aws

Panduan Administrasi Konsol

AWS RE: Posting Pribadi

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS RE: Posting Pribadi: Panduan Administrasi Konsol

Copyright © 2024 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 merupakan kekayaan masing-masing pemiliknya, yang mungkin atau mungkin tidak berafiliasi, terkait dengan, atau disponsori oleh Amazon.

Table of Contents

Apa itu AWS re:Post Private? 1
Akses Re: Post Private 1
Harga 2
Cara memulai 2
Prasyarat 3
Onboard ke Re:Post Private 4
Keamanan 5
Perlindungan data 6
Melindungi data dengan enkripsi 7
Enkripsi bergerak 7
Manajemen kunci 7
Bagaimana re:Post Private bekerja dengan IAM 7
re:post Kebijakan berbasis identitas pribadi 7
RE: posting Kebijakan berbasis sumber daya pribadi 9
Otorisasi berdasarkan tanda 10
Re: posting peran IAM Pribadi 10
Peran terkait layanan 10
Peran layanan 10
Menggunakan peran terkait layanan 11
Contoh kebijakan berbasis identitas 14
Kebijakan inline 17
AWS kebijakan terkelola 19
Pemecahan Masalah 22
Validasi kepatuhan 24
Ketangguhan 25
Keamanan Infrastruktur 26
Quotas 27
Kuota layanan 27
Batas pelambatan API 27
Buat, konfigurasikan, dan sesuaikan Re: post pribadi Anda 29
Buat re:Post pribadi baru 29
Mengelola akses ke pembuatan dan manajemen AWS Support kasus di re:Post Private 31
Menggunakan kebijakan AWS terkelola atau membuat kebijakan terkelola pelanggan 32
Contoh kebijakan IAM 33

Buat IAM role 34
Pemecahan Masalah 35
Mengatur dan mengelola akses pengguna 36
Kustomisasi re:Post pribadi Anda 36
Undang pengguna ke Re:Post pribadi Anda 37
Kelola re:Post pribadi Anda 38
Tambahkan pengguna dan grup 38
Menambahkan pengguna ke grup 39
Undang pengguna dan grup 39
Promosikan pengguna ke administrator 40
Hapus pengguna dan grup 40
Menambah atau menghapus AWS karyawan 41
Hapus Re: Post pribadi 41
Pemantauan RE: Post Private 43
Pemantauan CloudWatch dengan 43
Logging re:Post panggilan API Pribadi menggunakan AWS CloudTrail 44
re: posting informasi pribadi di CloudTrail 45
Memahami re:posting entri file log pribadi 46
Pemecahan Masalah 52
Tidak dapat mengatur re:Post pribadi saya di Wilayah tertentu AWS 52
Tidak dapat mengatur re:Post pribadi di akun saya 52
Tidak dapat mengelola pengguna atau grup dalam re:Post pribadi 52
Riwayat dokumen 53
..... liv

Apa itu AWS re:Post Private?

AWS re:Post Private adalah versi pribadi AWS re:Post untuk perusahaan dengan paket Enterprise Support atau Enterprise On-Ramp Support. Ini menyediakan akses ke pengetahuan dan pakar untuk mempercepat adopsi cloud dan meningkatkan produktivitas pengembang. Dengan Re:post pribadi khusus organisasi Anda, Anda dapat membangun komunitas pengembang khusus organisasi yang mendorong efisiensi dalam skala besar dan menyediakan akses ke sumber daya pengetahuan yang berharga. Selain itu, Re:Post Private memusatkan konten AWS teknis tepercaya dan menawarkan forum diskusi pribadi untuk meningkatkan cara tim Anda berkolaborasi secara internal dan dengan AWS untuk menghilangkan hambatan teknis, mempercepat inovasi, dan meningkatkan skala lebih efisien di cloud.

Untuk informasi selengkapnya, lihat AWS re:Post Private.

Akses Re: Post Private

Administrator menggunakan konsol AWS re:Post Private untuk membuat re:post pribadi khusus organisasi mereka. Ketika administrator membuat re:Post pribadi, mereka dapat memberi nama Re:post pribadi mereka dan menentukan subdomain di bawahnya. `*.private.repost.aws` Administrator untuk re:Post pribadi organisasi dapat mengonfigurasi akses pengguna menggunakan AWS IAM Identity Center dan menentukan salah satu sumber identitas berikut untuk otentikasi: Direktori Pusat Identitas, Direktori Aktif, atau penyedia identitas eksternal. Setelah mengkonfigurasi pengguna, administrator konsol dapat menetapkan peran admin Re:Post Private untuk satu atau lebih pengguna. administrator re:Post Private dapat menyesuaikan aplikasi re:Post pribadi mereka sesuai dengan branding organisasi dan kebutuhan pengetahuan. Anggota tim AWS akun, seperti Manajer Akun Teknis, yang akrab dengan arsitektur dan beban kerja organisasi secara otomatis ditambahkan ke re:post pribadi organisasi untuk kolaborasi.

Administrator untuk aplikasi Re:Post Private dapat menyesuaikan branding, menambahkan tag untuk mengklasifikasikan konten, dan memilih topik yang menarik bagi pengembang mereka untuk secara otomatis mengisi pelatihan dan konten teknis. Mereka juga dapat mengundang pengguna untuk bergabung dengan Re:Post pribadi mereka untuk meningkatkan kolaborasi. Untuk informasi selengkapnya, lihat AWS re:Post Private Administration Guide.

Pengguna non-administratif menggunakan aplikasi re:Post Private untuk masuk menggunakan kredenal yang dikonfigurasi oleh administrator mereka. Setelah masuk ke re:Post pribadi, pengguna dapat menelusuri atau mencari konten yang ada, termasuk pelatihan khusus dan konten teknis

yang mencakup topik minat mereka. Pengguna juga dapat mencari konten teknis AWS publik langsung dari re:Post pribadi mereka dan membuat utas pribadi untuk diskusi internal tentang konten AWS publik. Pengguna dapat secara kolaboratif memecahkan masalah AWS teknis dan mendapatkan bimbingan teknis dari pengguna lain dari Re: Post pribadi dengan mengajukan pertanyaan, memberikan tanggapan, atau menerbitkan artikel. Pengguna juga dapat mengubah utas diskusi menjadi AWS Support kasus. Pengguna dapat memilih untuk menambahkan tanggapan dari AWS Support ke Re: post pribadi. Untuk informasi selengkapnya, lihat AWS re:Post Private User Guide.

Harga

Hanya pelanggan dengan paket Dukungan Enterprise Support (ES) dan Enterprise On-Ramp (EOP) yang dapat berlangganan layanan Re:Post Private. Anda dapat memilih dari dua tingkatan harga yang tersedia - Tingkat gratis dan tingkat Standar. Tingkat Gratis memberi Anda kemampuan untuk menjelajahi dan mencoba kemampuan tingkat Standar secara penuh selama enam bulan sebelum Anda dapat dengan mulus beralih ke tingkat berbayar. Jika Anda menggunakan tingkat Standar, maka Anda dapat membayar langganan bulanan per biaya pengguna untuk menggunakan re:Post Private. Untuk informasi selengkapnya, silakan lihat Harga .

Cara memulai

Untuk memulai dengan re:Post Private, lihat. Prasyarat

Prasyarat

Anda harus memenuhi prasyarat berikut sebelum dapat membuat re:Post pribadi baru atau mengelola re:Post pribadi yang ada di AWS re:Post Private:

- Anda harus mendaftar untuk Enterprise atau Enterprise On-Ramp Support Plan.
- Anda harus mengaktifkan AWS IAM Identity Center di Wilayah yang sama di mana Anda ingin mengatur re:Post pribadi Anda.
- Anda harus membuat AWS Identity and Access Management peran yang memiliki izin yang diperlukan untuk membuat, mengelola, dan menyelesaikan AWS Support kasus untuk Anda. Layanan re:Post Private menggunakan peran ini untuk melakukan panggilan API ke. AWS Support Untuk informasi selengkapnya, lihat Mengelola akses ke pembuatan dan manajemen AWS Support kasus di re:Post Private.

Onboard untuk Re:Post Private melalui IAM Identity Center

Re: post Private terintegrasi dengan AWS IAM Identity Center untuk memberikan federasi identitas untuk tenaga kerja Anda. Melalui IAM Identity Center, pengguna diarahkan ke direktori perusahaan yang ada untuk masuk dengan kredensialnya yang ada. Kemudian, mereka masuk dengan mulus ke Re:post pribadi mereka. Ini memastikan bahwa pengaturan keamanan seperti kebijakan kata sandi dan otentikasi dua faktor diberlakukan. Menggunakan IAM Identity Center tidak memengaruhi konfigurasi IAM Anda yang ada.

Jika Anda tidak memiliki direktori pengguna yang ada atau memilih untuk tidak bergabung, maka IAM Identity Center menawarkan direktori pengguna terintegrasi yang dapat Anda gunakan untuk membuat pengguna dan grup untuk Re:Post Private. re:Post Private tidak mendukung penggunaan pengguna IAM dan peran untuk menetapkan izin dalam re:Post pribadi. Izin pengguna dalam Re: Post pribadi dikonfigurasi oleh administrator pada aplikasi Re:Post pribadi mereka.

Untuk informasi selengkapnya tentang Pusat Identitas IAM, lihat Apa itu Pusat Identitas AWS IAM (penerus AWS Single Sign-On). Untuk informasi selengkapnya tentang memulai dengan IAM Identity Center, lihat Memulai. Untuk menggunakan Pusat Identitas IAM, Anda juga harus AWS Organizations mengaktifkan akun tersebut.

> **Important**
>
> Re:post Private hanya mendukung instans organisasi dari IAM Identity Center.

Keamanan di Re: Post Private

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

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

- Keamanan cloud — AWS bertanggung jawab untuk melindungi infrastruktur yang menjalankan AWS layanan di AWS Cloud. AWS juga memberi Anda layanan yang dapat Anda gunakan dengan aman. Auditor pihak ketiga secara teratur menguji dan memverifikasi efektivitas keamanan kami sebagai bagian dari Program AWS Kepatuhan Program AWS Kepatuhan . Untuk mempelajari tentang program kepatuhan yang berlaku untuk AWS re:Post Private, lihat AWS Layanan dalam Lingkup oleh AWS Layanan Program Kepatuhan dalam Lingkup oleh Program .
- Keamanan di cloud — Tanggung jawab Anda ditentukan oleh AWS layanan yang Anda gunakan. Anda juga bertanggung jawab atas faktor-faktor lain, termasuk sensitivitas data Anda, persyaratan perusahaan Anda, dan hukum dan peraturan yang berlaku.

Dokumentasi ini membantu Anda memahami cara menerapkan model tanggung jawab bersama saat menggunakan re:Post Private. Topik berikut menunjukkan cara mengkonfigurasi re:Post Private untuk memenuhi tujuan keamanan dan kepatuhan Anda. Anda juga belajar cara menggunakan AWS layanan lain yang membantu Anda memantau dan mengamankan sumber daya Re:Post Private Anda.

Topik

- Perlindungan data di AWS re: Post Private
- Bagaimana re:Post Private bekerja dengan IAM
- Validasi kepatuhan untuk AWS re: Post Private
- Ketahanan di AWS re: Post Private
- Keamanan Infrastruktur di AWS re: Post Private

Perlindungan data di AWS re: Post Private

Model tanggung jawab AWS bersama model tanggung berlaku untuk perlindungan data di AWS re:Post Private. Seperti yang dijelaskan dalam model AWS ini, bertanggung jawab untuk melindungi infrastruktur global yang menjalankan semua AWS Cloud. Anda bertanggung jawab untuk mempertahankan kendali atas konten yang di-host pada infrastruktur ini. Anda juga bertanggung jawab atas tugas-tugas konfigurasi dan manajemen keamanan untuk AWS layanan yang Anda gunakan. Lihat informasi yang lebih lengkap tentang privasi data dalam Pertanyaan Umum Privasi Data. Lihat informasi tentang perlindungan data di Eropa di pos blog Model Tanggung Jawab Bersama dan GDPR AWS di Blog Keamanan AWS .

Untuk tujuan perlindungan data, kami menyarankan Anda melindungi Akun AWS kredensil dan mengatur pengguna individu dengan AWS IAM Identity Center atau 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.
- Siapkan API dan pencatatan aktivitas pengguna dengan AWS CloudTrail.
- Gunakan solusi AWS enkripsi, bersama dengan semua kontrol keamanan default di dalamnya AWS layanan.
- Gunakan layanan keamanan terkelola lanjut seperti Amazon Macie, yang membantu menemukan dan mengamankan data sensitif yang disimpan di Amazon S3.
- Jika Anda memerlukan modul kriptografi tervalidasi FIPS 140-2 saat mengakses AWS melalui antarmuka baris perintah atau API, gunakan titik akhir FIPS. Lihat informasi yang lebih lengkap tentang titik akhir FIPS yang tersedia di Standar Pemrosesan Informasi Federal (FIPS) 140-2.

Kami sangat merekomendasikan agar Anda tidak pernah memasukkan informasi identifikasi yang sensitif, seperti nomor rekening pelanggan Anda, ke dalam tanda atau bidang isian bebas seperti bidang Nama. Ini termasuk saat Anda bekerja dengan re:Post Private atau lainnya AWS layanan menggunakan konsol, API AWS CLI, atau AWS SDK. Data apa pun yang Anda masukkan ke dalam tanda atau bidang isian bebas yang digunakan untuk nama dapat digunakan untuk log penagihan atau log diagnostik. Saat Anda memberikan URL ke server eksternal, kami sangat menganjurkan

supaya Anda tidak menyertakan informasi kredensial di dalam URL untuk memvalidasi permintaan Anda ke server itu.

Melindungi data dengan enkripsi

Enkripsi diam

RE:Post Private menggunakan bucket Amazon Simple Storage Service, database Amazon DynamoDB, database Amazon Neptune, dan domain Layanan Amazon yang dienkripsi saat istirahat menggunakan kunci OpenSearch terkelola Amazon atau kunci yang dikelola pelanggan.

Enkripsi bergerak

Re: Post Private menggunakan protokol HTTPS untuk berkomunikasi dengan aplikasi klien Anda. Menggunakan HTTPS dan AWS tanda tangan untuk berkomunikasi dengan layanan lain atas nama aplikasi Anda.

Manajemen kunci

RE: Post Private terintegrasi dengan AWS Key Management Service dan mendukung AWS KMS kunci. Anda dapat menyesuaikan pengaturan enkripsi data untuk Re:Post pribadi Anda saat Anda membuatnya. Untuk melakukannya, Anda dapat memilih AWS KMS kunci yang ada atau membuat AWS KMS kunci baru.

Bagaimana re:Post Private bekerja dengan IAM

Sebelum Anda menggunakan IAM untuk mengelola akses ke AWS re:Post Private, Anda harus memahami fitur IAM mana yang tersedia untuk digunakan dengan re:Post Private. Untuk mendapatkan tampilan tingkat tinggi tentang bagaimana RE:Post Private dan AWS layanan lainnya bekerja dengan IAM, lihat AWS layanan yang bekerja dengan IAM di Panduan Pengguna IAM.

re:post Kebijakan berbasis identitas pribadi

Dengan kebijakan berbasis identitas IAM, Anda dapat menentukan tindakan yang diizinkan atau ditolak. re:Post Private mendukung tindakan tertentu. Untuk mempelajari semua elemen yang Anda gunakan dalam kebijakan JSON, lihat Referensi elemen kebijakan JSON IAM dalam Panduan Pengguna IAM.

Tindakan

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

Elemen `Action` dari kebijakan JSON menjelaskan tindakan yang dapat Anda gunakan untuk mengizinkan atau menolak akses dalam sebuah kebijakan. Tindakan kebijakan biasanya memiliki nama yang sama dengan operasi AWS API terkait. Ada beberapa pengecualian, misalnya tindakan hanya izin yang tidak memiliki operasi API yang cocok. Ada juga beberapa operasi yang memerlukan beberapa tindakan dalam suatu kebijakan. Tindakan tambahan ini disebut tindakan dependen.

Menyertakan tindakan dalam kebijakan untuk memberikan izin untuk melakukan operasi terkait.

Tindakan kebijakan di re:Post Private gunakan awalan berikut sebelum tindakan:. `repostspace:` Misalnya, untuk memberikan izin kepada seseorang untuk menjalankan operasi RE:Post Private `CreateSpace` API, Anda menyertakan `repostspace:CreateSpace` tindakan tersebut dalam kebijakan mereka. Pernyataan kebijakan harus menyertakan `NotAction` elemen `Action` atau. re:Post Private mendefinisikan serangkaian tindakannya sendiri yang menjelaskan tugas yang dapat Anda lakukan dengan layanan ini.

Untuk menetapkan beberapa tindakan dalam satu pernyataan, pisahkan dengan koma seperti berikut:

```
"Action": [
      "repostspace:CreateSpace",
      "repostspace:DeleteSpace"
```

Anda dapat menentukan beberapa tindakan menggunakan wildcard (*). Sebagai contoh, untuk menentukan semua tindakan yang dimulai dengan kata `Describe`, sertakan tindakan berikut:

```
"Action": "repostspace:Describe*"
```

Untuk melihat daftar tindakan Re:Post Private, lihat Tindakan yang ditentukan oleh re:Post Private di Panduan Pengguna IAM.

Sumber daya

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

Elemen kebijakan JSON `Resource` menentukan objek yang menjadi target penerapan tindakan. Pernyataan harus menyertakan elemen `Resource` atau `NotResource`. Praktik terbaiknya, tentukan sumber daya menggunakan Amazon Resource Name (ARN). Anda dapat melakukan ini untuk tindakan yang mendukung jenis sumber daya tertentu, yang dikenal sebagai izin tingkat sumber daya.

Untuk tindakan yang tidak mendukung izin di tingkat sumber daya, misalnya operasi pencantuman, gunakan wildcard (*) untuk menunjukkan bahwa pernyataan tersebut berlaku untuk semua sumber daya.

```
"Resource": "*"
```

Kunci syarat

re:post Private tidak menyediakan kunci kondisi khusus layanan apa pun, tetapi mendukung penggunaan kunci kondisi global. Untuk melihat semua kunci kondisi AWS global, lihat kunci konteks kondisi AWS global di Panduan Pengguna IAM.

Contoh

Untuk melihat contoh kebijakan berbasis identitas Re:Post Private, lihat. AWS re: Posting contoh kebijakan berbasis identitas pribadi

RE: posting Kebijakan berbasis sumber daya pribadi

Kebijakan berbasis sumber daya adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah kebijakan kepercayaan peran IAM 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 AWS terkelola dari IAM dalam kebijakan berbasis sumber daya.

re:Post Private tidak mendukung kebijakan berbasis sumber daya.

Otorisasi berdasarkan tanda

Re: Post Private mendukung penandaan sumber daya atau mengontrol akses berdasarkan tag. Untuk informasi selengkapnya, lihat Mengontrol akses ke sumber daya AWS menggunakan tag.

Re: posting peran IAM Pribadi

Peran IAM adalah entitas dalam AWS akun Anda yang memiliki izin tertentu.

Menggunakan kredensyal sementara dengan re:Post Private

Kami sangat menyarankan menggunakan kredensil sementara untuk masuk dengan federasi, mengambil peran IAM, atau untuk mengambil peran lintas akun. Anda memperoleh kredensil keamanan sementara dengan memanggil operasi AWS STS API seperti AssumeRoleatau. GetFederationToken

re:Post Private mendukung menggunakan kredensyal sementara.

Peran terkait layanan

Peran terkait AWS layanan memungkinkan layanan mengakses sumber daya di layanan lain untuk menyelesaikan tindakan bagi Anda. Peran terkait layanan muncul di akun IAM Anda dan dimiliki oleh layanan tersebut. Administrator IAM dapat melihat tetapi tidak dapat mengedit izin untuk peran terkait layanan.

Peran layanan

Fitur ini memungkinkan layanan untuk mengambil peran layanan untuk Anda. Peran ini memungkinkan layanan untuk mengakses sumber daya di layanan lain untuk menyelesaikan tindakan untuk Anda. Untuk informasi selengkapnya, lihat Membuat peran untuk mendelegasikan izin ke layanan AWS. Peran layanan muncul di akun IAM Anda dan dimiliki oleh akun tersebut. Ini berarti administrator IAM dapat mengubah izin untuk peran ini. Namun, melakukan hal itu dapat merusak fungsionalitas layanan.

Menggunakan peran terkait layanan untuk re:Post Private

AWS re:Post Private menggunakan peran terkait AWS Identity and Access Management layanan (IAM). Peran terkait layanan adalah jenis unik peran IAM yang ditautkan langsung ke re:Post Private. Peran terkait layanan telah ditentukan sebelumnya oleh Re:Post Private dan mencakup semua izin yang diperlukan layanan untuk memanggil layanan lain atas nama Anda. AWS

Peran terkait layanan membuat pengaturan re:Post Private lebih mudah karena Anda tidak perlu menambahkan izin yang diperlukan secara manual. re:Post Private mendefinisikan izin peran terkait layanan, dan kecuali ditentukan lain, hanya re:Post Private yang dapat mengambil perannya. Izin yang ditentukan mencakup kebijakan kepercayaan dan kebijakan izin, serta bahwa kebijakan izin tidak dapat dilampirkan ke entitas IAM lainnya.

Untuk informasi tentang layanan lain yang mendukung peran terkait layanan, lihat Layanan AWS yang Bekerja bersama IAM dan mencari layanan yang memiliki Ya dalam Peran Terkait Layanan. Pilih Ya bersama tautan untuk melihat dokumentasi peran tertaut layanan untuk layanan tersebut.

Izin peran terkait layanan untuk Re:Post Private

re:Post Private menggunakan peran terkait layanan bernama AWSServiceRoleForrePostPrivate. re:Post Private menggunakan peran terkait layanan ini untuk mempublikasikan data. CloudWatch

Peran AWSServiceRoleForrePostPrivate terkait layanan mempercayai layanan berikut untuk mengambil peran:

- `repostspace.amazonaws.com`

Kebijakan izin peran bernama `AWSrePostPrivateCloudWatchAccess` memungkinkan re:Post Private untuk menyelesaikan tindakan berikut pada sumber daya yang ditentukan:

- Aksi pada`cloudwatch`: `PutMetricData`

Anda harus mengonfigurasi izin agar pengguna, grup, atau peran Anda membuat, mengedit, atau menghapus peran terkait layanan. Untuk informasi selengkapnya, lihat Izin peran tertaut layanan dalam Panduan Pengguna IAM.

Untuk informasi selengkapnya, lihat AWSrePostPrivateCloudWatchAccess.

Membuat peran terkait layanan untuk Re:Post Private

Anda tidak perlu membuat peran terkait layanan secara manual. Saat Anda membuat re:Post pribadi pertama Anda di AWS Management Console, the, atau AWS API AWS CLI, re:Post Private membuat peran terkait layanan untuk Anda.

> **Important**
>
> Peran tertaut layanan ini dapat muncul di akun Anda jika Anda menyelesaikan tindakan di layanan lain yang menggunakan fitur yang disupport oleh peran ini. Juga, jika Anda menggunakan layanan re:Post Private sebelum 1 Desember 2023, ketika mulai mendukung peran terkait layanan, maka Re:Post Private membuat peran di akun Anda. `AWSServiceRoleForrePostPrivate` Untuk mempelajari lebih lanjut, lihat Peran baru muncul di saya Akun AWS.

Jika Anda menghapus peran tertaut layanan ini, dan ingin membuatnya lagi, Anda dapat mengulangi proses yang sama untuk membuat kembali peran tersebut di akun Anda. Saat Anda membuat re:Post pribadi pertama Anda, re:Post Private membuat peran terkait layanan untuk Anda lagi.

Di AWS CLI atau AWS API, buat peran terkait layanan dengan nama `repostspace.amazonaws.com` layanan. Untuk informasi selengkapnya, lihat Membuat peran tertaut layanan dalam Panduan Pengguna IAM. Jika Anda menghapus peran tertaut layanan ini, Anda dapat mengulang proses yang sama untuk membuat peran tersebut lagi.

Mengedit peran terkait layanan untuk re:Post Private

Re:post Private tidak mengizinkan Anda mengedit peran terkait `AWSServiceRoleForrePostPrivate` layanan. Setelah membuat peran terkait layanan, Anda tidak dapat mengubah nama peran karena berbagai entitas mungkin mereferensikan peran tersebut. Namun, Anda dapat menyunting penjelasan peran menggunakan IAM. Untuk informasi selengkapnya, lihat Mengedit peran tertaut layanan dalam Panduan Pengguna IAM.

Menghapus peran terkait layanan untuk re:Post Private

Anda tidak perlu menghapus peran `AWSServiceRoleForrePostPrivate` secara manual. Saat Anda menghapus re:Post pribadi Anda di AWS Management Console, the, atau AWS API AWS CLI, re:Post Private menghapus peran terkait layanan untuk Anda.

Anda juga dapat menggunakan konsol IAM, the AWS CLI, atau AWS API untuk menghapus peran terkait layanan secara manual.

Untuk menghapus peran terkait layanan secara manual menggunakan IAM

Gunakan konsol IAM, the AWS CLI, atau AWS API untuk menghapus peran AWSServiceRoleForrePostPrivate terkait layanan. Untuk informasi selengkapnya, lihat Menghapus peran tertaut layanan dalam Panduan Pengguna IAM.

Wilayah yang Didukung untuk re:Post Peran terkait layanan pribadi

Re:Post Private mendukung penggunaan peran terkait layanan di AWS Wilayah tempat layanan tersedia.

Nama Wilayah	Identitas wilayah	Support di re:Post Private
US East (Northern Virginia)	us-east-1	Ya
US East (Ohio)	us-east-2	Tidak
US West (Northern California)	us-west-1	Tidak
AS Barat (Oregon)	us-west-2	Ya
Afrika (Cape Town)	af-south-1	Tidak
Asia Pasifik (Hong Kong)	ap-east-1	Tidak
Asia Pasifik (Jakarta)	ap-southeast-3	Tidak
Asia Pasifik (Mumbai)	ap-south-1	Tidak
Asia Pacific (Osaka)	ap-northeast-3	Tidak
Asia Pasifik (Seoul)	ap-northeast-2	Tidak
Asia Pasifik (Singapura)	ap-southeast-1	Ya
Asia Pacific (Sydney)	ap-southeast-2	Ya
Asia Pacific (Tokyo)	ap-northeast-1	Tidak

Nama Wilayah	Identitas wilayah	Support di re:Post Private
Kanada (Pusat)	ca-sentral-1	Ya
Eropa (Frankfurt)	eu-central-1	Ya
Eropa (Irlandia)	eu-west-1	Ya
Eropa (London)	eu-west-2	Tidak
Eropa (Milan)	eu-south-1	Tidak
Eropa (Paris)	eu-west-3	Tidak
Eropa (Stockholm)	eu-north-1	Tidak
Timur Tengah (Bahrain)	me-south-1	Tidak
Timur Tengah (UEA)	me-central-1	Tidak
Amerika Selatan (Sao Paulo)	sa-east-1	Tidak

AWS re: Posting contoh kebijakan berbasis identitas pribadi

> **Note**
>
> Untuk keamanan yang lebih besar, buat pengguna federasi alih-alih pengguna IAM bila memungkinkan.

Secara default, AWS Identity and Access Management pengguna dan peran tidak memiliki izin untuk membuat atau memodifikasi sumber daya AWS re:Post Private. Mereka juga tidak dapat melakukan tugas menggunakan AWS Management Console, AWS CLI, atau AWS API. Administrator IAM harus membuat kebijakan IAM yang memberikan 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 berbasis identitas IAM menggunakan contoh dokumen kebijakan JSON ini, lihat Membuat kebijakan IAM di Panduan Pengguna IAM.

Topik

- Praktik terbaik kebijakan
- Mengizinkan pengguna melihat izin mereka sendiri

Praktik terbaik kebijakan

Kebijakan berbasis identitas menentukan apakah seseorang dapat membuat, mengakses, atau menghapus sumber daya Re:Post Private di akun Anda. Tindakan ini membuat Akun AWS Anda dikenai biaya. Ketika Anda membuat atau mengedit kebijakan berbasis identitas, ikuti panduan dan rekomendasi ini:

- Mulailah dengan kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit — Untuk mulai memberikan izin kepada pengguna dan beban kerja Anda, gunakan kebijakan AWS terkelola yang memberikan izin untuk banyak kasus penggunaan umum. Mereka tersedia di Anda Akun AWS. Kami menyarankan Anda mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola AWS pelanggan yang khusus untuk kasus penggunaan Anda. Untuk informasi selengkapnya, lihat Kebijakan yang dikelola AWS atau Kebijakan yang dikelola AWS untuk fungsi tugas dalam Panduan Pengguna IAM.
- Menerapkan izin dengan hak akses paling rendah – Ketika Anda menetapkan izin dengan kebijakan IAM, hanya berikan izin yang diperlukan untuk melakukan tugas. Anda melakukannya dengan mendefinisikan tindakan yang dapat diambil pada sumber daya tertentu dalam kondisi tertentu, yang juga dikenal sebagai izin dengan hak akses paling rendah. Untuk informasi selengkapnya tentang cara menggunakan IAM untuk mengajukan izin, lihat Kebijakan dan izin dalam IAM dalam Panduan Pengguna IAM.
- Gunakan kondisi dalam kebijakan IAM untuk membatasi akses lebih lanjut – Anda dapat menambahkan suatu kondisi ke kebijakan Anda untuk membatasi akses ke tindakan dan sumber daya. Sebagai contoh, Anda dapat menulis kondisi kebijakan untuk menentukan bahwa semua permintaan harus dikirim menggunakan SSL. Anda juga dapat menggunakan ketentuan untuk memberikan akses ke tindakan layanan jika digunakan melalui yang spesifik AWS layanan, seperti AWS CloudFormation. Untuk informasi selengkapnya, lihat Elemen kebijakan JSON IAM: Kondisi dalam Panduan Pengguna IAM.
- Gunakan IAM Access Analyzer untuk memvalidasi kebijakan IAM Anda untuk memastikan izin yang aman dan fungsional – IAM Access Analyzer memvalidasi kebijakan baru dan yang sudah ada sehingga kebijakan tersebut mematuhi bahasa kebijakan IAM (JSON) dan praktik terbaik IAM. IAM Access Analyzer menyediakan lebih dari 100 pemeriksaan kebijakan dan rekomendasi yang dapat ditindaklanjuti untuk membantu Anda membuat kebijakan yang aman dan fungsional. Untuk

informasi selengkapnya, lihat Validasi kebijakan IAM Access Analyzer dalam Panduan Pengguna IAM.

- Memerlukan otentikasi multi-faktor (MFA) - Jika Anda memiliki skenario yang mengharuskan pengguna IAM atau pengguna root di Anda, Akun AWS aktifkan MFA untuk keamanan tambahan. Untuk meminta MFA ketika operasi API dipanggil, tambahkan kondisi MFA pada kebijakan Anda. Untuk informasi selengkapnya, lihat Mengonfigurasi akses API yang dilindungi MFA dalam Panduan Pengguna IAM.

Untuk informasi selengkapnya tentang praktik terbaik dalam IAM, lihat Praktik terbaik keamanan dalam IAM dalam Panduan Pengguna IAM.

Mengizinkan pengguna melihat izin mereka sendiri

Contoh ini menunjukkan cara membuat kebijakan yang mengizinkan pengguna IAM melihat kebijakan inline dan terkelola yang dilampirkan ke identitas pengguna mereka. Kebijakan ini mencakup izin untuk menyelesaikan tindakan ini di konsol atau menggunakan API atau secara terprogram. AWS CLI AWS

```
{
    "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 inline

Kebijakan inline adalah kebijakan yang Anda buat dan kelola. Anda dapat menyematkan kebijakan sebaris langsung ke pengguna, grup, atau peran. Contoh kebijakan berikut menunjukkan cara menetapkan izin untuk melakukan tindakan AWS re:Post Private. Untuk informasi umum tentang kebijakan sebaris, lihat Mengelola kebijakan IAM di Panduan Pengguna AWS IAM. Anda dapat menggunakan AWS Management Console, AWS Command Line Interface (AWS CLI), atau AWS Identity and Access Management API untuk membuat dan menyematkan kebijakan sebaris.

Topik

- Akses hanya-baca ke re:Post Private
- Akses penuh ke re:Post Private

Akses hanya-baca ke re:Post Private

Kebijakan berikut memberikan akses baca ke pengguna untuk IAM Identity Center dan konsol Re:Post Private. Kebijakan ini memungkinkan pengguna untuk melakukan tindakan Re:Post Private yang hanya dibaca.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "organizations:DescribeOrganization",
                "organizations:DescribeAccount",

                "sso:DescribeRegisteredRegions",
```

```
                "sso:ListDirectoryAssociations",
                "sso:GetSSOStatus",
                "sso:GetManagedApplicationInstance",
                "sso:ListProfiles",
                "sso:GetProfile",
                "sso:ListProfileAssociations",

                "sso-directory:DescribeDirectory",
                "sso-directory:SearchUsers",
                "sso-directory:SearchGroups",

                "repostspace:GetSpace",
                "repostspace:ListSpaces",
                "repostspace:ListTagsForResource"
            ],
            "Resource": "*"
        }
    ]
}
```

Akses penuh ke re:Post Private

Kebijakan berikut memberikan akses penuh ke pengguna untuk IAM Identity Center dan konsol Re:Post Private. Kebijakan ini memungkinkan pengguna untuk melakukan semua tindakan Re:Post Private.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "organizations:DescribeOrganization",
                "organizations:DescribeAccount",

                "sso:DescribeRegisteredRegions",
                "sso:ListDirectoryAssociations",
                "sso:GetSSOStatus",
                "sso:GetManagedApplicationInstance",
                "sso:ListProfiles",
```

```
                "sso:GetProfile",
                "sso:ListProfileAssociations",

                "sso:CreateManagedApplicationInstance",
                "sso:DeleteManagedApplicationInstance",
                "sso:AssociateProfile",
                "sso:DisassociateProfile",

                "sso-directory:DescribeDirectory",
                "sso-directory:SearchUsers",
                "sso-directory:SearchGroups",

                "kms:ListAliases",
                "kms:DescribeKey",
                "kms:CreateGrant",
                "kms:RetireGrant",

                "repostspace:*"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS kebijakan terkelola untuk AWS re: Post Private

Menggunakan kebijakan AWS terkelola membuat menambahkan izin ke pengguna, grup, dan peran lebih mudah daripada menulis kebijakan sendiri. Dibutuhkan waktu dan keahlian untuk membuat kebijakan terkelola pelanggan IAM yang hanya memberi tim Anda izin yang mereka butuhkan. Gunakan kebijakan AWS terkelola untuk memulai dengan cepat. Kebijakan ini mencakup kasus penggunaan umum dan tersedia di AWS akun Anda. Untuk informasi selengkapnya tentang kebijakan AWS AWS terkelola, lihat kebijakan terkelola di Panduan Pengguna IAM.

AWS layanan memelihara dan memperbarui kebijakan AWS terkelola. Anda tidak dapat mengubah izin dalam kebijakan AWS terkelola. Layanan terkadang menambahkan izin tambahan ke kebijakan AWS terkelola untuk mendukung fitur baru. Jenis pembaruan ini akan memengaruhi semua identitas (pengguna, grup, dan peran) di mana kebijakan tersebut dilampirkan. Layanan kemungkinan besar akan memperbarui kebijakan AWS terkelola saat fitur baru diluncurkan atau saat operasi baru tersedia. Layanan tidak menghapus izin dari kebijakan AWS terkelola, sehingga pembaruan kebijakan tidak merusak izin yang ada.

Selain itu, AWS mendukung kebijakan terkelola untuk fungsi pekerjaan yang mencakup beberapa layanan. Misalnya, kebijakan `ReadOnlyAccess` AWS terkelola menyediakan akses hanya-baca ke semua AWS layanan dan sumber daya. Saat layanan meluncurkan fitur baru, AWS tambahkan izin hanya-baca untuk operasi dan sumber daya baru. Untuk informasi selengkapnya, lihat AWS kebijakan yang dikelola dalam Panduan Pengguna IAM.

Topik

- AWS kebijakan terkelola: AWSRepostSpaceSupportOperationsPolicy
- AWS kebijakan terkelola: AWSrePostPrivateCloudWatchAccess
- AWS re:Posting pembaruan Pribadi ke AWS kebijakan terkelola

AWS kebijakan terkelola: AWSRepostSpaceSupportOperationsPolicy

Kebijakan ini memungkinkan layanan AWS re:Post Private untuk membuat, mengelola, dan menyelesaikan AWS Support kasus yang dibuat melalui aplikasi web re:Post Private.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "RepostSpaceSupportOperations",
   "Effect": "Allow",
   "Action": [
    "support:AddAttachmentsToSet",
    "support:AddCommunicationToCase",
    "support:CreateCase",
    "support:DescribeCases",
    "support:DescribeCommunications",
    "support:ResolveCase"
   ],
   "Resource": "*"
  }
 ]
}
```

AWS kebijakan terkelola: AWSrePostPrivateCloudWatchAccess

Kebijakan ini memungkinkan layanan Re:Post Private untuk mempublikasikan data ke. CloudWatch

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "CloudWatchPublishMetrics",
   "Effect": "Allow",
   "Action": [
    "cloudwatch:PutMetricData"
   ],
   "Resource": "*",
   "Condition": {
    "StringEquals": {
     "cloudwatch:namespace": [
      "AWS/rePostPrivate",
      "AWS/Usage"
     ]
    }
   }
  }
 ]
}
```

AWS re:Posting pembaruan Pribadi ke AWS kebijakan terkelola

Lihat detail tentang pembaruan kebijakan AWS terkelola untuk re:Post Private sejak layanan ini mulai melacak perubahan ini. Untuk peringatan otomatis tentang perubahan pada halaman ini, berlangganan ke umpan RSS pada halaman Riwayat dokumen.

Tabel berikut menjelaskan pembaruan penting pada kebijakan yang dikelola Re:Post Private sejak 26 November 2023.

Perubahan	Deskripsi	Tanggal
Kebijakan baru - AWSrePost PrivateCloudWatchAccess	Kebijakan terkelola baru untuk mempublikasikan data ke CloudWatch	26 November 2023

Perubahan	Deskripsi	Tanggal
Kebijakan baru - AWSRepostSpaceSupportOperationsPolicy	Kebijakan terkelola baru untuk fitur AWS Support di AWS re:Post Private	26 November 2023
Re: Post Private mulai melacak perubahan	re:post Private mulai melacak perubahan untuk kebijakan yang dikelola AWS	26 November 2023

Pemecahan masalah AWS re: Posting identitas dan akses pribadi

Gunakan informasi berikut untuk membantu Anda mendiagnosis dan memperbaiki masalah umum yang mungkin Anda temui saat bekerja dengan Re:Post Private dan IAM.

Topik

- Saya tidak berwenang untuk melakukan tindakan di re:Post Private
- Saya tidak berwenang untuk melakukan iam: PassRole
- Saya ingin mengizinkan orang di luar saya Akun AWS untuk mengakses sumber daya Re:Post Private saya

Saya tidak berwenang untuk melakukan tindakan di re:Post Private

Jika Anda menerima pesan kesalahan bahwa Anda tidak memiliki otorisasi untuk melakukan tindakan, kebijakan Anda harus diperbarui agar Anda dapat melakukan tindakan tersebut.

Contoh kesalahan berikut terjadi ketika pengguna IAM `mateojackson` mencoba menggunakan konsol untuk melihat detail tentang suatu sumber daya *`my-example-widget`* rekaan, tetapi tidak memiliki izin `repostPrivate:`*`GetWidget`* rekaan.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 repostPrivate:GetWidget on resource: my-example-widget
```

Dalam hal ini, kebijakan untuk pengguna `mateojackson` harus diperbarui untuk mengizinkan akses ke sumber daya *`my-example-widget`* dengan menggunakan tindakan `repostPrivate:`*`GetWidget`*.

Jika Anda memerlukan bantuan, hubungi AWS administrator Anda. Administrator Anda adalah orang yang memberi Anda kredensial masuk.

Saya tidak berwenang untuk melakukan iam: PassRole

Jika Anda menerima kesalahan bahwa Anda tidak berwenang untuk melakukan `iam:PassRole` tindakan, kebijakan Anda harus diperbarui agar Anda dapat meneruskan peran ke Re:Post Private.

Beberapa AWS layanan memungkinkan Anda untuk meneruskan peran yang ada ke layanan tersebut alih-alih membuat peran layanan baru atau peran terkait layanan. Untuk melakukannya, Anda harus memiliki izin untuk meneruskan peran ke layanan.

Contoh kesalahan berikut terjadi ketika pengguna IAM bernama `marymajor` mencoba menggunakan konsol untuk melakukan tindakan di RE:Post Private. Namun, tindakan tersebut memerlukan layanan untuk mendapatkan izin yang diberikan oleh peran layanan. Mary tidak memiliki izin untuk meneruskan peran tersebut pada layanan.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Dalam kasus ini, kebijakan Mary harus diperbarui agar dia mendapatkan izin untuk melakukan tindakan `iam:PassRole` tersebut.

Jika Anda memerlukan bantuan, hubungi AWS administrator Anda. Administrator Anda adalah orang yang memberi Anda kredensial masuk.

Saya ingin mengizinkan orang di luar saya Akun AWS untuk mengakses sumber daya Re:Post Private saya

Anda dapat membuat peran yang dapat digunakan pengguna di akun lain atau orang-orang di luar organisasi Anda untuk mengakses sumber daya Anda. Anda dapat menentukan siapa saja yang dipercaya untuk mengambil peran tersebut. Untuk layanan yang mendukung kebijakan berbasis sumber daya atau daftar kontrol akses (ACL), Anda dapat menggunakan kebijakan tersebut untuk memberi orang akses ke sumber daya Anda.

Untuk mempelajari selengkapnya, periksa referensi berikut:

- Untuk mengetahui apakah re:Post Private mendukung fitur-fitur ini, lihat. Bagaimana re:Post Private bekerja dengan IAM

- Untuk mempelajari cara menyediakan akses ke sumber daya Anda di seluruh sumber daya Akun AWS yang Anda miliki, lihat Menyediakan akses ke pengguna IAM di pengguna lain Akun AWS yang Anda miliki di Panduan Pengguna IAM.
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda kepada pihak ketiga Akun AWS, lihat Menyediakan akses yang Akun AWS dimiliki oleh pihak ketiga dalam Panduan Pengguna IAM.
- Untuk mempelajari cara memberikan akses melalui federasi identitas, lihat Menyediakan akses ke pengguna terautentikasi eksternal (federasi identitas) dalam Panduan Pengguna IAM.
- Untuk mempelajari perbedaan antara menggunakan peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Akses sumber daya lintas akun di IAM di Panduan Pengguna IAM.

Validasi kepatuhan untuk AWS re: Post Private

Untuk mempelajari apakah an AWS layanan berada dalam lingkup program kepatuhan tertentu, lihat AWS layanan di Lingkup oleh Program Kepatuhan AWS layanan dan pilih program kepatuhan yang Anda minati. Untuk informasi umum, lihat Program AWS Kepatuhan Program AWS .

Anda dapat mengunduh laporan audit pihak ketiga menggunakan AWS Artifact. Untuk informasi selengkapnya, lihat Mengunduh Laporan di AWS Artifact .

Tanggung jawab kepatuhan Anda saat menggunakan AWS layanan ditentukan oleh sensitivitas data Anda, tujuan kepatuhan perusahaan Anda, dan hukum dan peraturan yang berlaku. AWS menyediakan sumber daya berikut untuk membantu kepatuhan:

- Panduan Memulai Cepat Keamanan dan Kepatuhan — Panduan penerapan ini membahas pertimbangan arsitektur dan memberikan langkah-langkah untuk menerapkan lingkungan dasar AWS yang berfokus pada keamanan dan kepatuhan.
- Arsitektur untuk Keamanan dan Kepatuhan HIPAA di Amazon Web Services — Whitepaper ini menjelaskan bagaimana perusahaan dapat menggunakan AWS untuk membuat aplikasi yang memenuhi syarat HIPAA.

> **Note**
>
> Tidak semua memenuhi AWS layanan syarat HIPAA. Untuk informasi selengkapnya, lihat Referensi Layanan yang Memenuhi Syarat HIPAA.

- AWS Sumber Daya AWS — Kumpulan buku kerja dan panduan ini mungkin berlaku untuk industri dan lokasi Anda.
- AWS Panduan Kepatuhan Pelanggan - Memahami model tanggung jawab bersama melalui lensa kepatuhan. Panduan ini merangkum praktik terbaik untuk mengamankan AWS layanan dan memetakan panduan untuk kontrol keamanan di berbagai kerangka kerja (termasuk Institut Standar dan Teknologi Nasional (NIST), Dewan Standar Keamanan Industri Kartu Pembayaran (PCI), dan Organisasi Internasional untuk Standardisasi (ISO)).
- Mengevaluasi Sumber Daya dengan Aturan dalam Panduan AWS Config Pengembang — AWS Config Layanan menilai seberapa baik konfigurasi sumber daya Anda mematuhi praktik internal, pedoman industri, dan peraturan.
- AWS Security Hub— Ini AWS layanan memberikan pandangan komprehensif tentang keadaan keamanan Anda di dalamnya AWS. Security Hub menggunakan kontrol keamanan untuk sumber daya AWS Anda serta untuk memeriksa kepatuhan Anda terhadap standar industri keamanan dan praktik terbaik. Untuk daftar layanan dan kontrol yang didukung, lihat Referensi kontrol Security Hub.
- Amazon GuardDuty — Ini AWS layanan mendeteksi potensi ancaman terhadap beban kerja Akun AWS, kontainer, dan data Anda dengan memantau lingkungan Anda untuk aktivitas mencurigakan dan berbahaya. GuardDuty dapat membantu Anda mengatasi berbagai persyaratan kepatuhan, seperti PCI DSS, dengan memenuhi persyaratan deteksi intrusi yang diamanatkan oleh kerangka kerja kepatuhan tertentu.
- AWS Audit ManagerIni AWS layanan membantu Anda terus mengaudit AWS penggunaan Anda untuk menyederhanakan cara Anda mengelola risiko dan kepatuhan terhadap peraturan dan standar industri.

Ketahanan di AWS re: Post Private

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 dengan latensi rendah, throughput tinggi, dan jaringan yang 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.

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

Keamanan Infrastruktur di AWS re: Post Private

Sebagai layanan terkelola, AWS re:Post Private dilindungi oleh prosedur keamanan jaringan AWS global yang dijelaskan dalam whitepaper Amazon Web Services: Tinjauan Proses Keamanan.

Anda menggunakan panggilan API yang AWS dipublikasikan untuk mengakses re:Post Private melalui jaringan. Klien harus mendukung Keamanan Lapisan Pengangkutan (TLS) 1.0 atau versi yang lebih baru. Kami merekomendasikan TLS 1.2 atau versi yang lebih baru. Klien juga harus mendukung suite cipher dengan perfect forward secrecy (PFS) seperti Ephemeral Diffie-Hellman (DHE) atau Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). Sebagian besar sistem modern seperti Java 7 dan versi lebih baru mendukung mode-mode ini.

Selain itu, permintaan harus ditandatangani dengan menggunakan ID kunci akses dan kunci akses rahasia yang terkait dengan AWS Identity and Access Management prinsipal. Atau Anda bisa menggunakan AWS Security Token Service (AWS STS) untuk membuat kredensial keamanan sementara guna menandatangani permintaan.

RE: posting kuota pribadi

AWS re:Post Private menyediakan re:Postingan pribadi yang dapat Anda gunakan di akun Anda di Wilayah tertentu. AWS Ketika Anda mendaftar untuk re:Post Private, AWS menetapkan kuota default (sebelumnya disebut sebagai batas) pada jumlah private re:Posts yang dapat Anda buat dan ukuran private re:Posts.

Kuota layanan

Berikut ini adalah kuota default untuk re:Post Private untuk akun Anda. AWS Anda dapat menggunakan konsol Service Quotas untuk melihat kuota default. Tak satu pun dari kuota ini dapat disesuaikan. Anda tidak dapat meminta kenaikan kuota.

Sumber daya	Default	Deskripsi	Dapat Disesuaikan
Jumlah Re pribadi: Posting	3	Jumlah maksimum Re: Posting pribadi di akun ini di Wilayah saat ini.	Tidak
Re pribadi gratis: Ukuran pos	10	Ukuran maksimum (dalam GB) dari Re: post pribadi gratis.	Tidak
Re pribadi standar: Ukuran pos	100	Ukuran maksimum (dalam GB) dari Re: post pribadi standar.	Tidak

Batas pelambatan API

Batas pembatasan berikut berlaku per akun, per Wilayah di re:Post Private. Kuota ini tidak dapat ditingkatkan.

Tindakan	Tingkat isi ulang token	Tingkat permintaan	
CreateSpace	1	1	

Tindakan	Tingkat isi ulang token	Tingkat permintaan	
ListSpaces	10	10	
GetSpace	10	10	
UpdateSpace	10	10	
DeleteSpace	1	1	
RegisterAdmin	10	100	
DeRegisterAdmin	10	100	
SendInvites	1	1	
TagResource	10	10	
UnTagResource	10	10	
ListTagsForResource	10	10	

Buat, konfigurasikan, dan sesuaikan Re: post pribadi Anda

Topik

- Buat re:Post pribadi baru
- Mengelola akses ke pembuatan dan manajemen AWS Support kasus di re:Post Private
- Mengatur dan mengelola akses pengguna menggunakan AWS IAM Identity Center
- Kustomisasi re:Post pribadi Anda
- Undang pengguna ke Re:Post pribadi Anda

Buat re:Post pribadi baru

Untuk membuat re:Post pribadi baru, ikuti langkah-langkah berikut:

1. Buka konsol Re:Post Private di https://console.aws.amazon.com/repost-private/.
2. Di beranda konsol, pilih Create private re:post.
3. Jika Anda belum memiliki IAM Identity Center yang dikonfigurasi untuk akun Anda, pilih Open Identity Center. Ikuti petunjuk di Memulai di Panduan Pengguna AWS IAM Identity Center.
4. Pada halaman Create private re:Post, untuk Harga, pilih Tingkat gratis atau Tingkat Standar berdasarkan kasus penggunaan Anda. Jika Anda sudah menggunakan Tingkat Gratis untuk akun Anda, maka opsi tingkat gratis tidak tersedia untuk Anda.
5. Di bawah Detail, lakukan hal berikut:

   Untuk Nama, masukkan nama unik untuk Re:post pribadi Anda.

   (Opsional) Untuk Deskripsi, masukkan deskripsi singkat untuk Re:post pribadi Anda.

   Untuk subdomain kustom, masukkan nama kustom untuk subdomain Anda.
6. (Opsional) Untuk menyesuaikan pengaturan enkripsi data Anda, di bawah Enkripsi data, pilih Sesuaikan pengaturan enkripsi. Kemudian, lakukan salah satu dari tindakan berikut:

   Untuk Memilih kunci AWS KMS, pilih AWS Key Management Service kunci atau Nama Sumber Daya Amazon (ARN).

   -atau-

Pilih Buat kunci AWS KMS. Kemudian, buat AWS KMS kuncinya.

7. (Opsional) Di bawah Akses layanan untuk integrasi kasus Support, pilih Aktifkan akses layanan untuk re:Post ini.

> **Note**
>
> Anda juga dapat mengaktifkan opsi ini setelah Anda membuat re:post pribadi.

Untuk Silakan pilih peran IAM yang ada di bawah ini atau buat peran baru di konsol IAM, gunakan bilah pencarian untuk menemukan peran IAM Anda yang ada.

-atau-

Pilih buat peran baru di konsol IAM.

Jika Anda memilih untuk membuat peran baru, ikuti instruksi diBuat IAM role.

Jika Anda memilih untuk menggunakan peran layanan yang ada, maka di bilah pencarian, masukkan ARN peran yang ingin Anda gunakan. Pilih peran dari daftar dropdown.

Untuk informasi selengkapnya, lihat Mengelola akses ke pembuatan dan manajemen AWS Support kasus di re:Post Private.

8. (Opsional) Di bawah Tag, pilih Tambahkan tag baru. Kemudian masukkan informasi berikut:

   Untuk Key, masukkan kunci tag kustom Anda.

   Untuk Nilai, masukkan nilai tag kustom Anda.

   Untuk menambahkan lebih banyak tag, pilih Tambahkan tag baru.

9. Pilih Buat Re:Post ini.

Halaman konfirmasi akan memberi tahu Anda bahwa Re:post pribadi Anda sedang dibuat. Anda dapat melihat status Re:Post pribadi di bidang Status. Ketika re:Post pribadi Anda dibuat, bidang Status menampilkan Membuat.

Dibutuhkan sekitar 30 menit untuk membuat Re: post pribadi. Ketika Re:Post pribadi Anda siap, bidang Status ditampilkan Online. Anda dapat menggunakan subdomain yang dihasilkan AWS untuk

re:Post pribadi Anda yang tercantum di bawah tab Pengaturan untuk mengakses re:Post pribadi Anda. Anda dapat melihat subdomain khusus untuk Re:Post pribadi Anda di bawah tab Pengaturan setelah peninjauan selesai.

Mengelola akses ke pembuatan dan manajemen AWS Support kasus di re:Post Private

Anda harus membuat peran AWS Identity and Access Management (IAM) untuk mengelola akses ke pembuatan dan manajemen AWS Support kasus dari AWS re:Post Private. Peran ini melakukan AWS Support tindakan berikut untuk Anda:

- CreateCase
- AddCommunicationToCase
- ResolveCase

Setelah Anda membuat peran IAM, lampirkan kebijakan IAM ke peran ini sehingga peran tersebut memiliki izin yang diperlukan untuk menyelesaikan tindakan ini. Anda memilih peran ini ketika Anda membuat Re:Post pribadi Anda di konsol Re:Post Private.

Pengguna di re:Post pribadi Anda memiliki izin yang sama dengan yang Anda berikan untuk peran IAM.

> **Important**
>
> Jika Anda mengubah peran IAM atau kebijakan IAM, maka perubahan Anda berlaku untuk re:post pribadi yang Anda konfigurasi.

Ikuti prosedur ini untuk membuat peran dan kebijakan IAM Anda.

Topik

- Menggunakan kebijakan AWS terkelola atau membuat kebijakan terkelola pelanggan
- Contoh kebijakan IAM
- Buat IAM role
- Pemecahan Masalah

Menggunakan kebijakan AWS terkelola atau membuat kebijakan terkelola pelanggan

Untuk memberikan izin peran, Anda dapat menggunakan kebijakan AWS terkelola atau kebijakan yang dikelola pelanggan.

> **Tip**
>
> Jika Anda tidak ingin membuat kebijakan secara manual, sebaiknya gunakan kebijakan AWS terkelola dan lewati prosedur ini. Kebijakan terkelola secara otomatis memiliki izin yang diperlukan untuk AWS Support. Anda tidak perlu memperbarui kebijakan secara manual. Untuk informasi selengkapnya, lihat AWS kebijakan terkelola: AWSRepostSpaceSupportOperationsPolicy.

Ikuti prosedur ini untuk membuat kebijakan dikelola pelanggan untuk peran Anda. Prosedur ini menggunakan editor kebijakan JSON di konsol IAM.

Untuk membuat kebijakan terkelola pelanggan untuk re:Post Private

1. Masuk ke AWS Management Console dan buka konsol IAM di https://console.aws.amazon.com/iam/.
2. Di panel navigasi, pilih Kebijakan.
3. Pilih Buat kebijakan.
4. Pilih tab JSON.
5. Masukkan JSON Anda, lalu ganti JSON default di editor. Anda dapat menggunakan kebijakan contoh.
6. Pilih Berikutnya: Tag.
7. (Opsional) Anda dapat menggunakan tag sebagai pasangan nilai kunci untuk menambahkan metadata ke kebijakan.
8. Pilih Selanjutnya: Tinjau.
9. Pada halaman Kebijakan ulasan, masukkan Nama, seperti *`rePostPrivateSupportPolicy`*, dan Deskripsi (opsional).
10. Tinjau halaman Ringkasan untuk melihat izin yang kebijakan izinkan, dan kemudian pilih Buat kebijakan.

Kebijakan ini menentukan tindakan yang dapat dilakukan peran tersebut. Untuk informasi selengkapnya, lihat Membuat kebijakan IAM (konsol) dalam Panduan Pengguna IAM.

Contoh kebijakan IAM

Anda dapat melampirkan contoh kebijakan berikut ke peran IAM Anda. Kebijakan ini memungkinkan peran memiliki izin penuh untuk semua tindakan yang diperlukan. AWS Support Setelah Anda mengonfigurasi re:Post pribadi dengan peran tersebut, setiap pengguna di re:Post pribadi Anda memiliki izin yang sama.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "RepostSpaceSupportOperations",
   "Effect": "Allow",
   "Action": [
    "support:AddAttachmentsToSet",
    "support:AddCommunicationToCase",
    "support:CreateCase",
    "support:DescribeCases",
    "support:DescribeCommunications",
    "support:ResolveCase"
   ],
   "Resource": "*"
  }
 ]
}
```

> **Note**
>
> Untuk daftar kebijakan AWS terkelola untuk re:Post Private, lihat. AWS kebijakan terkelola untuk AWS re: Post Private

Anda dapat memperbarui kebijakan untuk menghapus izin dari AWS Support.

Untuk deskripsi untuk setiap tindakan, lihat topik berikut di Referensi Otorisasi Layanan:

- Tindakan, sumber daya, dan kunci kondisi untuk AWS Support

- Tindakan, sumber daya, dan kunci kondisi untuk Service Quotas
- Tindakan, sumber daya, dan kunci kondisi untuk AWS Identity and Access Management

Buat IAM role

Setelah Anda membuat kebijakan, Anda harus membuat IAM role, dan kemudian melampirkan kebijakan untuk peran tersebut. Anda memilih peran ini saat membuat re:Post pribadi di konsol Re:Post Private.

Untuk membuat peran untuk pembuatan dan manajemen AWS Support kasus

1. Masuk ke AWS Management Console dan buka konsol IAM di https://console.aws.amazon.com/iam/.
2. Di panel navigasi, pilih Peran, lalu pilih Buat peran.
3. Untuk jenis entitas Tepercaya, pilih Kebijakan kepercayaan khusus.
4. Untuk kebijakan kepercayaan khusus, masukkan yang berikut ini:

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Principal": {
    "Service": "repostspace.amazonaws.com"
   },
   "Action": [
    "sts:AssumeRole",
    "sts:SetSourceIdentity"
   ]
  }
 ]
}
```

5. Pilih Berikutnya.
6. Di bawah Kebijakan izin, di bilah pencarian, masukkan kebijakan AWS terkelola atau kebijakan terkelola pelanggan yang Anda buat, seperti *rePostPrivateSupportPolicy*. Pilih kotak centang yang ada di sebelah kebijakan izin yang ingin dimiliki layanan.
7. Pilih Berikutnya.

8. Pada halaman Nama, tinjau, dan buat, untuk nama Peran, masukkan nama, seperti *rePostPrivateSupportRole*.
9. (Opsional) Untuk Deskripsi, masukkan deskripsi untuk peran tersebut.
10. Tinjau kebijakan kepercayaan dan izin.
11. (Opsional) Anda dapat menggunakan tag sebagai pasangan nilai kunci untuk menambahkan metadata ke peran. Untuk informasi lebih lanjut tentang penggunaan tanda dan IAM, lihat Penandaan sumber daya IAM.
12. Pilih Buat peran. Anda sekarang dapat memilih peran ini ketika Anda mengonfigurasi Re: Post pribadi di konsol Re:Post Private. Lihat Buat re:Post pribadi baru.

Untuk informasi selengkapnya, lihat Membuat peran untuk AWS layanan (konsol) di Panduan Pengguna IAM.

Pemecahan Masalah

Lihat topik berikut untuk mengelola akses ke RE:Post Private.

Daftar Isi

- Saya ingin membatasi pengguna tertentu di re:Post pribadi saya dari tindakan tertentu
- Ketika saya mengonfigurasi re:Post pribadi, saya tidak melihat peran IAM yang saya buat
- Peran IAM saya tidak memiliki izin
- Kesalahan mengatakan bahwa peran IAM saya tidak valid

Saya ingin membatasi pengguna tertentu di re:Post pribadi saya dari tindakan tertentu

Secara default, pengguna di re:Post pribadi Anda memiliki izin yang sama yang ditentukan dalam kebijakan IAM yang Anda lampirkan ke peran IAM yang Anda buat. Ini berarti bahwa siapa pun di Re:Post pribadi memiliki akses baca atau tulis untuk membuat dan mengelola AWS Support kasus, apakah mereka memiliki atau pengguna IAM Akun AWS atau tidak.

Kami merekomendasikan praktik terbaik berikut:

- Gunakan kebijakan IAM yang memiliki izin minimum yang diperlukan untuk. AWS Support Lihat AWS kebijakan terkelola: AWSRepostSpaceSupportOperationsPolicy.

Ketika saya mengonfigurasi re:Post pribadi, saya tidak melihat peran IAM yang saya buat

Jika peran IAM Anda tidak muncul dalam peran IAM untuk daftar Re:Post Private;, ini berarti bahwa peran tersebut tidak memiliki re:Post Private sebagai entitas tepercaya, atau peran tersebut telah dihapus. Anda dapat memperbarui peran yang ada, atau membuat yang lain. Lihat Buat IAM role.

Peran IAM saya tidak memiliki izin

Peran IAM yang Anda buat untuk re:Post pribadi Anda memerlukan izin untuk melakukan tindakan yang Anda inginkan. Misalnya, jika Anda ingin pengguna Anda di re:Post pribadi untuk membuat kasus dukungan, peran harus memiliki `support:CreateCase` izin. re:Post Private mengasumsikan peran ini untuk melakukan tindakan ini untuk Anda.

Jika Anda menerima kesalahan tentang izin yang hilang AWS Support, verifikasi bahwa kebijakan yang dilampirkan pada peran Anda memiliki izin yang diperlukan.

Lihat yang sebelumnyaContoh kebijakan IAM.

Kesalahan mengatakan bahwa peran IAM saya tidak valid

Verifikasi bahwa Anda memilih peran yang benar untuk konfigurasi re:Post pribadi Anda.

Mengatur dan mengelola akses pengguna menggunakan AWS IAM Identity Center

Re: Post Private terintegrasi dengan AWS IAM Identity Center untuk memberikan federasi identitas untuk tenaga kerja organisasi Anda. Gunakan Pusat Identitas IAM untuk membuat atau menghubungkan pengguna dari organisasi Anda dan mengelola akses mereka secara terpusat di semua AWS akun dan aplikasi mereka. Untuk informasi selengkapnya tentang Pusat Identitas IAM, lihat Apa itu Pusat Identitas AWS IAM (penerus AWS Single Sign-On). Untuk informasi selengkapnya tentang memulai dengan IAM Identity Center, lihat Memulai. Untuk menggunakan Pusat Identitas IAM, Anda juga harus AWS Organizations mengaktifkan akun tersebut.

Kustomisasi re:Post pribadi Anda

Anda dapat menambahkan satu atau lebih administrator ke re:Post pribadi Anda setelah Anda membuatnya. Administrator menggunakan aplikasi Re:Post Private untuk meluncurkan Re: Post

pribadi dan mengelola pengguna di dalamnya. Mereka dapat menyesuaikan branding untuk Re:post pribadi, menambahkan tag untuk mengklasifikasikan konten, dan memilih topik yang menarik untuk populasi konten otomatis. Untuk informasi selengkapnya, lihat AWS re:Post Private Administration Guide.

Undang pengguna ke Re:Post pribadi Anda

Anda dapat menambahkan satu atau lebih pengguna ke Re:Post pribadi Anda setelah Anda membuatnya. Anda dapat mengundang pengguna untuk berkolaborasi dalam Re: Post pribadi Anda. Pengguna menggunakan aplikasi re:Post Private untuk masuk menggunakan kredenal yang Anda konfigurasikan. Setelah masuk ke re:Post pribadi, pengguna dapat menelusuri atau mencari konten yang ada, termasuk pelatihan khusus dan konten teknis yang mencakup topik minat mereka. Untuk informasi selengkapnya, lihat AWS re:Post Private User Guide.

Kelola re:Post pribadi Anda di konsol Re:Post Private

Bagian ini menjelaskan bagaimana Anda dapat mengelola re:Post pribadi Anda di konsol AWS re:Post Private.

Topik

- Tambahkan pengguna dan grup ke re:Post pribadi Anda
- Tambahkan pengguna ke grup di re:Post pribadi Anda
- Undang pengguna dan grup ke Re:post pribadi Anda
- Promosikan pengguna di re:Posting pribadi Anda ke administrator
- Hapus pengguna atau grup dari Re:Post pribadi Anda
- Menambah atau menghapus AWS karyawan dari re:post pribadi Anda
- Hapus re:Post pribadi dari re:Post Private

Tambahkan pengguna dan grup ke re:Post pribadi Anda

Jika Anda seorang administrator, Anda dapat menambahkan pengguna dan grup ke re:Post pribadi Anda.

Tambahkan pengguna ke re:Post pribadi Anda

1. Buka konsol Re:Post Private di https://console.aws.amazon.com/repost-private/.
2. Di panel navigasi, pilih All my private re: Posts.
3. Pilih Re: Post pribadi yang ingin Anda kelola.
4. Pilih tab Pengguna.
5. Di bawah Pengguna, pilih Tambahkan pengguna dan grup.
6. Dari daftar, pilih pengguna yang ingin Anda tambahkan ke re:post pribadi Anda. Kemudian, pilih Assign.

Pengguna yang dipilih ditambahkan ke Re:Post pribadi Anda dan terdaftar di bawah tab Pengguna.

Tambahkan grup ke re:Post pribadi Anda

1. Buka konsol Re:Post Private di https://console.aws.amazon.com/repost-private/.
2. Di panel navigasi, pilih All my private re: Posts.
3. Pilih Re: Post pribadi yang ingin Anda kelola.
4. Pilih tab Grup.
5. Pilih Tambahkan pengguna dan grup.
6. Dari daftar, pilih grup yang ingin Anda tambahkan ke re:post pribadi Anda. Kemudian, pilih Assign.

Grup yang dipilih ditambahkan ke Re:Post pribadi Anda dan terdaftar di bawah tab Grup.

Tambahkan pengguna ke grup di re:Post pribadi Anda

Gunakan IAM Identity Center untuk menambahkan pengguna baru ke grup yang ada di re:Post pribadi Anda. Untuk informasi selengkapnya, lihat Menambahkan pengguna ke grup di Panduan Pengguna Pusat Identitas AWS IAM.

Undang pengguna dan grup ke Re:post pribadi Anda

Ikuti langkah-langkah berikut untuk mengundang pengguna dan grup ke re:Post pribadi Anda di AWS re:Post Private:

1. Buka konsol Re:Post Private di https://console.aws.amazon.com/repost-private/.
2. Di panel navigasi, pilih All my private re: Posts.
3. Pilih Re: Post pribadi yang ingin Anda kelola.
4. Untuk mengundang pengguna ke re:Post pribadi Anda, pilih tab Pengguna.

   Dari daftar, pilih pengguna yang ingin Anda undang ke re:post pribadi Anda. Kemudian, pilih Onboard user untuk re:post.
5. Di kotak dialog Re:Post pribadi pengguna Onboard ini, masukkan informasi berikut:

   Untuk Subjek, masukkan subjek untuk pesan email yang Anda kirim.

   Untuk Tubuh, masukkan pesan selamat datang untuk Re:post pribadi Anda.

   Pilih Kirim email orientasi.
6. Untuk mengundang grup ke re:Post pribadi Anda, pilih tab Grup.

Dari daftar, pilih grup yang ingin Anda undang ke re:post pribadi Anda. Kemudian, pilih grup Onboard untuk Re:post.

7. Dalam grup Onboard ke kotak dialog Re:Post pribadi ini, masukkan informasi berikut:

   Untuk Subjek, masukkan subjek untuk pesan email yang Anda kirim.

   Untuk Tubuh, masukkan pesan selamat datang untuk Re:post pribadi Anda.

   Pilih Kirim email orientasi.

Pesan selamat datang dikirim ke semua pengguna dan grup yang dipilih dengan informasi tentang cara masuk ke re:post pribadi Anda.

Promosikan pengguna di re:Posting pribadi Anda ke administrator

Untuk mempromosikan pengguna re:Post pribadi ke administrator, ikuti langkah-langkah berikut:

1. Buka konsol Re:Post Private di https://console.aws.amazon.com/repost-private/.
2. Di panel navigasi, pilih All my private re: Posts.
3. Pilih Re: Post pribadi yang ingin Anda kelola.
4. Pilih tab Pengguna.
5. Pilih satu atau beberapa pengguna yang ingin Anda promosikan ke administrator.
6. Pilih Edit peran, lalu pilih Buat admin.

Pengguna yang dipilih dipromosikan menjadi administrator. Di bawah tab Pengguna, Peran untuk pengguna ini diperbarui ke Administrator.

Hapus pengguna atau grup dari Re:Post pribadi Anda

Jika Anda seorang administrator, maka Anda dapat menghapus pengguna atau grup dari re:Post pribadi Anda.

Hapus pengguna dari re:Post pribadi Anda

1. Buka konsol Re:Post Private di https://console.aws.amazon.com/repost-private/.
2. Di panel navigasi, pilih All my private re: Posts.

3. Pilih Re: Post pribadi yang ingin Anda kelola.
4. Di bawah Pengguna, dari daftar, pilih pengguna yang ingin Anda hapus dari re:Post pribadi Anda. Kemudian, pilih Hapus.

Pengguna yang dipilih akan dihapus dari Re:post pribadi Anda. Informasi tentang pengguna yang dihapus tidak lagi muncul di bawah tab Pengguna.

Hapus grup dari re:Post pribadi Anda

1. Buka konsol Re:Post Private di https://console.aws.amazon.com/repost-private/.
2. Di panel navigasi, pilih All my private re: Posts.
3. Pilih Re: Post pribadi yang ingin Anda kelola.
4. Pilih tab Grup.
5. Dari daftar, pilih grup yang ingin Anda hapus dari Re:post pribadi Anda. Kemudian, pilih Hapus.

Grup yang dipilih akan dihapus dari Re:post pribadi Anda. Informasi tentang grup yang dihapus tidak lagi muncul di bawah tab Grup.

Menambah atau menghapus AWS karyawan dari re:post pribadi Anda

Jika Anda memiliki Paket Dukungan On-Ramp Enterprise atau Enterprise, Anda dapat menambahkan atau menghapus karyawan AWS dari re:Post pribadi Anda. Hubungi Concierge Support atau Technical Account Manager (TAM) Anda untuk informasi lebih lanjut.

Hapus re:Post pribadi dari re:Post Private

Untuk menghapus re:Post pribadi di AWS re:Post Private, ikuti langkah-langkah berikut:

1. Buka konsol Re:Post Private di https://console.aws.amazon.com/repost-private/.
2. Di panel navigasi, pilih All my private re: Posts.
3. Pilih re:Post pribadi yang ingin Anda kelola, lalu pilih Hapus.
4. Pilih semua opsi untuk mengakui dan mengonfirmasi bahwa Anda ingin menghapus re:post pribadi dan data yang terkait dengannya secara permanen.

> **Important**
>
> Ketika Anda menghapus private re:Post, semua informasi konfigurasi yang terkait dengan private re: post akan dihapus. Setelah re:post pribadi dihapus, Anda tidak dapat memulihkan konten apa pun darinya.

5. Masukkan nama Re:post pribadi Anda ketika diminta untuk persetujuan tertulis tambahan. Lalu, pilih Hapus.

Dibutuhkan sekitar 30 menit untuk Re:Post pribadi Anda dihapus.

Pemantauan AWS RE: Post Private

Pemantauan adalah bagian penting dalam menjaga keandalan, ketersediaan, dan kinerja AWS re: Post Private dan solusi Anda yang lainAWS. AWSmenyediakan alat pemantauan berikut untuk menonton RE: Post Private, melaporkan ketika ada sesuatu yang salah, dan mengambil tindakan otomatis bila perlu:

- Amazon CloudWatch memantau AWS sumber daya Anda dan aplikasi yang Anda jalankan AWS secara real time. Anda dapat mengumpulkan dan melacak metrik, membuat dasbor yang disesuaikan, dan mengatur alarm yang memberi tahu Anda atau mengambil tindakan saat metrik tertentu mencapai ambang batas yang ditentukan. Misalnya, Anda dapat CloudWatch melacak penggunaan CPU atau metrik lain dari instans Amazon EC2 Anda dan secara otomatis meluncurkan instans baru bila diperlukan. Untuk informasi selengkapnya, lihat Panduan CloudWatch Pengguna Amazon.
- AWS CloudTrailmenangkap panggilan API dan peristiwa terkait yang dibuat oleh atau untuk Anda Akun AWS dan mengirimkan file log ke bucket Amazon S3 yang Anda tentukan. Anda dapat mengidentifikasi pengguna dan akun mana yang memanggil AWS, alamat IP sumber yang melakukan panggilan, dan kapan panggilan tersebut terjadi. Untuk mengetahui informasi selengkapnya, lihat Panduan Pengguna AWS CloudTrail.

Memantau AWS re: Posting Pribadi dengan Amazon CloudWatch

Anda dapat memantau AWS re:Post Private menggunakan Amazon CloudWatch, yang mengumpulkan data mentah dan memprosesnya menjadi metrik hampir real-time yang dapat dibaca. Statistik ini disimpan selama 15 bulan sehingga Anda dapat mengakses informasi historis dan mendapatkan perspektif yang lebih baik tentang kinerja aplikasi atau layanan web Anda. Anda juga dapat mengatur alarm yang memperhatikan ambang batas tertentu dan mengirim notifikasi atau mengambil tindakan saat ambang batas tersebut terpenuhi. Untuk informasi selengkapnya, lihat Panduan CloudWatch Pengguna Amazon.

Layanan re:Post Private melaporkan metrik berikut di namespace. `AWS/rePostPrivate`

Metrik	Deskripsi
`NumberOfSpaces`	Jumlah Re pribadi: posting di akun saat ini.

Metrik	Deskripsi
	Unit: Count (Jumlah)
`NumberOfUsers`	Jumlah pengguna dalam Re: Post pribadi. Metrik ini menggunakan spaceID sebagai dimensi. Unit: Count (Jumlah)
`ContentSize`	Jumlah konten dalam Re: post pribadi. Metrik ini menggunakan spaceID sebagai dimensi. Unit: Bita

Dimensi berikut didukung untuk metrik Re: Post Private.

Dimensi	Deskripsi
`spaceId`	Pengidentifikasi unik untuk Re: post pribadi.

Logging AWS re: Posting panggilan API Pribadi menggunakan AWS CloudTrail

AWS re:Post Private terintegrasi denganAWS CloudTrail, layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atau AWS layanan di re:Post Private. CloudTrail menangkap semua panggilan API untuk re:Post Private sebagai acara. Panggilan yang diambil termasuk panggilan dari konsol Re:Post Private dan panggilan kode ke operasi RE:Post Private API. Jika Anda membuat jejak, Anda dapat mengaktifkan pengiriman CloudTrail acara secara terus menerus ke bucket Amazon S3, termasuk acara untuk re:Post Private. Jika Anda tidak mengonfigurasi jejak, Anda masih dapat melihat peristiwa terbaru di CloudTrail konsol dalam Riwayat acara. Dengan menggunakan informasi yang dikumpulkan oleh CloudTrail, Anda dapat menentukan permintaan yang dibuat untuk Re:Post Private, alamat IP dari mana permintaan itu dibuat, siapa yang membuat permintaan, kapan dibuat, dan detail tambahan.

Untuk mempelajari selengkapnya CloudTrail, lihat Panduan AWS CloudTrail Pengguna.

re: posting informasi pribadi di CloudTrail

CloudTrail diaktifkan pada Akun AWS saat Anda membuat akun. Ketika aktivitas terjadi di re:Post Private, aktivitas tersebut dicatat dalam suatu CloudTrail peristiwa bersama dengan peristiwa AWS layanan lainnya dalam riwayat Acara. Anda dapat melihat, mencari, dan mengunduh peristiwa terbaru di Akun AWS Anda. Untuk informasi selengkapnya, lihat Bekerja dengan riwayat CloudTrail Acara.

Untuk catatan acara yang sedang berlangsung di AndaAkun AWS, termasuk acara untuk re:Post Private, buat jejak. Jejak memungkinkan CloudTrail untuk mengirimkan file log ke bucket Amazon S3. Secara default, saat Anda membuat jejak di konsol, jejak tersebut berlaku untuk semua Wilayah AWS. Jejak mencatat peristiwa dari semua Wilayah di partisi AWS dan mengirimkan berkas log ke bucket Amazon S3 yang Anda tentukan. Selain itu, Anda dapat mengonfigurasi AWS layanan lain untuk menganalisis lebih lanjut dan menindaklanjuti data peristiwa yang dikumpulkan dalam CloudTrail log. Untuk informasi selengkapnya, lihat yang berikut:

- Membuat jejak untuk akun AWS Anda
- CloudTrail layanan dan integrasi yang didukung
- Mengonfigurasi notifikasi Amazon SNS untuk CloudTrail
- Menerima file CloudTrail log dari beberapa Wilayah dan Menerima file CloudTrail log dari beberapa akun

Semua tindakan re:Post Private dicatat oleh CloudTrail dan didokumentasikan dalam AWS re:Post Private API Reference. re:Post Private mendukung pencatatan tindakan berikut sebagai peristiwa dalam file log: CloudTrail

- CreateSpace
- DeleteSpace
- DeregisterAdmin
- GetSpace
- ListSpaces
- ListTagsForResource
- RegisterAdmin
- SendInvites
- TagResource
- UntagResource

- UpdateSpace

re:Post Private mendukung pencatatan AWS Support tindakan berikut sebagai peristiwa dalam file CloudTrail log:

- CreateCase
- AddCommunicationToCase
- ResolveCase

Setiap entri peristiwa atau log berisi informasi tentang siapa yang membuat permintaan tersebut. Informasi identitas membantu Anda menentukan hal berikut:

- Bahwa permintaan dibuat dengan kredensial pengguna root atau pengguna AWS Identity and Access Management (IAM).
- Bahwa permintaan tersebut dibuat dengan kredensial keamanan sementara untuk peran atau pengguna gabungan.
- Bahwa permintaan dibuat oleh layanan AWS lain.

Untuk informasi selengkapnya, lihat Elemen userIdentity CloudTrail .

Memahami re:posting entri file log pribadi

Trail adalah konfigurasi yang memungkinkan pengiriman peristiwa sebagai file log ke bucket Amazon S3 yang Anda tentukan. CloudTrail file log berisi satu atau lebih entri log. Peristiwa mewakili permintaan tunggal dari sumber manapun dan mencakup informasi tentang tindakan yang diminta, tanggal dan waktu tindakan, parameter permintaan, dan sebagainya. CloudTrail file log bukanlah jejak tumpukan yang diurutkan dari panggilan API publik, sehingga file tersebut tidak muncul dalam urutan tertentu.

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan `CreateSpace` tindakan.

```
{
   "eventVersion": "1.08",
   "userIdentity": {
       "type": "AssumedRole",
       "principalId": "AROAQM47QIR7WLEXAMPLE:user",
       "arn": "arn:aws:sts::123456789012:assumed-role/User/user",
```

```
        "accountId": "123456789012",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAQM47QIR7WLEXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/User",
                "accountId": "123456789012",
                "userName": "User"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-11-06T19:24:39Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-11-06T21:37:44Z",
    "eventSource": "repostspace.amazonaws.com",
    "eventName": "CreateSpace",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "205.251.233.176",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/118.0.0.0 Safari/537.36",
    "requestParameters": {
        "spaceName": "Test space name",
        "spaceSubdomain": "customsubdomain",
        "tagSet": {},
        "tier": "2000",
        "roleArn": "",
        "spaceDescription": "Test space description"
    },
    "responseElements": {
        "spaceId": "SPLPWvQmv9SIWYF30EXAMPLE",
        "Access-Control-Expose-Headers": "x-amzn-errortype, x-amzn-requestid, x-amzn-
errormessage, x-amzn-trace-id, x-amz-apigw-id, date"
    },
    "requestID": "71d815e0-6632-4ec9-9fac-92af3e4a86dc",
    "eventID": "30a6c3da-ce2e-4931-ba5d-b3cc7cf16ec8",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
```

```
}
```

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan `RegisterAdmin` tindakan.

```
 {
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAQM47QIR7WLEXAMPLE:user",
        "arn": "arn:aws:sts::123456789012:assumed-role/User/user",
        "accountId": "123456789012",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAQM47QIR7WLEXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/User",
                "accountId": "123456789012",
                "userName": "User"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-11-07T21:17:19Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-11-07T21:24:23Z",
    "eventSource": "repostspace.amazonaws.com",
    "eventName": "RegisterAdmin",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "205.251.233.183",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/118.0.0.0 Safari/537.36",
    "requestParameters": {
        "adminId": "08612310-a0f1-7063-3e54-fb2960444dd1",
        "spaceId": "SPlYNZE-ylQEmAXpmEXAMPLE"
    },
    "responseElements": {
        "Access-Control-Expose-Headers": "x-amzn-errortype, x-amzn-requestid, x-amzn-
errormessage, x-amzn-trace-id, x-amz-apigw-id, date"
```

```
    },
    "requestID": "9939ebbe-8599-4f9a-827b-4995e3006001",
    "eventID": "e1873b18-f80c-4934-9ff2-bf5b35c78031",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan `ListSpaces` tindakan.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAQM47QIR7WLEXAMPLE:user",
        "arn": "arn:aws:sts::123456789012:assumed-role/User/user",
        "accountId": "123456789012",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAQM47QIR7WLEXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/User",
                "accountId": "123456789012",
                "userName": "User"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-11-09T22:28:23Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-11-09T22:38:34Z",
    "eventSource": "repostspace.amazonaws.com",
    "eventName": "ListSpaces",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "205.251.233.176",
```

```
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36",
    "requestParameters": null,
    "responseElements": null,
    "requestID": "95be587b-c04f-4eb0-9269-12fee33ae2e3",
    "eventID": "9777da32-545f-44c4-af0b-1d9109b8cbc3",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan `ResolveCase` tindakan. Anda dapat menggunakan `sourceIdentity` elemen dalam entri log ini untuk mengidentifikasi pengguna yang menyelesaikan kasus ini.

```
 {
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAQM47QIR76DQZ7N5WX:create-support-case-
Uk1iHNTWQEOLmR2BR1FDJQ",
        "arn": "arn:aws:sts::123456789012:assumed-role/AWSRepostSpaceRole/create-
support-case-Uk1iHNTWQEOLmR2BR1FDJQ",
        "accountId": "123456789012",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAQM47QIR76DQZ7N5WX",
                "arn": "arn:aws:iam::123456789012:role/AWSRepostSpaceRole",
                "accountId": "123456789012",
                "userName": "AWSRepostSpaceRole"
            },
            "attributes": {
                "creationDate": "2023-11-17T21:46:42Z",
                "mfaAuthenticated": "false"
            },
            "sourceIdentity": "28e17330-10f1-705d-7cba-3a62a6b10e2e"
        }
    },
```

```
    "eventTime": "2023-11-17T21:46:44Z",
    "eventSource": "support.amazonaws.com",
    "eventName": "ResolveCase",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "54.68.27.29",
    "userAgent": "aws-sdk-nodejs/2.1363.0 linux/v16.20.2 exec-env/AWS_ECS_FARGATE
 promise",
    "requestParameters": {
        "caseId": "case-123456789012-muen-2023-75d2c35481b96357"
    },
    "responseElements": {
        "initialCaseStatus": "unassigned",
        "finalCaseStatus": "resolved"
    },
    "requestID": "594b91c6-df1c-47e4-a834-d67d67f34b9d",
    "eventID": "7fc9cbe4-c8d5-4d61-a016-e076de272fff",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111111111111",
    "eventCategory": "Management",
    "tlsDetails": {
        "clientProvidedHostHeader": "support.us-west-2.amazonaws.com"
    }
}
```

Pemecahan Masalah Re:Post Private

Informasi berikut dapat membantu Anda memecahkan masalah dengan AWS re:Post Private.

Topik

- Tidak dapat mengatur re:Post pribadi saya di Wilayah tertentu AWS
- Tidak dapat mengatur re:Post pribadi di akun saya
- Tidak dapat mengelola pengguna atau grup dalam re:Post pribadi

Tidak dapat mengatur re:Post pribadi saya di Wilayah tertentu AWS

Re:Post Private hanya tersedia di Wilayah AS Timur (Virginia N.), AS Barat (Oregon), Eropa (Frankfurt), Asia Pasifik (Singapura), Asia Pasifik (Sydney), Kanada (Tengah), dan Eropa (Irlandia). Pastikan Anda membuat Re:Post pribadi Anda di salah satu Wilayah ini.

Tidak dapat mengatur re:Post pribadi di akun saya

Pastikan Anda mengaktifkan AWS IAM Identity Center akun Anda dan menyiapkan Pusat Identitas IAM di Wilayah yang sama tempat Anda ingin membuat re:Post pribadi. Untuk informasi selengkapnya, lihat Prasyarat.

Tidak dapat mengelola pengguna atau grup dalam re:Post pribadi

Pastikan Anda memiliki izin yang diperlukan untuk mengedit re:Post pribadi dan mengelola pengguna dan grup dalam Re: Post pribadi. Untuk informasi selengkapnya, lihat AWS re: Posting contoh kebijakan berbasis identitas pribadi.

Riwayat dokumen

Tabel berikut menjelaskan rilis dokumentasi untuk AWS re:Post Private:

Perubahan	Deskripsi	Tanggal
Perbarui	Menambahkan US East (Virginia N.), Asia Pasifik (Sydney), Kanada (Tengah), dan Eropa (Irlandia) ke Wilayah yang didukung	10 Mei 2024
Perbarui	Menambahkan Asia Pasifik (Singapura) ke Wilayah yang didukung	Maret 6, 2024
Sumber daya baru	Menambahkan dokumentasi untuk kebijakan terkelola AWS untuk AWS re:Post Private	26 November 2023
Rilis awal	Rilis awal dari Re: Post Private Console Administration Guide	26 November 2023

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