungkin menerima pesan galat berikut:

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

1. Hapus tumpukan.

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

2. Inisialisasi ulang akun Anda.

```
rosa init
```

Langkah selanjutnya

- Kunjungi OpenShift dokumentasi.
- Buka Dukungan kasing atau kasing Red Hat Support.
- Temukan jawaban atas pertanyaan yang sering diajukan tentang Layanan OpenShift Red Hat di AWS.
- Untuk informasi lebih lanjut tentang model dukungan ROSA, lihatthe section called “Mendapatkan Dukungan”.

Mendapatkan ROSA dukungan

Dengan ROSA, Anda dapat menerima dukungan dari Dukungan dan tim dukungan Red Hat. Kasus Support dapat dibuka dengan salah satu organisasi, dan diarahkan ke tim yang tepat untuk menyelesaikan masalah Anda.

Buka Dukungan kasing

Paket Dukungan AWS Pengembang diperlukan untuk membuka kasus ROSA teknis, tetapi rencana Dukungan On-Ramp AWS Bisnis, Perusahaan, atau Perusahaan direkomendasikan untuk akses berkelanjutan ke dukungan ROSA teknis dan panduan arsitektur. Red Hat menggunakan Dukungan API untuk membuka kasing bagi pelanggan bila diperlukan. AWS Paket dukungan On-Ramp Bisnis, Perusahaan, dan Perusahaan memungkinkan akses telepon, web, dan obrolan berkelanjutan untuk mendukung teknisi. Untuk informasi lebih lanjut tentang Dukungan rencana, lihat Dukungan.

Untuk langkah-langkah untuk mengaktifkan Dukungan paket, lihat Bagaimana cara mendaftar Dukungan paket?

Untuk informasi tentang membuat Dukungan kasus, lihat Membuat kasus dukungan dan manajemen kasus.

Buka kasing Red Hat Support

ROSA Termasuk Red Hat Premium Support. Untuk menerima Red Hat Premium Support, navigasikan ke Red Hat Customer Portal dan gunakan support case tool untuk membuat tiket dukungan. Untuk informasi selengkapnya, lihat Cara terlibat dengan dukungan Red Hat.

Riwayat dokumen

Tabel berikut menjelaskan perubahan penting pada dokumentasi. Untuk notifikasi tentang pembaruan dokumentasi ini, Anda dapat berlangganan ke umpan RSS.

Perubahan	Deskripsi	Tanggal
Diperbarui ROSAImage RegistryOperatorPolicy	Memperbarui kebijakan AWS terkelola ROSAImage RegistryOperatorPolicy.	19 Mei 2025
Diperbarui ROSANode PoolManagementPolicy	Memperbarui kebijakan AWS terkelola ROSANodeP oolManagementPolicy .	5 Mei 2025
Diperbarui ROSAImage RegistryOperatorPolicy	Memperbarui kebijakan AWS terkelola ROSAImage RegistryOperatorPolicy.	16 April 2025
Diperbarui ROSAWorker InstancePolicy	Memperbarui kebijakan AWS terkelola ROSAWorke rInstancePolicy.	3 Maret 2025
Diperbarui ROSANode PoolManagementPolicy	Memperbarui kebijakan AWS terkelola ROSANodeP oolManagementPolicy.	24 Februari 2025
Diperbarui ROSAAmazon EBSCSIDriver OperatorPolicy	Memperbarui kebijakan AWS terkelola ROSAAmazon EBSCSIDriverOperatorPolicy.	17 Januari 2025
ROSA dengan ekspansi HCP Wilayah AWS	ROSA dengan pesawat kontrol host (HCP) kini tersedia di Middle East (UEA). Wilayah AWS	13 Mei 2024

ROSA dengan ekspansi HCP Wilayah AWS	ROSA dengan pesawat kontrol host (HCP) kini tersedia di Eropa (Paris). Wilayah AWS	6 Mei 2024
Diperbarui ROSANode PoolManagementPolicy	Memperbarui kebijakan AWS terkelola ROSANodeP oolManagementPolicy.	2 Mei 2024
ROSA dengan ekspansi HCP Wilayah AWS	ROSA dengan pesawat kontrol host (HCP) kini tersedia di Eropa (Spanyol). Wilayah AWS	29 April 2024
ROSAInstallerKebijakan yang Diperbarui	Memperbarui Kebijakan ROSAInstaller kebijakan AWS terkelola.	24 April 2024
ROSA dengan ekspansi HCP Wilayah AWS	ROSA dengan pesawat kontrol host (HCP) kini tersedia di Eropa (Zurich). Wilayah AWS	19 April 2024
ROSA dengan ekspansi HCP Wilayah AWS	ROSA dengan pesawat kontrol host (HCP) kini tersedia di Asia Pacific (Osaka). Wilayah AWS	17 April 2024
ROSAInstallerKebijakan dan ROSASRESupport Kebijakan yang Diperbarui	Memperbarui kebijakan AWS terkelola ROSAInstaller Kebijakan dan ROSASRESu pport Kebijakan.	10 April 2024
ROSA dengan ekspansi HCP Wilayah AWS	ROSA dengan pesawat kontrol host (HCP) kini tersedia di Asia Pacific (Hong Kong). Wilayah AWS	8 April 2024

ROSA dengan ekspansi HCP Wilayah AWS	ROSA dengan pesawat kontrol host (HCP) kini tersedia di Amerika Selatan (São Paulo). Wilayah AWS	1 April 2024
ROSA dengan ekspansi HCP Wilayah AWS	ROSA dengan pesawat kontrol host (HCP) kini tersedia di Middle East (Bahrain). Wilayah AWS	25 Maret 2024
ROSA dengan ekspansi HCP Wilayah AWS	ROSA dengan pesawat kontrol host (HCP) kini tersedia di Asia Pacific (Seoul). Wilayah AWS	Selasa, 14 Maret 2024
ROSA dengan ekspansi HCP Wilayah AWS	ROSA dengan pesawat kontrol host (HCP) kini tersedia di Africa (Cape Town). Wilayah AWS	5 Maret 2024
ROSAInstallerKebijakan yang Diperbarui	Memperbarui Kebijakan ROSAInstaller kebijakan AWS terkelola.	26 Januari 2024
ROSASRESupportKebijakan yang Diperbarui	Memperbarui Kebijakan ROSASRESupport kebijakan AWS terkelola.	22 Januari 2024
Diperbarui ROSAImage RegistryOperatorPolicy	Memperbarui kebijakan AWS terkelola ROSAImage RegistryOperatorPolicy.	12 Desember 2023
Diperbarui ROSAKube ControllerPolicy	Memperbarui kebijakan AWS terkelola ROSAKubeController Policy.	16 Oktober 2023

ROSAManageBerlangganan Diperbarui	Memperbarui kebijakan AWS terkelola ROSAManage Berlangganan.	1 Agustus 2023
Diperbarui ROSAKube ControllerPolicy	Memperbarui kebijakan AWS terkelola ROSAKubeController Policy.	13 Juli 2023
Ditambahkan halaman keamanan ROSA	Ketahanan dalam ROSA, Keamanan infrastruktur di ROSA, dan perlindungan data di halaman ROSA ditambahk an.	30 Juni 2023
Ditambahkan halaman opsi penyebaran	Halaman opsi penyebaran telah ditambahkan.	9 Juni 2023
Menambahkan kebijakan AWS terkelola baru ROSANode PoolManagementPolicy	Kebijakan AWS terkelola baru ROSANode PoolManag ementPolicy ditambahkan.	8 Juni 2023
Ditambahkan Kebijakan ROSAInstaller kebijakan AWS terkelola baru	Kebijakan AWS terkelola baru ROSAInstaller Kebijakan telah ditambahkan.	6 Juni 2023
Ditambahkan Kebijakan ROSASRESupport kebijakan AWS terkelola baru	Kebijakan AWS terkelola baru ROSASRESupport Kebijakan telah ditambahkan.	1 Juni 2023
Ditambahkan Ikhtisar tanggung jawab untuk ROSA	Ditambahkan Ikhtisar tanggung jawab untuk halaman ROSA.	26 Mei 2023
Diperbarui Apa itu Layanan OpenShift Red Hat di AWS?	Memperbarui Layanan OpenShift Red Hat di AWS halaman Apa itu.	24 Mei 2023

Menambahkan kebijakan AWS terkelola baru untuk peran operator ROSA	Kebijakan AWS terkelola baru ROSAImage RegistryOperatorPolicy ROSAKubeControllerPolicy,, dan ROSAKMSProvider Kebijakan ditambahkan.	27 April 2023
Menambahkan kebijakan AWS terkelola baru ROSAControl PlaneOperatorPolicy	Kebijakan AWS terkelola baru ROSAControl PlaneOperatorPolicy ditambahkan.	24 April 2023
Menambahkan kebijakan AWS terkelola baru untuk peran akun ROSA	Halaman kebijakan AWS terkelola baru untuk akun ROSA dan halaman peran operator ditambahkan.	20 April 2023
Ditambahkan halaman kuota layanan ROSA	Halaman kuota layanan ROSA telah ditambahkan.	22 Desember 2022
Ditambahkan halaman pemecahan masalah	Halaman pemecahan masalah telah ditambahkan.	1 November 2022
Ditambahkan memulai halaman	Halaman memulai telah ditambahkan.	12 Agustus 2022
Ditambahkan kebijakan AWS terkelola baru ROSAManage Berlangganan	Kebijakan AWS terkelola baru ROSAManage Langganan telah ditambahkan.	11 April 2022
Rilis awal	Rilis awal Panduan Layanan OpenShift Red Hat di AWS Pengguna.	24 Maret 2021

Terjemahan disediakan oleh mesin penerjemah. Jika konten terjemahan yang diberikan bertentangan dengan versi bahasa Inggris aslinya, utamakan versi bahasa Inggris.