Panduan Pengguna

AWS Support

Versi API 2013-04-15

AWS Support: Panduan Pengguna

Table of Contents

Memulai dengan AWS Support

AWS Support menawarkan berbagai rencana yang menyediakan akses ke alat dan keahlian yang mendukung keberhasilan dan kesehatan operasional AWS solusi Anda. Semua rencana dukungan menyediakan akses 24/7 ke layanan pelanggan, AWS dokumentasi, makalah teknis, dan forum dukungan. Untuk dukungan teknis dan lebih banyak sumber daya untuk merencanakan, menyebarkan, dan meningkatkan AWS lingkungan Anda, Anda dapat memilih rencana dukungan untuk kasus AWS penggunaan Anda.

> **Catatan**
>
> - Untuk membuat kasus dukungan di AWS Management Console, lihatMembuat kasus dukungan.
> - Untuk informasi selengkapnya tentang berbagai AWS Support paket, lihat Membandingkan AWS Support paket danMengubah AWS Support Rencana.
> - Paket Support menawarkan waktu respons yang berbeda untuk kasus dukungan Anda. Lihat Memilih kepelikan dan Waktu respons.

Topik

Membuat kasus dukungan dan manajemen kasus

Dalam AWS Management Console, Anda dapat membuat tiga jenis kasus pelanggan di AWS Support:

- Kasus Account and billing support (Dukungan akun dan penagihan) tersedia untuk semua pelanggan AWS . Anda dapat mendapatkan bantuan terkait pertanyaan penagihan dan akun.

- Permintaan Service limit increase (Kenaikan service limits) tersedia untuk semua pelanggan AWS . Untuk informasi selengkapnya tentang kuota layanan default, yang sebelumnya disebut sebagai batas, lihat kuota AWS layanan di. Referensi Umum AWS
- Kasus Technical support (Dukungan teknis) menghubungkan Anda ke dukungan teknis untuk mendapatkan bantuan terkait masalah teknis layanan dan, dalam beberapa kasus, aplikasi pihak ketiga. Jika Anda memiliki Basic Support, Anda tidak dapat membuat kasus dukungan teknis.

> **Catatan**
>
> - Untuk mengubah paket dukungan, lihat Mengubah AWS Support Rencana.
> - Untuk menutup akun, lihat Menutup Akun dalam Panduan Pengguna AWS Billing .
> - Untuk menemukan topik pemecahan masalah umum Layanan AWS, lihat. Sumber daya pemecahan masalah
> - Jika Anda adalah pelanggan AWS Partner yang merupakan bagian dari AWS Partner Network, dan Anda menggunakan Resold Support, hubungi AWS Partner langsung Anda untuk masalah terkait penagihan. AWS Support tidak dapat membantu masalah non-teknis untuk Resold Support, seperti penagihan dan manajemen akun. Untuk informasi selengkapnya, lihat topik berikut.
>   - Bagaimana AWS Mitra dapat menentukan AWS Support rencana dalam suatu organisasi
>   - AWS Partner-Led Support

Membuat kasus dukungan

Anda dapat membuat kasus dukungan di AWS Management Console Pusat Dukungan.

> **Catatan**
>
> - Anda dapat masuk ke Support Center sebagai pengguna root AWS akun Anda atau sebagai pengguna AWS Identity and Access Management (IAM). Untuk informasi selengkapnya, lihat Mengelola akses ke AWS Support Pusat.
> - Jika Anda tidak dapat masuk ke Pusat Dukungan dan membuat kasus dukungan, Anda dapat menggunakan halaman Hubungi Kamisebagai gantinya. Anda dapat menggunakan halaman ini untuk mendapatkan bantuan terkait masalah penagihan dan akun.

Untuk membuat kasus dukungan

1. Masuklah ke AWS Support Center Console.

   > **Tip**
   >
   > Di dalam AWS Management Console, Anda juga dapat memilih ikon tanda tanya ( ) dan kemudian memilih Support Center.

2. Pilih Buat kasus.
3. Pilih salah satu opsi berikut:
   - Akun dan penagihan
   - Teknis
   - Untuk kenaikan kuota layanan, pilih Mencari peningkatan limit layanan? dan kemudian ikuti instruksi untukMenciptakan peningkatan kuota layanan.
4. Pilih Layanan, Kategori, dan Tingkat Keparahan.

   > **Tip**
   >
   > Anda dapat menggunakan solusi yang direkomendasikan yang muncul untuk pertanyaan umum.

5. Pilih Langkah selanjutnya: Informasi tambahan
6. Pada halaman Informasi tambahan, untuk Subjek, masukkan judul tentang masalah Anda.
7. Untuk Deskripsi, ikuti petunjuk untuk menjelaskan kasus Anda, seperti berikut ini:
   - Pesan eror yang Anda terima
   - Langkah pemecahan masalah yang Anda ikuti
   - Bagaimana Anda mengakses layanan:
     - AWS Management Console
     - AWS Command Line Interface (AWS CLI)
     - Operasi API

8. (Opsional) Pilih Lampirkan file untuk menambahkan file yang relevan ke kasus Anda, seperti log kesalahan atau tangkapan layar. Anda dapat melampirkan hingga tiga file. Setiap file dapat mencapai 5 MB.
9. Pilih Langkah selanjutnya: Selesaikan sekarang atau hubungi kami.
10. Pada halaman Hubungi kami, pilih bahasa pilihan Anda.
11. Pilih metode kontak pilihan Anda. Anda dapat memilih salah satu opsi berikut:

    a. Web — Menerima balasan di Support Center.

    b. Obrolan — Mulai obrolan langsung dengan agen dukungan. Jika Anda tidak dapat terhubung ke obrolan, lihatPemecahan Masalah.

    c. Phone (Telepon) – Menerima panggilan telepon dari agen dukungan. Jika Anda memilih opsi ini, masukkan informasi berikut:

    - Negara atau wilayah
    - Nomor telepon
    - (Opsional) Ekstensi

> **Catatan**
>
> - Opsi kontak yang muncul tergantung pada jenis kasus dan rencana dukungan Anda.
> - Anda dapat memilih Buang draf untuk menghapus draf kasus dukungan Anda.

12. (Opsional) Jika Anda memiliki paket Business, Enterprise On-Ramp, atau Enterprise Support, opsi Kontak tambahan akan muncul. Anda dapat memasukkan alamat email orang untuk memberi tahu ketika status kasus berubah. Jika Anda masuk sebagai pengguna IAM, sertakan alamat email Anda. Jika Anda masuk dengan alamat email dan kata sandi akun root Anda, Anda tidak perlu menyertakan alamat email Anda

> **Note**
>
> Jika Anda memiliki paket Dukungan Dasar, opsi Kontak tambahan tidak tersedia. Namun, kontak Operations (Operasi) yang ditentukan dalam bagian Alternate Contacts (Kontak Alternatif) dari halaman Akun Saya menerima salinan korespondensi kasus, tetapi hanya untuk jenis kasus akun dan penagihan, serta teknis.

13. Tinjau detail kasus Anda dan kemudian pilih Kirim. Nomor ID kasus dan ringkasan muncul.

Mendeskripsikan masalah Anda

Buat deskripsi Anda sedetail mungkin. Sertakan informasi sumber daya yang relevan, serta hal lain yang dapat membantu kami memahami masalah Anda. Misalnya, untuk memecahkan masalah kinerja, termasuk stempel waktu dan log. Untuk permintaan fitur atau pertanyaan panduan umum, sertakan deskripsi lingkungan dan tujuan Anda. Dalam semua kasus, ikuti Description Guidance (Panduan Deskripsi) yang muncul di formulir pengajuan kasus Anda.

Ketika Anda memberikan detail sebanyak mungkin, Anda meningkatkan kemungkinan kasus Anda dapat diselesaikan dengan cepat.

Memilih kepelikan

Anda mungkin cenderung untuk selalu membuat kasus dukungan pada kepelikan tertinggi yang diizinkan oleh paket dukungan Anda. Namun, sebaiknya Anda memilih kepelikan tertinggi untuk kasus yang tidak dapat dikerjakan atau yang secara langsung memengaruhi aplikasi produksi. Untuk informasi tentang membangun layanan Anda sehingga kehilangan satu sumber daya tidak memengaruhi aplikasi Anda, lihat makalah teknis Membangun Aplikasi Tahan Gangguan di AWS.

Tabel berikut mencantumkan tingkat kepelikan, waktu respons, dan contoh masalah.

> **Catatan**
>
> - Anda tidak dapat mengubah kode kepelikan untuk kasus dukungan setelah Anda membuatnya. Jika situasi Anda berubah, bekerjalah dengan AWS Support agen untuk kasus dukungan Anda.
> - Untuk informasi selengkapnya tentang tingkat keparahan, lihat Referensi AWS Support API.

Kepelikan	Kode tingkat keparahan	Waktu respons pertama	Deskripsi dan paket dukungan
Panduan umum	`low`	24 jam	Anda memiliki pertanyaan pengembangan umum atau Anda ingin meminta fitur. (*Paket Pengembang, Bisnis, Enterprise On-Ramp, atau Enterprise Support)
Sistem terganggu	`normal`	12 jam	Fungsi nonkritis dari aplikasi Anda berperilaku tidak normal atau Anda memiliki pertanyaan pengembangan yang bersifat segera. (*Paket Pengembang, Bisnis, Enterprise On-Ramp, atau Enterprise Support)
Sistem produksi terganggu	`high`	4 jam	Fungsi penting dari aplikasi Anda terganggu atau menurun. (Paket Bisnis, Enterprise On-Ramp, atau Enterprise Support)
Sistem produksi turun	`urgent`	1 jam	Bisnis Anda terdampak signifikan. Fungsi penting dari aplikasi Anda tidak tersedia. (Paket Bisnis, Enterprise On-Ramp, atau Enterprise Support)
Sistem kritis bisnis turun	`critical`	15 menit	Bisnis Anda terancam risiko. Fungsi penting aplikasi Anda tidak tersedia (Enterprise Support plan). Perhatikan bahwa ini adalah 30 menit untuk paket Enterprise On-Ramp Support.

Waktu respons

Kami melakukan segala upaya yang wajar untuk menanggapi permintaan awal Anda dalam jangka waktu yang ditunjukkan. Untuk informasi tentang ruang lingkup dukungan untuk setiap AWS Support paket, lihat AWS Support fitur.

Jika Anda memiliki paket Business, Enterprise On-Ramp, atau Enterprise Support, Anda memiliki akses 24/7 untuk dukungan teknis. *Untuk Support Developer, target respons untuk kasus dukungan

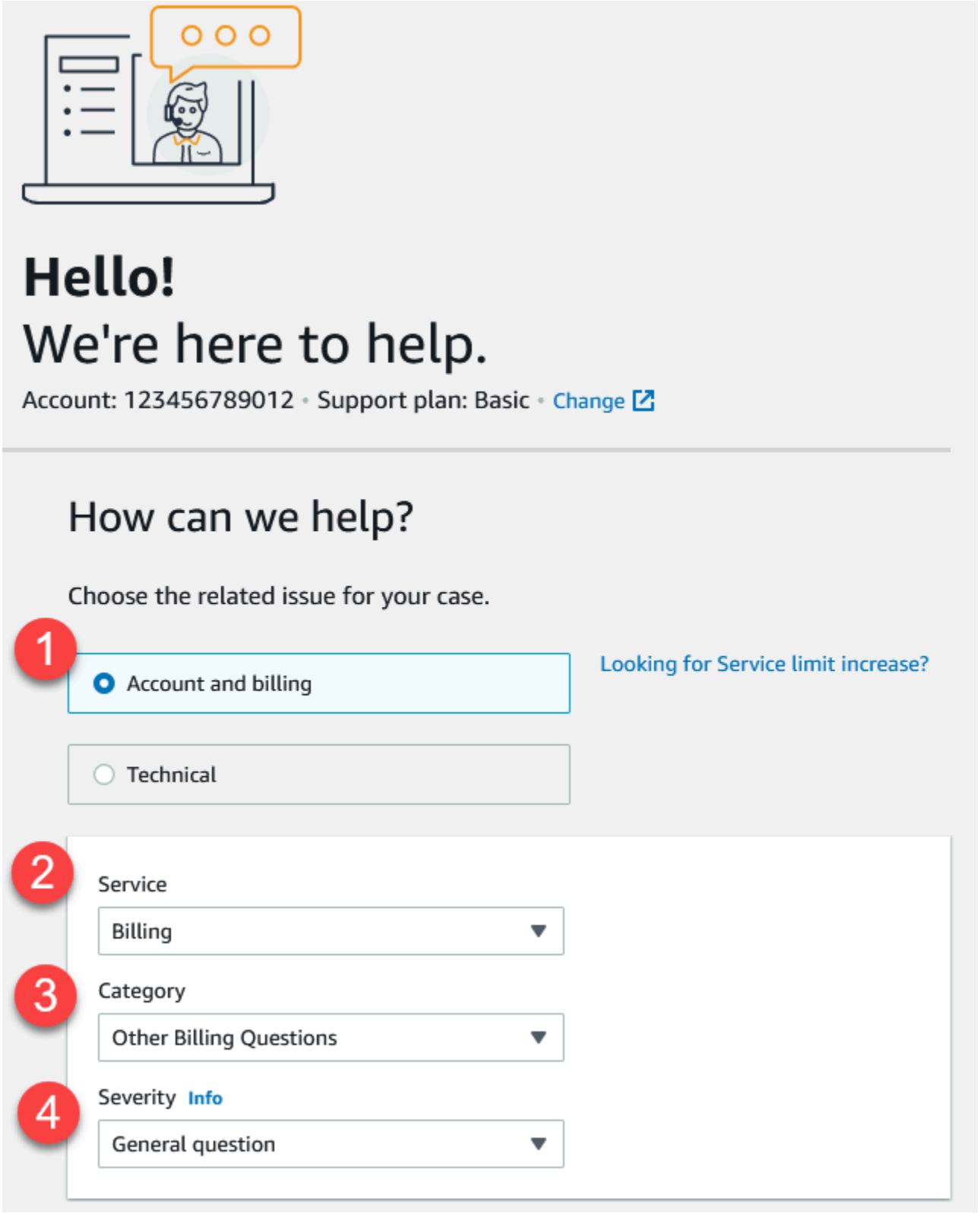
dihitung dalam jam kerja. Jam kerja umumnya didefinisikan sebagai 08:00 hingga 18:00 di negara pelanggan, tidak termasuk hari libur dan akhir pekan. Waktu ini dapat bervariasi di negara dengan beberapa zona waktu. Informasi negara pelanggan muncul di bagian Informasi Kontak pada halaman Akun Saya di halaman AWS Management Console.

> **Note**
>
> Jika Anda memilih bahasa Jepang sebagai bahasa kontak pilihan Anda untuk kasus dukungan, dukungan dalam bahasa Jepang mungkin tersedia sebagai berikut:
>
> - Jika Anda memerlukan layanan pelanggan untuk kasus dukungan non-teknis, atau jika Anda memiliki paket Dukungan Pengembang dan memerlukan dukungan teknis, dukungan dalam bahasa Jepang tersedia selama jam kerja di Jepang yang didefinisikan sebagai pukul 09:00 hingga 06:00 Waktu Standar Jepang (GMT+9), tidak termasuk hari libur dan akhir pekan.
> - Jika Anda memiliki paket Business, Enterprise On-Ramp, atau Enterprise Support, dukungan teknis tersedia 24/7 dalam bahasa Jepang.
>
> Jika Anda memilih bahasa Mandarin sebagai bahasa kontak pilihan Anda untuk kasus dukungan, dukungan dalam bahasa Mandarin mungkin tersedia sebagai berikut:
>
> - Jika Anda memerlukan layanan pelanggan untuk kasus dukungan non-teknis, dukungan dalam bahasa Mandarin tersedia pukul 09:00 hingga 18:00 (GMT+8), tidak termasuk hari libur dan akhir pekan.
> - Jika Anda memiliki paket Dukungan Pengembang, dukungan teknis dalam bahasa Mandarin tersedia selama jam kerja yang umumnya didefinisikan sebagai pukul 08:00 hingga 18:00 di negara Anda sebagaimana diatur dalam Akun Saya, tidak termasuk hari libur dan akhir pekan. Waktu ini dapat bervariasi di negara-negara dengan beberapa zona waktu.
> - Jika Anda memiliki paket Business, Enterprise On-Ramp, atau Enterprise Support, dukungan teknis tersedia 24/7 dalam bahasa Mandarin.
>
> Jika Anda memilih bahasa Korea sebagai bahasa kontak pilihan Anda untuk kasus dukungan, dukungan dalam bahasa Korea mungkin tersedia sebagai berikut:

- Jika Anda memerlukan layanan pelanggan untuk kasus dukungan non-teknis, dukungan dalam bahasa Korea tersedia selama jam kerja di Korea yang didefinisikan sebagai 09:00 hingga 18:00 Waktu Standar Korea (GMT+9), tidak termasuk hari libur dan akhir pekan.
- Jika Anda memiliki paket Dukungan Pengembang, dukungan teknis dalam bahasa Korea tersedia selama jam kerja yang umumnya didefinisikan sebagai pukul 08:00 hingga 18:00 di negara Anda sebagaimana diatur dalam Akun Saya, tidak termasuk hari libur dan akhir pekan. Waktu ini dapat bervariasi di negara-negara dengan beberapa zona waktu.
- Jika Anda memiliki paket Business, Enterprise On-Ramp, atau Enterprise Support, dukungan teknis tersedia 24/7 dalam bahasa Korea.

Contoh: Buat kasus dukungan untuk akun dan penagihan

Contoh berikut adalah kasus dukungan untuk masalah penagihan dan akun.



1. Buat kasus - Pilih jenis kasing yang akan dibuat. Dalam contoh ini, jenis kasusnya adalah Akun dan penagihan.

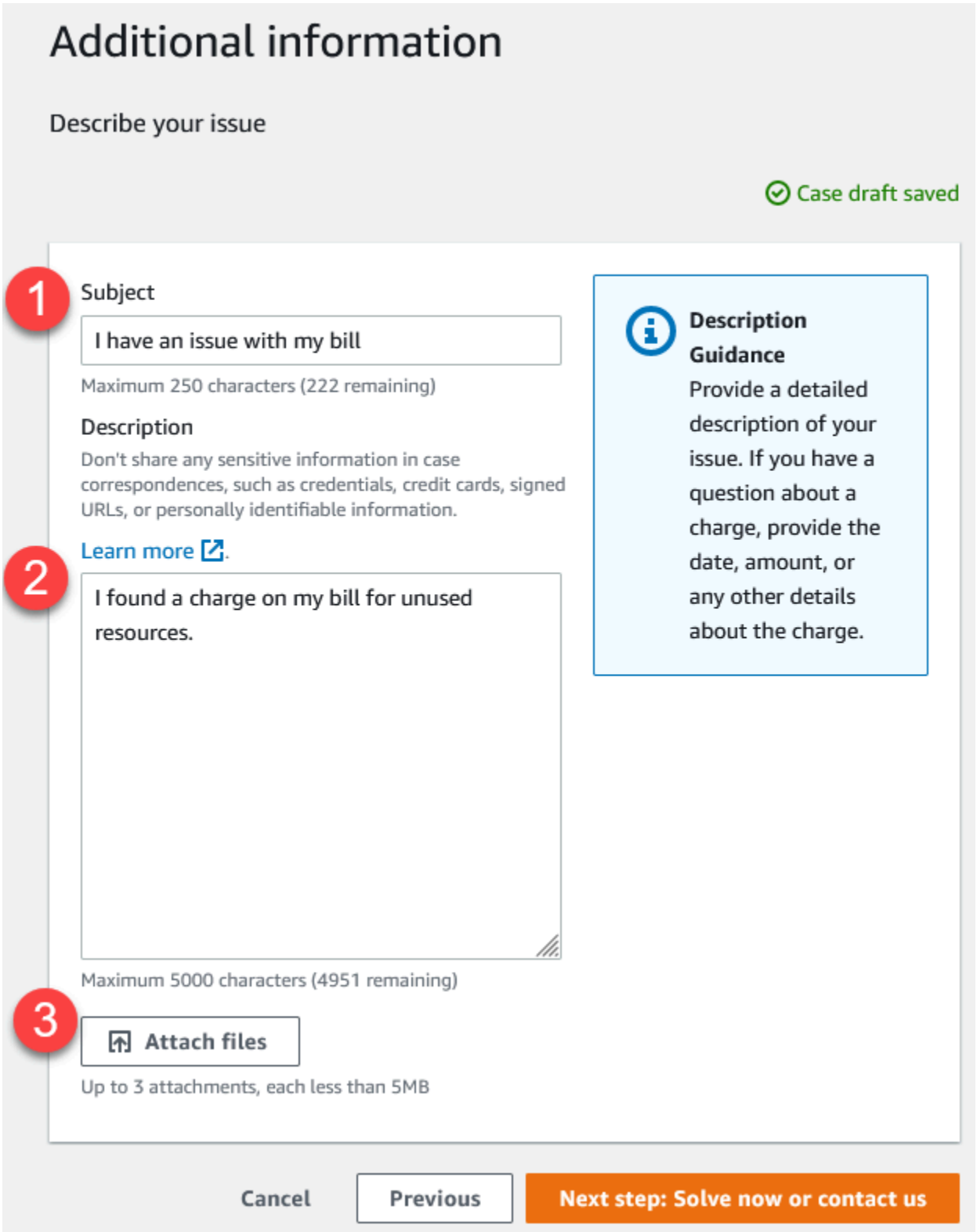
> **Note**
>
> Jika Anda memiliki paket Basic Support, Anda tidak dapat membuat kasus dukungan teknis.

2. Service (Layanan) – Jika pertanyaan Anda memengaruhi beberapa layanan, pilih layanan yang paling sesuai.
3. Category (Kategori) – Pilih kategori yang paling sesuai dengan kasus penggunaan Anda. Saat Anda memilih kategori, tautan ke informasi yang mungkin menyelesaikan masalah Anda muncul di bawah ini.
4. Severity (Kepelikan) – Pelanggan dengan paket dukungan berbayar dapat memilih tingkat kepelikan General guidance (Panduan umum) (waktu respons 1 hari) atau System impaired (Gangguan sistem) (waktu respons 12 jam). Pelanggan dengan paket Dukungan Bisnis juga dapat memilih Production system impaired (Gangguan sistem produksi) (respons 4 jam) atau Production system down (Kerusakan sistem produksi) (respons 1 jam). Pelanggan dengan paket Enterprise On-Ramp atau Enterprise Support dapat memilih sistem Business-critical down (respons 15 menit untuk Enterprise Support dan respons 30 menit untuk Enterprise On-Ramp).

   Waktu respons adalah untuk respons pertama dari AWS Support. Waktu respons ini tidak berlaku untuk tanggapan berikutnya. Untuk masalah pihak ketiga, waktu respons bisa lebih lama, tergantung pada ketersediaan personel terampil. Untuk informasi selengkapnya, lihat Memilih kepelikan.

   > **Note**
   >
   > Berdasarkan pilihan kategori, Anda mungkin diminta untuk informasi lebih lanjut.

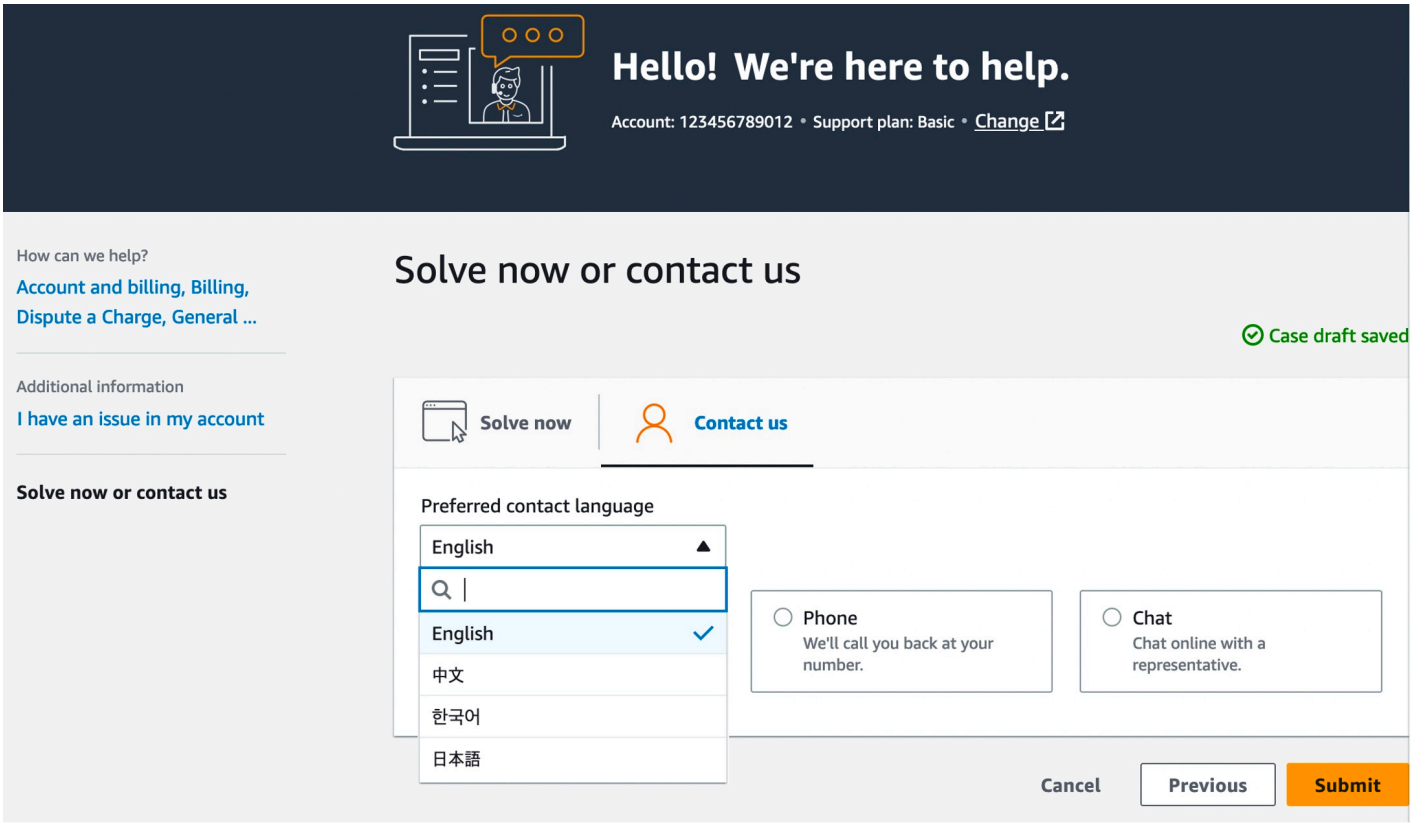
Setelah Anda menentukan jenis kasus dan klasifikasi, Anda dapat menentukan deskripsi dan bagaimana Anda ingin dihubungi.



1. Subject (Subjek) – Masukkan judul yang menjelaskan masalah Anda secara singkat.

2. Deskripsi - Jelaskan kasus dukungan Anda. Ini adalah informasi terpenting yang Anda berikanAWS Support. Untuk beberapa kombinasi layanan dan kategori, prompt muncul dengan informasi terkait. Gunakan tautan ini untuk membantu menyelesaikan masalah Anda. Untuk informasi selengkapnya, lihat Mendeskripsikan masalah Anda.
3. Lampiran - Lampirkan tangkapan layar dan file lain yang dapat membantu agen pendukung menyelesaikan kasus Anda lebih cepat. Anda dapat melampirkan hingga tiga file. Setiap file dapat mencapai 5 MB.

Setelah Anda menambahkan detail kasus Anda, Anda dapat memilih bagaimana Anda ingin dihubungi.



1. Bahasa kontak pilihan — Pilih bahasa pilihan Anda. Saat ini Anda dapat memilih bahasa Mandarin, Inggris, Jepang, atau Korea. Opsi kontak yang disesuaikan dalam bahasa pilihan Anda akan ditampilkan oleh paket dukungan Anda.
2. Pilih metode kontak. Opsi kontak yang muncul tergantung pada jenis kasus dan rencana dukungan Anda.
   - Jika Anda memilih Web (Web), Anda dapat membaca dan menanggapi kemajuan kasus di Pusat Dukungan.

- Pilih Obrolan atau Telepon. Jika Anda memilih Phone (Telepon), Anda diminta untuk memberikan nomor telepon.

3. Pilih Submit (Kirim) ketika informasi Anda lengkap dan Anda siap untuk membuat kasus.

> **Note**
>
> Jika Anda memilih bahasa Jepang sebagai bahasa kontak pilihan Anda untuk kasus dukungan, dukungan dalam bahasa Jepang mungkin tersedia sebagai berikut:
>
> - Jika Anda memerlukan layanan pelanggan untuk kasus dukungan non-teknis, atau jika Anda memiliki paket Dukungan Pengembang dan memerlukan dukungan teknis, dukungan dalam bahasa Jepang tersedia selama jam kerja di Jepang yang didefinisikan sebagai pukul 09:00 hingga 18:00 Waktu Standar Jepang (GMT+9), tidak termasuk hari libur dan akhir pekan.
> - Jika Anda memiliki paket Business, Enterprise On-Ramp, atau Enterprise Support, dukungan teknis tersedia 24/7 dalam bahasa Jepang.
>
> Jika Anda memilih bahasa Mandarin sebagai bahasa kontak pilihan Anda untuk kasus dukungan, dukungan dalam bahasa Mandarin mungkin tersedia sebagai berikut:
>
> - Jika Anda memerlukan layanan pelanggan untuk kasus dukungan non-teknis, dukungan dalam bahasa Mandarin tersedia pukul 09:00 hingga 18:00 (GMT+8), tidak termasuk hari libur dan akhir pekan.
> - Jika Anda memiliki paket Dukungan Pengembang, dukungan teknis dalam bahasa Mandarin tersedia selama jam kerja yang umumnya didefinisikan sebagai pukul 08:00 hingga 18:00 di negara Anda sebagaimana diatur dalam Akun Saya, tidak termasuk hari libur dan akhir pekan. Waktu ini dapat bervariasi di negara-negara dengan beberapa zona waktu.
> - Jika Anda memiliki paket Business, Enterprise On-Ramp, atau Enterprise Support, dukungan teknis tersedia 24/7 dalam bahasa Mandarin.
>
> Jika Anda memilih bahasa Korea sebagai bahasa kontak pilihan Anda untuk kasus dukungan, dukungan dalam bahasa Korea mungkin tersedia sebagai berikut:

- Jika Anda memerlukan layanan pelanggan untuk kasus dukungan non-teknis, dukungan dalam bahasa Korea tersedia selama jam kerja di Korea yang didefinisikan sebagai 09:00 hingga 18:00 Waktu Standar Korea (GMT+9), tidak termasuk hari libur dan akhir pekan.
- Jika Anda memiliki paket Dukungan Pengembang, dukungan teknis dalam bahasa Korea tersedia selama jam kerja yang umumnya didefinisikan sebagai pukul 08:00 hingga 18:00 di negara Anda sebagaimana diatur dalam Akun Saya, tidak termasuk hari libur dan akhir pekan. Waktu ini dapat bervariasi di negara-negara dengan beberapa zona waktu.
- Jika Anda memiliki paket Business, Enterprise On-Ramp, atau Enterprise Support, dukungan teknis tersedia 24/7 dalam bahasa Korea.

Pemecahan Masalah

Jika Anda mengalami kesulitan saat membuat atau mengelola kasus dukungan, lihat informasi pemecahan masalah berikut.

Saya ingin membuka kembali obrolan langsung untuk kasus saya

Anda dapat membalas kasus dukungan yang ada untuk membuka jendela obrolan lain. Untuk informasi selengkapnya, lihat Memperbarui kasus dukungan yang ada.

Saya tidak dapat terhubung ke obrolan langsung

Jika Anda memilih opsi Obrolan tetapi tidak dapat terhubung ke jendela obrolan, pertama-tama lakukan pemeriksaan berikut:

- Pastikan bahwa Anda telah mengonfigurasi browser Anda untuk mengizinkan jendela pop-up di Support Center.

  > **Note**
  >
  > Tinjau pengaturan untuk browser Anda. Untuk informasi selengkapnya, lihat situs web Bantuan Chrome dan Dukungan Firefox.

- Pastikan bahwa Anda telah mengkonfigurasi jaringan Anda sehingga Anda dapat menggunakanAWS Support:
  - Jaringan Anda dapat mengakses `*.connect.us-east-1.amazonaws.com`titik akhir.

> **Note**
>
> KarenaAWS GovCloud (US), titik akhir adalah`*.connect-fips.us-east-1.amazonaws.com`.

- Firewall Anda mendukung koneksi soket web.

Jika Anda masih tidak dapat terhubung ke jendela obrolan, hubungi AWS Support menggunakan opsi email atau kontak telepon.

Menciptakan peningkatan kuota layanan

Untuk meningkatkan kinerja layanan, permintaan meningkat ke service quotas (sebelumnya disebut sebagai batas).

> **Note**
>
> Anda dapat menggunakan layanan Service Quotas untuk meminta peningkatan layanan Anda. Saat ini, Service Quotas tidak mendukung kuota layanan untuk semua layanan. Untuk informasi lebih, lihat Apa Service Quotas? dalam Panduan Pengguna Service Quotas.

Untuk membuat kasus dukungan untuk peningkatan kuota layanan

1. Masuk ke AWS Support Center Console.

   > **Tip**
   >
   > DalamAWS Management Console, Anda juga dapat memilih ikon tanda tanya ( ) dan kemudian memilih Pusat Support.

2. Pilih Buat kasus.
3. Pilih Mencari batas layanan meningkat?
4. Untuk meminta peningkatan, ikuti petunjuknya. Opsi yang memungkinkan mencakup hal:

   - Jenis batas

- Keparahan

> **Note**
>
> Berdasarkan pilihan kategori, prompt dapat meminta informasi lebih.

5. Untuk Permintaan, pilih Wilayah.
6. Untuk Limit, pilih jenis batas layanan.
7. Untuk nilai batas baru, masukkan nilai yang Anda inginkan.
8. (Opsional) Untuk meminta kenaikan lain, pilih Tambahkan permintaan lain.
9. Untuk Deskripsi kasus, jelaskan kasus dukungan Anda.
10. Untuk halaman Opsi kontak, pilih bahasa pilihan Anda dan bagaimana Anda ingin dihubungi. Anda dapat memilih salah satu opsi:

    - Web - Terima balasan di Pusat Support.
    - Obrolan - Mulai obrolan langsung dengan agen dukungan. Jika Anda tidak dapat terhubung ke chat, lihatPemecahan Masalah.
    - Phone (Telepon) – Menerima panggilan telepon dari agen dukungan. Jika Anda memilih opsi ini:
        - Negara/Wilayah
        - Nomor telepon
        - (Opsional) Ekstensi
11. Pilih Submit (Kirim). Nomor ID kasus dan ringkasan muncul.

Memperbarui, menyelesaikan, dan membuka kembali kasus Anda

Setelah membuat kasus dukungan, Anda dapat memantau status kasus Anda di Pusat Dukungan. Kasus baru dimulai dengan status Unassigned (Belum Ditugaskan). Ketika agen dukungan mulai bekerja pada kasus, status berubah ke Work in Progress (Dalam Proses). Agen dukungan mungkin menanggapi kasus Anda untuk meminta informasi lebih lanjut (Pending Customer Action (Menunggu Tindakan Pelanggan)) atau untuk memberi tahu Anda bahwa kasus sedang diselidiki (Pending Amazon Action (Menunggu Tindakan Amazon)).

Ketika kasus Anda diperbarui, Anda menerima email dengan korespondensi dan tautan ke kasus di Pusat Dukungan. Gunakan tautan dalam pesan email untuk membuka kasus dukungan. Anda tidak dapat menanggapi korespondensi kasus melalui email.

> **Catatan**
>
> - Anda harus masuk ke kasus dukunganAkun AWS yang mengajukan kasus dukungan. Jika Anda masuk sebagai pengguna AWS Identity and Access Management (IAM), Anda harus memiliki izin yang diperlukan untuk melihat kasus dukungan. Untuk informasi selengkapnya, lihat Mengelola akses ke AWS Support Pusat.
> - Jika Anda tidak menanggapi kasus dalam waktu beberapa hari,AWS Support terselesaikan kasus secara otomatis.
> - Kasus Support yang telah dalam keadaan terselesaikan selama lebih dari 14 hari tidak dapat dibuka kembali. Jika Anda memiliki masalah serupa yang terkait dengan kasus terselesaikan, Anda dapat membuat kasus terkait. Untuk informasi selengkapnya, lihat Membuat kasus terkait.

Topik

Memperbarui kasus dukungan yang ada

Anda dapat memperbarui kasus Anda untuk memberikan informasi lebih lanjut untuk agen dukungan. Misalnya, Anda dapat membalas korespondensi, memulai obrolan langsung lainnya, menambahkan penerima email tambahan, dan sebagainya. Namun, Anda tidak dapat memperbarui tingkat keparahan kasus setelah Anda membuatnya. Untuk informasi selengkapnya, lihat Memilih kepelikan.

Untuk memperbarui kasus dukungan yang ada

1. Masuk ke AWS Support Center Console.

> **Tip**
>
> DalamAWS Management Console, Anda juga dapat memilih ikon tanda tanya () dan kemudian memilih Pusat Support.

2. Di bawah Buka kasus dukungan, pilih Subjek kasus dukungan.
3. Pilih Balas. Di bagian Korespondensi, Anda juga dapat membuat salah satu perubahan berikut:
   - Berikan informasi yang diminta agen dukungan
   - Pengunggahan lampiran File
   - Mengubah metode kontak pilihan Anda
   - Tambahkan alamat email untuk menerima pembaruan kasus
4. Pilih Submit (Kirim).

> **Tip**
>
> Jika Anda menutup jendela obrolan dan ingin memulai obrolan langsung lainnya, tambahkan Balas ke kasus dukungan Anda, pilih Obrolan, lalu pilih Kirim. Jendela obrolan pop-up baru terbuka.

Menyelesaikan kasus dukungan

Bila Anda puas dengan respons atau masalah Anda terpecahkan, Anda dapat menyelesaikan kasus di Pusat Dukungan.

Untuk menyelesaikan kasus dukungan

1. Masuklah ke AWS Support Center Console.

> **Tip**
>
> DalamAWS Management Console, Anda juga dapat memilih ikon tanda tanya () dan kemudian memilih Pusat Support.

2. Di bawah Open support cases (Buka kasus dukungan), pilih Subject (Subjek) kasus dukungan yang ingin Anda selesaikan.
3. (Opsional) Pilih Balas dan di bagian Korespondensi, masukkan alasan Anda menyelesaikan kasus ini, lalu pilih Kirim. Misalnya, Anda dapat memasukkan informasi tentang bagaimana Anda memperbaiki masalah sendiri jika Anda memerlukan informasi ini untuk referensi di future.
4. Pilih Resolve case (Selesaikan kasus).
5. Di kotak dialog, pilih Ok (Oke) untuk menyelesaikan kasus ini.

> **Note**
>
> JikaAWS Support menyelesaikan kasus Anda untuk Anda, Anda dapat menggunakan tautan umpan balik untuk memberikan informasi lebih lanjut tentang pengalaman AndaAWS Support.

Example : Tautan Umpan Balik

Screenshot berikut menunjukkan link umpan balik dalam korespondensi kasus di Pusat Support.

Please let us know if we helped resolve your issue:

If YES, click here:
https://console.aws.amazon.com/support/feedback?eventId=1234567890&language=en&questionnaireId=Support-HMD-Yes

If NO, click here:
https://console.aws.amazon.com/support/feedback?eventId=1234567890&language=en&questionnaireId=Support-HMD-No

Membuka kembali kasus terselesaikan

Jika mengalami masalah yang sama lagi, Anda dapat membuka kembali kasus awal. Berikan detail tentang kapan masalah terjadi lagi dan apa langkah pemecahan masalah yang Anda coba. Sertakan nomor kasus terkait sehingga agen dukungan dapat merujuk ke korespondensi sebelumnya.

> **Catatan**
>
> - Anda dapat membuka kembali kasus dukungan hingga 14 hari sejak masalah teratasi. Namun, Anda tidak dapat membuka kembali kasus yang tidak aktif selama lebih dari 14 hari. Anda dapat membuat kasus baru atau kasus terkait. Untuk informasi selengkapnya, lihat Membuat kasus terkait.
> - Jika Anda membuka kembali kasus yang ada yang memiliki informasi berbeda dari masalah Anda saat ini, agen dukungan mungkin meminta Anda untuk membuat kasus baru.

Untuk membuka kembali kasus terselesaikan

1. Masuklah ke AWS Support Center Console.

   > **Tip**
   >
   > DalamAWS Management Console, Anda juga dapat memilih ikon tanda tanya ( ) dan kemudian memilih Pusat Support.

2. Pilih View all cases (Lihat semua kasus) dan kemudian pilih Subject (Subjek) atau Case ID (ID Kasus) kasus dukungan yang ingin Anda buka kembali.
3. Pilih Reopen case (Buka lagi kasus).
4. Di bawah Correspondence (Korespondensi), untuk Reply (Balas), masukkan detail kasus.
5. (Opsional) Pilih Choose files (Pilih file) untuk melampirkan file ke kasus Anda. Anda bisa melampirkan hingga 3 file.
6. Untuk Contact methods (Metode kontak), pilih salah satu opsi berikut:
   - Web (Web) – Dapatkan pemberitahuan melalui email dan Pusat Dukungan.
   - Chat (Obrolan) – Mengobrol daring dengan agen dukungan.

- Phone (Telepon) – Menerima panggilan telepon dari agen dukungan.

7. (Opsional) Untuk Additional contacts (Kontak tambahan), masukkan alamat email untuk orang lain yang Anda ingin menerima korespondensi kasus.
8. Tinjau detail kasus Anda dan pilih Submit (Kirim).

Membuat kasus terkait

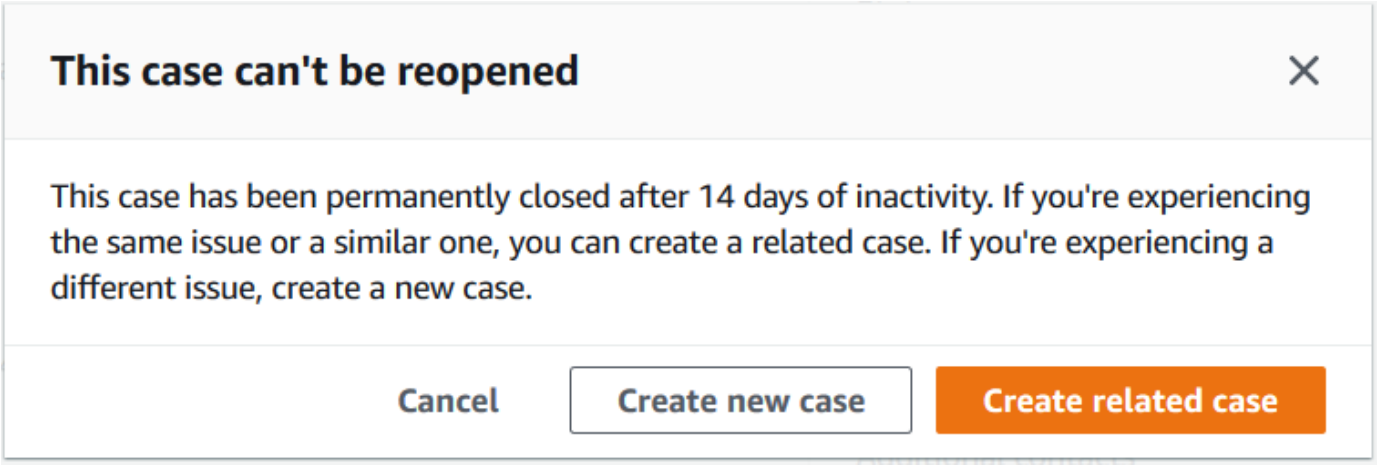
Setelah 14 hari tidak aktif, Anda tidak dapat membuka kembali kasus terselesaikan. Jika Anda memiliki masalah serupa yang terkait dengan kasus terselesaikan, Anda dapat membuat kasus terkait. Kasus terkait ini akan mencakup tautan ke kasus yang telah diselesaikan sebelumnya, sehingga agen dukungan dapat meninjau detail kasus dan korespondensi sebelumnya. Jika Anda mengalami masalah lain, kami menyarankan Anda untuk membuat kasus baru.

Untuk membuat kasus terkait

1. Masuklah ke AWS Support Center Console.

> **Tip**
>
> DalamAWS Management Console, Anda juga dapat memilih ikon tanda tanya () dan kemudian memilih Pusat Support.

2. Pilih View all cases (Lihat semua kasus) dan kemudian pilih Subject (Subjek) atau Case ID (ID Kasus) kasus dukungan yang ingin Anda buka kembali.
3. Pilih Reopen case (Buka lagi kasus).
4. Di kotak dialog, pilih Create related case (Buat kasus terkait). Informasi kasus sebelumnya akan secara otomatis ditambahkan ke kasus terkait Anda. Jika Anda memiliki masalah yang berbeda, pilih Create new case (Buat kasus baru).

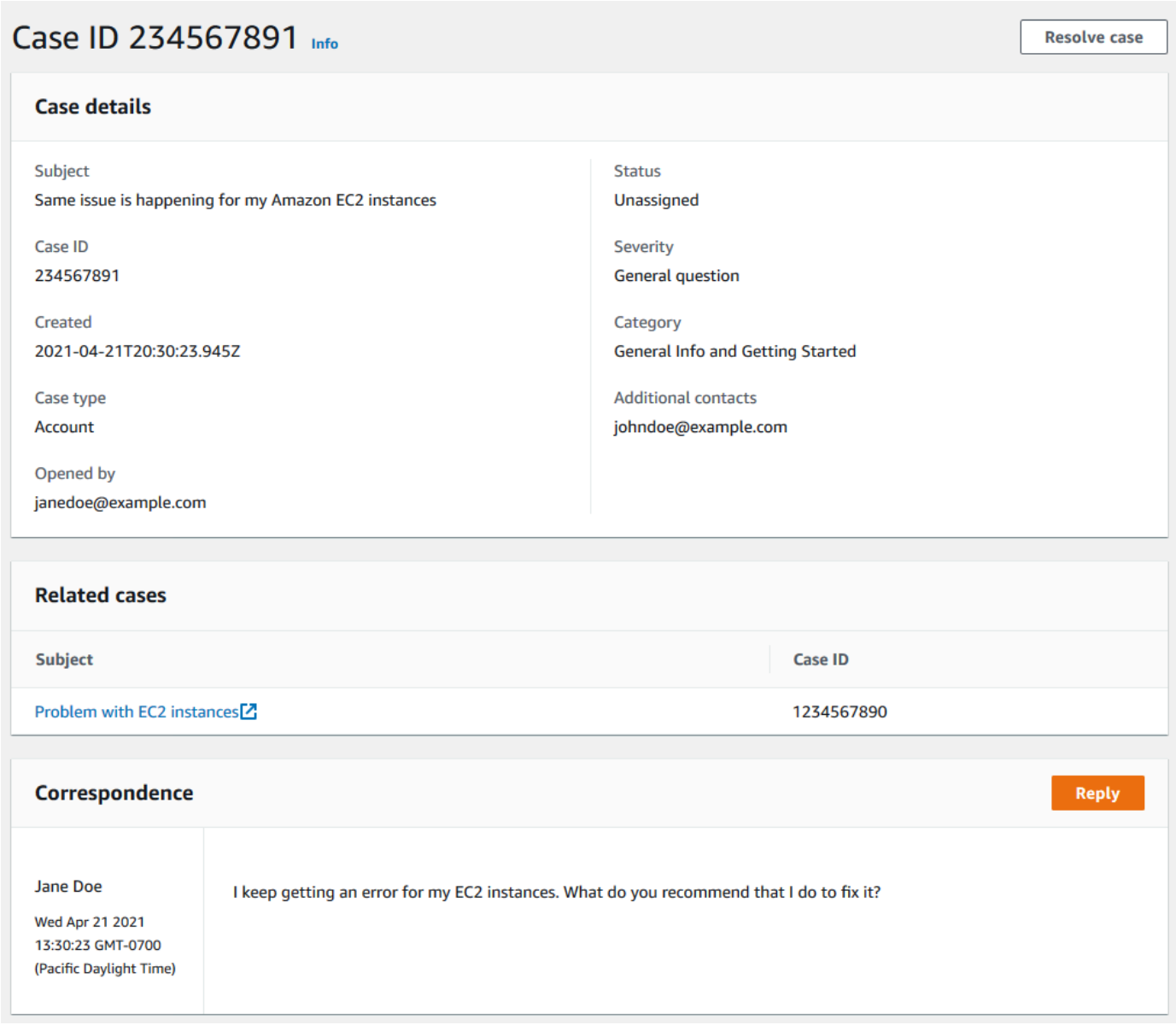


5. Ikuti langkah yang sama untuk membuat kasus Anda. Lihat Membuat kasus dukungan.

> **Note**
>
> Secara default, kasus terkait Anda memiliki Type (Jenis), Category (Kategori), dan Severity (Kepelikan) yang sama dengan kasus sebelumnya. Anda dapat memperbarui detail kasus sesuai kebutuhan.

6. Tinjau detail kasus Anda dan pilih Submit (Kirim).

   Setelah Anda membuat kasus tersebut, kasus sebelumnya muncul di bagian Related cases (Kasus terkait), seperti dalam contoh berikut.



Riwayat kasus

Anda dapat melihat informasi riwayat kasus hingga 24 bulan setelah membuat kasus.

AWS Support Rekomendasi

> **Note**
>
> AWS Support Rekomendasi diberikan sebagai 'Layanan Pratinjau" sebagaimana didefinisikan oleh Ketentuan AWS Layanan. Layanan Pratinjau dapat berubah dan dibatalkan. Pelajari selengkapnya.

AWS Support Rekomendasi menawarkan bantuan pemecahan masalah yang dipersonalisasi untuk masalah akun dan teknis selama alur pembuatan kasus di konsol AWS Support Tengah. AWS Support Rekomendasi bergantung pada detail kasus dan akun yang masuk untuk merespons dengan solusi yang disesuaikan untuk menyelesaikan masalah Anda.

Untuk menganalisis masalah, AWS Support Rekomendasi menanyakan informasi—seperti AccountID, Pengidentifikasi sumber daya AWS , atau pesan galat—dalam lingkup kebijakan/izin pengguna yang disetujui. Pelajari selengkapnya.

Topik

- Mengelola akses ke AWS Support Rekomendasi
- Pemantauan dan pencatatan untuk AWS Support Rekomendasi

Mengelola akses ke AWS Support Rekomendasi

> **Note**
>
> AWS Support Rekomendasi diberikan sebagai 'Layanan Pratinjau" sebagaimana didefinisikan oleh Ketentuan AWS Layanan. Layanan Pratinjau dapat berubah dan dibatalkan. Pelajari selengkapnya.

Anda dapat menggunakan AWS Identity and Access Management (IAM) untuk mengelola akses ke AWS Support Rekomendasi di konsol AWS Support Tengah selama alur pembuatan kasus.

Topik

- AWS Support Rekomendasi tindakan
- Contoh kebijakan IAM untuk Rekomendasi AWS Support

AWS Support Rekomendasi tindakan

Anda dapat menentukan tindakan AWS Support Rekomendasi dalam kebijakan IAM untuk menyediakan akses penuh, menolak akses lengkap, atau menyediakan/menolak akses ke tindakan tertentu.

Tindakan	Deskripsi
`StartSupportTroubleshooting`	Memulai sesi pemecahan masalah terpandu untuk membantu mendiagnosis dan menyelesa ikan masalah akun atau teknis selama alur pembuatan kasus di konsol Tengah. AWS Support
`GetSupportTroubleshootingRe sponse`	Ambil status dan output saat ini dari sesi pemecahan masalah yang dimulai dengan. StartSupportTroubleshooting Termasuk permintaan interaktif untuk informasi lebih lanjut dan rekomendasi untuk menyelesaikan masalah berdasarkan tanggapan sebelumnya.

Contoh kebijakan IAM untuk Rekomendasi AWS Support

Anda dapat menggunakan contoh kebijakan berikut untuk mengelola akses ke AWS Support Rekomendasi.

Akses penuh ke AWS Support Rekomendasi

Kebijakan berikut memungkinkan pengguna akses penuh ke AWS Support Rekomendasi.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "supportrecommendations:StartSupportTroubleshooting",
                "supportrecommendations:GetSupportTroubleshootingResponse"
            ],
```

```
            "Resource": "*"
        }
    ]
}
```

Tolak akses ke AWS Support Rekomendasi

Kebijakan berikut tidak mengizinkan pengguna mengakses AWS Support Rekomendasi.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "supportrecommendations:*",
            "Resource": "*"
        }
    ]
}
```

Pemantauan dan pencatatan untuk AWS Support Rekomendasi

> **Note**
>
> AWS Support Rekomendasi diberikan sebagai 'Layanan Pratinjau" sebagaimana didefinisikan oleh Ketentuan AWS Layanan. Layanan Pratinjau dapat berubah dan dibatalkan. Pelajari selengkapnya.

Pemantauan adalah bagian penting dalam menjaga keandalan, ketersediaan, dan kinerja AWS Support Rekomendasi dan AWS solusi Anda yang lain. AWS menyediakan alat pemantauan berikut untuk menonton AWS Support Rekomendasi, melaporkan ketika ada sesuatu yang salah, dan mengambil tindakan otomatis bila perlu:

- AWS CloudTrailmenangkap panggilan API dan peristiwa terkait yang dibuat oleh atau atas nama AWS akun Anda dan mengirimkan file log ke bucket Amazon S3 yang Anda tentukan. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. Untuk informasi selengkapnya, lihat Panduan Pengguna AWS CloudTrail.

Topik

AWS Support Rekomendasi Pencatatan panggilan dengan AWS CloudTrail

> **Note**
>
> AWS Support Rekomendasi diberikan sebagai 'Layanan Pratinjau" sebagaimana didefinisikan oleh Ketentuan AWS Layanan. Layanan Pratinjau dapat berubah dan dibatalkan. Pelajari selengkapnya.

AWS Support Rekomendasi terintegrasi dengan AWS CloudTrail, layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atau AWS layanan. CloudTrail menangkap panggilan API untuk AWS Support Rekomendasi sebagai peristiwa. Panggilan yang diambil termasuk panggilan dari konsol AWS Support Pusat dan panggilan kode ke AWS Support Rekomendasi.

Jika Anda membuat jejak, Anda dapat mengaktifkan pengiriman CloudTrail acara secara terus menerus ke bucket Amazon Simple Storage Service (Amazon S3), termasuk peristiwa untuk Rekomendasi. AWS Support 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 AWS Support Rekomendasi, alamat IP dari mana permintaan dibuat, siapa yang membuat permintaan, kapan dibuat, dan detail tambahan.

Untuk mempelajari selengkapnya CloudTrail, termasuk cara mengonfigurasi dan mengaktifkannya, lihat Panduan AWS CloudTrail Pengguna.

AWS Support Rekomendasi informasi di CloudTrail

CloudTrail diaktifkan di AWS akun Anda saat Anda membuat akun. Ketika aktivitas acara yang didukung terjadi di AWS Support Rekomendasi, aktivitas tersebut dicatat dalam suatu CloudTrail peristiwa bersama dengan peristiwa AWS layanan lainnya dalam riwayat Acara. Anda dapat melihat, mencari, dan mengunduh acara terbaru di AWS akun Anda. Untuk informasi selengkapnya, lihat Melihat peristiwa dengan riwayat CloudTrail acara.

Untuk catatan peristiwa yang sedang berlangsung di AWS akun Anda, termasuk acara untuk AWS Support Rekomendasi, buat jejak. Jejak memungkinkan CloudTrail untuk mengirimkan file log ke

bucket Amazon S3. Secara default, saat Anda membuat jejak di konsol tersebut, jejak diterapkan ke semua Wilayah AWS . Jejak mencatat peristiwa dari semua Wilayah di AWS partisi dan mengirimkan file 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 berikut:

- Gambaran umum untuk membuat jejak
- 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 panggilan AWS Support Rekomendasi dicatat oleh CloudTrail. Setiap entri peristiwa atau log berisi informasi tentang siapa yang membuat permintaan tersebut. Informasi identitas membantu Anda menentukan berikut ini:

- Apakah permintaan itu dibuat dengan kredenal pengguna root atau AWS Identity and Access Management (IAM).
- Apakah permintaan tersebut dibuat dengan kredensial keamanan sementara untuk satu peran atau pengguna terfederasi.
- Apakah permintaan itu dibuat oleh AWS layanan lain.

Untuk informasi selengkapnya, lihat elemen CloudTrail UserIdentity.

Anda juga dapat menggabungkan file log AWS Support Rekomendasi dari beberapa AWS Wilayah dan beberapa AWS akun ke dalam satu bucket Amazon S3.

Memahami AWS Support Rekomendasi entri berkas log

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 menunjukkan satu permintaan dari sumber mana pun. Ini mencakup informasi tentang operasi yang diminta, tanggal dan waktu operasi, parameter permintaan, dan sebagainya. CloudTrail file log bukanlah jejak tumpukan yang diurutkan dari panggilan API publik, jadi file tersebut tidak muncul dalam urutan tertentu.

Example : Entri log untuk **`StartSupportTroubleshooting`**

Contoh berikut menunjukkan entri CloudTrail log untuk `StartSupportTroubleshooting` operasi.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::111122223333:user/Admin",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    },
    "eventTime": "2023-09-11T16:34:13Z",
    "eventSource": "supportrecommendations.amazonaws.com",
    "eventName": "StartSupportTroubleshooting",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "72.21.198.67",
    "userAgent": "signin.amazonaws.com",
    "requestParameters": {
        "message": "..."
    },
    "responseElements": null,
    "requestID": "4c4d5fc8-c403-4f82-9544-41f820e0fa01",
    "eventID": "2f4630ac-5c27-4f0d-b93f-63742d6fc85e",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```


Example : Entri log untuk **`GetSupportTroubleshootingResponse`**

Contoh berikut menunjukkan entri CloudTrail log untuk `GetSupportTroubleshootingResponse` operasi.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::111122223333:user/Admin",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    },
```

```
    "eventTime": "2023-09-11T16:34:13Z",
    "eventSource": "supportrecommendations.amazonaws.com",
    "eventName": "GetSupportTroubleshootingResponse",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "72.21.198.67",
    "userAgent": "signin.amazonaws.com",
    "requestParameters": {
        "conversationId": "..."
    },
    "responseElements": null,
    "requestID": "4c4d5fc8-c403-4f82-9544-41f820e0fa01",
    "eventID": "2f4630ac-5c27-4f0d-b93f-63742d6fc85e",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```


Menggunakan AWS Support dengan AWS SDK

AWS kit pengembangan perangkat lunak (SDK) tersedia untuk banyak bahasa pemrograman populer. Setiap SDK menyediakan API, contoh kode, dan dokumentasi yang memudahkan developer untuk membangun aplikasi dalam bahasa pilihan mereka.

Dokumentasi SDK	Contoh kode
AWS SDK for C++	AWS SDK for C++ contoh kode
AWS CLI	AWS CLI contoh kode
AWS SDK for Go	AWS SDK for Go contoh kode
AWS SDK for Java	AWS SDK for Java contoh kode
AWS SDK for JavaScript	AWS SDK for JavaScript contoh kode
AWS SDK for Kotlin	AWS SDK for Kotlin contoh kode
AWS SDK for .NET	AWS SDK for .NET contoh kode

Dokumentasi SDK	Contoh kode
AWS SDK for PHP	AWS SDK for PHP contoh kode
AWS Tools for PowerShell	Alat untuk contoh PowerShell kode
AWS SDK for Python (Boto3)	AWS SDK for Python (Boto3) contoh kode
AWS SDK for Ruby	AWS SDK for Ruby contoh kode
AWS SDK for Rust	AWS SDK for Rust contoh kode
AWS SDK untuk SAP ABAP	AWS SDK untuk SAP ABAP contoh kode
AWS SDK for Swift	AWS SDK for Swift contoh kode

Ketersediaan contoh

Tidak dapat menemukan apa yang Anda butuhkan? Minta contoh kode menggunakan tautan Berikan umpan balik di bagian bawah halaman ini.

Tentang API AWS Support

API AWS Support menyediakan akses ke beberapa fitur di Pusat Dukungan AWS.

API menyediakan dua grup operasi yang berbeda:

- Operasi Manajemen kasus dukungan untuk mengelola seluruh siklus hidup kasus dukungan AWS, dari menciptakan kasus sampai menyelesaikannya
- Operasi AWS Trusted Advisor untuk mengakses pemeriksaan AWS Trusted Advisor

> **Note**
>
> Anda harus memiliki paket Business, Enterprise On-Ramp, atau Enterprise Support untuk menggunakan API. AWS Support Untuk informasi selengkapnya, lihat AWS Support.

Untuk informasi lebih lanjut tentang operasi dan tipe data yang disediakan oleh AWS Support, lihat Referensi API AWS Support.

Topik

Manajemen kasus dukungan

Anda dapat menggunakan API untuk melakukan tugas-tugas berikut:

- Membuka kasus dukungan
- Mendapatkan daftar dan informasi detail tentang kasus dukungan terbaru
- Memfilter pencarian Anda untuk kasus dukungan berdasarkan tanggal dan pengidentifikasi kasus, termasuk kasus yang diselesaikan
- Tambahkan komunikasi dan lampiran file ke kasus Anda, dan tambahkan penerima email untuk korespondensi kasus. Anda dapat melampirkan hingga tiga file. Setiap file bisa sampai 5 MB

- Menyelesaikan kasus Anda

AWS SupportAPI mendukung CloudTrail pencatatan untuk mendukung operasi manajemen kasus. Untuk informasi selengkapnya, lihat Mencatat panggilan API AWS Support dengan AWS CloudTrail.

Untuk contoh kode yang menunjukkan cara mengelola seluruh siklus hidup kasus dukungan, lihat Contoh kode untuk AWS Support menggunakan AWS SDK..

AWS Trusted Advisor

Anda dapat menggunakan operasi Trusted Advisor untuk melakukan tugas-tugas berikut:

- Dapatkan nama dan pengidentifikasi untuk pemeriksaan Trusted Advisor
- Meminta pemeriksaan Trusted Advisor dijalankan terhadap akun dan sumber daya AWS
- Dapatkan ringkasan dan informasi detail untuk hasil pemeriksaan Trusted Advisor
- Segarkan pemeriksaan Trusted Advisor Anda
- Dapatkan status setiap pemeriksaan Trusted Advisor

AWS SupportAPI mendukung CloudTrail pencatatan untuk Trusted Advisor operasi. Untuk informasi selengkapnya, lihat AWS Trusted Advisorinformasi dalam CloudTrail logging.

Anda dapat menggunakan Amazon CloudWatch Events untuk memantau perubahan pada hasil pemeriksaan AndaTrusted Advisor. Untuk informasi selengkapnya, lihat Memantau hasil AWS Trusted Advisor pemeriksaan dengan Amazon EventBridge.

Untuk kode Java yang menunjukkan bagaimana menggunakan operasi Trusted Advisor, lihat Menggunakan Trusted Advisor sebagai layanan web.

Titik akhir

AWS Support adalah layanan global. Ini berarti bahwa titik akhir apa pun yang Anda gunakan akan memperbarui kasus dukungan Anda di Konsol Pusat Dukungan.

Misalnya, jika Anda menggunakan titik akhir AS Timur (Virginia N.) untuk membuat kasus, Anda dapat menggunakan titik akhir AS Barat (Oregon) atau Eropa (Irlandia) untuk menambahkan korespondensi ke kasus yang sama.

Anda dapat menggunakan endpoint berikut untuk AWS Support API:

- AS Timur (Virginia N.) - https://support.us-east-1.amazonaws.com
- AS Barat (Oregon) - https://support.us-west-2.amazonaws.com
- Eropa (Irlandia) - https://support.eu-west-1.amazonaws.com

> **Important**
>
> - Jika Anda memanggil CreateCaseoperasi untuk membuat kasus dukungan pengujian, kami sarankan Anda menyertakan baris subjek, seperti TEST CASE-tolong abaikan. Setelah Anda selesai dengan kasus dukungan pengujian Anda, hubungi ResolveCaseoperasi untuk menyelesaikannya.
> - Untuk memanggil AWS Trusted Advisor operasi di AWS Support API, Anda harus menggunakan titik akhir AS Timur (Virginia N.). Saat ini, titik akhir AS Barat (Oregon) dan Eropa (Irlandia) tidak mendukung operasi. Trusted Advisor

Untuk informasi selengkapnya tentang AWS titik akhir, lihat AWS Supporttitik akhir dan kuota di. Referensi Umum Amazon Web

Dukungan di SDK AWS

Kit Pengembangan Perangkat Lunak (SDK) AWS Command Line Interface (AWS CLI) dan AWS termasuk dukungan untuk API AWS Support.

Untuk daftar bahasa yang mendukung AWS Support API, pilih nama operasi, seperti CreateCase, dan di bagian Lihat Juga, pilih bahasa pilihan Anda.

AWS Support Rencana

Anda dapat mengubah AWS Support Paket untuk akun Anda berdasarkan kebutuhan bisnis Anda.

Topik

Fitur AWS Support Rencana

AWS Support menawarkan lima paket dukungan:

- Basic
- Developer
- Bisnis
- Perusahaan On-Ramp
- Perusahaan

Basic Support menawarkan dukungan untuk pertanyaan akun dan penagihan dan peningkatan service quotas. Paket lain menawarkan sejumlah kasus dukungan teknis dengan pay-by-the-month harga dan tidak ada kontrak jangka panjang.

Semua AWS pelanggan secara otomatis memiliki akses 24x7 ke fitur-fitur Basic Support ini:

- O ne-on-one tanggapan untuk pertanyaan akun dan penagihan
- Forum dukungan
- Pemeriksaan kondisi layanan
- Dokumentasi, makalah teknis, dan panduan praktik terbaik

Pelanggan dengan paket Dukungan Developer memiliki akses ke fitur tambahan berikut:

- Panduan praktik terbaik
- Alat diagnostik sisi klien

- Dukungan arsitektur blok bangunan: panduan tentang cara menggunakan AWS produk, fitur, dan layanan bersama
- Mendukung jumlah kasus dukungan yang tidak terbatas yang dapat dibuka oleh pengguna mana pun dengan izin.

Selain itu, pelanggan dengan paket Business, Enterprise On-Ramp, atau Enterprise Support memiliki akses ke fitur-fitur berikut:

- Panduan kasus penggunaan — AWS Produk, fitur, dan layanan apa yang digunakan untuk mendukung kebutuhan spesifik Anda dengan sebaik-baiknya.
- AWS Trusted Advisor— Fitur AWS Support, yang memeriksa lingkungan pelanggan dan mengidentifikasi peluang untuk menghemat uang, menutup kesenjangan keamanan, dan meningkatkan keandalan dan kinerja sistem. Anda dapat mengakses semua Trusted Advisor cek.
- AWS Support API untuk berinteraksi dengan Support Center dan Trusted Advisor. Anda dapat menggunakan API AWS Support untuk mengotomatiskan manajemen kasus dukungan dan operasi Trusted Advisor .
- Dukungan perangkat lunak pihak ketiga – Bantuan dengan sistem operasi instans Amazon Elastic Compute Cloud (Amazon EC2) dan konfigurasinya. Juga, bantu kinerja komponen perangkat lunak pihak ketiga yang paling populer di AWS. Dukungan perangkat lunak pihak ketiga tidak tersedia untuk pelanggan pada paket Basic atau Developer Support.
- Mendukung jumlah pengguna AWS Identity and Access Management (IAM) yang tidak terbatas yang dapat membuka kasus dukungan teknis.

Selain itu, pelanggan dengan paket Enterprise On-Ramp atau Enterprise Support memiliki akses ke fitur-fitur ini:

- Panduan arsitektur aplikasi — Panduan konsultatif tentang bagaimana layanan cocok bersama untuk memenuhi kasus penggunaan, beban kerja, atau aplikasi spesifik Anda.
- Manajemen kejadian infrastruktur – Keterlibatan jangka pendek dengan AWS Support untuk mendapatkan pemahaman mendalam tentang kasus penggunaan Anda. Setelah analisis, memberikan bimbingan arsitektur dan penskalaan untuk suatu kejadian.
- Manajer akun teknis – Bekerja sama dengan manajer akun teknis (TAM) untuk kasus dan aplikasi penggunaan spesifik Anda.
- Perutean kasus sarung tangan putih.
- Ulasan bisnis manajemen.

Untuk informasi selengkapnya tentang fitur dan harga untuk setiap paket dukungan, lihat AWS Supportdan Bandingkan AWS Support paket. Beberapa fitur, seperti telepon 24x7 dan dukungan obrolan, tidak tersedia dalam semua bahasa.

Mengubah AWS Support Rencana

Anda dapat menggunakan konsol AWS Support Paket untuk mengubah paket dukungan untuk paket Anda Akun AWS. Untuk mengubah paket dukungan, Anda harus memiliki izin AWS Identity and Access Management (IAM) atau masuk ke akun Anda sebagai pengguna root. Untuk informasi selengkapnya, lihat Mengelola akses ke AWS Support Paket dan AWS kebijakan terkelola untuk AWS Support Rencana.

Untuk mengubah paket dukungan

1. Masuk ke konsol AWS Support Paket di https://console.aws.amazon.com/support/plans/home.
2. (Opsional) Pada halaman AWS Support Paket, bandingkan rencana dukungan. Untuk informasi lebih lanjut tentang harga, kunjungi halaman detail harga.
3. (Opsional) Di bawah contoh AWS Support harga, pilih Lihat contoh, lalu pilih salah satu opsi paket dukungan untuk melihat perkiraan biaya.
4. Saat Anda memutuskan paket, pilih Tinjau downgrade atau Tinjau upgrade untuk paket yang Anda inginkan.

   > **Catatan**
   >
   > - Jika Anda mendaftar untuk paket dukungan berbayar, Anda bertanggung jawab untuk berlangganan minimal satu bulan AWS Support. Untuk informasi lebih lanjut, lihat AWS Support FAQ.
   > - Jika Anda memiliki paket Enterprise On-Ramp atau Enterprise Support, pada kotak dialog Konfirmasi Ubah rencana, hubungi AWS Supportuntuk mengubah paket dukungan Anda.

5. Di kotak dialog Ubah konfirmasi rencana, Anda dapat memperluas item dukungan untuk melihat fitur yang ingin ditambahkan atau dihapus dari akun Anda.

   Di bawah Harga, Anda dapat melihat biaya satu kali yang diproyeksikan untuk paket dukungan baru.
6. Pilih Terima dan setuju.

Informasi terkait

Untuk informasi selengkapnya tentang AWS Support Paket, lihat AWS Support FAQ. Anda juga dapat memilih Hubungi kami dari konsol Support Plans.

Untuk menutup akun, lihat Menutup Akun dalam Panduan Pengguna AWS Billing .

AWS Trusted Advisor

Trusted Advisor mengacu pada praktik terbaik yang dipelajari dari melayani ratusan ribu AWS pelanggan. Trusted Advisor memeriksa AWS lingkungan Anda, dan kemudian membuat rekomendasi ketika ada peluang untuk menghemat uang, meningkatkan ketersediaan dan kinerja sistem, atau membantu menutup kesenjangan keamanan.

Jika Anda memiliki paket Dukungan Dasar atau Pengembang, Anda dapat menggunakan Trusted Advisor konsol untuk mengakses semua pemeriksaan dalam kategori Batas Layanan dan enam pemeriksaan dalam kategori Keamanan.

Jika Anda memiliki paket Business, Enterprise On-Ramp, atau Enterprise Support, Anda dapat menggunakan Trusted Advisor konsol dan AWS Trusted Advisor API untuk mengakses semua Trusted Advisor pemeriksaan. Anda juga dapat menggunakan Amazon CloudWatch Events untuk memantau status Trusted Advisor pemeriksaan. Untuk informasi selengkapnya, lihat Memantau hasil AWS Trusted Advisor pemeriksaan dengan Amazon EventBridge.

Anda dapat mengakses Trusted Advisor di AWS Management Console. Untuk informasi selengkapnya tentang mengontrol akses ke Trusted Advisor konsol, lihatKelola akses ke AWS Trusted Advisor.

Untuk informasi selengkapnya, lihat Trusted Advisor.

Topik

- Memulai dengan Trusted Advisor Rekomendasi
- Memulai dengan Trusted Advisor API
- Menggunakan Trusted Advisor sebagai layanan web
- Tampilan organisasi untuk AWS Trusted Advisor
- Lihat AWS Trusted Advisor cek yang didukung oleh AWS Config
- MelihatAWS Security Hub kontrol diAWS Trusted Advisor
- Ikut serta AWS Compute Optimizer untuk Trusted Advisor cek
- Memulai dengan AWS Trusted Advisor Prioritas
- Memulai dengan AWS Trusted Advisor Engage (Pratinjau)
- AWS Trusted Advisor periksa referensi
- Ubah log untuk AWS Trusted Advisor

Memulai dengan Trusted Advisor Rekomendasi

Anda dapat menggunakan halaman Trusted Advisor Rekomendasi Trusted Advisor konsol untuk meninjau hasil pemeriksaan untuk Anda Akun AWS dan kemudian ikuti langkah-langkah yang disarankan untuk memperbaiki masalah apa pun. Misalnya, Trusted Advisor mungkin menyarankan Anda menghapus sumber daya yang tidak terpakai untuk mengurangi tagihan bulanan Anda, seperti instans Amazon Elastic Compute Cloud (Amazon EC2).

Anda juga dapat menggunakan AWS Trusted Advisor API untuk melakukan operasi pada Trusted Advisor pemeriksaan Anda. Untuk informasi selengkapnya, lihat Referensi AWS Trusted Advisor API

Topik

Masuk ke Trusted Advisor konsol

Anda dapat melihat cek dan status setiap cek di Trusted Advisor konsol.

> **Note**
>
> Anda harus memiliki izin AWS Identity and Access Management (IAM) untuk mengakses konsol. Trusted Advisor Untuk informasi selengkapnya, lihat Kelola akses ke AWS Trusted Advisor.

Untuk masuk ke Trusted Advisor konsol

1. Masuk ke Trusted Advisor konsol di https://console.aws.amazon.com/trustedadvisor/home.

2. Pada halaman Trusted Advisor Rekomendasi, lihat ringkasan untuk setiap kategori cek:

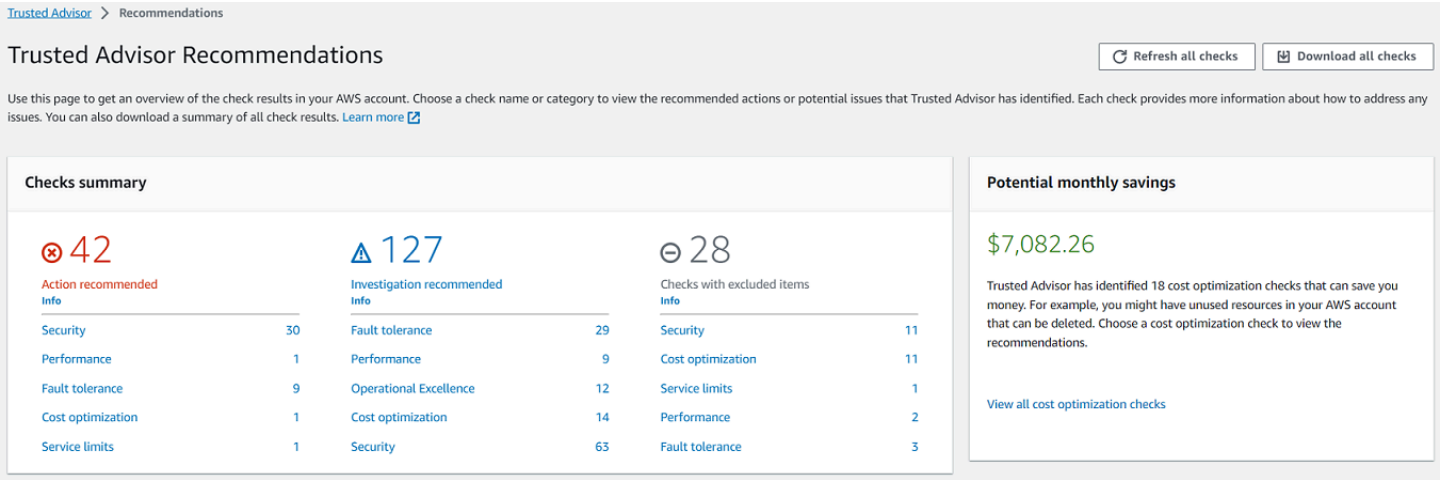
   - Tindakan direkomendasikan (merah) — Trusted Advisor merekomendasikan tindakan untuk pemeriksaan. Misalnya, pemeriksaan yang mendeteksi masalah keamanan untuk sumber daya IAM Anda mungkin merekomendasikan langkah-langkah mendesak.
   - Investigasi direkomendasikan (kuning) — Trusted Advisor mendeteksi kemungkinan masalah untuk pemeriksaan. Misalnya, pemeriksaan yang mencapai kuota untuk sumber daya mungkin merekomendasikan cara untuk menghapus sumber daya yang tidak digunakan.
   - Cek dengan item yang dikecualikan (abu-abu) - Jumlah cek yang telah mengecualikan item, seperti sumber daya yang ingin diabaikan oleh cek. Misalnya, ini mungkin instans Amazon EC2 yang Anda tidak ingin cek untuk mengevaluasi.

3. Anda dapat melakukan hal berikut di halaman Trusted Advisor Rekomendasi:

   - Untuk menyegarkan semua cek di akun Anda, pilih Segarkan semua cek.
   - Untuk membuat file.xls yang menyertakan semua hasil pemeriksaan, pilih Unduh semua cek.
   - Di bawah Ringkasan cek, pilih kategori centang, seperti Keamanan, untuk melihat hasilnya.
   - Di bawah Potensi tabungan bulanan, Anda dapat melihat berapa banyak yang dapat Anda hemat untuk akun Anda dan pengoptimalan biaya memeriksa rekomendasi.
   - Di bawah Perubahan terbaru, Anda dapat melihat perubahan untuk memeriksa status dalam 30 hari terakhir. Pilih nama centang untuk melihat hasil terbaru untuk pemeriksaan itu atau pilih ikon panah untuk melihat halaman berikutnya.

Example : Trusted Advisor Rekomendasi

Contoh berikut menunjukkan ringkasan hasil pemeriksaan untuk Akun AWS.



Melihat kategori pemeriksaan

Anda dapat melihat deskripsi dan hasil pemeriksaan untuk kategori pemeriksaan berikut:

- Optimalisasi biaya — Rekomendasi yang berpotensi menghemat uang Anda. Pemeriksaan ini menyoroti sumber daya yang tidak terpakai dan peluang untuk mengurangi tagihan Anda.
- Kinerja – Rekomendasi yang dapat meningkatkan kecepatan dan respons aplikasi Anda.
- Keamanan — Rekomendasi untuk pengaturan keamanan yang dapat membuat AWS solusi Anda lebih aman.
- Toleransi kesalahan — Rekomendasi yang membantu meningkatkan ketahanan solusi Anda AWS . Pemeriksaan ini menyoroti kekurangan redundansi dan sumber daya yang digunakan secara berlebihan.
- Batas layanan — Memeriksa penggunaan untuk akun Anda dan apakah akun Anda mendekati atau melebihi batas (juga dikenal sebagai kuota) untuk AWS layanan dan sumber daya.
- Keunggulan Operasional — Rekomendasi untuk membantu Anda mengoperasikan AWS lingkungan Anda secara efektif, dan dalam skala besar.

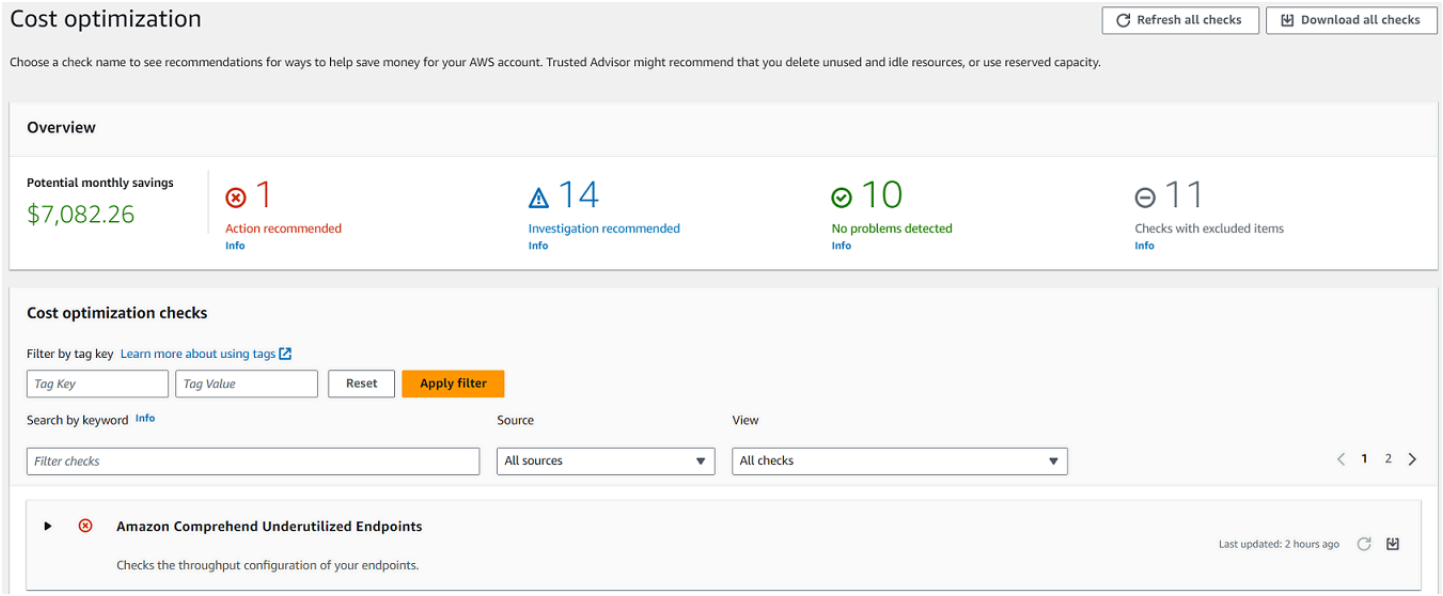
Untuk melihat kategori pemeriksaan

1. Masuk ke Trusted Advisor konsol di https://console.aws.amazon.com/trustedadvisor/home.
2. Di panel navigasi, pilih kategori centang.
3. Pada halaman kategori, lihat ringkasan untuk setiap kategori cek:
   - Tindakan direkomendasikan (merah) — Trusted Advisor merekomendasikan tindakan untuk pemeriksaan.
   - Investigasi direkomendasikan (kuning) — Trusted Advisor mendeteksi kemungkinan masalah untuk pemeriksaan.
   - Tidak ada masalah yang terdeteksi (hijau) — Trusted Advisor tidak mendeteksi masalah untuk pemeriksaan.
   - Item yang dikecualikan (abu-abu) - Jumlah cek yang telah mengecualikan item, seperti sumber daya yang ingin diabaikan oleh cek.
4. Untuk setiap pemeriksaan, pilih ikon refresh
   ()
   untuk menyegarkan cek ini.

5. Pilih ikon unduhan
   ( )
   untuk membuat file.xls yang menyertakan hasil pemeriksaan ini.

Example : Kategori pengoptimalan biaya

Contoh berikut menunjukkan 10 (hijau) cek yang tidak memiliki masalah.



Melihat pemeriksaan spesifik

Perluas cek untuk melihat deskripsi pemeriksaan lengkap, sumber daya Anda yang terpengaruh, langkah-langkah yang disarankan, dan tautan ke informasi selengkapnya.

Untuk melihat pemeriksaan tertentu

1. Masuk ke Trusted Advisor konsol di https://console.aws.amazon.com/trustedadvisor/home.
2. Di panel navigasi, pilih kategori centang.
3. Pilih nama pemeriksaan untuk melihat deskripsi dan detail berikut:

   - Alert Criteria (Kriteria Peringatan) – Menjelaskan ambang batas ketika pemeriksaan akan mengubah status.
   - Recommended Action (Tindakan yang Disarankan) – Menjelaskan tindakan yang disarankan untuk pemeriksaan ini.
   - Additional Resources (Sumber Daya Tambahan) – Daftar terkait dokumentasi AWS .

- Tabel yang mencantumkan item yang terpengaruh di akun Anda. Anda dapat menyertakan atau mengecualikan item ini dari hasil pemeriksaan.

4. (Opsional) Untuk mengecualikan item sehingga tidak muncul di hasil pemeriksaan:

   a. Pilih item dan pilih Exclude & Refresh.

   b. Untuk melihat semua item yang dikecualikan, pilih Item yang dikecualikan.

5. (Opsional) Untuk memasukkan item sehingga cek mengevaluasi mereka lagi:

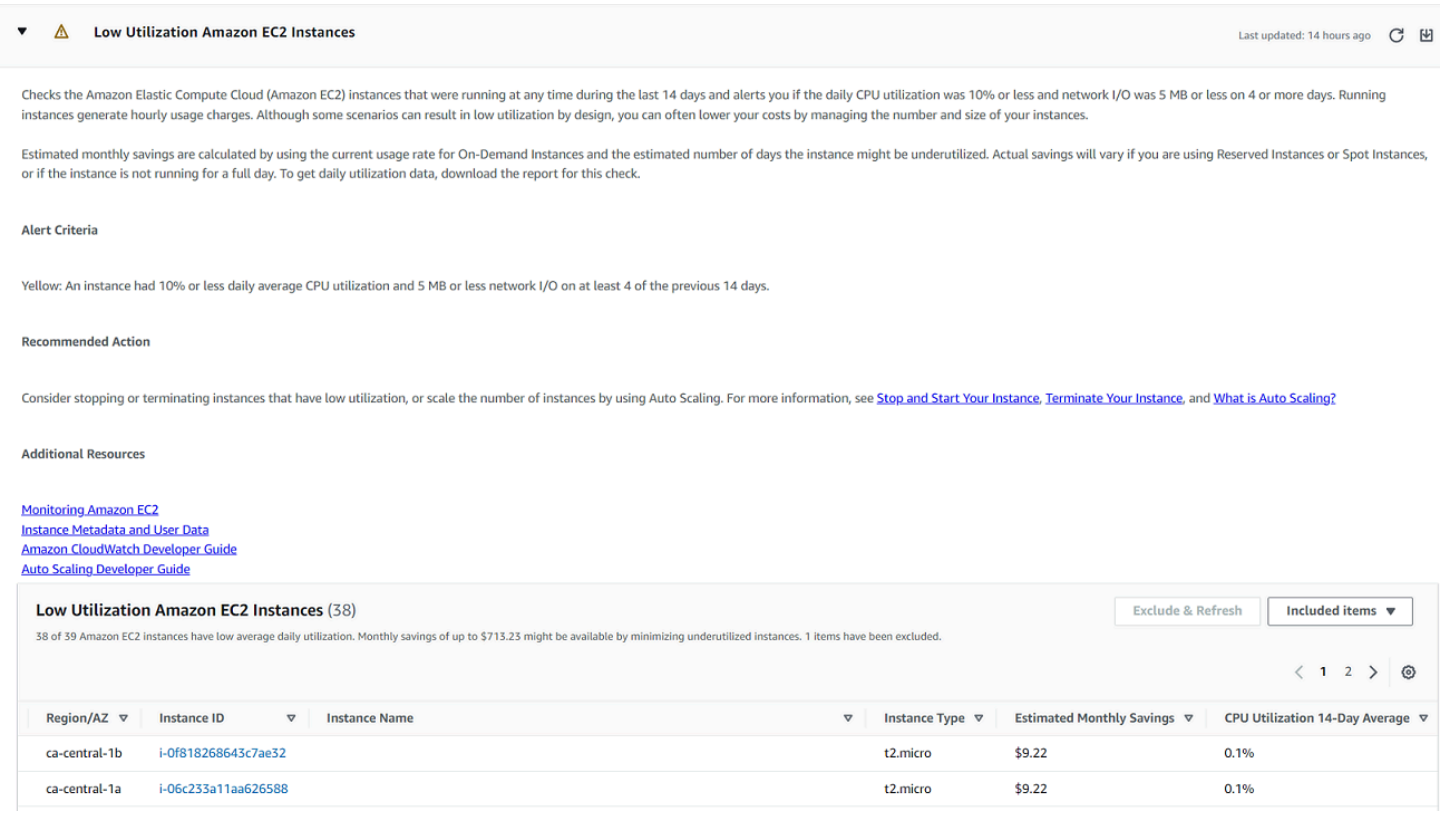
   a. Pilih Item yang dikecualikan, pilih item, lalu pilih Sertakan & Segarkan.

   b. Untuk melihat semua item yang disertakan, pilih item Termasuk.

6. Pilih ikon pengaturan
   ( ).
   Di kotak dialog Preferensi, Anda dapat menentukan jumlah item atau properti yang akan ditampilkan, lalu pilih Konfirmasi.

Example : Pemeriksaan optimasi biaya

Low Utilization Amazon EC2 Instances (Instans Amazon EC2 Penggunaan Rendah) berikut memeriksa daftar instans yang terpengaruh di akun. Pemeriksaan ini mengidentifikasi 38 instans Amazon EC2 yang memiliki penggunaan rendah dan menyarankan Anda menghentikan atau menghentikan sumber daya.



Memfilter pemeriksaan Anda

Pada halaman kategori pemeriksaan, Anda dapat menentukan hasil pemeriksaan yang ingin Anda lihat. Misalnya, Anda dapat memfilter berdasarkan pemeriksaan yang telah mendeteksi kesalahan di akun Anda sehingga Anda dapat menyelidiki masalah mendesak terlebih dahulu.

Jika Anda memiliki pemeriksaan yang mengevaluasi item di akun Anda, seperti AWS sumber daya, Anda dapat menggunakan filter tag untuk hanya menampilkan item yang memiliki tag yang ditentukan.

Untuk memfilter pemeriksaan

1. Masuk ke Trusted Advisor konsol di https://console.aws.amazon.com/trustedadvisor/home.
2. Di panel navigasi atau halaman Trusted Advisor Rekomendasi, pilih kategori centang.
3. Untuk Cari berdasarkan kata kunci, masukkan kata kunci dari nama cek atau deskripsi untuk memfilter hasil Anda.
4. Untuk daftar View (Tampilan), tentukan cek untuk dilihat:

   - Semua cek — Daftar semua cek untuk kategori ini.

- Tindakan yang direkomendasikan - Daftar cek yang menyarankan Anda mengambil tindakan. Pemeriksaan ini disorot dengan warna merah.
- Investigasi direkomendasikan — Daftar cek yang menyarankan Anda mengambil tindakan yang mungkin. Cek ini disorot dengan warna kuning.
- Tidak ada masalah yang terdeteksi - Daftar pemeriksaan yang tidak memiliki masalah. Pemeriksaan ini disorot dengan warna hijau.
- Cek dengan item yang dikecualikan — Cek daftar yang Anda tentukan untuk mengecualikan item dari hasil pemeriksaan.

5. Jika menambahkan tag ke AWS sumber daya, seperti instans atau AWS CloudTrail jejak Amazon EC2, Anda dapat memfilter hasil sehingga pemeriksaan hanya menampilkan item yang memiliki tag yang ditentukan.

   Untuk Filter menurut tag, masukkan kunci tag dan nilai, lalu pilih Terapkan filter.
6. Dalam tabel untuk pemeriksaan, hasil pemeriksaan hanya menampilkan item yang memiliki kunci dan nilai yang ditentukan.
7. Untuk menghapus filter berdasarkan tanda, pilih Reset (Atur Ulang).

Informasi terkait

Untuk informasi selengkapnya tentang penandaan Trusted Advisor, lihat topik berikut:

- AWS Support memungkinkan kemampuan penandaan untuk Trusted Advisor
- Menandai AWS sumber daya di Referensi Umum AWS

Menyegarkan hasil pemeriksaan

Anda dapat menyegarkan pemeriksaan untuk mendapatkan hasil terbaru untuk akun Anda. Jika Anda memiliki paket Pengembang atau Dukungan Dasar, Anda dapat masuk ke Trusted Advisor konsol untuk menyegarkan cek. Jika Anda memiliki paket Business, Enterprise On-Ramp, atau Enterprise Support, Trusted Advisor secara otomatis menyegarkan cek di akun Anda setiap minggu.

Untuk menyegarkan Trusted Advisor cek

1. Arahkan ke AWS Trusted Advisor konsol di https://console.aws.amazon.com/trustedadvisor.
2. Pada halaman Trusted Advisor Rekomendasi atau kategori centang, pilih Segarkan semua pemeriksaan.

Anda juga dapat menyegarkan pemeriksaan tertentu dengan cara berikut:

- Pilih ikon refresh () untuk pemeriksaan individual.
- Gunakan Operasi API RefreshTrustedAdvisorCheck.

> **Catatan**
>
> - Trusted Advisor secara otomatis menyegarkan beberapa pemeriksaan beberapa kali sehari, seperti masalah risiko AWS Well-Architected tinggi untuk pemeriksaan keandalan. Mungkin perlu beberapa jam agar perubahan muncul di akun Anda. Untuk pemeriksaan yang diperbarui secara otomatis ini, Anda tidak dapat memilih ikon penyegaran () untuk menyegarkan hasil secara manual.
> - Jika mengaktifkan AWS Security Hub akun, Anda tidak dapat menggunakan Trusted Advisor konsol untuk menyegarkan kontrol Security Hub. Untuk informasi selengkapnya, lihat Segarkan Security Hub.

Mengunduh hasil pemeriksaan

Anda dapat mengunduh hasil pemeriksaan untuk mendapatkan ikhtisar Trusted Advisor di akun Anda. Anda dapat mengunduh hasil untuk semua pemeriksaan atau pemeriksaan tertentu.

Untuk mengunduh cek hasil dari Trusted Advisor Rekomendasi

1. Arahkan ke AWS Trusted Advisor konsol di https://console.aws.amazon.com/trustedadvisor.
   - Untuk mengunduh semua hasil pemeriksaan, di halaman Trusted Advisor Rekomendasi atau kategori centang, pilih Unduh semua cek.
   - Untuk mengunduh hasil pemeriksaan untuk pemeriksaan tertentu, pilih nama centang, lalu pilih ikon unduhan ().

2. Simpan atau buka file .xls. File berisi informasi ringkasan yang sama dari konsol Trusted Advisor , seperti nama pemeriksaan, deskripsi, status, sumber daya yang terpengaruh, dan sebagainya.

Tampilan organisasi

Anda dapat mengatur fitur tampilan organisasi untuk membuat laporan untuk semua akun anggota di AWS organisasi Anda. Untuk informasi selengkapnya, lihat Tampilan organisasi untuk AWS Trusted Advisor.

Preferensi

Pada Trusted Advisor halaman Kelola, Anda dapat menonaktifkan Trusted Advisor.

Pada halaman Notifikasi, Anda dapat mengonfigurasi pesan email mingguan Anda untuk ringkasan cek. Lihat Menyiapkan preferensi pemberitahuan.

Pada halaman Organisasi Anda, Anda dapat mengaktifkan atau menonaktifkan akses tepercaya dengan AWS Organizations. Ini diperlukan untuk Tampilan organisasi untuk AWS Trusted Advisor fitur, Trusted Advisor Prioritas, dan Trusted Advisor Engage.

Menyiapkan preferensi pemberitahuan

Tentukan siapa yang dapat menerima pesan Trusted Advisor email mingguan untuk hasil pemeriksaan dan bahasa. Anda menerima pemberitahuan email tentang ringkasan cek Anda untuk Trusted Advisor Rekomendasi seminggu sekali.

Pemberitahuan email untuk Trusted Advisor Rekomendasi tidak menyertakan hasil untuk Trusted Advisor Prioritas. Untuk informasi selengkapnya, lihat Kelola pemberitahuan Trusted Advisor Prioritas.

Untuk mengatur preferensi pemberitahuan

1. Masuk ke Trusted Advisor konsol di https://console.aws.amazon.com/trustedadvisor/home.
2. Di panel navigasi, di bawah Preferensi, pilih Pemberitahuan.
3. Untuk Rekomendasi, pilih siapa yang akan diberitahukan untuk hasil pemeriksaan Anda. Anda dapat menambah dan menghapus kontak dari halaman Pengaturan Akun di AWS Billing and Cost Management konsol.

4. Untuk Bahasa, pilih bahasa untuk pesan email.
5. Pilih Simpan preferensi Anda.

Menyiapkan tampilan organisasi

Jika Anda mengatur akun AWS Organizations, Anda dapat membuat laporan untuk semua akun anggota di organisasi Anda. Untuk informasi selengkapnya, lihat Tampilan organisasi untuk AWS Trusted Advisor.

Nonaktifkan Trusted Advisor

Saat Anda menonaktifkan layanan ini, Trusted Advisor tidak akan melakukan pemeriksaan apa pun pada akun Anda. Siapa pun yang mencoba mengakses Trusted Advisor konsol atau menggunakan operasi API akan menerima pesan kesalahan akses ditolak.

Untuk menonaktifkan Trusted Advisor

1. Masuk ke Trusted Advisor konsol di https://console.aws.amazon.com/trustedadvisor/home.
2. Di panel navigasi, di bawah Preferensi, pilih Kelola Trusted Advisor.
3. Di bawah Trusted Advisor, matikan Diaktifkan. Tindakan ini menonaktifkan Trusted Advisor semua cek di akun Anda.
4. Anda kemudian dapat menghapus secara manual dari akun Anda. Untuk informasi selengkapnya, lihat Menghapus peran terkait layanan untuk Trusted Advisor.

Informasi terkait

Untuk informasi selengkapnya Trusted Advisor, lihat topik berikut:

- Bagaimana cara saya mulai menggunakan Trusted Advisor?
- AWS Trusted Advisor periksa referensi

Memulai dengan Trusted Advisor API

Referensi AWS Trusted Advisor API ditujukan untuk programmer yang membutuhkan informasi rinci tentang operasi Trusted Advisor API dan tipe data. API ini menyediakan akses ke Trusted Advisor rekomendasi untuk akun Anda atau semua akun dalam AWS Organisasi Anda. Trusted Advisor API menggunakan metode HTTP yang mengembalikan hasil dalam format JSON.

> **Note**
>
> - Anda harus memiliki paket Business, Enterprise On-Ramp, atau Enterprise Support untuk menggunakan API Trusted Advisor
> - Jika Anda memanggil AWS Trusted Advisor API dari akun yang tidak memiliki paket Business, Enterprise On-Ramp, atau Enterprise Support, maka Anda akan menerima pengecualian Access Denied. Untuk informasi selengkapnya tentang mengubah paket dukungan, lihat AWS Support.

Anda dapat menggunakan AWS Trusted Advisor API untuk mendapatkan daftar pemeriksaan dan deskripsi, rekomendasi, dan sumber daya untuk rekomendasi. Anda juga dapat memperbarui siklus hidup rekomendasi. Untuk mengelola rekomendasi, gunakan operasi API berikut:

- Gunakan operasi ListChecks, ListRecommendationsGetRecommendation, dan ListRecommendationResourcesAPI untuk melihat rekomendasi dan akun serta sumber daya terkait.
- Gunakan operasi UpdateRecommendationLifecycleAPI untuk memperbarui siklus hidup rekomendasi yang dikelola oleh Trusted Advisor Prioritas.
- Gunakan operasi BatchUpdateRecommendationResourceExclusionAPI untuk menyertakan atau mengecualikan satu atau beberapa sumber daya dari Trusted Advisor hasil Anda.
- Panggilan ListOrganizationRecommendationsGetOrganizationRecommendation, ListOrganizationRecommendationResources, ListOrganizationRecommendationAccounts, dan UpdateOrganizationRecommendationLifecycleAPI hanya mendukung rekomendasi yang dikelola oleh Trusted Advisor Priority. Rekomendasi ini juga disebut sebagai rekomendasi yang diprioritaskan. Anda dapat melihat dan mengelola rekomendasi yang diprioritaskan dari manajemen atau akun admin yang didelegasikan jika Anda telah mengaktifkan Prioritas Trusted Advisor. Jika Prioritas tidak diaktifkan, maka Anda menerima pengecualian Akses Ditolak saat Anda membuat permintaan.

Untuk informasi selengkapnya, lihat AWS Trusted Advisor di AWS Support User Guide.

Untuk otentikasi permintaan, lihat Proses Penandatanganan Versi Tanda Tangan 4.

Menggunakan Trusted Advisor sebagai layanan web

> **Note**
>
> Trusted Advisor operasi tidak akan didukung oleh AWS Trusted Advisor Support API pada tahun 2024. Silakan gunakan AWS Trusted Advisor API baru untuk mengakses pemeriksaan dan rekomendasi praktik terbaik secara terprogram.

AWS Support Layanan ini memungkinkan Anda untuk menulis aplikasi yang berinteraksi dengan AWS Trusted Advisor. Topik ini menunjukkan kepada Anda cara mendapatkan daftar Trusted Advisor cek, menyegarkan salah satunya, dan kemudian mendapatkan hasil terperinci dari cek. Tugas-tugas ini ditunjukkan di Java. Untuk informasi tentang dukungan untuk bahasa lainnya, lihat Tools untuk Amazon Web Services.

Topik

Dapatkan daftar Trusted Advisor cek yang tersedia

Cuplikan kode Java berikut membuat instance AWS Support klien yang dapat Anda gunakan untuk memanggil semua operasi Trusted Advisor API. Selanjutnya, kode mendapatkan daftar Trusted Advisor pemeriksaan dan `CheckId` nilai yang sesuai dengan memanggil operasi DescribeTrustedAdvisorChecksAPI. Anda dapat menggunakan informasi ini untuk membangun antarmuka pengguna yang memungkinkan pengguna untuk memilih pemeriksaan yang ingin mereka jalankan atau segarkan.

```
private static AWSSupport createClient()
{
    return AWSSupportClientBuilder.defaultClient();
}
// Get the List of Available Trusted Advisor Checks
```

```
public static void getTAChecks() {
    // Possible language parameters: "en" (English), "ja" (Japanese), "fr" (French),
 "zh" (Chinese)
    DescribeTrustedAdvisorChecksRequest request = new
 DescribeTrustedAdvisorChecksRequest().withLanguage("en");
    DescribeTrustedAdvisorChecksResult result =
 createClient().describeTrustedAdvisorChecks(request);
    for (TrustedAdvisorCheckDescription description : result.getChecks()) {
        // Do something with check description.
        System.out.println(description.getId());
        System.out.println(description.getName());
    }
}
```

Segarkan daftar Trusted Advisor cek yang tersedia

Cuplikan kode Java berikut membuat instance AWS Support klien yang dapat Anda gunakan untuk menyegarkan Trusted Advisor data.

```
// Refresh a Trusted Advisor Check
// Note: Some checks are refreshed automatically, and they cannot be refreshed by using
 this operation.
// Specifying the check ID of a check that is automatically refreshed causes an
 InvalidParameterValue error.
public static void refreshTACheck(final String checkId) {
    RefreshTrustedAdvisorCheckRequest request = new
 RefreshTrustedAdvisorCheckRequest().withCheckId(checkId);
    RefreshTrustedAdvisorCheckResult result =
 createClient().refreshTrustedAdvisorCheck(request);
    System.out.println("CheckId: " + result.getStatus().getCheckId());
    System.out.println("Milliseconds until refreshable: " +
 result.getStatus().getMillisUntilNextRefreshable());
    System.out.println("Refresh Status: " + result.getStatus().getStatus());
}
```

Polling Trusted Advisor cek untuk perubahan status

Setelah mengirimkan permintaan untuk menjalankan Trusted Advisor pemeriksaan guna menghasilkan data status terbaru, Anda menggunakan operasi DescribeTrustedAdvisorCheckRefreshStatusesAPI untuk meminta kemajuan proses pemeriksaan, dan kapan data baru siap untuk diperiksa.

Potongan kode Java berikut mengambil status pemeriksaan yang diminta di bagian berikut menggunakan nilai yang sesuai di variabel `CheckId`. Selain itu, kode menunjukkan beberapa kegunaan lain dari Trusted Advisor layanan:

1. Anda dapat memanggil `getMillisUntilNextRefreshable` dengan melintasi objek yang terkandung dalam instans `DescribeTrustedAdvisorCheckRefreshStatusesResult`. Anda dapat menggunakan nilai yang dikembalikan untuk menguji apakah Anda ingin kode Anda melanjutkan dengan menyegarkan pemeriksaan tersebut.
2. Jika `timeUntilRefreshable` sama dengan nol, Anda dapat meminta penyegaran pemeriksaan.
3. Dengan menggunakan status yang dikembalikan, Anda dapat terus melakukan polling untuk perubahan status; potongan kode menetapkan interval polling ke sepuluh detik yang disarankan. Jika statusnya `enqueued` atau `in_progress`, putaran kembali dan meminta status lain. Jika panggilan mengembalikan `successful`, putaran berakhir.
4. Akhirnya, kode mengembalikan sebuah instans dari tipe data `DescribeTrustedAdvisorCheckResultResult` yang dapat Anda gunakan untuk melintasi informasi yang dihasilkan oleh pemeriksaan tersebut.

Catatan: Gunakan permintaan penyegaran tunggal sebelum polling untuk status permintaan tersebut.

```
// Retrieves TA refresh statuses. Multiple checkId's can be submitted.
public static List<TrustedAdvisorCheckRefreshStatus> getTARefreshStatus(final String...
 checkIds) {
    DescribeTrustedAdvisorCheckRefreshStatusesRequest request =
            new
 DescribeTrustedAdvisorCheckRefreshStatusesRequest().withCheckIds(checkIds);
    DescribeTrustedAdvisorCheckRefreshStatusesResult result =
            createClient().describeTrustedAdvisorCheckRefreshStatuses(request);
    return result.getStatuses();
}
// Retrieves a TA check status, and checks to see if it has finished processing.
public static boolean isTACheckStatusInTerminalState(final String checkId) {
    // Since we only submitted one checkId to getTARefreshStatus, just retrieve the
 only element in the list.
    TrustedAdvisorCheckRefreshStatus status = getTARefreshStatus(checkId).get(0);
    // Valid statuses are:
    // 1. "none", the check has never been refreshed before.
    // 2. "enqueued", the check is waiting to be processed.
    // 3. "processing", the check is in the midst of being processed.
```

```
    // 4. "success", the check has succeeded and finished processing - refresh data is
 available.
    // 5. "abandoned", the check has failed to process.
    return status.getStatus().equals("abandoned") ||
 status.getStatus().equals("success");
}
// Enqueues a Trusted Advisor check refresh. Periodically polls the check refresh
 status for completion.
public static TrustedAdvisorCheckResult getFreshTACheckResult(final String checkId)
 throws InterruptedException {
    refreshTACheck(checkId);
    while(!isTACheckStatusInTerminalState(checkId)) {
        Thread.sleep(10000);
    }
    return getTACheckResult(checkId);
}
// Retrieves fresh TA check data whenever possible.
// Note: Some checks are refreshed automatically, and they cannot be refreshed by using
 this operation. This method
// is only functional for checks that can be refreshed using the
 RefreshTrustedAdvisorCheck operation.
public static void pollForTACheckResultChanges(final String checkId) throws
 InterruptedException {
    String checkResultStatus = null;
    do {
        TrustedAdvisorCheckResult result = getFreshTACheckResult(checkId);
        if (checkResultStatus != null && !checkResultStatus.equals(result.getStatus()))
 {
            break;
        }
        checkResultStatus = result.getStatus();
        // The rule refresh has completed, but due to throttling rules the checks may
 not be refreshed again
        // for a short period of time.
        // Since we only submitted one checkId to getTARefreshStatus, just retrieve the
 only element in the list.
        TrustedAdvisorCheckRefreshStatus refreshStatus =
 getTARefreshStatus(checkId).get(0);
        Thread.sleep(refreshStatus.getMillisUntilNextRefreshable());
    } while(true);
    // Signal that a TA check has changed check result status here.
}
```

Minta hasil Trusted Advisor cek

Setelah Anda memilih cek untuk hasil rinci yang Anda inginkan, Anda mengirimkan permintaan menggunakan operasi DescribeTrustedAdvisorCheckResult API.

> **Tip**
>
> Nama dan deskripsi untuk Trusted Advisor cek dapat berubah sewaktu-waktu. Kami menyarankan Anda menentukan ID pemeriksaan dalam kode Anda untuk secara unik mengidentifikasi pemeriksaan. Anda dapat menggunakan operasi DescribeTrustedAdvisorChecksAPI untuk mendapatkan ID cek.

Potongan kode Java berikut menggunakan instans `DescribeTrustedAdvisorChecksResult` yang direferensikan oleh variabel `result` yang diperoleh di potongan kode sebelumnya. Daripada mendefinisikan pemeriksaan secara interaktif melalui antarmuka pengguna, setelah Anda mengirimkan permintaan untuk menjalankan potongan kode tersebut, kirim permintaan untuk pemeriksaan pertama dalam daftar yang akan dijalankan dengan menentukan nilai indeks 0 di setiap panggilan `result.getChecks().get(0)`. Selanjutnya, kode mendefinisikan sebuah instans dari `DescribeTrustedAdvisorCheckResultRequest` yang diberikan ke sebuah instans dari `DescribeTrustedAdvisorCheckResultResult` yang disebut `checkResult`. Anda dapat menggunakan struktur anggota tipe data ini untuk melihat hasil pemeriksaan.

```
// Request a Trusted Advisor Check Result
public static TrustedAdvisorCheckResult getTACheckResult(final String checkId) {
    DescribeTrustedAdvisorCheckResultRequest request = new
 DescribeTrustedAdvisorCheckResultRequest()
            // Possible language parameters: "en" (English), "ja" (Japanese),
 "fr" (French), "zh" (Chinese)
            .withLanguage("en")
            .withCheckId(checkId);
    DescribeTrustedAdvisorCheckResultResult requestResult =
 createClient().describeTrustedAdvisorCheckResult(request);
    return requestResult.getResult();
}
```

Catatan: Meminta Hasil Trusted Advisor Pemeriksaan tidak menghasilkan data hasil yang diperbarui.

Tampilkan detail Trusted Advisor cek

Cuplikan kode Java berikut berulang atas `DescribeTrustedAdvisorCheckResultResult` instance yang dikembalikan di bagian sebelumnya untuk mendapatkan daftar sumber daya yang ditandai oleh cek. Trusted Advisor

```
// Show ResourceIds for flagged resources.
for (TrustedAdvisorResourceDetail flaggedResource :
    result1.getResult().getFlaggedResources())
{
    System.out.println(
        "The resource for this ResourceID has been flagged: " +
        flaggedResource.getResourceId());
}
```

Tampilan organisasi untuk AWS Trusted Advisor

Tampilan organisasi memungkinkan Anda melihat pemeriksaan Trusted Advisor untuk semua akun di AWS Organizations Anda. Setelah mengaktifkan fitur ini, Anda dapat membuat laporan untuk mengumpulkan hasil pemeriksaan untuk semua akun anggota di organisasi Anda. Laporan ini mencakup ringkasan hasil pemeriksaan dan informasi tentang sumber daya yang terpengaruh untuk setiap akun. Misalnya, Anda dapat menggunakan laporan untuk mengidentifikasi akun di organisasi Anda yang menggunakan AWS Identity and Access Management (IAM) dengan pemeriksaan Penggunaan IAM atau apakah Anda memiliki tindakan yang disarankan untuk bucket Amazon Simple Storage Service (Amazon S3) dengan pemeriksaan Izin Bucket Amazon S3.

Topik

Prasyarat

Anda harus memenuhi persyaratan berikut untuk mengaktifkan tampilan organisasi:

- Akun Anda harus menjadi anggota dari Organisasi AWS.
- Organizations Anda harus mengaktifkan semua fitur untuk Organisasi. Untuk informasi selengkapnya, lihat Mengaktifkan semua fitur di organisasi Anda dalam PanduanAWS Organizations Pengguna.
- Akun manajemen di organisasi Anda harus memiliki paket Bisnis, Korporasi, Korporasi, atau Korporasi. Anda dapat menemukan paket Support Anda dariAWS Support Pusat atau dari halaman Paket Dukungan. Lihat Bandingkan paket AWS Support.
- Anda harus masuk sebagai pengguna di akun manajemen (atau menjalankan peran yang setara). Apakah Anda masuk sebagai pengguna IAM atau IAM role, Anda harus memiliki kebijakan dengan izin yang diperlukan. Lihat Menggunakan kebijakan IAM untuk mengizinkan akses ke tampilan organisasi.

Mengaktifkan tampilan organisasi

Setelah Anda memenuhi prasyarat, ikuti langkah berikut untuk mengaktifkan tampilan organisasi. Setelah Anda mengaktifkan fitur ini, hal berikut terjadi:

- Trusted Advisor diaktifkan sebagai layanan tepercaya di organisasi Anda. Untuk informasi lebih lanjut, lihat Mengaktifkan akses tepercaya dengan layanan AWS lainnya dalam Panduan Pengguna AWS Organizations.
- Dibuat`AWSServiceRoleForTrustedAdvisorReporting` service-linked-role untuk Anda di akun manajemen di organisasi Anda. Peran ini mencakup izin yang Trusted Advisor perlukan untuk memanggil Organizations atas nama Anda. Peran terkait layanan ini terkunci dan Anda tidak dapat menghapusnya secara manual. Untuk informasi selengkapnya, lihat Menggunakan peran terkait layanan untuk Trusted Advisor.

Anda mengaktifkan tampilan organisasi dari konsol Trusted Advisor.

Untuk mengaktifkan tampilan organisasi

1. Masuk sebagai administrator di akun manajemen organisasi dan buka konsol AWS Trusted Advisor di https://console.aws.amazon.com/trustedadvisor.

2. Di panel navigasi, di bawah Preferensi, pilih Organisasi Anda.
3. Di bawah Aktifkan akses tepercaya denganAWS Organizations, aktifkan Diaktifkan.

> **Note**
>
> Mengaktifkan tampilan organisasi untuk akun manajemen tidak memberikan pemeriksaan yang sama untuk semua akun anggota. Misalnya, jika semua akun anggota Anda memiliki Support Dasar, akun tersebut tidak akan memiliki pemeriksaan yang sama dengan akun manajemen Anda. AWS SupportPaket menentukanTrusted Advisor pemeriksaan mana yang tersedia untuk akun.

Menyegarkan pemeriksaan Trusted Advisor

Sebelum membuat laporan untuk organisasi Anda, sebaiknya segarkan status pemeriksaan Trusted Advisor. Anda dapat mengunduh laporan tanpa menyegarkan pemeriksaan Trusted Advisor, tetapi laporan Anda mungkin tidak memiliki informasi terbaru.

Jika Anda memiliki paket Bisnis, Korporasi, Korporasi,Trusted Advisor secara otomatis menyegarkan pemeriksaan di akun Anda setiap minggu.

> **Note**
>
> Jika Anda memiliki akun di organisasi yang memiliki paket dukungan Developer atau Dasar, pengguna untuk akun tersebut harus masuk ke konsol Trusted Advisor untuk menyegarkan pemeriksaan. Anda tidak dapat menyegarkan pemeriksaan untuk semua akun dari akun manajemen organisasi.

Untuk menyegarkan pemeriksaan Trusted Advisor

1. Navigasikan ke AWS Trusted Advisor konsol di https://console.aws.amazon.com/trustedadvisor.
2. Pada halaman Trusted AdvisorRekomendasi, pilih Refresh all checks. Tindakan ini akan menyegarkan semua pemeriksaan di akun Anda.

Anda juga dapat menyegarkan pemeriksaan tertentu dengan cara berikut:

- Gunakan Operasi API RefreshTrustedAdvisorCheck.
- Pilih ikon penyegaran
  ( )
  untuk pemeriksaan individu.

Membuat laporan tampilan organisasi

Setelah mengaktifkan tampilan organisasi, Anda dapat membuat laporan sehingga Anda dapat melihat hasil pemeriksaan Trusted Advisor untuk organisasi Anda.

Anda dapat membuat hingga 50 laporan. Jika Anda membuat laporan melebihi kuota ini, Trusted Advisor menghapus laporan paling awal. Anda tidak dapat memulihkan laporan yang dihapus.

Untuk membuat laporan tampilan organisasi

1. Masuk ke akun manajemen organisasi dan buka konsol AWS Trusted Advisor di https://console.aws.amazon.com/trustedadvisor.
2. Di panel navigasi, pilih Tampilan Organisasi.
3. Pilih Buat laporan.
4. Secara default, laporan mencakup semua Wilayah AWS, kategori pemeriksaan, pemeriksaan, dan status sumber daya. Pada Create report (Buat laporan), Anda dapat menggunakan opsi filter untuk menyesuaikan laporan Anda. Misalnya, Anda dapat menghapus pilihan All (Semua) untuk Region (Wilayah), lalu menentukan Wilayah tertentu untuk disertakan dalam laporan.
   a. Masukkan Nama untuk laporan itu.
   b. Untuk Format, pilih JSON atau CSV.
   c. Untuk Region (Wilayah), tentukan AWS Wilayah atau pilih All (Semua).
   d. Untuk kategori Periksa, pilih kategori cek atau pilih Semua.
   e. Untuk Checks (Pemeriksaan), pilih pemeriksaan spesifik untuk kategori tersebut atau pilih All (Semua).

   > **Note**
   >
   > Filter kategori Periksa menimpa filter Cek. Misalnya, jika Anda memilih kategori Keamanan dan kemudian memilih nama centang tertentu, laporan Anda menyertakan semua hasil pemeriksaan untuk kategori tersebut. Untuk membuat

laporan hanya untuk pemeriksaan tertentu, simpan default Semua nilai untuk kategori Periksa dan kemudian pilih nama centang Anda.

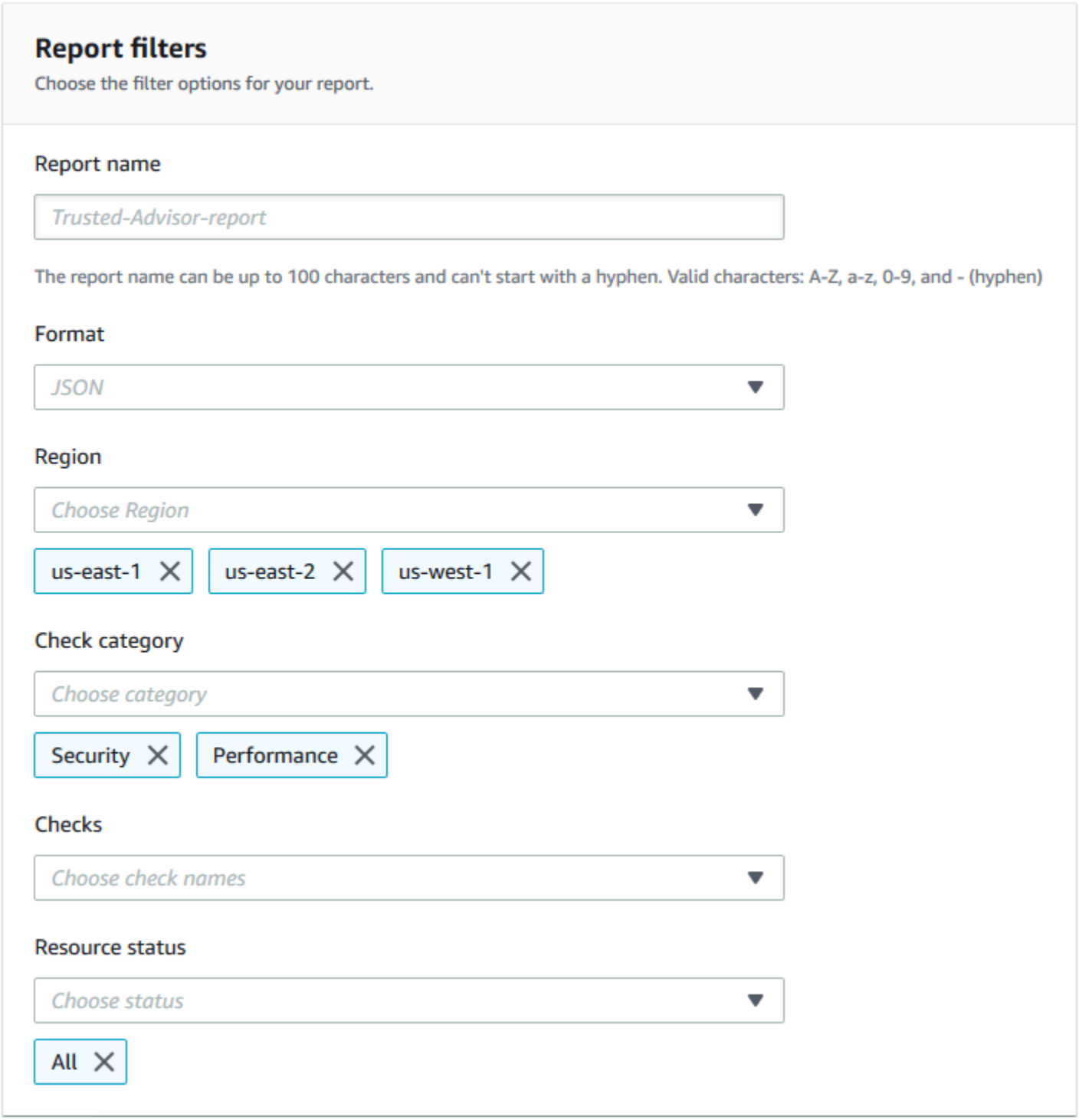
f. Untuk Resource status (Status sumber daya), pilih status untuk difilter, seperti Warning (Peringatan), atau pilih All (Semua).

5. Untuk AWSOrganisasi, pilih unit organisasi (OU) untuk disertakan dalam laporan Anda. Untuk informasi lebih lanjut tentang OU, lihat Mengelola unit organisasi dalam Panduan Pengguna AWS Organizations.
6. Pilih Buat laporan.

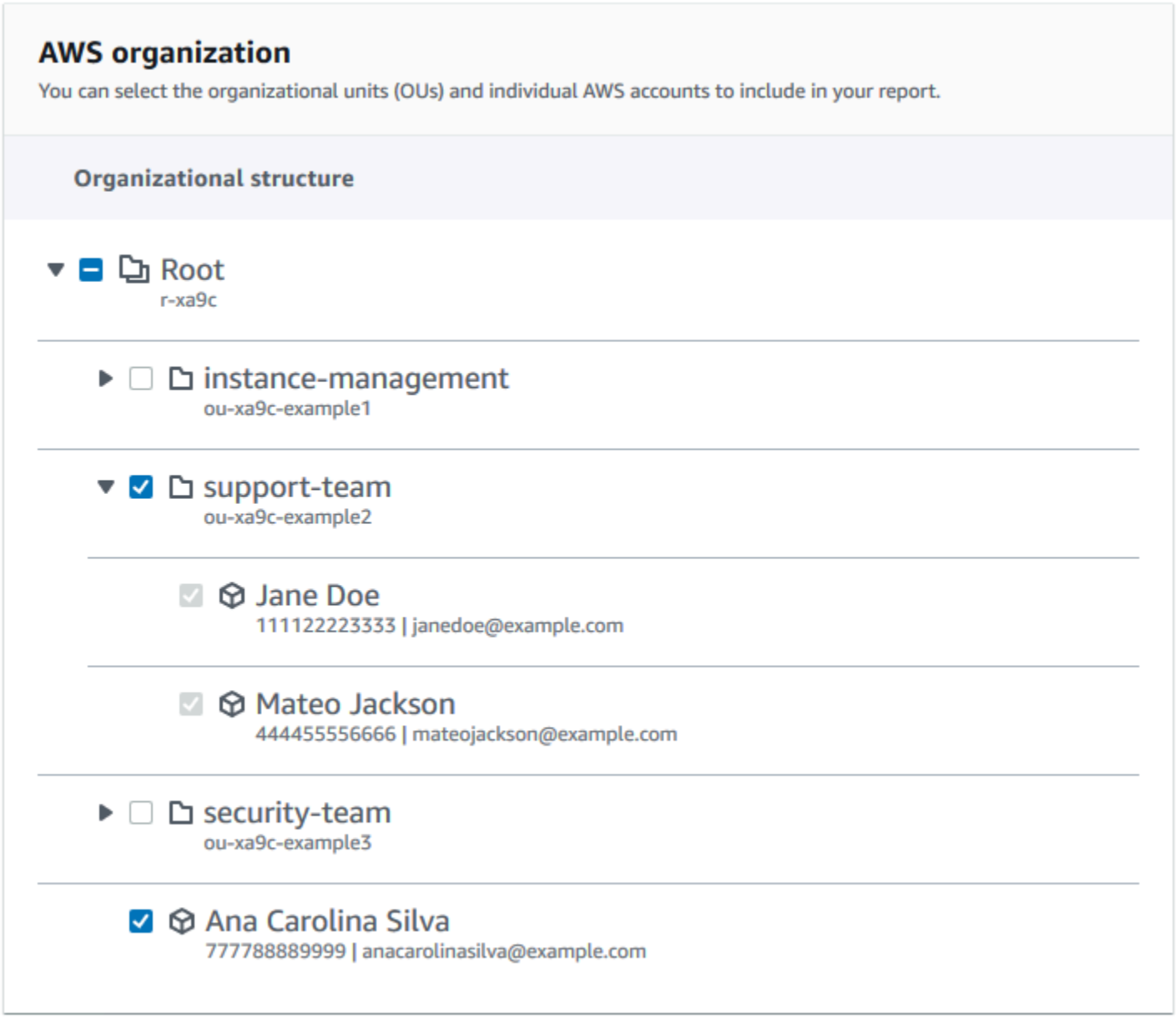
Example : Membuat opsi filter laporan

Contoh berikut membuat laporan JSON untuk hal berikut:

- Tiga Kawasan AWS
- Semua pemeriksaan Security (Keamanan) dan Performance (Kinerja)



Pada contoh berikut, laporan mencakup OU support-team (tim-dukungan) dan satu akun AWS yang merupakan bagian dari organisasi.



Catatan

- Jumlah waktu yang diperlukan untuk membuat laporan tergantung pada jumlah akun dalam organisasi dan jumlah sumber daya di setiap akun.
- Anda tidak dapat membuat lebih dari satu laporan pada satu waktu, kecuali laporan saat ini telah berjalan selama lebih dari 6 jam.
- Segarkan halaman jika Anda tidak melihat laporan muncul di halaman.

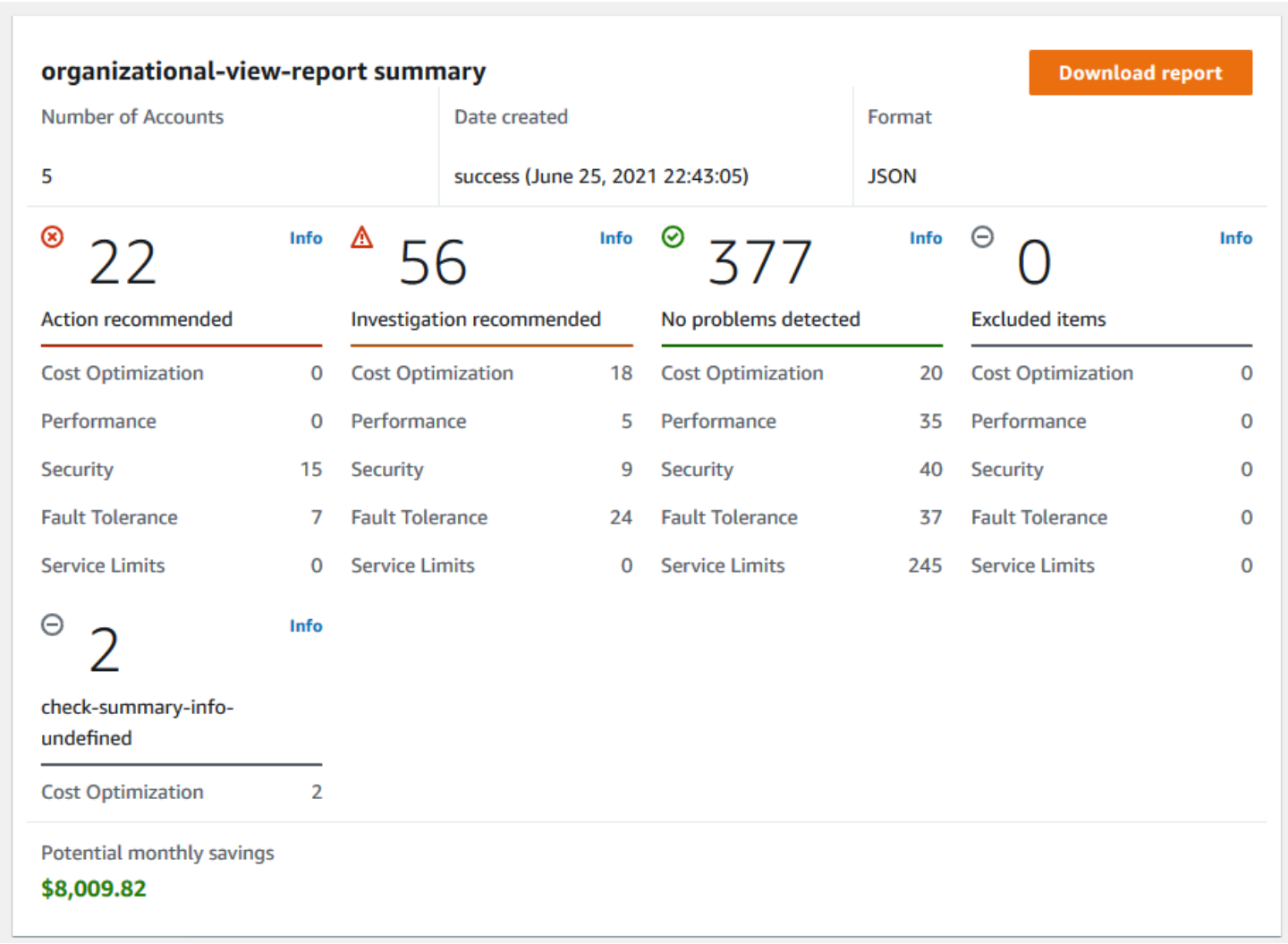
Melihat ringkasan laporan

Setelah laporan siap, Anda dapat melihat ringkasan laporan dari konsol Trusted Advisor. Hal ini memungkinkan Anda melihat ringkasan hasil pemeriksaan di seluruh organisasi dengan cepat.

Untuk melihat ringkasan laporan

1. Masuk ke akun manajemen organisasi dan buka konsol AWS Trusted Advisor di https://console.aws.amazon.com/trustedadvisor.
2. Di panel navigasi, pilih Tampilan Organisasi.
3. Pilih nama laporan.
4. Pada halaman Summary (Ringkasan), lihat status pemeriksaan untuk setiap kategori. Anda juga dapat memilih Unduh laporan.

Example : Ringkasan laporan untuk organisasi



Mengunduh laporan tampilan organisasi

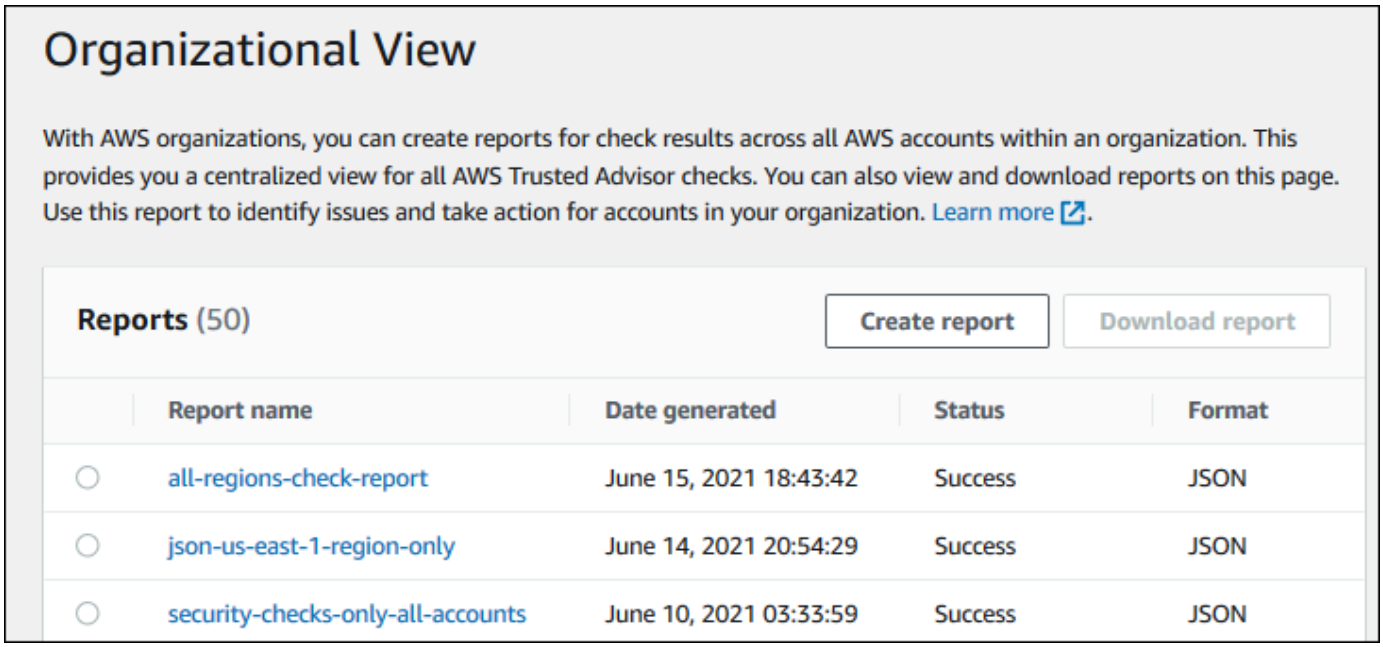
Setelah laporan Anda siap, unduh laporan tersebut dari konsol Trusted Advisor. Laporan ini adalah file.zip yang berisi tiga file:

- `summary.json` – Berisi ringkasan hasil pemeriksaan untuk setiap kategori pemeriksaan.
- `schema.json` – Berisi skema untuk pemeriksaan yang ditentukan dalam laporan.
- File sumber daya (.json atau .csv) – Berisi informasi detail tentang status pemeriksaan untuk sumber daya di organisasi Anda.

Untuk mengunduh laporan tampilan organisasi

1. Masuk ke akun manajemen organisasi dan buka konsol AWS Trusted Advisor di https://console.aws.amazon.com/trustedadvisor.
2. Di panel navigasi, pilih Tampilan Organisasi.

   Halaman Organizational View (Tampilan Organisasi) menampilkan laporan yang tersedia untuk diunduh.
3. Pilih laporan, pilih Unduh laporan, lalu simpan file. Anda hanya dapat mengunduh satu laporan dalam satu waktu.



4. Buka filenya.
5. Gunakan editor teks untuk membuka file `.json` atau aplikasi spreadsheet untuk membuka file `.csv`.

> **Note**
>
> Anda mungkin menerima beberapa file jika laporan berukuran 5 MB atau lebih besar.

Example : file summary.json

File `summary.json` menunjukkan jumlah akun dalam organisasi dan status pemeriksaan di setiap kategori.

Trusted Advisor menggunakan kode warna berikut untuk hasil pemeriksaan:

- `Green` – Trusted Advisor tidak mendeteksi masalah untuk pemeriksaan.
- `Yellow` – Trusted Advisor mendeteksi kemungkinan masalah untuk pemeriksaan.
- `Red` – Trusted Advisor mendeteksi eror dan merekomendasikan tindakan untuk pemeriksaan.
- `Blue` – Trusted Advisor tidak dapat menentukan status pemeriksaan.

Pada contoh berikut, dua pemeriksaan `Red`, satu `Green`, dan satu `Yellow`.


```
{
    "numAccounts": 3,
    "filtersApplied": {
        "accountIds": ["123456789012","111122223333","111111111111"],
        "checkIds": "All",
        "categories": [
            "security",
            "performance"
        ],
        "statuses": "All",
        "regions": [
            "us-west-1",
            "us-west-2",
            "us-east-1"
        ],
        "organizationalUnitIds": [
            "ou-xa9c-EXAMPLE1",
            "ou-xa9c-EXAMPLE2"
        ]
    },
    "categoryStatusMap": {
        "security": {
            "statusMap": {
                "ERROR": {
                    "name": "Red",
                    "count": 2
                },
                "OK": {
                    "name": "Green",
                    "count": 1
                },
                "WARN": {
```

```
                    "name": "Yellow",
                    "count": 1
                }
            },
            "name": "Security"
        }
    },
    "accountStatusMap": {
        "123456789012": {
            "security": {
                "statusMap": {
                    "ERROR": {
                        "name": "Red",
                        "count": 2
                    },
                    "OK": {
                        "name": "Green",
                        "count": 1
                    },
                    "WARN": {
                        "name": "Yellow",
                        "count": 1
                    }
                },
                "name": "Security"
            }
        }
    }
}
```

Example : file schema.json

File `schema.json` termasuk skema untuk pemeriksaan dalam laporan. Contoh berikut termasuk ID dan properti untuk pemeriksaan Kebijakan Kata Sandi IAM (DqdJqYeRm5)Yw2K9puPzl

```
{
    "Yw2K9puPzl": [
        "Password Policy",
        "Uppercase",
        "Lowercase",
        "Number",
        "Non-alphanumeric",
        "Status",
```

```
        "Reason"
    ],
    "DqdJqYeRm5": [
        "Status",
        "IAM User",
        "Access Key",
        "Key Last Rotated",
        "Reason"
    ],
    ...
}
```

Example : file resources.csv

File `resources.csv` mencakup informasi tentang sumber daya dalam organisasi. Contoh ini menunjukkan beberapa kolom data yang muncul dalam laporan, seperti berikut:

- ID Akun dari akun yang terpengaruh
- ID pemeriksaan Trusted Advisor
- ID sumber daya
- Stempel waktu laporan
- Nama lengkap pemeriksaan Trusted Advisor
- Kategori pemeriksaan Trusted Advisor
- ID akun unit organisasi induk (OU) atau root

AccountId	CheckId	ResourceId	TimeStamp	CheckName	Category
1.11122E+11	Qch7DwouX1	LnW14f1M40NMjmMLvY5(	1.58983E+12	Low Utilization Amazon EC2 Instances	Cost Optimizing
1.11122E+11	HCP4007jGY	dJrQZXw36ZdswBeo9WUl	1.58983E+12	Security Groups - Specific Ports Unrestricted	Security
1.11122E+11	HCP4007jGY	1hzakmTbWd5UmAM_a0L	1.58983E+12	Security Groups - Specific Ports Unrestricted	Security
4.44456E+11	1iG5NDGVre	dJrQZXw36ZdswBeo9WUl	1.58983E+12	Security Groups - Unrestricted Access	Security
4.44456E+11	1iG5NDGVre	1hzakmTbWd5UmAM_a0L	1.58983E+12	Security Groups - Unrestricted Access	Security
4.44456E+11	Pfx0RwqBli	vioZmlba45kf2JWIe_W0j5	1.58983E+12	Amazon S3 Bucket Permissions	Security
4.44456E+11	Pfx0RwqBli	wAvASS3YOwy6WWxIBHf	1.58983E+12	Amazon S3 Bucket Permissions	Security
1.23457E+11	Pfx0RwqBli	LIc4zRaUSiIGRSlmqaMa5V	1.58983E+12	Amazon S3 Bucket Permissions	Security
1.23457E+11	Pfx0RwqBli	gWB27TMXof2evYzMSYBg	1.58983E+12	Amazon S3 Bucket Permissions	Security
7.77789E+11	Pfx0RwqBli	M3LBsF0e15Cl9Mxppapcx	1.58983E+12	Amazon S3 Bucket Permissions	Security
7.77789E+11	Yw2K9puPzl	47DEQpj8HBSa-_TImW-5J(	1.58983E+12	IAM Password Policy	Security
7.77789E+11	H7IgTzjTYb	1xHQ5ovV8bS0H1Z-t7Kbib	1.58983E+12	Amazon EBS Snapshots	Fault Tolerance
7.77789E+11	wuy7G1zxql	10F6p6VAF0F-MuL6Dc-dl1	1.58983E+12	Amazon EC2 Availability Zone Balance	Fault Tolerance

File sumber daya hanya berisi entri jika hasil pemeriksaan ada di tingkat sumber daya. Anda mungkin tidak melihat pemeriksaan dalam laporan karena alasan berikut:

- Beberapa pemeriksaan, seperti MFA on Root Account (MFA pada Akun Root), tidak memiliki sumber daya dan tidak akan muncul dalam laporan. Pemeriksaan tanpa sumber daya muncul di file `summary.json` sebagai gantinya.
- Beberapa pemeriksaan hanya menunjukkan sumber daya jika mereka `Red` atau `Yellow`. Jika semua sumber daya `Green`, mereka mungkin tidak muncul di laporan Anda.
- Jika akun tidak diaktifkan untuk layanan yang memerlukan pemeriksaan, pemeriksaan tersebut mungkin tidak muncul dalam laporan. Misalnya, jika Anda tidak menggunakan Instans Cadangan Amazon Elastic Compute Cloud di organisasi Anda, pemeriksaan Kedaluwarsa Sewa Instans Cadangan Amazon EC2 tidak akan muncul dalam laporan Anda.
- Akun belum menyegarkan hasil pemeriksaan. Hal ini mungkin terjadi saat pengguna dengan paket Basic atau Developer Support masuk ke konsol Trusted Advisor untuk pertama kalinya. Jika Anda memiliki paket Bisnis, Korporasi, pendaftaran akun dapat memakan waktu hingga satu minggu bagi pengguna untuk melihat hasil pemeriksaan. Untuk informasi selengkapnya, lihat Menyegarkan pemeriksaan Trusted Advisor.
- Jika hanya akun manajemen organisasi yang mengaktifkan rekomendasi untuk pemeriksaan, laporan tidak akan menyertakan sumber daya untuk akun lain di organisasi.

Untuk file sumber daya, Anda dapat menggunakan perangkat lunak umum, seperti Microsoft Excel, untuk membuka format berkas.csv. Anda dapat menggunakan file.csv untuk analisis satu kali dari semua pemeriksaan di semua akun di organisasi Anda. Jika Anda ingin menggunakan laporan Anda dengan aplikasi, Anda dapat mengunduh laporan berupa file.json sebagai gantinya.

Format file.json memberikan fleksibilitas lebih dari format file.csv untuk kasus penggunaan tingkat lanjut, seperti agregasi dan analitik lanjutan dengan beberapa set data. Misalnya, Anda dapat menggunakan antarmuka SQL dengan layanan AWS, seperti Amazon Athena untuk menjalankan kueri pada laporan Anda. Anda juga dapat menggunakan Amazon QuickSight untuk membuat dasbor dan memvisualkan data Anda. Untuk informasi selengkapnya, lihat Menggunakan layanan AWS lainnya untuk melihat laporan Trusted Advisor.

Menonaktifkan tampilan organisasi

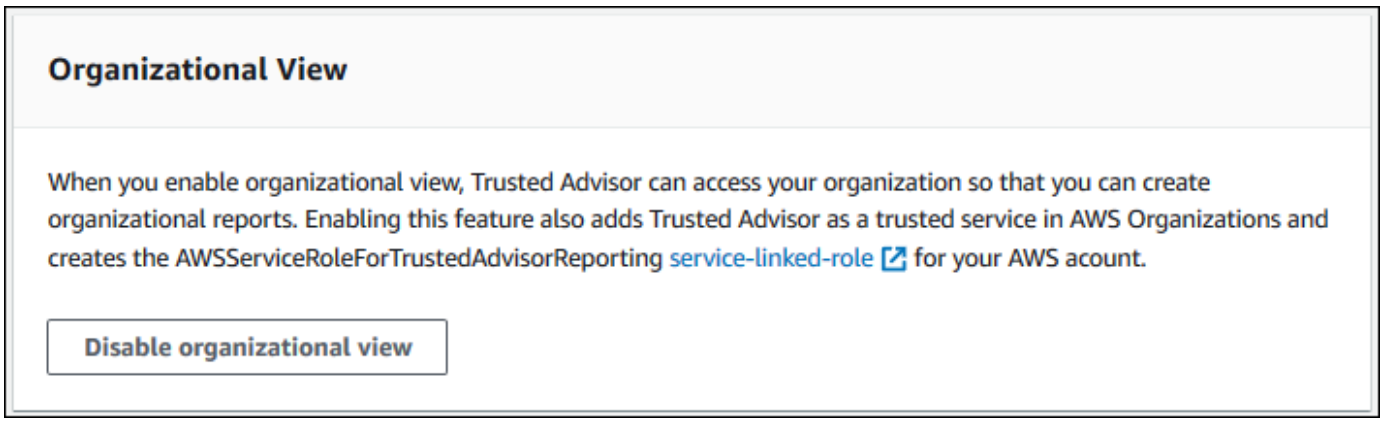
Ikuti prosedur ini untuk menonaktifkan tampilan organisasi. Anda harus masuk ke akun manajemen organisasi atau mengambil peran dengan izin yang diperlukan untuk menonaktifkan fitur ini. Anda tidak dapat menonaktifkan fitur ini dari akun lain di organisasi.

Setelah Anda menonaktifkan fitur ini, hal berikut terjadi:

- Trusted Advisor dihapus sebagai layanan tepercaya di Organizations.
- Peran terkait layanan `AWSServiceRoleForTrustedAdvisorReporting` dibuka di akun manajemen organisasi. Ini berarti Anda dapat menghapusnya secara manual jika diperlukan.
- Anda tidak dapat membuat, melihat, atau mengunduh laporan untuk organisasi Anda. Untuk mengakses laporan yang dibuat sebelumnya, Anda harus mengaktifkan kembali tampilan organisasi dari konsol Trusted Advisor. Lihat Mengaktifkan tampilan organisasi.

Untuk menonaktifkan tampilan organisasi untuk Trusted Advisor

1. Masuk ke akun manajemen organisasi dan buka konsol AWS Trusted Advisor di https://console.aws.amazon.com/trustedadvisor.
2. Di panel navigasi, pilih Preferensi.
3. Di bawah Organizational View (Tampilan Organisasi), pilih Disable organizational view (Nonaktifkan tampilan organisasi).



Setelah Anda menonaktifkan tampilan organisasi, Trusted Advisor tidak lagi menggabungkan pemeriksaan dari akun AWS di organisasi Anda. Namun, peran terkait layanan `AWSServiceRoleForTrustedAdvisorReporting` tetap ada di akun manajemen organisasi hingga Anda menghapusnya melalui konsol IAM, API IAM, atau AWS Command Line Interface (AWS CLI). Untuk informasi selengkapnya, lihat Menghapus peran tertaut layanan dalam Panduan Pengguna IAM.

> **Note**
>
> Anda dapat menggunakan layanan AWS lainnya untuk melakukan kueri dan memvisualkan data Anda untuk laporan tampilan organisasi. Untuk informasi selengkapnya, lihat sumber daya berikut.

- Melihat rekomendasi AWS Trusted Advisor sesuai skala dengan AWS Organizations dalam Blog Manajemen & Pengelolaan AWS
- Menggunakan layanan AWS lainnya untuk melihat laporan Trusted Advisor

Menggunakan kebijakan IAM untuk mengizinkan akses ke tampilan organisasi

Anda dapat menggunakan kebijakan AWS Identity and Access Management (IAM) berikut untuk mengizinkan pengguna atau peran dalam akun Anda mengakses tampilan organisasi di AWS Trusted Advisor.

Example : Akses penuh ke tampilan organisasi

Kebijakan berikut mengizinkan akses penuh ke fitur tampilan organisasi. Pengguna dengan izin ini dapat melakukan hal berikut:

- Mengaktifkan dan menonaktifkan tampilan organisasi
- Membuat, melihat, dan mengunduh laporan

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ReadStatement",
            "Effect": "Allow",
            "Action": [
                "organizations:ListAccountsForParent",
                "organizations:ListAccounts",
                "organizations:ListRoots",
                "organizations:DescribeOrganization",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListAWSServiceAccessForOrganization",
                "trustedadvisor:DescribeAccount",
                "trustedadvisor:DescribeChecks",
                "trustedadvisor:DescribeCheckSummaries",
                "trustedadvisor:DescribeAccountAccess",
                "trustedadvisor:DescribeOrganization",
                "trustedadvisor:DescribeReports",
```

```
                "trustedadvisor:DescribeServiceMetadata",
                "trustedadvisor:DescribeOrganizationAccounts",
                "trustedadvisor:ListAccountsForParent",
                "trustedadvisor:ListRoots",
                "trustedadvisor:ListOrganizationalUnitsForParent"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CreateReportStatement",
            "Effect": "Allow",
            "Action": [
                "trustedadvisor:GenerateReport"
            ],
            "Resource": "*"
        },
        {
            "Sid": "ManageOrganizationalViewStatement",
            "Effect": "Allow",
            "Action": [
                "organizations:EnableAWSServiceAccess",
                "organizations:DisableAWSServiceAccess",
                "trustedadvisor:SetOrganizationAccess"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CreateServiceLinkedRoleStatement",
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/
reporting.trustedadvisor.amazonaws.com/AWSServiceRoleForTrustedAdvisorReporting"
        }
    ]
}
```

Example : Akses baca ke tampilan organisasi

Kebijakan berikut mengizinkan akses baca-saja ke tampilan organisasi untuk Trusted Advisor. Pengguna dengan izin ini hanya dapat melihat dan mengunduh laporan yang ada.

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

```
    "Statement": [
        {
            "Sid": "ReadStatement",
            "Effect": "Allow",
            "Action": [
                "organizations:ListAccountsForParent",
                "organizations:ListAccounts",
                "organizations:ListRoots",
                "organizations:DescribeOrganization",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListAWSServiceAccessForOrganization",
                "trustedadvisor:DescribeAccount",
                "trustedadvisor:DescribeChecks",
                "trustedadvisor:DescribeCheckSummaries",
                "trustedadvisor:DescribeAccountAccess",
                "trustedadvisor:DescribeOrganization",
                "trustedadvisor:DescribeReports",
                "trustedadvisor:ListAccountsForParent",
                "trustedadvisor:ListRoots",
                "trustedadvisor:ListOrganizationalUnitsForParent"
            ],
            "Resource": "*"
        }
    ]
}
```

Anda dapat membuat kebijakan IAM sendiri. Untuk informasi selengkapnya, lihat langkah Membuat Kebijakan IAM dalam Panduan Pengguna IAM.

> **Note**
>
> Jika Anda mengaktifkan AWS CloudTrail di akun Anda, peran berikut dapat muncul di entri log Anda:
>
> - `AWSServiceRoleForTrustedAdvisorReporting` – Peran terkait layanan Trusted Advisor untuk mengakses akun di organisasi Anda.
> - `AWSServiceRoleForTrustedAdvisor` – Peran terkait layanan Trusted Advisor untuk mengakses layanan di organisasi Anda.

Untuk informasi selengkapnya tentang peran terkait layanan, lihat Menggunakan peran terkait layanan untuk Trusted Advisor.

Menggunakan layanan AWS lainnya untuk melihat laporan Trusted Advisor

Ikuti tutorial ini untuk mengunggah dan melihat data Anda dengan menggunakan layanan AWS lainnya. Dalam topik ini, Anda membuat bucket Amazon Simple Storage Service (Amazon S3) untuk menyimpan laporan Anda dan templat AWS CloudFormation untuk membuat sumber daya di akun Anda. Kemudian, Anda dapat menggunakan Amazon Athena untuk menganalisis atau menjalankan kueri untuk laporan Anda atau Amazon QuickSight untuk memvisualkan data tersebut di dasbor.

Untuk informasi dan contoh untuk memvisualkan data laporan Anda, lihat Melihat rekomendasi AWS Trusted Advisor sesuai skala dengan AWS Organizations dalam Blog Manajemen & Pemerintahan AWS.

Prasyarat

Sebelum memulai tutorial ini, Anda harus memenuhi persyaratan berikut:

- Masuklah sebagai pengguna AWS Identity and Access Management (IAM) dengan izin administrator.
- Gunakan Wilayah AWS US East (N. Virginia) untuk mengatur layanan dan sumber daya AWS dengan cepat.
- Buat QuickSight akun Amazon. Untuk informasi lebih lanjut, lihat Memulai dengan Analisis Data QuickSight di Amazon di Panduan QuickSight Pengguna Amazon.

Mengunggah laporan ke Amazon S3

Setelah mengunduh laporan `resources.json` Anda, unggah file tersebut ke Amazon S3. Anda harus menggunakan bucket di Wilayah US East (N. Virginia).

Untuk mengunggah laporan ke bucket Amazon S3

1. Masuklah ke AWS Management Console di https://console.aws.amazon.com/.
2. Gunakan Region selector (Pemilih wilayah) dan pilih Wilayah US East (N. Virginia).
3. Buka konsol Amazon S3 di https://console.aws.amazon.com/s3/.

4. Dari daftar bucket, pilih bucket S3, lalu salin namanya. Anda menggunakan nama tersebut dalam prosedur berikutnya.
5. Pada halaman *nama ember*, pilih Buat folder, masukkan nama**folder1**, lalu pilih Simpan.
6. Pilih folder1.
7. Di folder1, pilih Upload (Unggah) dan pilih file `resources.json`.
8. Pilih Next (Selanjutnya), biarkan opsi default, lalu pilih Upload (Unggah).

> **Note**
>
> Jika Anda mengunggah laporan baru ke bucket ini, ganti nama file `.json` setiap kali Anda mengunggahnya sehingga Anda tidak menimpa laporan yang ada. Misalnya, Anda dapat menambahkan stempel waktu ke setiap file, seperti `resources-timestamp.json`, `resources-timestamp2.json`, dan sebagainya.

Membuat sumber daya Anda menggunakan AWS CloudFormation

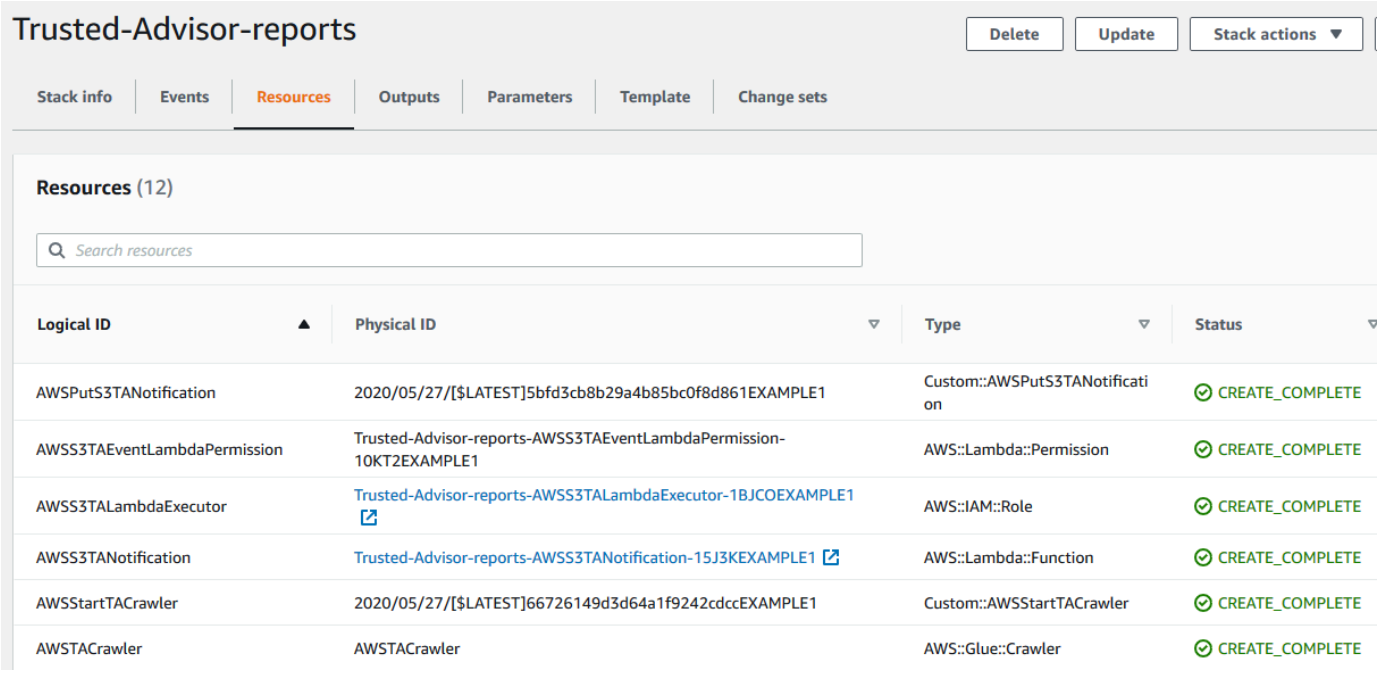
Setelah Anda mengunggah laporan Anda ke Amazon S3, unggah templat YAML berikut untuk AWS CloudFormation. Templat ini memberi tahu AWS CloudFormation sumber daya apa yang akan dibuat untuk akun Anda sehingga layanan lain dapat menggunakan data laporan dalam bucket S3. Templat tersebut menciptakan sumber daya untuk IAM, AWS Lambda, dan AWS Glue.

Untuk membuat sumber daya Anda dengan AWS CloudFormation

1. Unduh trusted-advisor-reports-templatefile.zip.
2. Buka filenya.
3. Buka file templat dalam editor teks.
4. Untuk parameter `BucketName` dan `FolderName`, ganti nilai-nilai untuk *`your-bucket-name-here`* dan *`folder1`* dengan nama bucket dan nama folder di akun Anda.
5. Simpan file.
6. Buka konsol AWS CloudFormation di https://console.aws.amazon.com/cloudformation.
7. Jika belum, di Region selector (Pemilih wilayah), pilih Wilayah US East (N. Virginia).
8. Di panel navigasi, pilih Stacks (Tumpukan).
9. Pilih Create stack (Buat tumpukan) dan pilih With new resources (standard) (Dengan sumber daya baru (standar)).

10. Pada halaman Create stack (Buat tumpukan), di bawah Specify templat (Tentukan templat), pilih Upload a template file (Pengunggahan file templat), lalu pilih Choose file (Pilih file).
11. Pilih file YAML dan pilih Next (Selanjutnya).
12. Pada halaman Specify stack details (Tentukan detail tumpukan), masukkan nama untuk tumpukan, seperti **`Organizational-view-Trusted-Advisor-reports`**, dan pilih Next (Selanjutnya).
13. Pada halaman Configure stack options (Konfigurasi opsi tumpukan), biarkan opsi default, lalu pilih Next (Selanjutnya).
14. Pada halaman Review (Ulasan)**`Organizational-view-Trusted-Advisor-reports`**, tinjau opsi Anda. Di bagian bawah halaman, pilih kotak centang untuk I acknowledge that AWS CloudFormation might create IAM resources (Saya mengetahui bahwa AWS CloudFormation mungkin membuat sumber daya IAM).
15. Pilih Buat tumpukan.

    Tumpukan membutuhkan waktu sekitar 5 menit untuk dibuat.
16. Setelah tumpukan berhasil dibuat, tab Resources (Sumber Daya) muncul seperti contoh berikut.



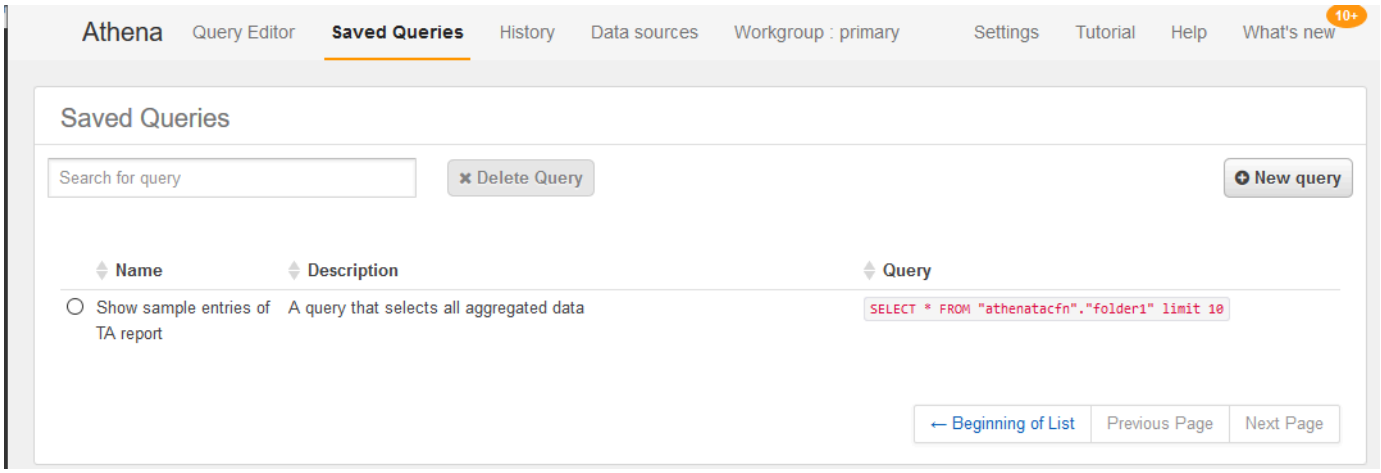
Kueri data di Amazon Athena

Setelah Anda memiliki sumber daya Anda, Anda dapat melihat data di Athena. Gunakan Athena untuk membuat kueri dan menganalisis hasil laporan, seperti mencari hasil pemeriksaan khusus untuk akun di organisasi.

> **Catatan**
>
> - Gunakan Wilayah US East (N. Virginia)
> - Jika Anda baru mengenal Athena, Anda harus menentukan lokasi hasil kueri sebelum dapat menjalankan kueri untuk laporan Anda. Sebaiknya tentukan bucket S3 yang berbeda untuk lokasi ini. Untuk informasi selengkapnya, lihat Menentukan lokasi hasil kueri di Panduan Pengguna Amazon Athena.

Untuk kueri data di Athena

1. Buka konsol Athena di https://console.aws.amazon.com/athena/.
2. Jika belum, di Region selector (Pemilih wilayah), pilih Wilayah US East (N. Virginia).
3. Pilih Saved Queries (Kueri tersimpan) dan di kolom pencarian, masukkan **`Show sample`**.
4. Pilih kueri yang muncul, seperti Show sample entries of TA report (Tampilkan entri sampel dari laporan TA).



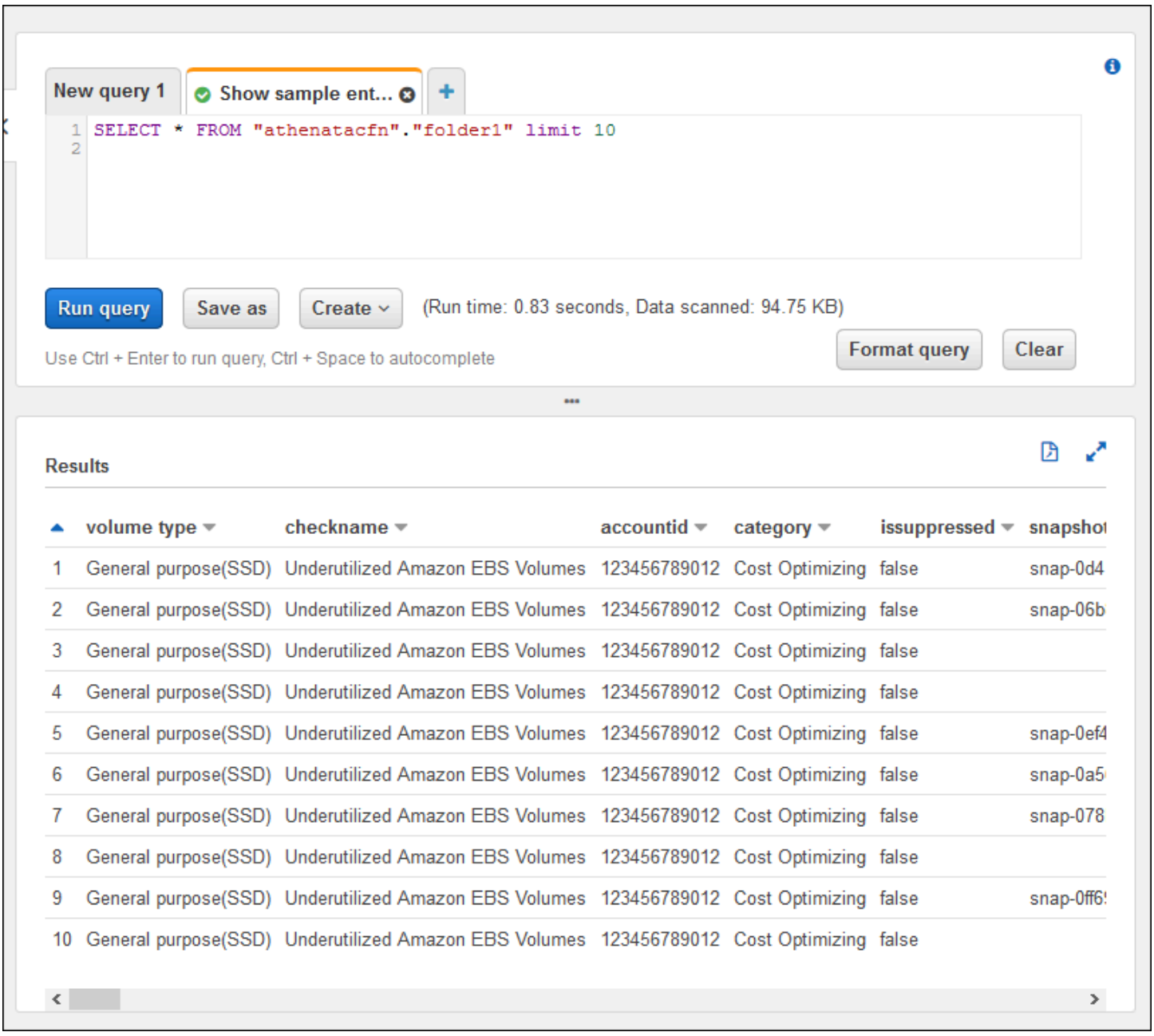
Kueri akan terlihat seperti berikut.

```
SELECT * FROM "athenatacfn"."folder1" limit 10
```

5. Pilih Run query (Jalankan kueri). Hasil kueri Anda akan muncul.

Example : Kueri Athena

Contoh berikut menunjukkan 10 entri sampel dari laporan.



Untuk informasi lebih lanjut, lihat Menjalankan Kueri SQL Menggunakan Amazon Athena di Panduan Pengguna Amazon Athena.

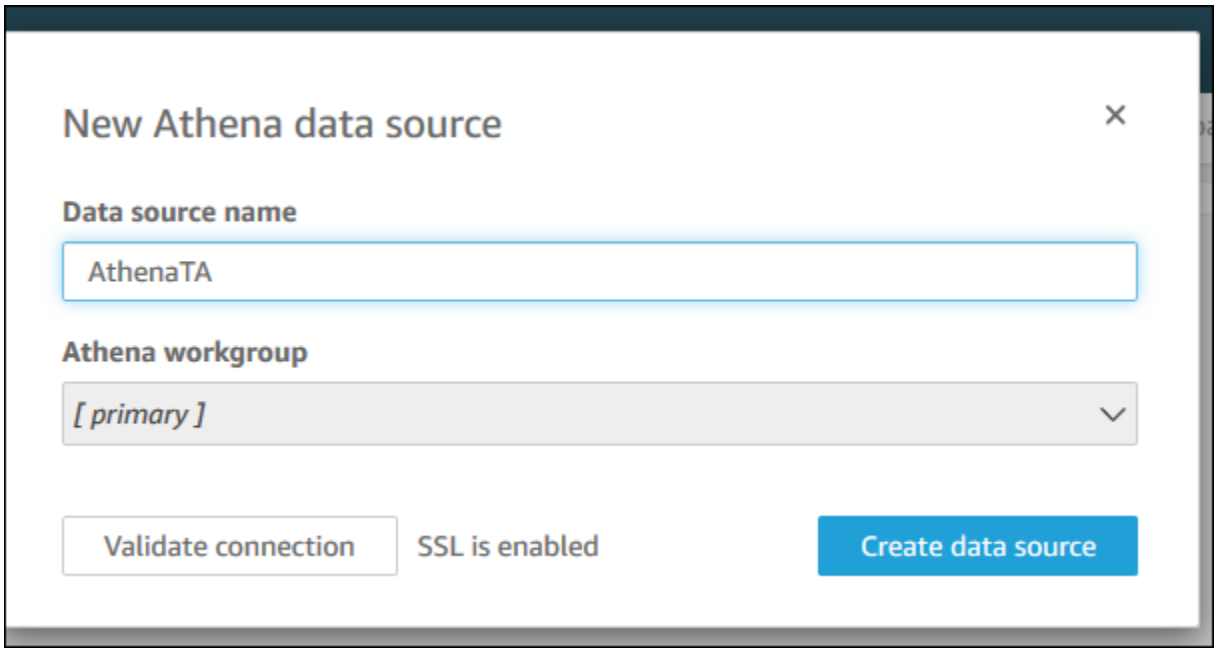
Membuat dasbor di Amazon QuickSight

Anda juga dapat mengatur Amazon QuickSight sehingga Anda dapat melihat data Anda di dasbor dan memvisualkan informasi laporan Anda.

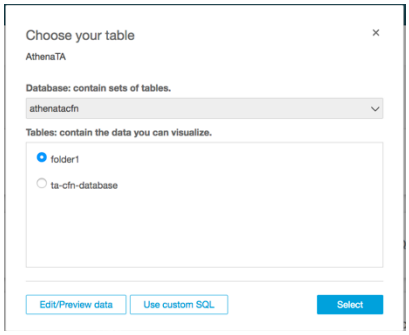
> **Note**
>
> Anda harus menggunakan Wilayah US East (N. Virginia).

Untuk membuat dasbor di Amazon QuickSight

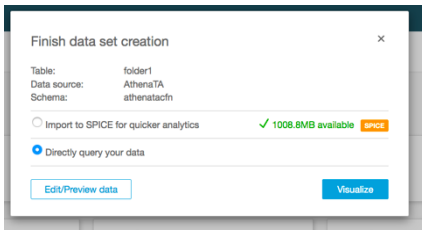
1. Arahkan ke QuickSight konsol Amazon dan masuk ke akun.
2. Pilih New analysis (Analisis baru), New dataset (Set data baru), lalu pilih Athena (Athena).
3. Di kotak dialog New Athena data source (Sumber data Athena baru), masukkan nama sumber data, seperti AthenaTA (AthenaTA), lalu pilih Create data source (Buat sumber data).



4. Di kotak dialog Choose your table (Pilih meja Anda), pilih tabel athenatacfn, pilih folder1, lalu pilih Select (Pilih).



5. Di kotak dialog Finish data set creation (Selesaikan pembuatan set data), pilih Directly query your data (Kueri data Anda secara langsung), lalu pilih Visualize (Visualkan).

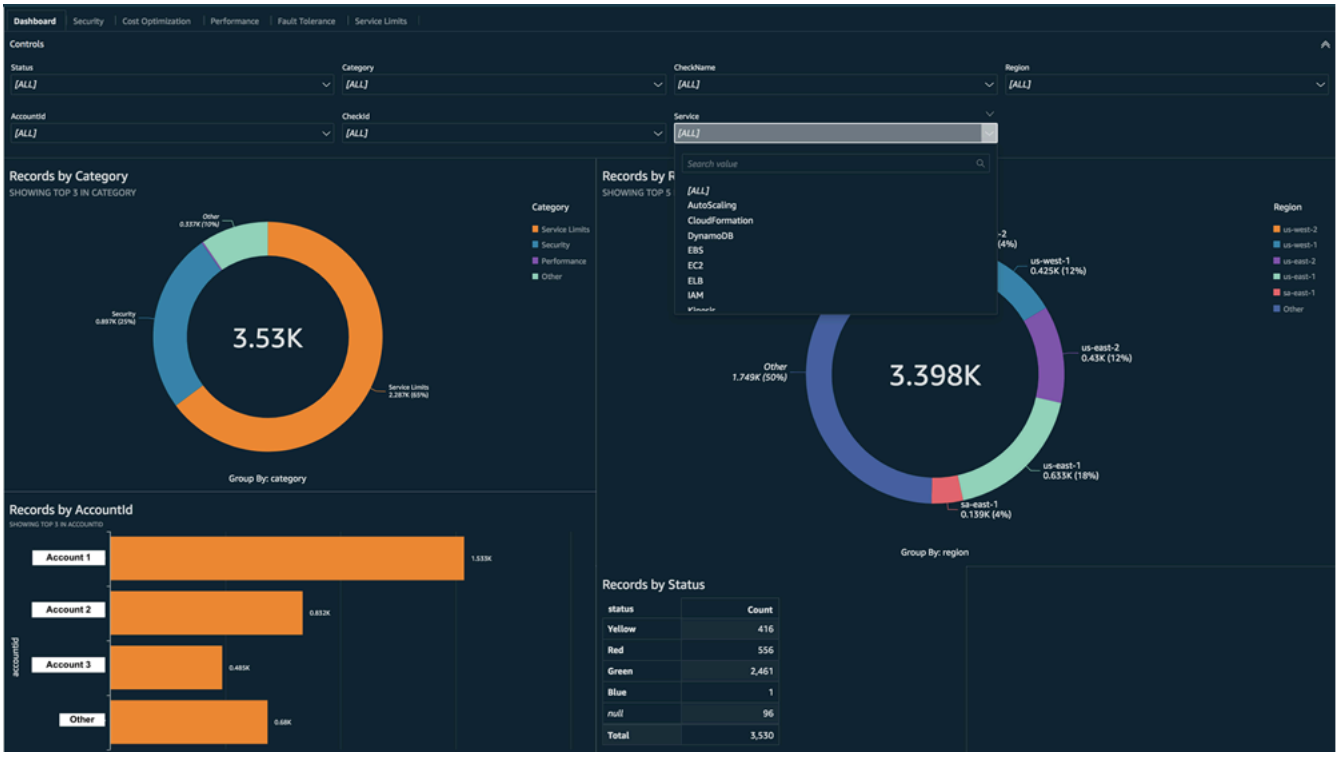


Anda sekarang dapat membuat dasbor di Amazon QuickSight. Untuk informasi selengkapnya, lihat Bekerja dengan Dasbor di Panduan QuickSight Pengguna Amazon.

Example : QuickSight Dasbor Amazon

Contoh dasbor berikut menunjukkan informasi tentang pemeriksaan Trusted Advisor, seperti berikut:

- ID akun yang terpengaruh
- Ringkasan berdasarkan Kawasan AWS
- Kategori pemeriksaan
- Status pemeriksaan
- Jumlah entri dalam laporan untuk setiap akun



> **Note**
>
> Jika Anda memiliki eror izin saat membuat dasbor Anda, pastikan bahwa Amazon QuickSight dapat menggunakan Athena. Untuk informasi lebih lanjut, lihat Saya Tidak Bisa Connect ke Amazon Athena di Panduan QuickSight Pengguna Amazon Athena.

Untuk informasi selengkapnya dan contoh tambahan untuk memvisualkan data laporan Anda, lihat Melihat rekomendasi AWS Trusted Advisor sesuai skala dengan AWS Organizations dalam Blog Manajemen & Pengelolaan AWS.

Pemecahan Masalah

Jika Anda memiliki masalah dengan tutorial ini, lihat kiat pemecahan masalah berikut.

Saya tidak melihat data terbaru dalam laporan saya

Ketika Anda membuat laporan, fitur tampilan organisasi tidak secara otomatis menyegarkan pemeriksaan Trusted Advisor di organisasi Anda. Untuk mendapatkan hasil pemeriksaan terbaru, segarkan pemeriksaan untuk akun manajemen dan setiap akun anggota dalam organisasi. Untuk informasi selengkapnya, lihat Menyegarkan pemeriksaan Trusted Advisor.

Saya memiliki kolom duplikat dalam laporan

Konsol Athena mungkin menampilkan eror berikut di tabel Anda jika laporan Anda memiliki kolom duplikat.

```
HIVE_INVALID_METADATA: Hive metadata for table folder1 is invalid: Table
descriptor contains duplicate columns
```

Misalnya, jika Anda menambahkan kolom dalam laporan yang sudah ada, hal ini dapat menyebabkan masalah saat Anda mencoba melihat data laporan di konsol Athena. Anda dapat mengikuti langkah-langkah berikut untuk memperbaiki masalah ini.

Temukan kolom duplikat

Anda dapat menggunakan konsol AWS Glue untuk melihat skema dan dengan cepat mengidentifikasi jika Anda memiliki kolom duplikat dalam laporan Anda.

Untuk menemukan kolom duplikat

1. Buka konsol AWS Glue di https://console.aws.amazon.com/glue/.
2. Jika belum, di Region selector (Pemilih wilayah), pilih Wilayah US East (N. Virginia).
3. Di panel navigasi, pilih Tables (Tabel).
4. Pilih nama folder Anda, seperti ***folder1***, lalu di bawah Schema (Skema), lihat nilai untuk Column name (Nama kolom).

   Jika Anda memiliki kolom duplikat, Anda harus mengunggah laporan baru ke bucket Amazon S3 Anda. Lihat bagian berikut Mengunggah laporan baru.

Mengunggah laporan baru

Setelah Anda mengidentifikasi kolom duplikat, kami sarankan Anda mengganti laporan yang sudah ada dengan yang baru. Hal ini memastikan bahwa sumber daya yang dibuat dari tutorial ini menggunakan data laporan terbaru dari organisasi Anda.

Untuk mengunggah laporan baru

1. Jika belum, segarkan pemeriksaan Trusted Advisor untuk akun di organisasi Anda. Lihat Menyegarkan pemeriksaan Trusted Advisor.
2. Buat dan unduh laporan JSON lainnya di konsol Trusted Advisor. Lihat Membuat laporan tampilan organisasi. Anda harus menggunakan file JSON untuk tutorial ini.

3. Masuk ke AWS Management Console dan buka konsol Amazon S3 di https://console.aws.amazon.com/s3/.
4. Pilih bucket Amazon S3 dan pilih folder *folder1*.
5. Pilih laporan *resources*.json sebelumnya dan pilih Delete (Hapus).
6. Pada halaman Delete objects (Hapus objek), di bawah Permanently delete objects? (Hapus objek secara permanen?), masukkan **permanently delete**, lalu pilih Delete objects (Hapus objek).
7. Di bucket S3 Anda, pilih Upload (Unggah) dan kemudian tentukan laporan baru. Tindakan ini secara otomatis memperbarui tabel Athena Anda dan sumber daya crawler AWS Glue dengan data laporan terbaru. Perlu waktu beberapa menit untuk menyegarkan sumber daya Anda.
8. Masukkan kueri baru di konsol Athena. Lihat Kueri data di Amazon Athena.

> **Note**
>
> Jika Anda masih memiliki masalah dengan tutorial ini, Anda dapat membuat kasus dukungan teknis di Pusat AWS Support.

Lihat AWS Trusted Advisor cek yang didukung oleh AWS Config

AWS Configadalah layanan yang terus-menerus menilai, mengaudit, dan mengevaluasi konfigurasi sumber daya Anda untuk pengaturan yang Anda inginkan. AWS Configmenyediakan aturan terkelola, yang merupakan pemeriksaan kepatuhan yang telah ditentukan sebelumnya dan dapat disesuaikan yang AWS Config digunakan untuk mengevaluasi apakah AWS sumber daya Anda mematuhi praktik terbaik umum.

AWS ConfigKonsol memandu Anda melalui konfigurasi dan aktivasi aturan terkelola. Anda juga dapat menggunakan AWS Command Line Interface (AWS CLI) atau AWS Config API untuk meneruskan kode JSON yang menentukan konfigurasi aturan terkelola. Anda dapat menyesuaikan perilaku aturan terkelola agar sesuai dengan kebutuhan Anda. Anda dapat menyesuaikan parameter aturan untuk menentukan atribut yang harus dimiliki sumber daya Anda untuk mematuhi aturan. Untuk mempelajari lebih lanjut tentang mengaktifkanAWS Config, lihat Panduan AWS Config Pengembang.

AWS Configaturan terkelola memberi daya pada serangkaian Trusted Advisor pemeriksaan di semua kategori. Saat Anda mengaktifkan aturan terkelola tertentu, Trusted Advisor pemeriksaan terkait akan

diaktifkan secara otomatis. Untuk melihat Trusted Advisor pemeriksaan mana yang didukung oleh aturan AWS Config terkelola tertentu, lihatAWS Trusted Advisor periksa referensi.

Pemeriksaan AWS Config bertenaga tersedia untuk pelanggan dengan paket AWSBusiness Support, AWSEnterprise On-Ramp, dan Enterprise AWSSupport. Jika Anda mengaktifkan AWS Config dan memiliki salah satu paket AWS Support ini, Anda akan secara otomatis melihat rekomendasi yang didukung oleh aturan AWS Config terkelola yang diterapkan terkait.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan berdasarkan pembaruan yang dipicu perubahan pada aturan terkelola. AWS Config Permintaan penyegaran tidak diizinkan. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

Pemecahan Masalah

Jika Anda memiliki masalah dengan integrasi ini, lihat informasi pemecahan masalah berikut.

Daftar Isi

Saya baru saja mengaktifkan perekaman dan aturan terkelola untukAWS Config, tetapi saya tidak melihat Trusted Advisor pemeriksaan yang sesuai.

Setelah AWS Config aturan menghasilkan hasil evaluasi, Anda melihat hasilnya Trusted Advisor dalam waktu dekat. Jika Anda memiliki masalah dengan fitur ini, buat kasus dukungan teknis di AWS SupportPusat.

Saya menerapkan aturan AWS Config terkelola yang sama dua kali, apa yang akan saya lihat? Trusted Advisor

Anda melihat entri terpisah dalam hasil Trusted Advisor pemeriksaan untuk setiap aturan terkelola yang Anda instal.

Saya mematikan rekaman untuk AWS Config di AWS Wilayah. Apa yang akan saya lihatTrusted Advisor?

Jika Anda menonaktifkan perekaman sumber daya untuk AWS Config di AWS Wilayah, maka Trusted Advisor tidak lagi menerima data untuk aturan dan pemeriksaan terkelola terkait di Wilayah tersebut. Hasil aturan terkelola yang ada tetap masuk AWS Config dan masuk Trusted Advisor hingga AWS Config kedaluwarsa, berdasarkan kebijakan penyimpanan perekam. Jika Anda menghapus aturan terkelola, maka data Trusted Advisor cek biasanya dihapus dalam waktu dekat.

MelihatAWS Security Hub kontrol diAWS Trusted Advisor

Setelah Anda mengaktifkanAWS Security Hub untuk AndaAkun AWS, Anda dapat melihat kontrol keamanan Anda dan temuan mereka diTrusted Advisor konsol. Anda dapat menggunakan kontrol Security Hub untuk mengidentifikasi kerentanan keamanan di akun Anda dengan cara yang sama seperti Anda dapat menggunakanTrusted Advisor pemeriksaan. Anda dapat melihat status pemeriksaan, daftar sumber daya yang terpengaruh, dan kemudian mengikuti rekomendasi Security Hub untuk mengatasi masalah keamanan Anda. Anda dapat menggunakan fitur ini untuk menemukan rekomendasi keamanan dariTrusted Advisor dan Security Hub di satu lokasi yang nyaman.

> **Catatan**
>
> - DariTrusted Advisor, Anda dapat melihat kontrol dalam standar keamanan Praktik Terbaik KeamananAWS Dasar kecuali untuk kontrol yang memiliki Category: Recover > Resilience. Untuk daftar kontrol yang didukung, lihat kontrol Praktik Terbaik KeamananAWS Dasar di PanduanAWS Security Hub Pengguna.
>
>   Untuk informasi selengkapnya tentang kategori Security Hub, lihat Kategori kontrol.
> - Saat ini, ketika Security Hub menambahkan kontrol baru ke standar keamanan Praktik Terbaik KeamananAWS Dasar, mungkin ada penundaan dua hingga empat minggu

sebelum Anda dapat melihatnyaTrusted Advisor. Kerangka waktu ini adalah upaya terbaik dan tidak dijamin.

Topik

Prasyarat

Anda harus memenuhi persyaratan berikut untuk mengaktifkan Security HubTrusted Advisor

- Anda harus memiliki paket Support Bisnis, Korporasi, atau Korporasi untuk fitur ini. Anda dapat menemukan paket Support Anda dari AWS SupportPusat atau dari halaman Paket Dukungan. Untuk informasi selengkapnya, lihat MembandingkanAWS Support paket.
- Anda harus mengaktifkan perekaman sumber dayaAWS Config untukWilayah AWS yang Anda inginkan untuk kontrol Security Hub Anda. Untuk informasi selengkapnya, lihat Mengaktifkan dan mengonfigurasiAWS Config.
- Anda harus mengaktifkan Security Hub dan memilih standar AWSkeamanan Praktik Terbaik Keamanan Dasar v1.0.0. Jika Anda belum melakukannya, lihat MenyiapkanAWS Security Hub di PanduanAWS Security Hub Pengguna.

> **Note**
>
> Jika Anda menyelesaikan prasyarat ini, Anda dapat melompat keMelihat temuan Security Hub.

TentangAWS Organizations akun

Jika Anda menyelesaikan prasyarat untuk akun manajemen, integrasi ini diaktifkan secara otomatis untuk semua akun anggota di organisasi Anda. Akun anggota individual tidak perlu dihubungiAWS

Support untuk mengaktifkan fitur ini. Namun, akun anggota di organisasi Anda harus mengaktifkan Security Hub jika mereka ingin melihat temuan merekaTrusted Advisor.

Jika Anda ingin menonaktifkan integrasi ini untuk akun anggota tertentu, lihatNonaktifkan fitur ini untukAWS Organizations akun.

Melihat temuan Security Hub

Setelah Anda mengaktifkan Security Hub untuk akun Anda, diperlukan waktu hingga 24 jam agar temuan Security Hub Anda muncul di halaman KeamananTrusted Advisor konsol.

Untuk melihat Security HubTrusted Advisor

1. Arahkan ke Trusted Advisorkonsol, lalu pilih kategori Keamanan.
2. Di bidang Cari berdasarkan kata kunci, masukkan nama kontrol atau deskripsi di bidang.

   > **Tip**
   >
   > Untuk Sumber, Anda dapat memilih AWS Security Hubuntuk memfilter kontrol Security Hub.

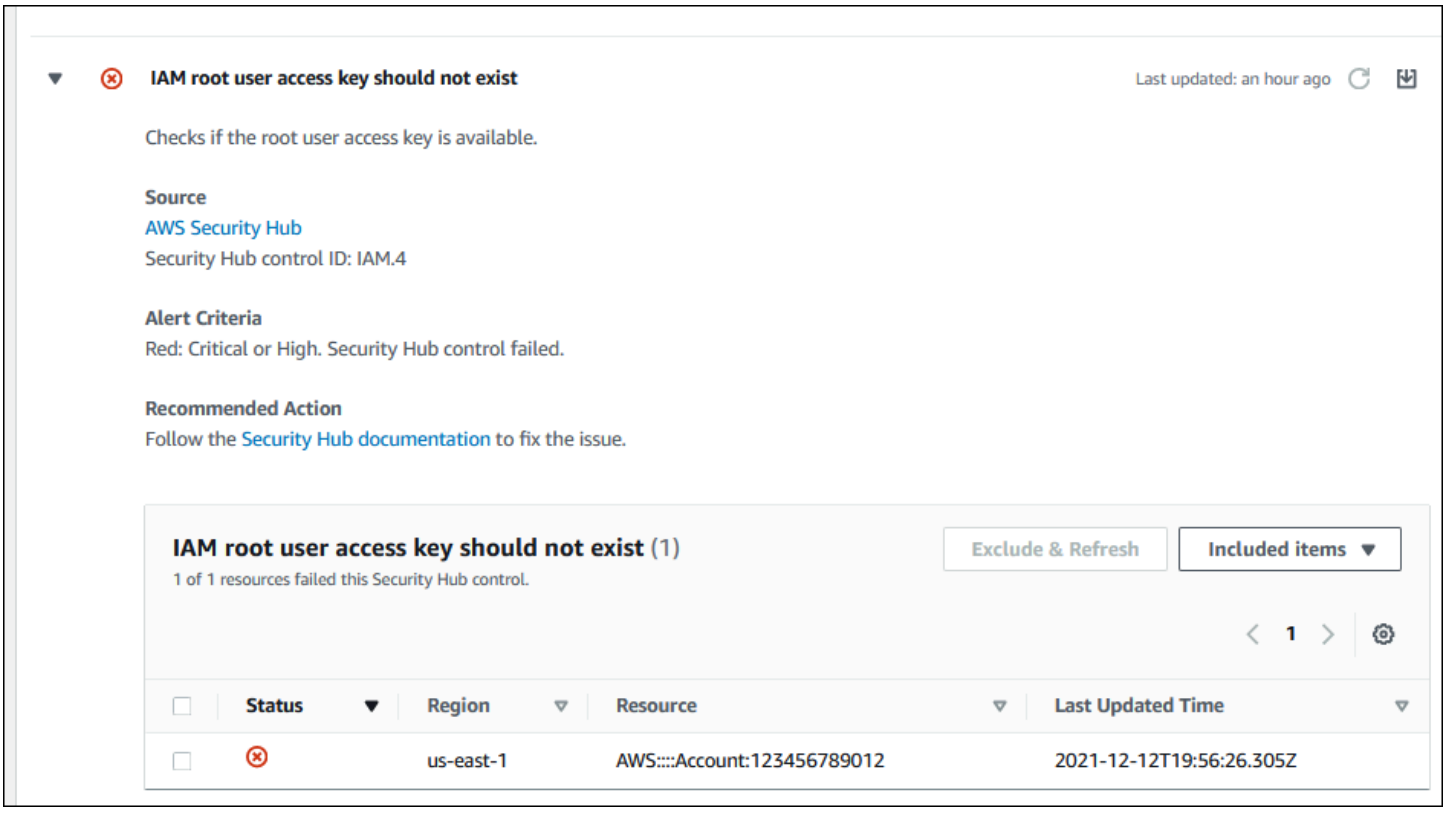
3. Pilih nama Security Hub untuk melihat informasi berikut:

   - Deskripsi — Menjelaskan bagaimana kontrol ini memeriksa akun Anda untuk kerentanan keamanan.
   - Sumber - Apakah cek berasal dariAWS Trusted Advisor atauAWS Security Hub. Untuk kontrol Security Hub, Anda dapat menemukan ID kontrol.
   - Kriteria Peringatan - Status kontrol. Misalnya, jika Security Hub mendeteksi masalah penting, statusnya mungkin Merah: Kritis atau Tinggi.
   - Tindakan yang Disarankan - Gunakan tautan dokumentasi Security Hub untuk menemukan langkah-langkah yang disarankan untuk memperbaiki masalah.
   - Sumber daya Security Hub - Anda dapat menemukan sumber daya di akun tempat Security Hub mendeteksi masalah.

> **Catatan**
>
> - Anda harus menggunakan Security Hub untuk mengecualikan sumber daya dari temuan Anda. Saat ini, Anda tidak dapat menggunakanTrusted Advisor konsol untuk mengecualikan item dari kontrol Security Hub. Untuk informasi selengkapnya, lihat Mengatur status alur kerja untuk temuan.
> - Fitur tampilan organisasi mendukung integrasi ini dengan Security Hub. Anda dapat melihat temuan untuk kontrol Security Hub di seluruh organisasi, lalu membuat dan mengunduh laporan. Untuk informasi selengkapnya, lihat Tampilan organisasi untuk AWS Trusted Advisor.

Example Contoh: Kontrol Security Hub untuk kunci akses pengguna IAM seharusnya tidak ada

Berikut ini adalah contoh temuan untuk kontrol Security Hub diTrusted Advisor konsol.



Segarkan Security Hub

Setelah Anda mengaktifkan standar keamanan, dibutuhkan waktu hingga dua jam untuk Security Hub untuk mendapatkan temuan untuk sumber daya Anda. Kemudian memerlukan waktu hingga 24

jam agar data tersebut muncul diTrusted Advisor konsol. Jika Anda baru saja mengaktifkan standar keamanan AWSFoundational Security Best Practices v1.0.0, periksaTrusted Advisor konsol lagi nanti.

> **Note**
>
> - Jadwal penyegaran untuk setiap kontrol Security Hub bersifat periodik atau perubahan yang dipicu. Saat ini, Anda tidak dapat menggunakanTrusted Advisor konsol atauAWS Support API untuk menyegarkan kontrol Security Hub Anda. Untuk informasi selengkapnya, lihat Menjadwalkan pemeriksaan keamanan.
> - Anda harus menggunakan Security Hub jika ingin mengecualikan sumber daya dari temuan Anda. Saat ini, Anda tidak dapat menggunakanTrusted Advisor konsol untuk mengecualikan item dari kontrol Security Hub. Untuk informasi selengkapnya, lihat Mengatur status alur kerja untuk temuan.

Nonaktifkan Security Hub dariTrusted Advisor

Ikuti prosedur ini jika Anda tidak ingin informasi Security Hub Anda muncul diTrusted Advisor konsol. Prosedur ini hanya menonaktifkan integrasi Security Hub denganTrusted Advisor. Ini tidak akan memengaruhi konfigurasi Anda dengan Security Hub. Anda dapat terus menggunakan konsol Security Hub untuk melihat kontrol keamanan, sumber daya, dan rekomendasi Anda.

Untuk menonaktifkan integrasi Security Hub

1. Hubungi AWS Supportdan minta untuk menonaktifkan integrasi Security Hub denganTrusted Advisor.

   SetelahAWS Support menonaktifkan fitur ini, Security Hub tidak lagi mengirimkan data keTrusted Advisor. Data Security Hub Anda akan dihapus dariTrusted Advisor.
2. Jika Anda ingin mengaktifkan integrasi ini lagi, hubungi AWS Support.

Nonaktifkan fitur ini untukAWS Organizations akun

Jika Anda telah menyelesaikan prosedur sebelumnya untuk akun manajemen, integrasi Security Hub secara otomatis dihapus dari semua akun anggota di organisasi Anda. Akun anggota individual di organisasi Anda tidak perlu menghubungiAWS Support secara terpisah.

Jika Anda adalah akun anggota di organisasi, Anda dapat menghubungiAWS Support untuk menghapus fitur ini hanya dari akun Anda.

Pemecahan Masalah

Jika Anda mengalami masalah dengan integrasi ini, lihat informasi pemecahan masalah berikut.

Daftar Isi

Saya tidak melihat temuan Security Hub diTrusted Advisor konsol

Pastikan bahwa Anda menyelesaikan langkah-langkah berikut:

- Anda memiliki paket Business, Enterprise On-Ramp, atau Enterprise Support.
- Anda mengaktifkan perekaman sumber daya diAWS Config dalam Wilayah yang sama dengan Security Hub.
- Anda mengaktifkan Security Hub dan memilih standar AWSkeamanan Praktik Terbaik Keamanan Dasar v1.0.0.
- Kontrol baru dari Security Hub ditambahkan sebagai pemeriksaan dalamTrusted Advisor waktu dua hingga empat minggu. Lihat catatannya.

Untuk informasi lain, lihat Prasyarat.

Saya mengkonfigurasi Security Hub danAWS Config benar, tetapi temuan saya masih hilang

Diperlukan waktu hingga dua jam Security Hub mendapatkan temuan untuk sumber daya Anda. Kemudian memerlukan waktu hingga 24 jam agar data tersebut muncul diTrusted Advisor konsol. PeriksaTrusted Advisor konsol lagi nanti.

> **Catatan**
>
> - Hanya temuan Anda untuk kontrol dalam standar keamanan Praktik Terbaik KeamananAWS Dasar yang akan munculTrusted Advisor kecuali untuk kontrol yang memiliki Category: Recover > Resilience.
> - Jika ada masalah layanan dengan Security Hub atau Security Hub tidak tersedia, diperlukan waktu hingga 24 jam agar temuan Anda munculTrusted Advisor. PeriksaTrusted Advisor konsol lagi nanti.

Saya ingin menonaktifkan kontrol Security Hub tertentu

Security Hub mengirimkan data Anda secaraTrusted Advisor otomatis. Jika Anda menonaktifkan kontrol Security Hub atau tidak lagi memiliki sumber daya untuk kontrol itu, temuan Anda tidak akan munculTrusted Advisor.

Anda dapat masuk ke konsol Security Hub dan memverifikasi apakah kontrol Anda diaktifkan atau dinonaktifkan.

Jika Anda menonaktifkan kontrol Security Hub atau menonaktifkan semua kontrol untukAWS standar keamanan Praktik Terbaik Keamanan Dasar, temuan Anda diarsipkan dalam lima hari ke depan. Periode lima hari untuk mengarsipkan ini adalah perkiraan dan upaya terbaik saja, dan tidak dijamin. Ketika temuan Anda diarsipkan, mereka dihapus dariTrusted Advisor.

Untuk informasi lain, lihat topik berikut:

- Menonaktifkan dan mengaktifkan kontrol individu
- Menonaktifkan atau mengaktifkan standar keamanan

Saya ingin menemukan sumber daya Security Hub yang dikecualikan

DariTrusted Advisor konsol, Anda dapat memilih nama kontrol Security Hub, lalu memilih opsi Item yang dikecualikan. Opsi ini menampilkan semua sumber daya yang ditekan di Security Hub.

Jika status alur kerja untuk sumber daya diatur keSUPPRESSED, maka sumber daya yang dikecualikan item diTrusted Advisor. Anda tidak dapat menekan sumber daya Security Hub dariTrusted Advisor konsol. Untuk melakukannya, gunakan konsol Security Hub. Untuk informasi selengkapnya, lihat Mengatur status alur kerja untuk temuan.

Saya ingin mengaktifkan atau menonaktifkan fitur ini untuk akun anggota milikAWS organisasi

Secara default, akun anggota mewarisi fitur dari akun manajemen untukAWS Organizations. Jika akun manajemen telah mengaktifkan fitur tersebut, maka semua akun di organisasi juga akan memiliki fitur tersebut. Jika Anda memiliki akun anggota dan ingin membuat perubahan khusus untuk akun Anda, Anda harus menghubungi AWS Support.

Saya melihat beberapaWilayah AWS sumber daya terpengaruh yang sama untuk pemeriksaan Security Hub

BeberapaLayanan AWS bersifat global dan tidak spesifik untuk Wilayah, seperti IAM dan Amazon CloudFront. Secara default, sumber daya global seperti bucket Amazon S3 muncul di Wilayah Timur AS (N. Virginia).

Untuk pemeriksaan Security Hub yang mengevaluasi sumber daya untuk layanan global, Anda mungkin melihat lebih dari satu item untuk sumber daya yang terpengaruh. Misalnya, jika`Hardware MFA should be enabled for the root user` pemeriksaan mengidentifikasi bahwa akun Anda belum mengaktifkan fitur ini, maka Anda akan melihat beberapa Wilayah dalam tabel untuk sumber daya yang sama.

Anda dapat mengonfigurasi Security HubAWS Config sehingga beberapa Wilayah tidak akan muncul untuk sumber daya yang sama. Untuk informasi selengkapnya, lihat Kontrol Praktik TerbaikAWS Dasar yang mungkin ingin Anda nonaktifkan.

Saya mematikan Security Hub atauAWS Config di Wilayah

Jika Anda menghentikan perekaman sumber daya denganAWS Config atau menonaktifkan Security Hub diWilayah AWS,Trusted Advisor tidak lagi menerima data untuk kontrol apa pun di Wilayah

tersebut. Trusted Advisormenghapus temuan Security Hub Anda dalam 7-9 hari. Kerangka waktu ini adalah upaya terbaik dan tidak dijamin. Untuk informasi selengkapnya, lihat Menonaktifkan Security Hub.

Untuk menonaktifkan fitur ini untuk akun Anda, lihatNonaktifkan Security Hub dariTrusted Advisor.

Kontrol saya diarsipkan di Security Hub, tetapi saya masih melihat temuan diTrusted Advisor

KetikaRecordState status berubahARCHIVED untuk temuan,Trusted Advisor menghapus temuan untuk kontrol Security Hub dari akun Anda. Anda mungkin masih melihat temuan tersebut hingga 7-9 hari sebelum dihapus.Trusted Advisor Kerangka waktu ini adalah upaya terbaik dan tidak dijamin.

Saya masih tidak dapat melihat temuan Security Hub saya

Jika Anda masih memiliki masalah dengan fitur ini, Anda dapat membuat kasus dukungan teknis di AWS SupportPusat.

Ikut serta AWS Compute Optimizer untuk Trusted Advisor cek

Compute Optimizer adalah layanan yang menganalisis konfigurasi dan metrik pemanfaatan sumber daya Anda. AWS Layanan ini melaporkan apakah sumber daya Anda dikonfigurasi dengan benar untuk efisiensi dan keandalan. Ini juga menyarankan perbaikan yang dapat Anda terapkan untuk meningkatkan kinerja beban kerja. Dengan Compute Optimizer, Anda akan melihat rekomendasi yang sama dalam pemeriksaan. Trusted Advisor

Anda dapat memilih salah satu akun Anda Akun AWS , atau semua akun anggota yang merupakan bagian dari organisasi AWS Organizations. Untuk informasi selengkapnya, lihat Memulai di Panduan AWS Compute Optimizer Pengguna.

Setelah Anda memilih Compute Optimizer, pemeriksaan berikut menerima data dari fungsi Lambda dan volume Amazon EBS Anda. Diperlukan waktu hingga 12 jam untuk menghasilkan temuan dan rekomendasi pengoptimalan. Kemudian dapat memakan waktu hingga 48 jam untuk melihat hasil Anda Trusted Advisor untuk pemeriksaan berikut:

Optimasi biaya

- Volume Amazon EBS yang disediakan secara berlebihan
- AWS Lambda fungsi yang disediakan secara berlebihan untuk ukuran memori

Kinerja

- Volume Amazon EBS yang kurang disediakan
- AWS Lambda fungsi yang kurang disediakan untuk ukuran memori

> **Catatan**
>
> - Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali sehari. Permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.
> - Trusted Advisor sudah memiliki Volume Amazon EBS yang Kurang Digunakan dan pemeriksaan Volume Magnetik Amazon EBS yang Terlalu Digunakan.
>
> Setelah Anda ikut serta dengan Compute Optimizer, sebaiknya gunakan volume Amazon EBS yang baru disediakan secara berlebihan dan pemeriksaan volume Amazon EBS yang kurang disediakan.

Informasi terkait

Untuk informasi selengkapnya, lihat topik berikut.

- Melihat rekomendasi volume Amazon EBS di AWS Compute Optimizer Panduan Pengguna
- Melihat rekomendasi fungsi Lambda di Panduan Pengguna AWS Compute Optimizer
- Mengkonfigurasi memori fungsi Lambda di AWS Lambda Panduan Pengembang
- Minta modifikasi pada volume Amazon EBS Anda di Panduan Pengguna Amazon EC2

Memulai dengan AWS Trusted Advisor Prioritas

Trusted AdvisorPrioritas membantu Anda mengamankan dan mengoptimalkan Anda Akun AWS untuk mengikuti praktik AWS terbaik. Dengan Trusted Advisor Priority, Akun AWS tim Anda dapat secara proaktif memantau akun Anda dan membuat rekomendasi yang diprioritaskan ketika mereka mengidentifikasi peluang untuk Anda.

Misalnya, tim akun Anda dapat mengidentifikasi apakah pengguna root AWS akun Anda tidak memiliki otentikasi multi-faktor (MFA). Tim akun Anda dapat membuat rekomendasi sehingga

Anda dapat segera mengambil tindakan pada pemeriksaan, sepertiMFA on Root Account. Rekomendasi muncul sebagai rekomendasi prioritas aktif di halaman Trusted Advisor Prioritas konsol. Trusted Advisor Anda kemudian mengikuti rekomendasi untuk menyelesaikannya.

Trusted AdvisorRekomendasi prioritas berasal dari dua sumber ini:

- Layanan AWS— Layanan sepertiTrusted Advisor,AWS Security Hub, dan AWS Well-Architected secara otomatis membuat rekomendasi. Tim akun Anda membagikan rekomendasi ini kepada Anda sehingga rekomendasi tersebut muncul di Trusted Advisor Prioritas.
- Tim akun Anda — Tim akun Anda dapat membuat rekomendasi manual.

Trusted AdvisorPrioritas membantu Anda fokus pada rekomendasi yang paling penting. Anda dan tim akun Anda dapat memantau siklus hidup rekomendasi, dari titik ketika tim akun Anda membagikan rekomendasi, hingga saat Anda mengakui, menyelesaikan, atau mengabaikannya. Anda dapat menggunakan Trusted Advisor Priority untuk menemukan rekomendasi untuk semua akun anggota di organisasi Anda.

Topik

Prasyarat

Anda harus memenuhi persyaratan berikut untuk menggunakan Trusted Advisor Prioritas:

- Anda harus memiliki paket Enterprise Support.
- Akun Anda harus menjadi bagian dari organisasi yang telah mengaktifkan semua fitur diAWS Organizations. Untuk informasi selengkapnya, lihat Mengaktifkan semua fitur di organisasi Anda dalam Panduan Pengguna AWS Organizations.
- Organisasi Anda harus mengaktifkan akses tepercaya keTrusted Advisor. Untuk mengaktifkan akses tepercaya, masuk sebagai akun manajemen. Buka halaman Organisasi Anda di Trusted Advisor konsol.
- Anda harus masuk ke AWS akun Anda untuk melihat rekomendasi Trusted Advisor Prioritas untuk akun Anda.
- Anda harus masuk ke akun manajemen organisasi atau akun administrator yang didelegasikan untuk melihat rekomendasi gabungan di seluruh organisasi Anda. Untuk petunjuk tentang cara mendaftarkan akun administrator yang didelegasikan, lihatDaftarkan administrator yang didelegasikan.
- Anda harus memiliki izin AWS Identity and Access Management (IAM) untuk mengakses Trusted Advisor Prioritas. Untuk informasi tentang cara mengontrol akses ke Trusted Advisor Prioritas, lihat Kelola akses ke AWS Trusted Advisor danAWS kebijakan terkelola untuk AWS Trusted Advisor.

Aktifkan Trusted Advisor Prioritas

Mintalah tim akun Anda untuk mengaktifkan fitur ini untuk Anda. Anda harus memiliki paket Enterprise Support dan menjadi pemilik akun manajemen untuk organisasi Anda. Jika halaman Trusted Advisor Prioritas di konsol mengatakan bahwa Anda memerlukan akses tepercayaAWS Organizations, lalu pilih Aktifkan akses tepercaya dengan AWS Organizations. Untuk informasi selengkapnya, lihat bagian Prasyarat.

Lihat rekomendasi yang diprioritaskan

Setelah tim akun Anda mengaktifkan Trusted Advisor Prioritas untuk Anda, Anda dapat melihat rekomendasi terbaru untuk AWS akun Anda.

Untuk melihat rekomendasi yang diprioritaskan

1. Masuk ke konsol Trusted Advisor di https://console.aws.amazon.com/trustedadvisor/home.
2. Pada halaman Trusted AdvisorPrioritas, Anda dapat melihat item berikut:

   Jika Anda menggunakan akun Administrator AWS Organizations Manajemen atau Delegasi, alihkan ke tab Akun Saya.

- Tindakan yang diperlukan — Jumlah rekomendasi yang menunggu tanggapan atau sedang berlangsung.
- Ikhtisar — Informasi berikut:
  - Rekomendasi yang diberhentikan dalam 90 hari terakhir
  - Rekomendasi yang diselesaikan dalam 90 hari terakhir
  - Rekomendasi tanpa pembaruan dalam lebih dari 30 hari
  - Rata-rata waktu untuk menyelesaikan rekomendasi

3. Pada tab Aktif, rekomendasi yang diprioritaskan Aktif menunjukkan rekomendasi yang diprioritaskan oleh tim akun untuk Anda. Tab Tertutup menunjukkan rekomendasi yang diselesaikan atau diberhentikan.

   - Untuk memfilter hasil Anda, gunakan opsi berikut:
     - Rekomendasi — Masukkan kata kunci untuk mencari berdasarkan nama. Ini bisa berupa nama cek, atau nama khusus yang dibuat oleh tim akun Anda.
     - Status — Apakah rekomendasi sedang menunggu tanggapan, sedang berlangsung, diberhentikan, atau diselesaikan.
     - Sumber — Asal usul rekomendasi yang diprioritaskan. Rekomendasi dapat berasal dariLayanan AWS, Akun AWS tim Anda, atau acara layanan yang direncanakan.
     - Kategori — Kategori rekomendasi, seperti keamanan atau pengoptimalan biaya.
     - Usia — Saat tim akun Anda membagikan rekomendasi dengan Anda.

4. Pilih rekomendasi untuk mempelajari lebih lanjut tentang detailnya, sumber daya yang terpengaruh, dan tindakan yang disarankan. Anda kemudian dapat mengakui atau mengabaikan rekomendasi tersebut.

Untuk melihat rekomendasi yang diprioritaskan di semua akun di organisasi Anda AWS

Akun manajemen dan administrator yang didelegasikan Trusted Advisor Prioritas dapat melihat rekomendasi yang dikumpulkan di seluruh organisasi Anda.

> **Note**
>
> Akun anggota tidak memiliki akses ke rekomendasi gabungan.

1. Masuk ke konsol Trusted Advisor di https://console.aws.amazon.com/trustedadvisor/home.
2. Pada halaman Trusted AdvisorPrioritas, pastikan Anda berada di tab Organisasi Saya.
3. Untuk melihat rekomendasi untuk satu akun, pilih akun dari daftar tarik-turun Pilih akun dari organisasi Anda. Atau, Anda dapat melihat rekomendasi di semua akun Anda.

   Pada tab Organisasi Saya, Anda dapat melihat item berikut:

   - Tindakan yang diperlukan: Jumlah rekomendasi di seluruh organisasi Anda yang sedang menunggu respons atau sedang berlangsung.
   - Ikhtisar: Menampilkan item berikut:

     - Rekomendasi yang diberhentikan dalam 90 hari terakhir.

     - Rekomendasi yang diselesaikan dalam 90 hari terakhir.

     - Rekomendasi tanpa pembaruan di lebih dari 30 hari.

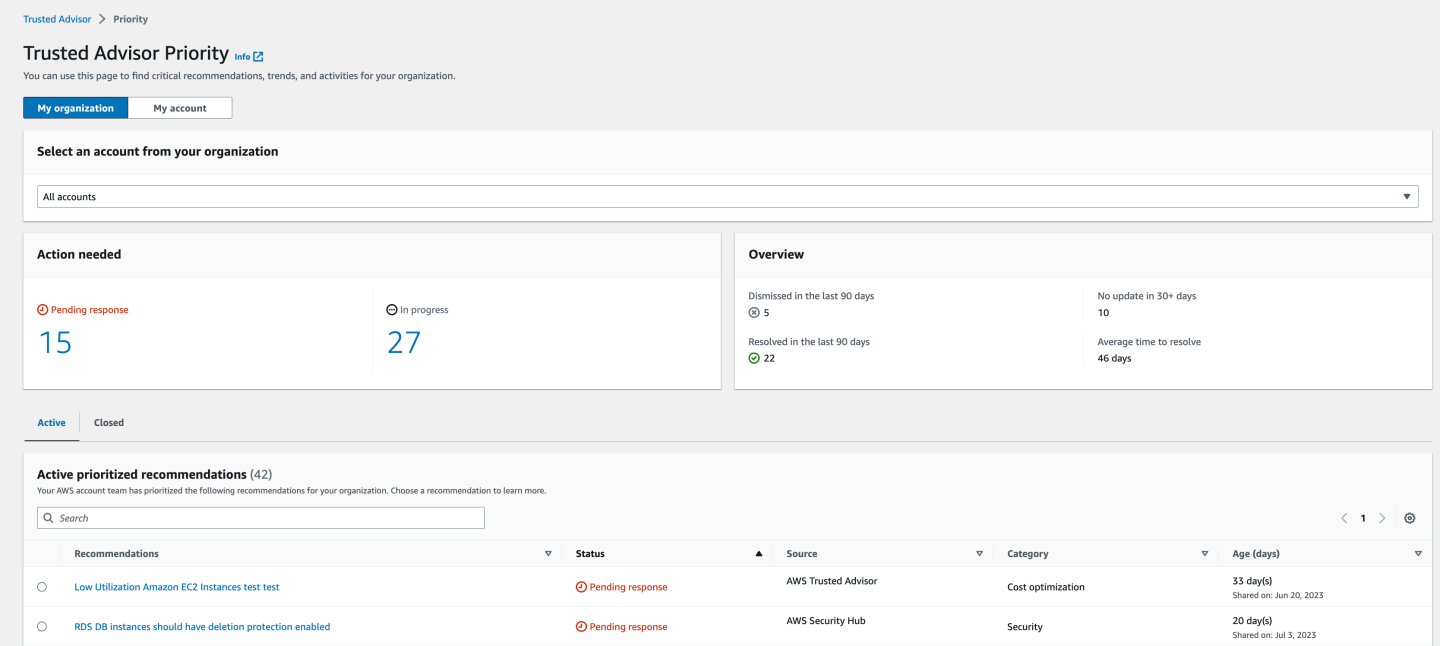
     - Rata-rata waktu yang dibutuhkan untuk menyelesaikan rekomendasi.
4. Di bawah tab Aktif, bagian Rekomendasi prioritas Aktif menunjukkan rekomendasi yang diprioritaskan oleh tim akun untuk Anda. Tab Tertutup menunjukkan rekomendasi yang diselesaikan atau diberhentikan.

   Untuk memfilter hasil Anda, gunakan opsi berikut:

   - Rekomendasi — Masukkan kata kunci untuk mencari berdasarkan nama. Ini bisa berupa nama cek, atau nama khusus yang dibuat oleh tim akun Anda.
   - Status — Apakah rekomendasi sedang menunggu tanggapan, sedang berlangsung, diberhentikan, atau diselesaikan.
   - Sumber — Asal usul rekomendasi yang diprioritaskan. Rekomendasi dapat berasal dariLayanan AWS, Akun AWS tim Anda, atau acara layanan yang direncanakan.
   - Kategori — Kategori rekomendasi, seperti keamanan atau pengoptimalan biaya.
   - Usia — Saat tim akun Anda membagikan rekomendasi dengan Anda.
5. Pilih rekomendasi untuk melihat detail tambahan, akun dan sumber daya yang terpengaruh, dan tindakan yang disarankan. Anda kemudian dapat mengakui atau mengabaikan rekomendasi tersebut.

Example : Rekomendasi Trusted Advisor prioritas

Contoh berikut menunjukkan 15 rekomendasi yang sedang menunggu tanggapan dan 27 rekomendasi yang sedang berlangsung di bawah bagian Tindakan yang diperlukan. Gambar berikut menunjukkan dua rekomendasi yang menunggu respons di tab Rekomendasi prioritas aktif.



Akui rekomendasi

Di bawah tab Aktif, Anda dapat mempelajari lebih lanjut tentang rekomendasi dan kemudian memutuskan apakah Anda ingin mengakuinya.

Untuk mengakui rekomendasi

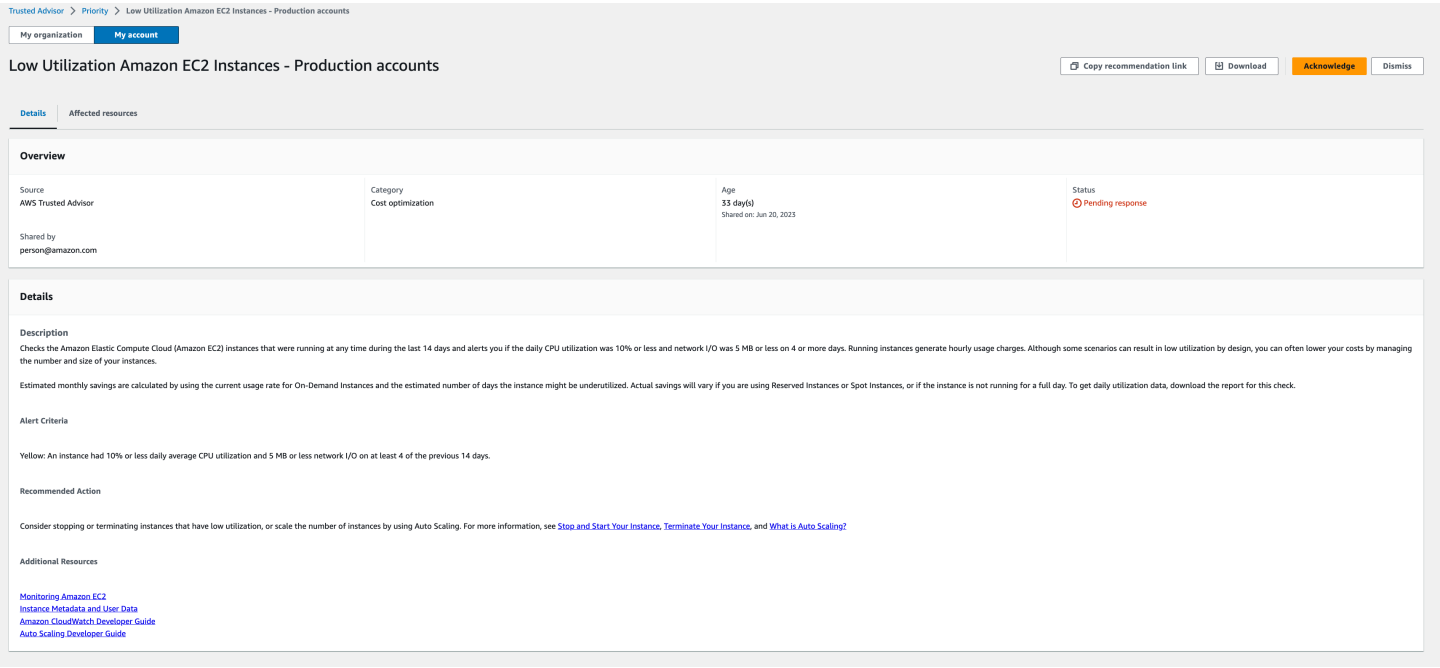
1. Masuk ke konsol Trusted Advisor di https://console.aws.amazon.com/trustedadvisor/home.
2. Jika Anda menggunakan akun Administrator AWS Organizations Manajemen atau Delegasi, alihkan ke tab Akun Saya.
3. Pada halaman Trusted AdvisorPrioritas, di bawah tab Aktif, pilih nama rekomendasi.
4. Di bagian Detail, Anda dapat meninjau tindakan yang disarankan untuk menyelesaikan rekomendasi.
5. Di bagian Sumber daya yang terpengaruh, Anda dapat meninjau sumber daya yang terpengaruh dan memfilter berdasarkan Status.
6. Pilih Akui.
7. Di kotak dialog Akui rekomendasi, pilih Akui.

Status rekomendasi berubah menjadi Sedang berlangsung. Rekomendasi yang sedang berlangsung atau menunggu respons muncul di tab Aktif di halaman Trusted Advisor Prioritas.

8. Ikuti tindakan yang disarankan untuk menyelesaikan rekomendasi. Untuk informasi selengkapnya, lihat Selesaikan rekomendasi.

Example : Rekomendasi manual dari Trusted Advisor Prioritas

Gambar berikut menunjukkan rekomendasi Instans EC2 Pemanfaatan Rendah yang menunggu respons.



Untuk mengakui rekomendasi untuk semua akun di organisasi Anda AWS

Akun manajemen atau administrator yang didelegasikan Trusted Advisor dapat menerima rekomendasi untuk semua akun yang terpengaruh.

> **Note**
>
> Akun anggota tidak memiliki akses ke rekomendasi gabungan.

1. Masuk ke konsol Trusted Advisor di https://console.aws.amazon.com/trustedadvisor/home.
2. Pada halaman Trusted AdvisorPrioritas, pastikan Anda berada di tab Organisasi saya.

3. Di tab Aktif, pilih nama rekomendasi.
4. Pilih Akui.
5. Di kotak dialog Akui rekomendasi, pilih Akui.

   Status rekomendasi berubah menjadi Sedang berlangsung.
6. Ikuti tindakan yang disarankan untuk menyelesaikan rekomendasi. Untuk informasi selengkapnya, lihat Selesaikan rekomendasi.
7. Untuk melihat detail rekomendasi, pilih nama rekomendasi.

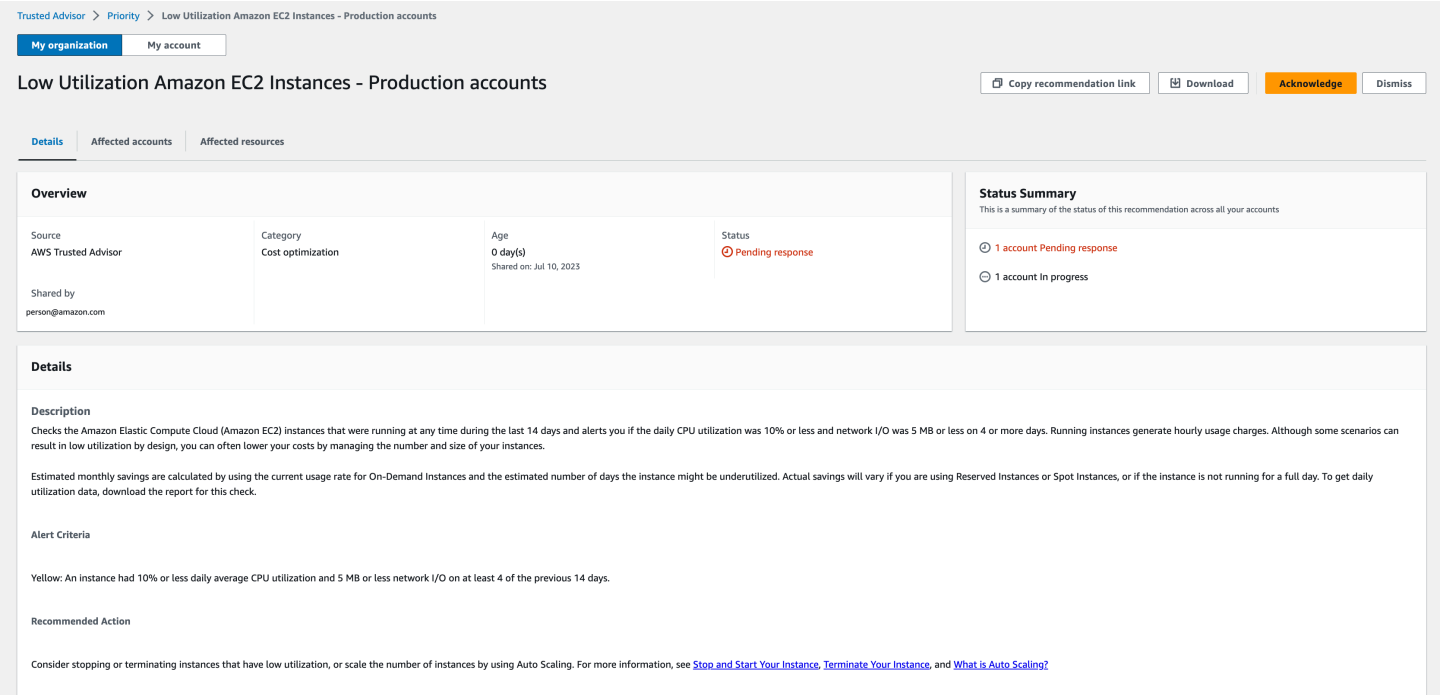
   Di bagian Detail, Anda dapat meninjau informasi berikut tentang rekomendasi:

   - Ikhtisar rekomendasi dan bagian Detail yang mencakup tindakan rekomendasi yang harus diselesaikan.

     Ringkasan Status yang menampilkan rekomendasi di semua akun yang terpengaruh.
   - Di bagian Akun yang terpengaruh, Anda dapat meninjau sumber daya yang terpengaruh di semua akun Anda. Anda dapat memfilter berdasarkan nomor Akun dan Status.
   - Di bagian Sumber daya yang terpengaruh, Anda dapat meninjau sumber daya yang terpengaruh di semua akun Anda. Anda dapat memfilter berdasarkan nomor Akun dan Status.

Example : Rekomendasi manual dari Trusted Advisor Prioritas

Gambar berikut menunjukkan rekomendasi Instans Amazon EC2 Pemanfaatan Rendah yang menunggu respons. Satu akun yang terpengaruh telah mengakui rekomendasi tersebut. Akun lain sedang menunggu respons, membuat status rekomendasi Respons tertunda.



Memberhentikan rekomendasi

Anda juga dapat mengabaikan rekomendasi. Ini berarti Anda mengakui rekomendasi tersebut, tetapi Anda tidak akan mengatasinya. Anda dapat mengabaikan rekomendasi jika tidak relevan dengan akun Anda. Misalnya, jika Anda memiliki tes Akun AWS yang ingin dihapus, Anda tidak perlu mengikuti tindakan yang disarankan.

Untuk menolak rekomendasi

1. Masuk ke konsol Trusted Advisor di https://console.aws.amazon.com/trustedadvisor/home.
2. Jika Anda menggunakan akun Administrator AWS Organizations Manajemen atau Delegasi, alihkan ke tab Akun Saya.
3. Pada halaman Trusted AdvisorPrioritas, di bawah tab Aktif, pilih nama rekomendasi.
4. Pada halaman detail rekomendasi, tinjau informasi tentang sumber daya yang terpengaruh.
5. Jika rekomendasi ini tidak berlaku untuk akun Anda, pilih Singkirkan.
6. Dalam kotak dialog Singkirkan rekomendasi, pilih alasan mengapa Anda tidak akan membahas rekomendasi tersebut.
7. (Opsional) Masukkan catatan yang merinci mengapa Anda menolak rekomendasi. Jika Anda memilih Lainnya, Anda harus memasukkan deskripsi di bagian Catatan.

8. Pilih Singkirkan. Status rekomendasi berubah menjadi Dihentikan dan muncul di tab Ditutup pada halaman Trusted Advisor Prioritas.

Untuk mengabaikan rekomendasi untuk semua akun di organisasi Anda AWS

Akun manajemen atau administrator Trusted Advisor Prioritas yang terdelgasi dapat mengabaikan rekomendasi untuk semua akun mereka.

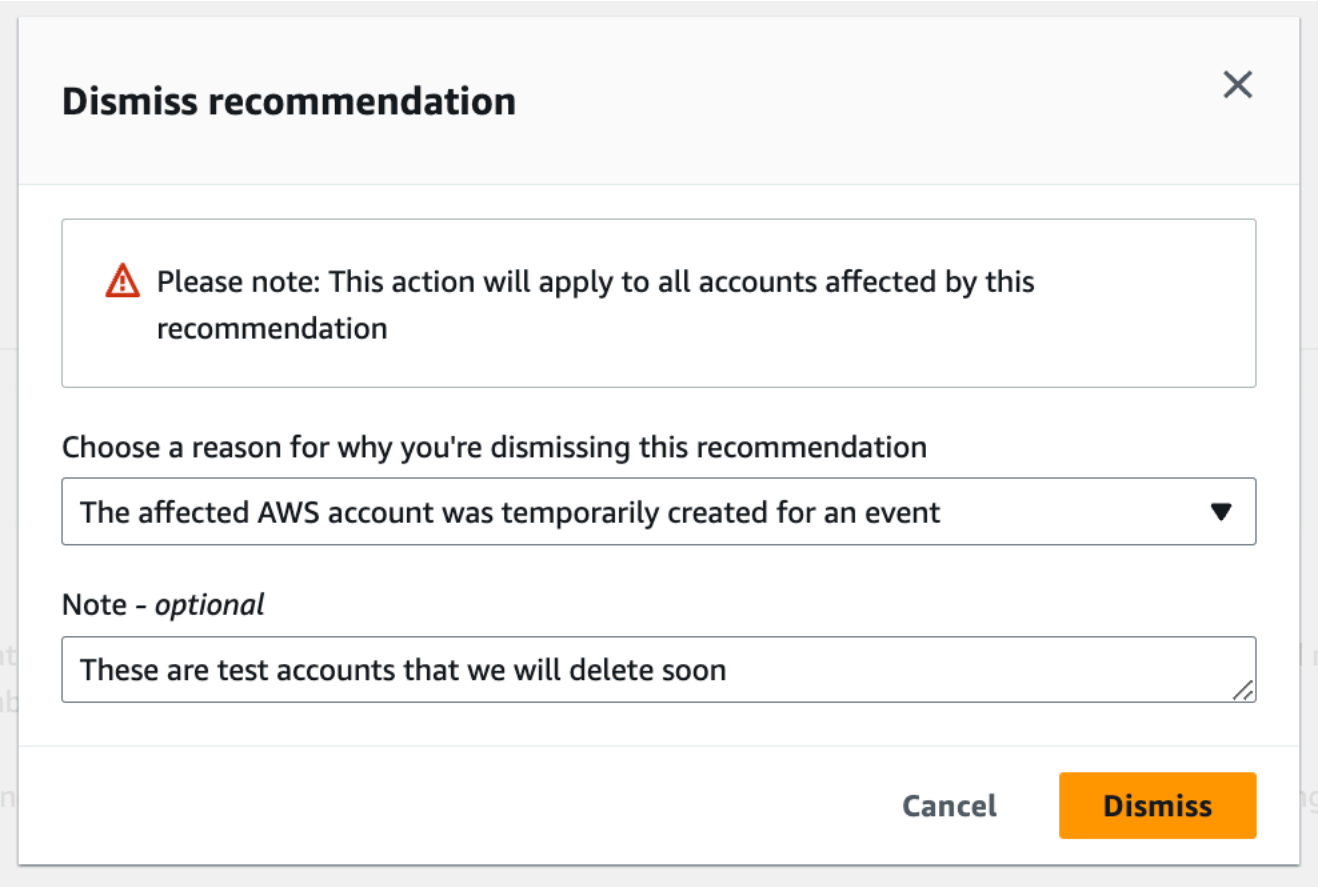
1. Masuk ke konsol Trusted Advisor di https://console.aws.amazon.com/trustedadvisor/home.
2. Pada halaman Trusted Advisor Prioritas, pastikan Anda berada di tab Organisasi Saya.
3. Di tab Aktif, pilih nama rekomendasi.
4. Jika rekomendasi ini tidak berlaku untuk akun Anda, pilih Singkirkan.
5. Dalam kotak dialog Singkirkan rekomendasi, pilih alasan mengapa Anda tidak akan membahas rekomendasi tersebut.
6. (Opsional) Masukkan catatan yang merinci mengapa Anda menolak rekomendasi. Jika Anda memilih Lainnya, maka Anda harus memasukkan deskripsi di bagian Catatan.
7. Pilih Singkirkan. Status rekomendasi berubah menjadi Diberhentikan. Rekomendasi muncul di tab Tertutup pada halaman Trusted Advisor Prioritas.

> **Note**
>
> Anda dapat memilih nama rekomendasi dan memilih Lihat catatan untuk menemukan alasan pemecatan. Jika tim akun Anda menolak rekomendasi untuk Anda, alamat email mereka akan muncul di sebelah catatan.

Trusted AdvisorPrioritas juga memberi tahu tim akun Anda bahwa Anda menolak rekomendasi tersebut.

Example : Memberhentikan rekomendasi dari Prioritas Trusted Advisor

Contoh berikut menunjukkan bagaimana Anda dapat mengabaikan rekomendasi.



Selesaikan rekomendasi

Setelah Anda mengakui rekomendasi dan menyelesaikan tindakan yang disarankan, Anda dapat menyelesaikan rekomendasi.

> **Tip**
>
> Setelah Anda menyelesaikan rekomendasi, Anda tidak dapat membukanya kembali. Jika Anda ingin meninjau kembali rekomendasi nanti, lihatMemberhentikan rekomendasi.

Untuk menyelesaikan rekomendasi

1. Masuk ke konsol Trusted Advisor di https://console.aws.amazon.com/trustedadvisor/home.
2. Pada halaman Trusted Advisor Prioritas, pastikan Anda berada di tab Organisasi Saya.
3. Pada halaman Trusted AdvisorPrioritas, pilih rekomendasi, lalu pilih Selesaikan.

4. Di kotak dialog Selesaikan rekomendasi, pilih Selesaikan. Rekomendasi yang diselesaikan muncul di bawah tab Tertutup pada halaman Trusted Advisor Prioritas. Trusted Advisor Prioritas memberi tahu tim akun Anda bahwa Anda telah menyelesaikan rekomendasi.

Untuk menyelesaikan rekomendasi untuk semua akun di AWS organisasi Anda

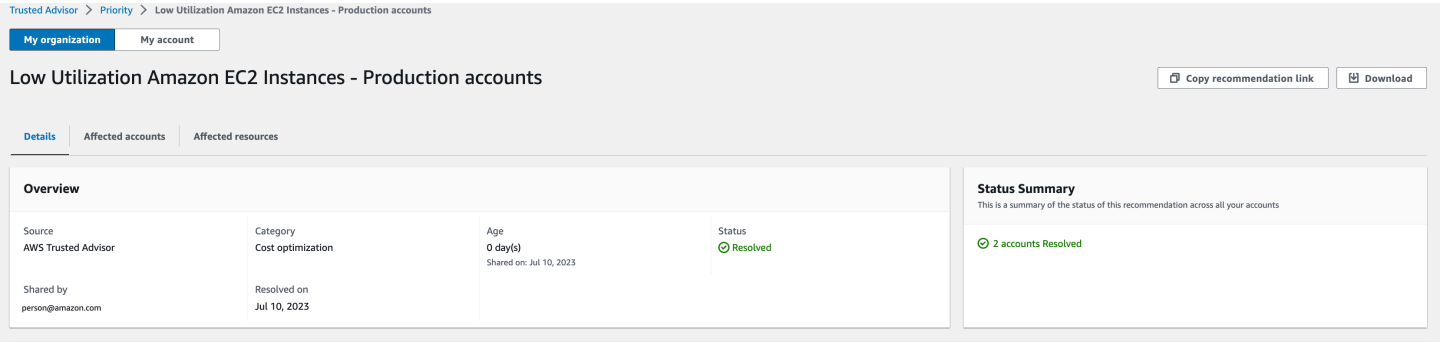
Akun manajemen atau administrator yang didelegasikan Trusted Advisor Prioritas dapat menyelesaikan rekomendasi untuk semua akun mereka.

> **Note**
>
> Akun anggota tidak memiliki akses ke rekomendasi gabungan.

1. Masuk ke konsol Trusted Advisor di https://console.aws.amazon.com/trustedadvisor/home.
2. Jika Anda menggunakan akun Administrator AWS Organizations Manajemen atau Delegasi, alihkan ke tab Akun Saya.
3. Di tab Aktif, pilih nama rekomendasi.
4. Jika rekomendasi tidak berlaku untuk akun Anda, pilih Selesaikan.
5. Di kotak dialog Selesaikan rekomendasi, pilih Selesaikan. Rekomendasi yang diselesaikan muncul di bawah tab Tertutup pada halaman Trusted Advisor Prioritas. Trusted Advisor Prioritas memberi tahu tim akun Anda bahwa Anda telah menyelesaikan rekomendasi.

Example : Rekomendasi manual dari Trusted Advisor Prioritas

Contoh berikut menunjukkan rekomendasi Instans Amazon EC2 Pemanfaatan Rendah yang diselesaikan.



Buka kembali rekomendasi

Setelah Anda mengabaikan rekomendasi, Anda atau tim akun Anda dapat membuka kembali rekomendasi tersebut.

Untuk membuka kembali rekomendasi

1. Masuk ke konsol Trusted Advisor di https://console.aws.amazon.com/trustedadvisor/home.
2. Jika Anda menggunakan akun Administrator AWS Organizations Manajemen atau Delegasi, alihkan ke tab Akun Saya.
3. Pada halaman Trusted AdvisorPrioritas, pilih tab Tertutup.
4. Di bawah Rekomendasi tertutup, pilih rekomendasi yang diberhentikan, lalu pilih Buka kembali.
5. Di kotak dialog Reopen rekomendasi, jelaskan mengapa Anda membuka kembali rekomendasi.
6. Pilih Buka Kembali. Status rekomendasi berubah menjadi Sedang berlangsung dan muncul di bawah tab Aktif.

   > **Tip**
   >
   > Anda dapat memilih nama rekomendasi dan kemudian memilih Lihat catatan untuk menemukan alasan pembukaan kembali. Jika tim akun Anda membuka kembali rekomendasi untuk Anda, nama mereka akan muncul di sebelah catatan.

7. Ikuti langkah-langkah dalam detail rekomendasi.

Untuk membuka kembali rekomendasi untuk semua akun di organisasi Anda AWS

Akun manajemen atau administrator yang didelegasikan Trusted Advisor Prioritas dapat membuka kembali rekomendasi untuk semua akun mereka.

> **Note**
>
> Akun anggota tidak memiliki akses ke rekomendasi gabungan.

1. Masuk ke konsol Trusted Advisor di https://console.aws.amazon.com/trustedadvisor/home.
2. Pada halaman Trusted Advisor Prioritas, pastikan Anda berada di tab Organisasi Saya.
3. Di bawah Rekomendasi tertutup, pilih rekomendasi yang diberhentikan, lalu pilih Buka kembali.

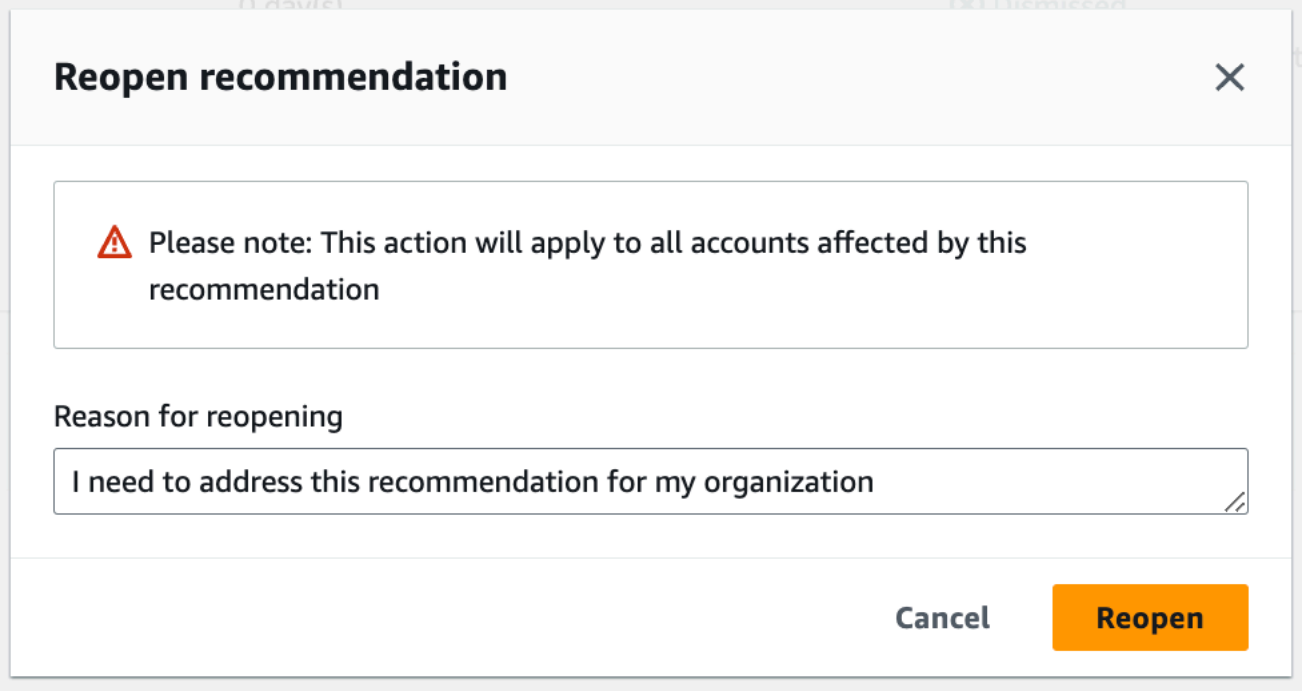
4. Di kotak dialog Reopen rekomendasi, jelaskan mengapa Anda membuka kembali rekomendasi.
5. Pilih Buka Kembali. Status rekomendasi berubah menjadi Sedang berlangsung dan muncul di bawah tab Aktif.

> **Tip**
>
> Anda dapat memilih nama rekomendasi dan memilih Lihat catatan untuk menemukan alasan pembukaan kembali. Jika tim akun Anda membuka kembali rekomendasi untuk Anda, nama mereka akan muncul di sebelah catatan.

6. Ikuti langkah-langkah dalam detail rekomendasi.

Example : Buka kembali rekomendasi dari Prioritas Trusted Advisor

Contoh berikut menunjukkan rekomendasi yang ingin Anda buka kembali.



Unduh detail rekomendasi

Anda juga dapat mengunduh hasil rekomendasi yang diprioritaskan dari Trusted Advisor Priority.

> **Note**
>
> Saat ini, Anda hanya dapat mengunduh satu rekomendasi sekaligus.

Untuk mengunduh rekomendasi

1. Masuk ke konsol Trusted Advisor di https://console.aws.amazon.com/trustedadvisor/home.
2. Pada halaman Trusted AdvisorPrioritas, pilih rekomendasi, lalu pilih Unduh.
3. Buka file untuk melihat detail rekomendasi.

Daftarkan administrator yang didelegasikan

Anda dapat menambahkan akun anggota yang merupakan bagian dari organisasi Anda sebagai administrator yang didelegasikan. Akun administrator yang didelegasikan dapat meninjau, mengakui, menyelesaikan, mengabaikan, dan membuka kembali rekomendasi di Prioritas. Trusted Advisor

Setelah Anda mendaftarkan akun, Anda harus memberikan administrator yang didelegasikan AWS Identity and Access Management izin yang diperlukan untuk mengakses Trusted Advisor Prioritas. Untuk informasi selengkapnya, silakan lihat Kelola akses ke AWS Trusted Advisor dan AWS kebijakan terkelola untuk AWS Trusted Advisor.

Anda dapat mendaftarkan hingga lima akun anggota. Hanya akun manajemen yang dapat menambahkan administrator yang didelegasikan untuk organisasi. Anda harus masuk ke akun manajemen organisasi untuk mendaftar atau membatalkan pendaftaran administrator yang didelegasikan.

Untuk mendaftarkan administrator yang didelegasikan

1. Masuk ke Trusted Advisor konsol di https://console.aws.amazon.com/trustedadvisor/home sebagai akun manajemen.
2. Di panel navigasi, di bawah Preferensi, pilih Organisasi Anda.
3. Di bawah Administrator yang didelegasikan, pilih Daftarkan akun baru.
4. Di kotak dialog, masukkan ID akun anggota, lalu pilih Daftar.
5. (Opsional) Untuk membatalkan pendaftaran akun, pilih akun dan pilih Deregister. Di kotak dialog, pilih Deregister lagi.

Administrator yang didelegasikan deregister

Ketika Anda membatalkan pendaftaran akun anggota, akun tersebut tidak lagi memiliki akses yang sama ke Trusted Advisor Prioritas sebagai akun manajemen. Akun yang tidak lagi menjadi administrator yang didelegasikan tidak akan menerima pemberitahuan email dari Trusted Advisor Prioritas.

Untuk membatalkan pendaftaran administrator yang didelegasikan

1. Masuk ke Trusted Advisor konsol di https://console.aws.amazon.com/trustedadvisor/home sebagai akun manajemen.
2. Di panel navigasi, di bawah Preferensi, pilih Organisasi Anda.
3. Di bawah Administrator yang didelegasikan, pilih akun lalu pilih Deregister.
4. Di kotak dialog, pilih Deregister.

Kelola pemberitahuan Trusted Advisor Prioritas

Trusted AdvisorPrioritas memberikan pemberitahuan melalui email. Pemberitahuan email ini mencakup ringkasan rekomendasi yang diprioritaskan oleh tim akun Anda untuk Anda. Anda dapat menentukan frekuensi yang Anda terima pembaruan dari Trusted Advisor Prioritas.

Jika Anda mendaftarkan akun anggota sebagai administrator yang didelegasikan, mereka juga dapat mengatur akun mereka untuk menerima pemberitahuan email Trusted Advisor Prioritas.

Trusted AdvisorPemberitahuan email prioritas tidak menyertakan hasil pemeriksaan untuk akun individual dan terpisah dari pemberitahuan mingguan untuk Trusted Advisor Rekomendasi. Untuk informasi selengkapnya, lihat Menyiapkan preferensi pemberitahuan.

> **Note**
>
> Hanya akun manajemen atau administrator yang didelegasikan yang dapat mengatur pemberitahuan email Trusted Advisor Prioritas.

Untuk mengelola notifikasi Trusted Advisor Prioritas

1. Masuk ke Trusted Advisor konsol di https://console.aws.amazon.com/trustedadvisor/home sebagai akun administrator manajemen atau delegasi.

2. Di panel navigasi, di bawah Preferensi, pilih Pemberitahuan.
3. Di bawah Prioritas, Anda dapat memilih opsi berikut.
    a. Harian — Terima pemberitahuan email setiap hari.
    b. Mingguan — Terima pemberitahuan email seminggu sekali.
    c. Pilih notifikasi yang akan diterima:
        - Ringkasan rekomendasi yang diprioritaskan
        - Tanggal resolusi
4. Untuk Penerima, pilih kontak lain yang ingin Anda terima notifikasi email. Anda dapat menambahkan dan menghapus kontak dari halaman Pengaturan Akun di konsol AWS Billing and Cost Management.
5. Untuk Bahasa, pilih bahasa untuk notifikasi email.
6. Pilih Simpan preferensi Anda.

> **Note**
>
> Trusted AdvisorPrioritas mengirimkan pemberitahuan email dari noreply@notifications.trustedadvisor.us-west-2.amazonaws.com alamat. Anda mungkin perlu memverifikasi bahwa klien email Anda tidak mengidentifikasi email ini sebagai spam.

Nonaktifkan Trusted Advisor Prioritas

Hubungi tim akun Anda dan minta mereka menonaktifkan fitur ini untuk Anda. Setelah fitur ini dinonaktifkan, rekomendasi yang diprioritaskan tidak lagi muncul di konsol AndaTrusted Advisor.

Jika Anda menonaktifkan Trusted Advisor Prioritas dan kemudian mengaktifkannya lagi nanti, Anda masih dapat melihat rekomendasi yang dikirim tim akun Anda sebelum Anda menonaktifkan Trusted Advisor Prioritas.

Memulai dengan AWS Trusted Advisor Engage (Pratinjau)

> **Note**
>
> AWS Trusted AdvisorEngage dalam rilis pratinjau dan dapat berubah sewaktu-waktu. Anda dapat melihat persyaratan layanan pratinjau di sini https://aws.amazon.com/service-terms/.

Anda dapat menggunakan AWS Trusted Advisor Engage untuk mendapatkan hasil maksimal dari AWS Support Rencana Anda dengan memudahkan Anda melihat, meminta, dan melacak semua keterlibatan proaktif Anda, dan berkomunikasi dengan Akun AWS tim Anda tentang keterlibatan yang sedang berlangsung.

Misalnya, Anda dapat meminta “Tinjauan Bisnis Manajemen” ke Akun AWS tim Anda dengan masuk ke halaman Engage di dalam AWS Trusted Advisor konsol. Kemudian, seorang AWS ahli akan ditugaskan untuk permintaan Anda, dan menindaklanjuti seluruh keterlibatan.

Topik

Prasyarat

Anda harus mengambil tindakan yang diperlukan untuk memenuhi persyaratan berikut untuk menggunakan Trusted Advisor Engage:

- Anda harus memiliki paket Enterprise On-Ramp Support.

- Akun Anda harus menjadi bagian dari organisasi yang telah mengaktifkan semua fitur diAWS Organizations. Untuk informasi selengkapnya, lihat Mengaktifkan semua fitur di organisasi Anda dalam Panduan Pengguna AWS Organizations.
- Organisasi Anda harus mengaktifkan akses tepercaya keTrusted Advisor. Anda dapat mengaktifkan akses tepercaya dengan masuk sebagai akun manajemen dan membuka halaman Organisasi Anda di Trusted Advisor konsol.
- Anda harus memiliki izin AWS Identity and Access Management (IAM) untuk mengakses Trusted Advisor Engage. Untuk informasi tentang cara mengontrol akses ke Trusted Advisor Engage, lihatKelola akses ke AWS Trusted Advisor.

> **Note**
>
> Akun apa pun dalam AWS Organisasi dapat membuat permintaan keterlibatan. Jika akun pemilik Keterlibatan pindah ke AWS Organisasi lain, Keterlibatan hanya akan dapat diakses oleh akun tersebut. Untuk membatasi kontrol, lihatContoh Kebijakan Kontrol Layanan untuk AWS Trusted Advisor.

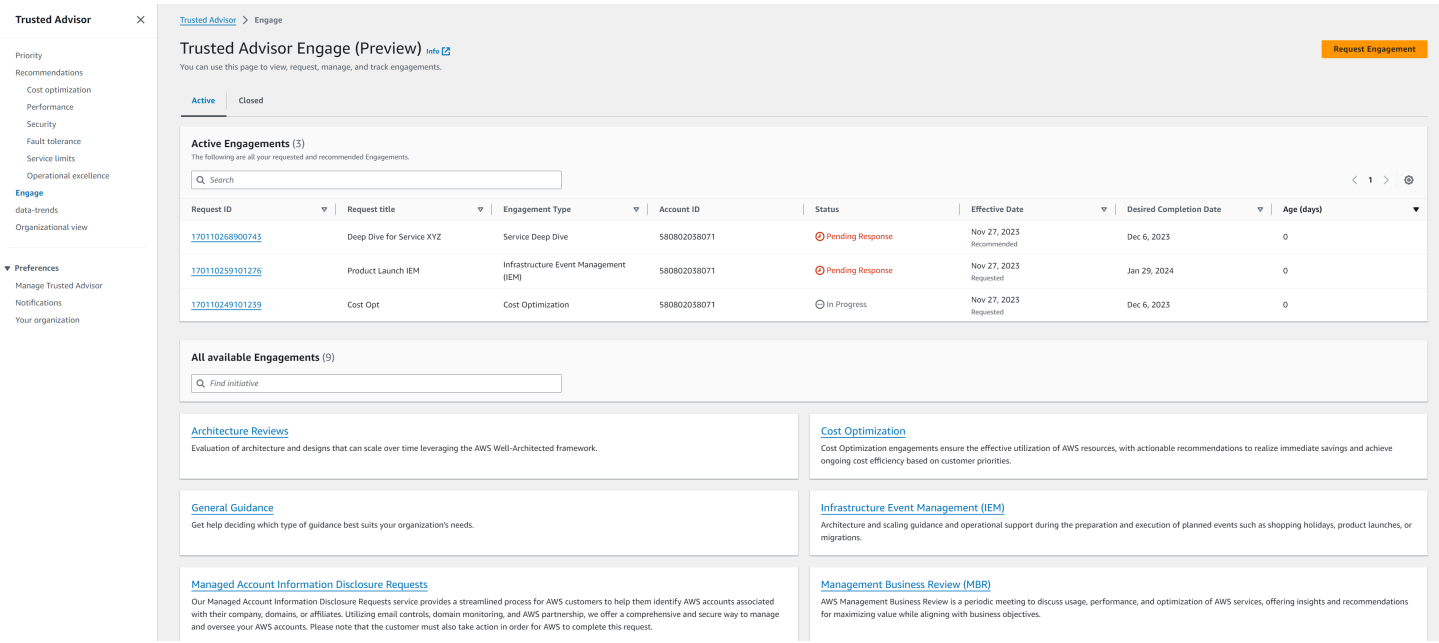
Lihat Dasbor Keterlibatan

Setelah memperoleh hak akses, Anda dapat mengakses halaman Trusted Advisor Engage di dalam Trusted Advisor konsol untuk melihat dasbor tempat Anda dapat mengelola keterlibatan dengan tim AndaAkun AWS.

Untuk mengelola Keterlibatan Anda:

1. Masuk ke Trusted Advisor konsol di https://console.aws.amazon.com/trustedadvisor/home.
2. Pada halaman Trusted AdvisorEngage, Anda dapat melihat:
   - Tombol Permintaan Keterlibatan
   - Tabel Keterlibatan Aktif
   - Tabel Keterlibatan Tertutup
   - Semua Katalog Keterlibatan yang Tersedia

Example : Dasbor Keterlibatan



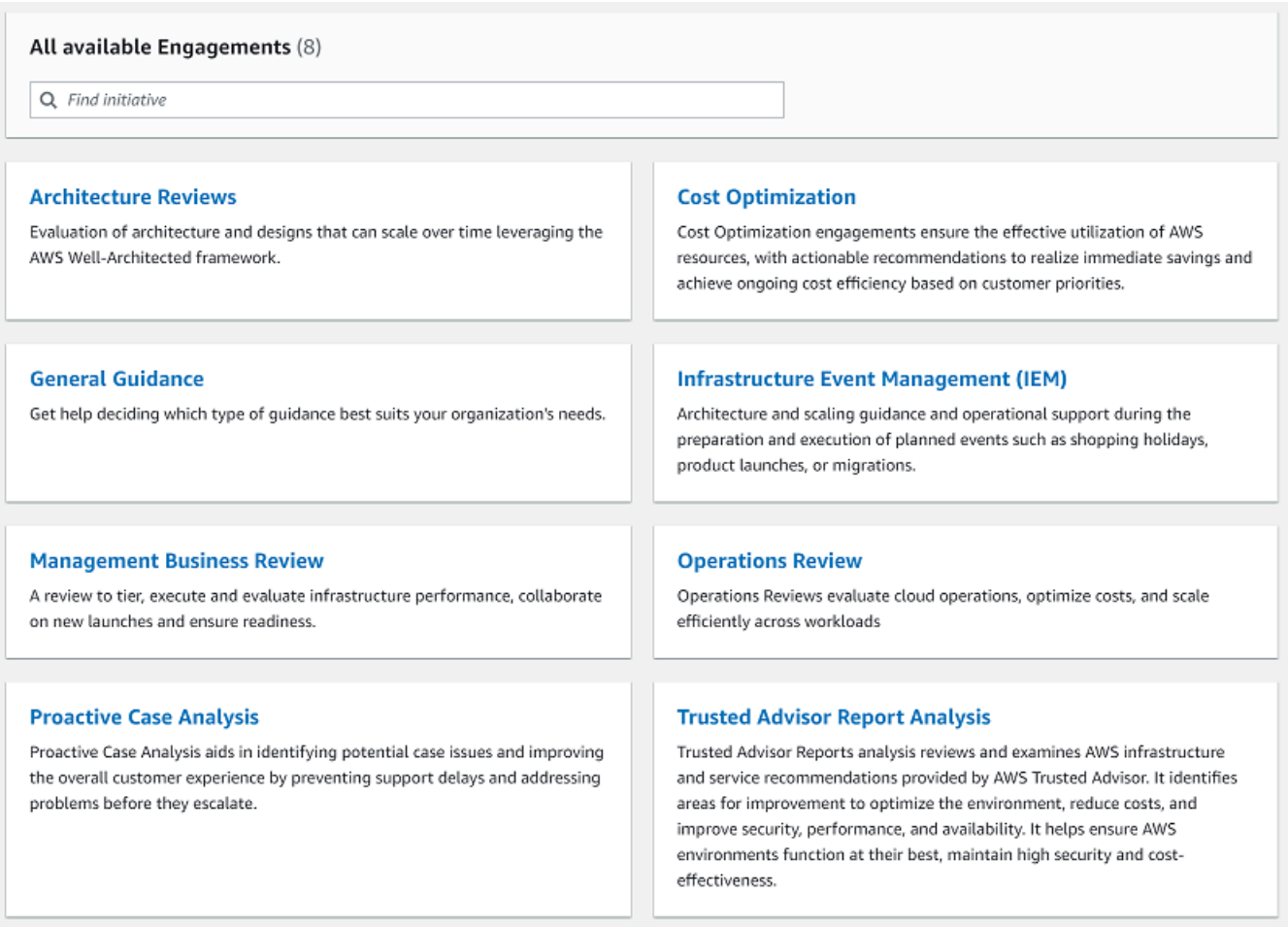
Lihat Katalog Jenis Keterlibatan

Anda dapat melihat katalog jenis keterlibatan untuk menemukan jenis keterlibatan terbaru yang dapat Anda minta ke tim AndaAkun AWS.

Untuk melihat katalog jenis keterlibatan:

1. Masuk ke Trusted Advisor konsol di https://console.aws.amazon.com/trustedadvisor/home.
2. Di halaman Trusted AdvisorEngage, Anda dapat menemukan katalog jenis Keterlibatan.

Example : Katalog Jenis Keterlibatan



Minta Keterlibatan

Anda dapat meminta keterlibatan ke Akun AWS tim Anda sesuai dengan jenis keterlibatan yang disertakan dalam AWS Support Plan Anda.

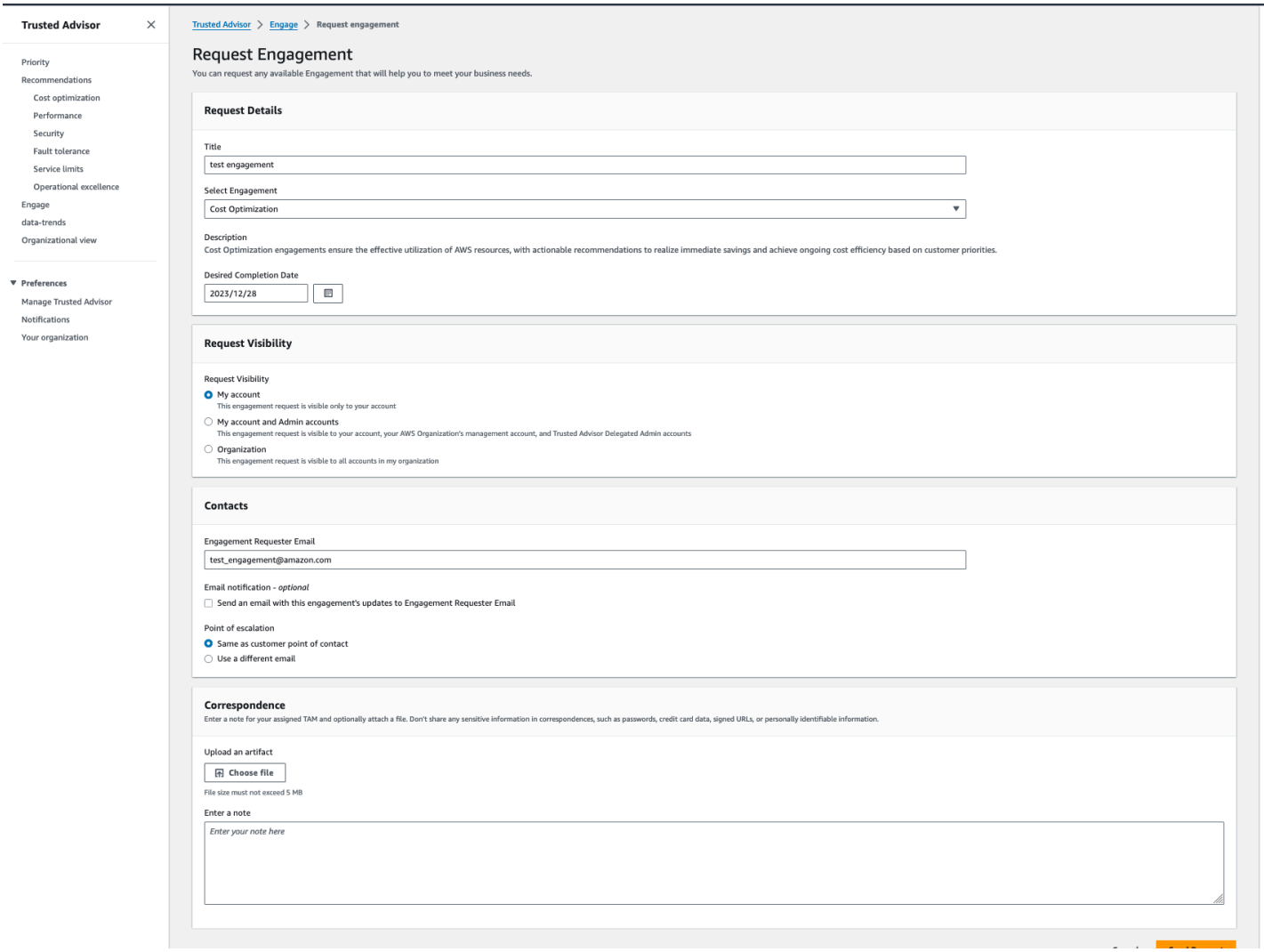
Untuk meminta Keterlibatan:

1. Masuk ke Trusted Advisor konsol di https://console.aws.amazon.com/trustedadvisor/home.
2. Pada halaman Trusted AdvisorEngage, pilih Minta Keterlibatan.
3. Isi:
   - Judul
   - Pilih Keterlibatan: jenis Keterlibatan yang ingin Anda minta.

- Tanggal Penyelesaian yang Diinginkan: tanggal penyelesaian yang diinginkan dari Keterlibatan. Setiap Jenis Keterlibatan memiliki lead time yang berbeda yang dihitung dalam tanggal penyelesaian minimum yang diinginkan.
- Minta Visibilitas:
  - Akun saya: permintaan keterlibatan ini hanya dapat dilihat oleh akun Anda.
  - Akun saya dan akun Admin: permintaan keterlibatan ini dapat dilihat oleh akun Anda, dan akun Manajemen dan semua akun Admin Delegasi AWS Organisasi Anda.
  - Organisasi: Permintaan keterlibatan ini dapat dilihat oleh semua akun di AWS Organisasi Anda.
- Email Pemohon Keterlibatan: alamat email yang AWS akan digunakan sebagai titik kontak utama untuk Keterlibatan ini.
- Pengaturan notifikasi email: pilih apakah Email Pemohon Keterlibatan akan menerima pemberitahuan email tentang keterlibatan.
- Titik eskalasi: alamat email yang AWS akan digunakan saat eskalasi diperlukan untuk Keterlibatan ini.
- Korespondensi: catatan dan lampiran file opsional bagi Anda untuk memberikan rincian mengenai Keterlibatan ini.

4. Pilih Kirim Permintaan.

Example : Permintaan Keterlibatan



Mengedit Keterlibatan

Anda dapat mengedit detail pada permintaan keterlibatan Anda.

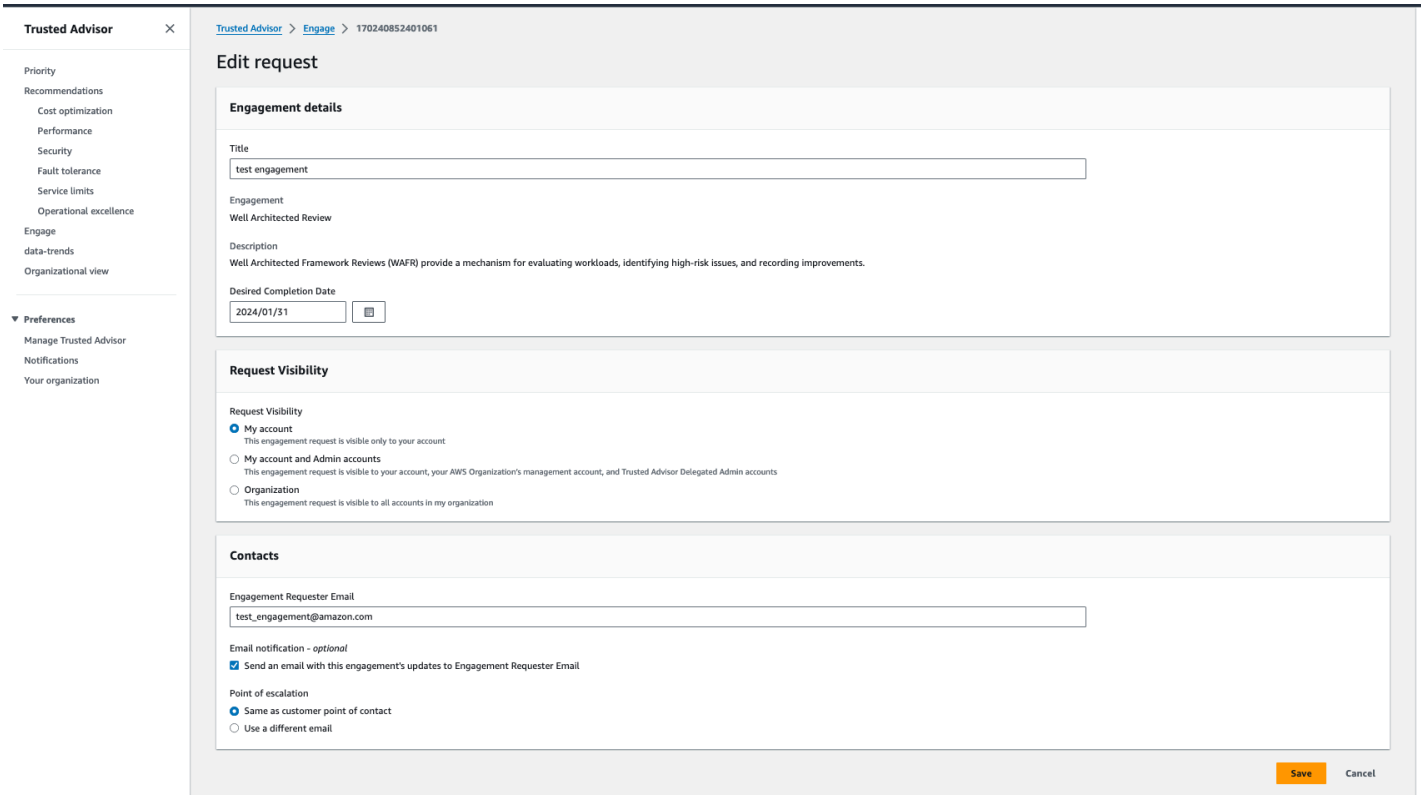
Untuk mengedit Keterlibatan:

1. Masuk ke Trusted Advisor konsol di https://console.aws.amazon.com/trustedadvisor/home.
2. Pada halaman Trusted AdvisorEngage, pilih keterlibatan yang ada.
3. Pilih Edit.
4. Anda dapat mengedit:
    - Judul

- Tanggal Penyelesaian yang Diinginkan: tanggal penyelesaian yang diinginkan dari Keterlibatan. Setiap Jenis Keterlibatan memiliki lead time yang berbeda yang dihitung dalam tanggal penyelesaian minimum yang diinginkan.
- Minta Visibilitas:
  - Akun saya: permintaan keterlibatan ini hanya dapat dilihat oleh akun Anda.
  - Akun saya dan akun Admin: permintaan keterlibatan ini dapat dilihat oleh akun Anda, dan akun Manajemen dan semua akun Admin Delegasi AWS Organisasi Anda.
  - Organisasi: Permintaan keterlibatan ini dapat dilihat oleh semua akun di AWS Organisasi Anda.
- Email Pemohon Keterlibatan: alamat email yang AWS akan digunakan sebagai titik kontak utama untuk Keterlibatan ini.
- Pengaturan notifikasi email: pilih apakah Email Pemohon Keterlibatan akan menerima pemberitahuan email tentang keterlibatan.
- Titik eskalasi: alamat email yang AWS akan digunakan saat eskalasi diperlukan untuk Keterlibatan ini.

5. Pilih Simpan.

Example : Edit Keterlibatan



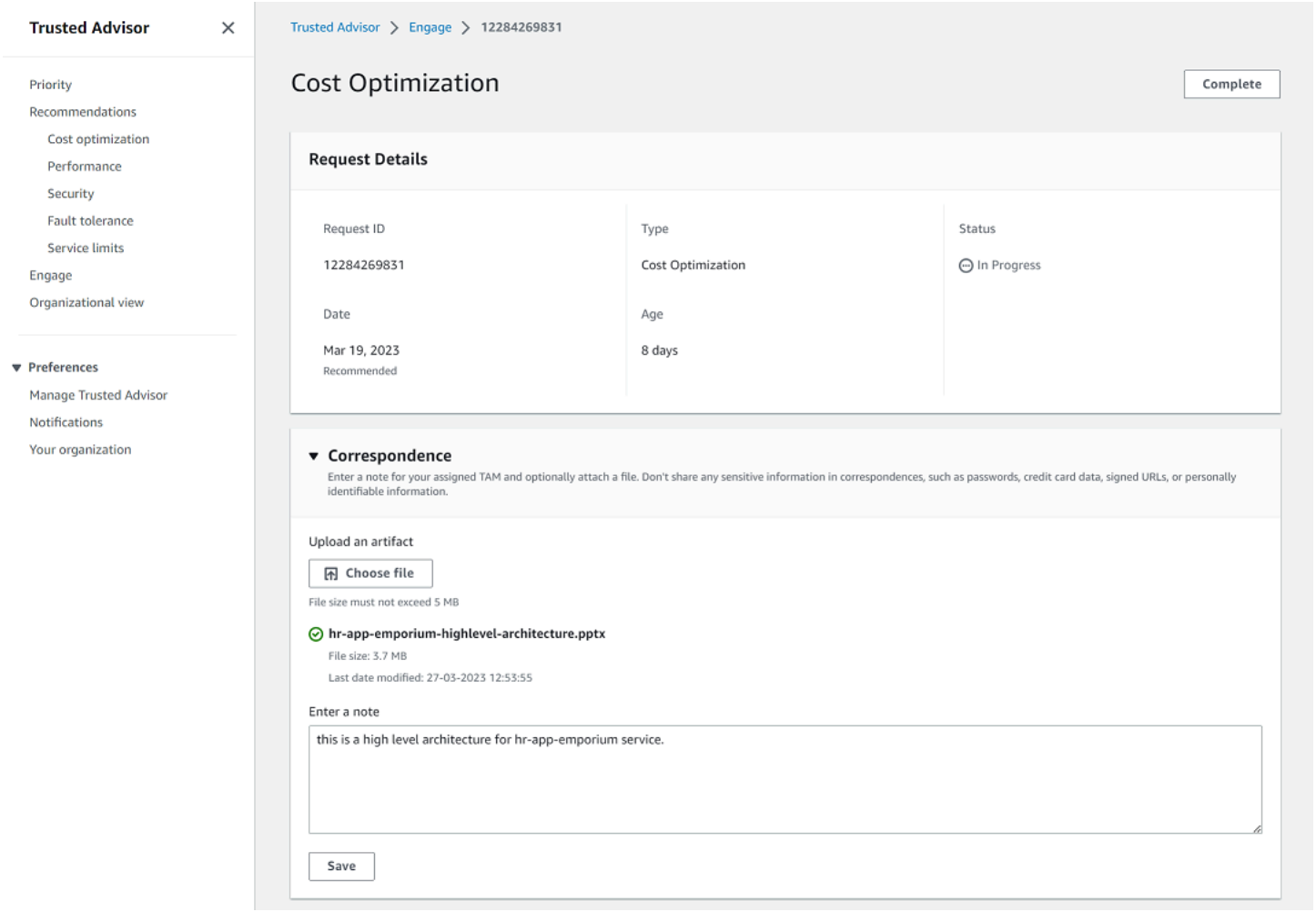
Kirim Lampiran dan Catatan

Anda dapat berkomunikasi dengan Akun AWS tim Anda tentang keterlibatan individu dengan mengirimkan catatan dan lampiran file untuk mendukung permintaan keterlibatan Anda. Anda dapat menyertakan satu lampiran dan catatan per komunikasi, Anda hanya dapat melampirkan file ke keterlibatan dengan Akun AWS yang sama yang meminta keterlibatan, dan Anda tidak dapat menghapus lampiran atau catatan setelah komunikasi dikirim.

Untuk melampirkan file atau menambahkan catatan ke permintaan Keterlibatan Aktif:

1. Masuk ke Trusted Advisor konsol di https://console.aws.amazon.com/trustedadvisor/home.
2. Pada halaman Trusted AdvisorEngage, pilih ID keterlibatan aktif yang ingin Anda lampirkan file atau tambahkan catatan.
3. Pilih Korespondensi untuk memperluas formulir.
4. Masukkan catatan untuk TAM yang Anda tetapkan dan lampirkan file secara opsional. Jangan membagikan informasi sensitif apa pun dalam korespondensi, seperti kata sandi, data kartu kredit, URL yang ditandatangani, atau informasi identitas pribadi.
5. Pilih Simpan.

Example : Tambahkan Catatan dan Lampirkan File ke Keterlibatan



Mengubah Status Keterlibatan

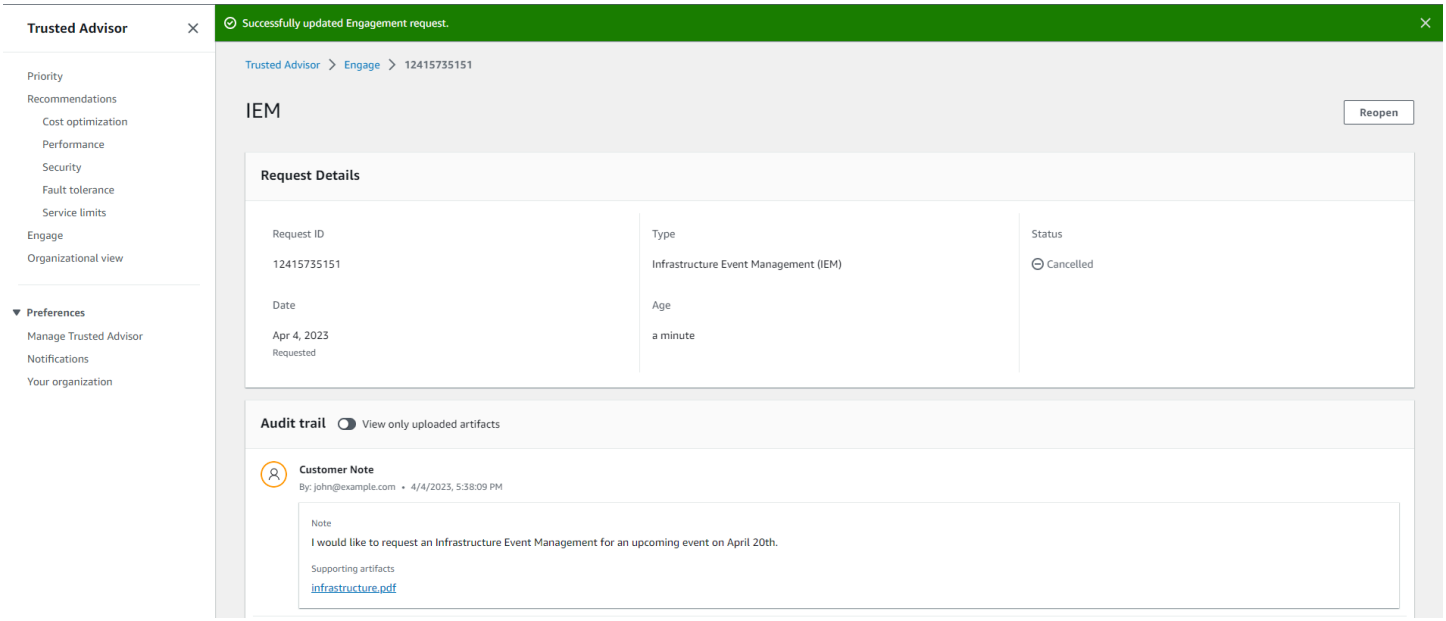
Anda dapat mengubah status keterlibatan tersebut untuk membatalkan keterlibatan yang menunggu tanggapan, menyelesaikan keterlibatan yang sedang berlangsung, dan membuka kembali keterlibatan yang telah ditandai sebagai dibatalkan atau ditutup.

Untuk mengubah status Keterlibatan:

1. Masuk ke Trusted Advisor konsol di https://console.aws.amazon.com/trustedadvisor/home.
2. Pada halaman Trusted AdvisorEngage, pilih ID keterlibatan aktif yang ingin Anda ubah statusnya.
3. Pada halaman Detail Keterlibatan, Anda dapat mengubah status menjadi Dibatalkan atau Selesai.

- Anda dapat memilih Batal ketika status keterlibatan adalah Respons Tertunda.
- Anda dapat memilih Selesai saat status keterlibatan sedang berlangsung.
- Anda dapat memilih Buka Kembali untuk keterlibatan tertutup. Keterlibatan yang dibatalkan pindah ke Respons Tertunda, sementara keterlibatan Selesai pindah ke Sedang Berlangsung.

Example : Ubah Status Keterlibatan



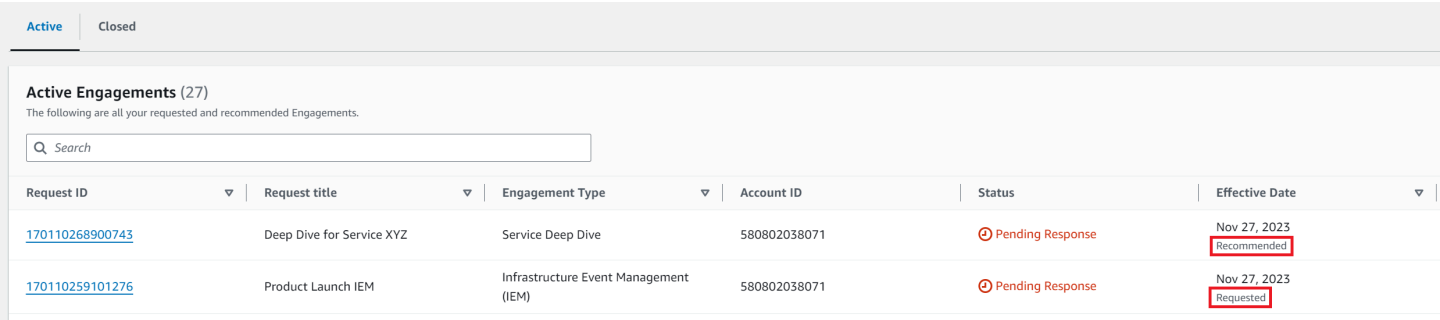
Membedakan Antara Keterlibatan yang Direkomendasikan dan yang Diminta

Anda dapat mengidentifikasi sumber keterlibatan untuk mengetahui apakah keterlibatan diminta oleh Anda atau direkomendasikan oleh tim AndaAkun AWS.

Untuk melihat berbagai sumber Keterlibatan Aktif:

1. Masuk ke Trusted Advisor konsol di https://console.aws.amazon.com/trustedadvisor/home.
2. Pada halaman Trusted AdvisorEngage, lihat kolom Tanggal Efektif untuk membedakan antara Keterlibatan yang Direkomendasikan dan yang Diminta:
   - Direkomendasikan: Permintaan keterlibatan yang dibuat oleh Akun AWS tim Anda.
   - Diminta: Permintaan keterlibatan yang dibuat oleh pengguna.

Example : Membedakan Antara Keterlibatan yang Direkomendasikan dan Diminta



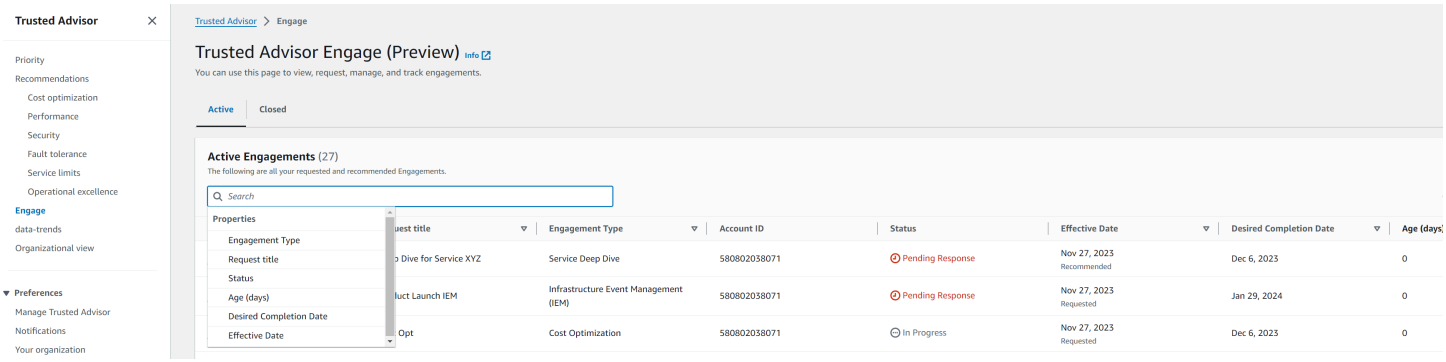
Keterlibatan Pencarian

Anda dapat mencari keterlibatan aktif dan tertutup yang ada menggunakan filter.

Untuk mencari Keterlibatan:

1. Masuk ke Trusted Advisor konsol di https://console.aws.amazon.com/trustedadvisor/home.
2. Pada halaman Trusted AdvisorEngage, Anda dapat memilih dari filter berikut:
   - Umur (hari)
   - Jenis Keterlibatan
   - Permintaan Judul
   - Status
   - Tanggal Penyelesaian yang Diinginkan
   - Tanggal Efektif

Example : Cari Keterlibatan



AWS Trusted Advisor periksa referensi

Anda dapat melihat semua nama Trusted Advisor cek, deskripsi, dan ID dalam referensi berikut. Anda juga dapat masuk ke Trusted Advisorkonsol untuk melihat informasi selengkapnya tentang pemeriksaan, tindakan yang disarankan, dan statusnya.

Jika Anda memiliki paket Business, Enterprise On-Ramp, atau Enterprise Support, Anda juga dapat menggunakan AWS Trusted Advisor API dan AWS Command Line Interface (AWS CLI) untuk mengakses cek Anda. Untuk informasi selengkapnya, lihat topik berikut.

- Memulai dengan Trusted Advisor API
- AWS Trusted Advisor Referensi API

> **Note**
>
> Jika Anda memiliki paket Dukungan Dasar dan Dukungan Pengembang, Anda dapat menggunakan Trusted Advisor konsol untuk mengakses semua pemeriksaan dalam Batas layanan kategori dan pemeriksaan berikut dalam kategori keamanan:
>
> - Cuplikan Publik Amazon EBS
> - Cuplikan Publik Amazon RDS
> - Izin Bucket Amazon S3
> - MFA pada Akun Root
> - Grup Keamanan — Port Tertentu Tidak Dibatasi

Kategori pemeriksaan

- Optimasi biaya
- Kinerja
- Keamanan
- Toleransi kesalahan
- Batas layanan
- Keunggulan Operasional

Optimasi biaya

Anda dapat menggunakan pemeriksaan berikut untuk kategori pengoptimalan biaya.

Periksa nama

- AWSAkun Bukan Bagian dari AWS Organizations
- Amazon Comprehend Endpoint yang Kurang Digunakan
- Volume Amazon EBS yang disediakan secara berlebihan
- Amazon EC2 Instans Konsolidasi untuk Microsoft SQL Server
- Instans Amazon EC2 disediakan secara berlebihan untuk Microsoft SQL Server
- Instans Amazon EC2 Dihentikan
- Kedaluwarsa Sewa Instans Cadangan Amazon EC2
- Optimasi Instans Cadangan Amazon EC2
- Repositori Amazon ECR Tanpa Kebijakan Siklus Hidup Dikonfigurasi
- Optimasi Node ElastiCache Cadangan Amazon
- Optimasi Instans Cadangan OpenSearch Layanan Amazon
- Amazon RDS Idle DB Instances
- Optimasi Node Cadangan Amazon Redshift
- Optimasi Instans Cadangan Amazon Relational Database Service (RDS)
- Amazon Route 53 Set Rekor Sumber Daya Latensi
- Kebijakan Siklus Hidup Bucket Amazon S3 Dikonfigurasi
- Konfigurasi Batalkan Unggahan Multipart Amazon S3 Tidak Lengkap
- Bucket berkemampuan versi Amazon S3 tanpa kebijakan siklus hidup yang dikonfigurasi
- Fungsi AWS Lambda dengan Waktu Habis Berlebihan
- Fungsi AWS Lambda dengan Tingkat Eror Tinggi
- AWS Lambdafungsi yang disediakan secara berlebihan untuk ukuran memori
- AWS Well-Architectedmasalah risiko tinggi untuk optimalisasi biaya
- Penyeimbang Beban Idle
- Instans Amazon EC2 Penggunaan Rendah
- Savings Plan
- Alamat IP Elastis yang Tidak Terkait

- Volume Amazon EBS yang Kurang Digunakan
- Cluster Pergeseran Merah Amazon yang Kurang Digunakan

AWSAkun Bukan Bagian dari AWS Organizations

Deskripsi

Memeriksa apakah AWS akun merupakan bagian AWS Organizations dari akun manajemen yang sesuai.

AWS Organizationsadalah layanan manajemen akun untuk mengkonsolidasikan beberapa AWS akun ke dalam organisasi yang dikelola secara terpusat. Ini memungkinkan Anda menyusun akun secara terpusat untuk konsolidasi penagihan dan menerapkan kebijakan kepemilikan dan keamanan saat beban kerja Anda meningkat. AWS

Anda dapat menentukan id akun manajemen menggunakan MasterAccountIdparameter AWS Config aturan.

Untuk informasi selengkapnya, lihat Apa itu AWS Organizations?

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

```
c18d2gz127
```

Sumber

```
AWS Config Managed Rule: account-part-of-organizations
```

Kriteria Peringatan

Kuning: AWS Akun ini bukan bagian dariAWS Organizations.

Tindakan yang Direkomendasikan

Tambahkan AWS akun ini sebagai bagian dariAWS Organizations.

Untuk informasi selengkapnya, lihat Tutorial: Membuat dan mengonfigurasi organisasi.

Kolom laporan

- Status
- Wilayah
- Sumber daya
- AWS ConfigAturan
- Parameter Input
- Waktu Terakhir Diperbarui

Amazon Comprehend Endpoint yang Kurang Digunakan

Deskripsi

Memeriksa konfigurasi throughput titik akhir Anda. Pemeriksaan ini memberi tahu Anda saat titik akhir tidak digunakan secara aktif untuk permintaan inferensi waktu nyata. Titik akhir yang tidak digunakan selama lebih dari 15 hari berturut-turut dianggap kurang dimanfaatkan. Semua titik akhir memperoleh biaya berdasarkan set throughput, dan lamanya waktu titik akhir aktif.

> **Note**
>
> Pemeriksaan ini secara otomatis disegarkan sekali sehari. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

`Cm24dfsM12`

Kriteria Peringatan

Kuning: Titik akhir aktif, tetapi belum digunakan untuk permintaan inferensi waktu nyata dalam 15 hari terakhir.

Tindakan yang Direkomendasikan

Jika titik akhir belum digunakan dalam 15 hari terakhir, sebaiknya Anda menentukan kebijakan penskalaan sumber daya dengan menggunakan Application Autoscaling.

Jika titik akhir memiliki kebijakan penskalaan yang ditentukan dan belum digunakan dalam 30 hari terakhir, pertimbangkan untuk menghapus titik akhir dan menggunakan inferensi asinkron. Untuk informasi selengkapnya, lihat Menghapus titik akhir dengan Amazon Comprehend.

Kolom laporan

- Status
- Wilayah
- Titik akhir ARN
- Unit Inferensi yang Diberikan
- AutoScaling Status
- Alasan
- Waktu Terakhir Diperbarui

Volume Amazon EBS yang disediakan secara berlebihan

Deskripsi

Memeriksa volume Amazon Elastic Block Store (Amazon EBS) yang berjalan kapan saja selama periode lookback. Pemeriksaan ini memberi tahu Anda jika ada volume EBS yang disediakan secara berlebihan untuk beban kerja Anda. Ketika Anda memiliki volume yang terlalu banyak disediakan, Anda membayar untuk sumber daya yang tidak digunakan. Meskipun beberapa skenario dapat menghasilkan optimasi yang rendah berdasarkan desain, Anda sering dapat menurunkan biaya dengan mengubah konfigurasi volume EBS Anda. Perkiraan penghematan bulanan dihitung dengan menggunakan tingkat penggunaan saat ini untuk volume EBS. Penghematan aktual akan bervariasi jika volumenya tidak ada selama sebulan penuh.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

`COr6dfpM03`

Kriteria Peringatan

Kuning: Volume EBS yang disediakan secara berlebihan selama periode lookback. Untuk menentukan apakah volume disediakan secara berlebihan, kami mempertimbangkan semua CloudWatch metrik default (termasuk IOPS dan throughput). Algoritma yang digunakan untuk mengidentifikasi volume EBS yang disediakan secara berlebihan mengikuti praktik terbaik. AWS Algoritma diperbarui ketika pola baru telah diidentifikasi.

Tindakan yang Direkomendasikan

Pertimbangkan perampingan volume yang memiliki pemanfaatan rendah.

Untuk informasi selengkapnya, lihat Ikut serta AWS Compute Optimizer untuk Trusted Advisor cek.

Kolom laporan

- Status
- Wilayah
- ID Volume
- Jenis Volume
- Ukuran Volume (GB)
- Volume Dasar IOPS
- Volume Burst IOPS
- Throughput Volume Burst
- Jenis Volume yang Direkomendasikan
- Ukuran Volume yang Direkomendasikan (GB)
- IOPS Dasar Volume yang Direkomendasikan
- Volume Burst IOPS yang Direkomendasikan
- Throughput Dasar Volume yang Direkomendasikan
- Throughput Volume Burst yang Direkomendasikan
- Periode Lookback (hari)
- Peluang Tabungan (%)
- Perkiraan Tabungan Bulanan
- Estimasi Mata Uang Tabungan Bulanan

- Waktu Terakhir Diperbarui

Amazon EC2 Instans Konsolidasi untuk Microsoft SQL Server

Deskripsi

Memeriksa instans Amazon Elastic Compute Cloud (Amazon EC2) yang menjalankan SQL Server dalam 24 jam terakhir. Pemeriksaan ini memberi tahu Anda jika instans Anda memiliki kurang dari jumlah minimum lisensi SQL Server. Dari Microsoft SQL Server Licensing Guide, Anda membayar 4 lisensi vCPU bahkan jika sebuah instance hanya memiliki 1 atau 2 vCPU. Anda dapat mengkonsolidasikan instance SQL Server yang lebih kecil untuk membantu menurunkan biaya.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

`Qsdfp3A4L2`

Kriteria Peringatan

Kuning: Sebuah instance dengan SQL Server memiliki kurang dari 4 vCPU.

Tindakan yang Direkomendasikan

Pertimbangkan untuk mengkonsolidasikan beban kerja SQL Server yang lebih kecil ke dalam instance dengan setidaknya 4 vCPU.

Sumber Daya Tambahan

- Microsoft SQL Server aktif AWS
- Lisensi Microsoft pada AWS
- Panduan Lisensi Microsoft SQL Server

Kolom laporan

- Status

- Wilayah
- ID Instans
- Tipe Instans
- vCPU
- vCPU minimum
- Edisi SQL Server
- Waktu Terakhir Diperbarui

Instans Amazon EC2 disediakan secara berlebihan untuk Microsoft SQL Server

Deskripsi

Memeriksa instans Amazon Elastic Compute Cloud (Amazon EC2) yang menjalankan SQL Server dalam 24 jam terakhir. Database SQL Server memiliki batas kapasitas komputasi untuk setiap instance. Sebuah instance dengan SQL Server Standard edition dapat menggunakan hingga 48 vCPU. Sebuah instance dengan SQL Server Web dapat menggunakan hingga 32 vCPU. Pemeriksaan ini memberi tahu Anda jika instance melebihi batas vCPU ini.

Jika instans Anda disediakan secara berlebihan, Anda membayar harga penuh tanpa menyadari peningkatan kinerja. Anda dapat mengelola jumlah dan ukuran instans Anda untuk membantu menurunkan biaya.

Perkiraan penghematan bulanan dihitung dengan menggunakan keluarga instans yang sama dengan jumlah maksimum vCPU yang dapat digunakan instans SQL Server dan harga On-Demand. Penghematan aktual akan bervariasi jika Anda menggunakan Instans Cadangan (RI) atau jika instans tidak berjalan selama sehari penuh.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

`Qsdfp3A4L1`

Kriteria Peringatan

- Merah: Sebuah instance dengan edisi SQL Server Standard memiliki lebih dari 48 vCPU.
- Merah: Sebuah instance dengan edisi Web SQL Server memiliki lebih dari 32 vCPU.

Tindakan yang Direkomendasikan

Untuk edisi Standar SQL Server, pertimbangkan untuk mengubah ke instance dalam keluarga instance yang sama dengan 48 vCPU. Untuk edisi Web SQL Server, pertimbangkan untuk mengubah ke instance dalam keluarga instance yang sama dengan 32 vCPU. Jika intensif memori, pertimbangkan untuk mengubah ke instans R5 yang dioptimalkan memori. Untuk informasi selengkapnya, lihat Praktik Terbaik untuk Menerapkan Microsoft SQL Server di Amazon EC2.

Sumber Daya Tambahan

- Microsoft SQL Server aktif AWS
- Anda dapat menggunakan Launch Wizard untuk menyederhanakan penyebaran SQL Server Anda di EC2.

Kolom laporan

- Status
- Wilayah
- ID Instans
- Tipe Instans
- vCPU
- Edisi SQL Server
- vCPU maksimum
- Jenis Instance yang Direkomendasikan
- Perkiraan Tabungan Bulanan
- Waktu Terakhir Diperbarui

Instans Amazon EC2 Dihentikan

Deskripsi

Memeriksa apakah ada instans Amazon EC2 yang telah dihentikan selama lebih dari 30 hari.

Anda dapat menentukan jumlah nilai hari yang diizinkan dalam AllowedDaysAWS Configparameter.

Untuk informasi selengkapnya, lihat Mengapa saya dikenakan biaya untuk Amazon EC2 ketika semua instans saya dihentikan?

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

```
c18d2gz150
```

Sumber

```
AWS Config Managed Rule: ec2-stopped-instance
```

Kriteria Peringatan

- Kuning: Ada instans Amazon EC2 yang dihentikan selama lebih dari jumlah hari yang diizinkan.

Tindakan yang Direkomendasikan

Tinjau instans Amazon EC2 yang telah dihentikan selama 30 hari atau lebih. Untuk menghindari biaya yang tidak perlu, hentikan setiap contoh yang tidak lagi diperlukan.

Untuk informasi selengkapnya, lihat Mengakhiri instans Anda.

Sumber Daya Tambahan

- Harga Sesuai Permintaan Amazon EC2

Kolom laporan

- Status
- Wilayah
- Sumber daya
- AWS ConfigAturan
- Parameter Input

- Waktu Terakhir Diperbarui

Kedaluwarsa Sewa Instans Cadangan Amazon EC2

Deskripsi

Memeriksa Instans Cadangan Amazon EC2 yang dijadwalkan kedaluwarsa dalam 30 hari ke depan, atau telah kedaluwarsa dalam 30 hari sebelumnya.

Instans Cadangan tidak diperpanjang secara otomatis. Anda dapat terus menggunakan instans Amazon EC2 yang dicakup oleh reservasi tanpa gangguan, tetapi Anda akan dikenakan tarif Sesuai Permintaan. Instans Cadangan Baru dapat memiliki parameter yang sama dengan yang kedaluwarsa, atau Anda dapat membeli Instans Cadangan dengan parameter yang berbeda.

Perkiraan penghematan bulanan adalah perbedaan antara tarif Instans Sesuai Permintaan dan Cadangan untuk jenis instans yang sama.

ID pemeriksaan

`1e93e4c0b5`

Kriteria Peringatan

- Kuning: Sewa Instans Cadangan berakhir dalam waktu kurang dari 30 hari.
- Kuning: Sewa Instans Cadangan berakhir dalam 30 hari sebelumnya.

Tindakan yang Direkomendasikan

Pertimbangkan untuk membeli Instans Cadangan baru untuk menggantikan yang mendekati akhir masa jabatannya. Untuk informasi selengkapnya, lihat Cara Membeli Instans Cadangan dan Membeli Instans Cadangan.

Sumber Daya Tambahan

- Instans Cadangan
- Jenis Instance

Kolom laporan

- Status
- Zona
- Tipe Instans
- Platform

- Hitungan Instance
- Biaya Bulanan Saat Ini
- Perkiraan Tabungan Bulanan
- Tanggal Kedaluwarsa
- ID Instans Terpesan
- Alasan

Optimasi Instans Cadangan Amazon EC2

Deskripsi

Bagian penting dari penggunaan AWS melibatkan menyeimbangkan pembelian Instans Cadangan (RI) Anda dengan penggunaan Instans Sesuai Permintaan Anda. Pemeriksaan ini memberikan rekomendasi tentang RI mana yang akan membantu mengurangi biaya yang dikeluarkan dari penggunaan Instans Sesuai Permintaan.

Kami membuat rekomendasi ini dengan menganalisis penggunaan On-Demand Anda selama 30 hari terakhir. Kami kemudian mengkategorikan penggunaan ke dalam kategori yang memenuhi syarat untuk reservasi. Kami mensimulasikan setiap kombinasi pemesanan dalam kategori penggunaan yang dihasilkan untuk mengidentifikasi jumlah yang direkomendasikan dari setiap jenis RI yang akan dibeli. Proses simulasi dan pengoptimalan ini memungkinkan kami memaksimalkan penghematan biaya Anda. Pemeriksaan ini mencakup rekomendasi berdasarkan Instans Cadangan Standar dengan opsi pembayaran di muka sebagian.

Pemeriksaan ini tidak tersedia untuk akun yang ditautkan dalam penagihan gabungan. Rekomendasi untuk cek ini hanya tersedia untuk akun pembayaran.

ID pemeriksaan

`cX3c2R1chu`

Kriteria Peringatan

Kuning: Mengoptimalkan penggunaan RI di muka sebagian dapat membantu mengurangi biaya.

Tindakan yang Direkomendasikan

Lihat halaman Cost Explorer untuk rekomendasi yang lebih detail dan disesuaikan. Selain itu, lihat panduan pembelian untuk memahami cara membeli RI dan opsi yang tersedia.

Sumber Daya Tambahan

- Informasi tentang RI dan bagaimana mereka dapat menghemat uang Anda dapat ditemukan di sini.
- Untuk informasi selengkapnya tentang rekomendasi ini, lihat Pertanyaan Pemeriksaan Optimasi Instans Cadangan di Trusted Advisor FAQ.

Kolom laporan

- Wilayah
- Tipe Instans
- Platform
- Jumlah RI yang Direkomendasikan untuk Dibeli
- Pemanfaatan RI Rata-rata yang Diharapkan
- Estimasi Tabungan dengan Rekomendasi (Bulanan)
- Biaya di muka RI
- Perkiraan biaya RI (Bulanan)
- Perkiraan Biaya Sesuai Permintaan Pasca Rekomendasi Pembelian RI (Bulanan)
- Perkiraan Break Even (Bulan)
- Periode Lookback (Hari)
- Jangka Waktu (Tahun)

Repositori Amazon ECR Tanpa Kebijakan Siklus Hidup Dikonfigurasi

Deskripsi

Memeriksa apakah repositori ECR Amazon pribadi memiliki setidaknya satu kebijakan siklus hidup yang dikonfigurasi. Kebijakan siklus hidup memungkinkan Anda menentukan seperangkat aturan untuk secara otomatis membersihkan gambar kontainer lama atau yang tidak digunakan. Ini memberi Anda kontrol atas manajemen siklus hidup gambar, memungkinkan repositori Amazon ECR terorganisir dengan lebih baik, dan membantu menurunkan biaya penyimpanan secara keseluruhan.

Untuk informasi selengkapnya, lihat Kebijakan Siklus Hidup.

ID pemeriksaan

`c18d2gz128`

Sumber

```
AWS Config Managed Rule: ecr-private-lifecycle-policy-configured
```

Kriteria Peringatan

Kuning: Repositori pribadi Amazon ECR tidak memiliki kebijakan siklus hidup yang dikonfigurasi.

Tindakan yang Direkomendasikan

Pertimbangkan untuk membuat setidaknya satu kebijakan siklus hidup untuk repositori ECR Amazon pribadi Anda.

Untuk informasi selengkapnya, lihat Membuat kebijakan siklus hidup.

Sumber Daya Tambahan

- Kebijakan siklus hidup.
- Membuat kebijakan siklus hidup.
- Contoh kebijakan siklus hidup.

Kolom laporan

- Status
- Wilayah
- Sumber daya
- AWS ConfigAturan
- Parameter Input
- Waktu Terakhir Diperbarui

Optimasi Node ElastiCache Cadangan Amazon

Deskripsi

Memeriksa penggunaan Anda ElastiCache dan memberikan rekomendasi tentang pembelian Node Cadangan. Rekomendasi ini ditawarkan untuk mengurangi biaya yang dikeluarkan dari penggunaan ElastiCache On-Demand. Kami membuat rekomendasi ini dengan menganalisis penggunaan On-Demand Anda selama 30 hari terakhir.

Kami menggunakan analisis ini untuk mensimulasikan setiap kombinasi reservasi dalam kategori penggunaan yang dihasilkan. Ini memungkinkan kami untuk merekomendasikan jumlah setiap jenis Node Cadangan untuk dibeli untuk memaksimalkan penghematan Anda. Cek ini mencakup

rekomendasi berdasarkan opsi pembayaran di muka sebagian dengan komitmen 1 tahun atau 3 tahun.

Pemeriksaan ini tidak tersedia untuk akun yang ditautkan dalam penagihan gabungan. Rekomendasi untuk cek ini hanya tersedia untuk akun pembayaran.

ID pemeriksaan

`h3L1otH3re`

Kriteria Peringatan

Kuning: Mengoptimalkan pembelian Node ElastiCache Cadangan dapat membantu mengurangi biaya.

Tindakan yang Direkomendasikan

Lihat halaman Cost Explorer untuk rekomendasi yang lebih rinci, opsi penyesuaian (misalnya, periode lihat kembali, opsi pembayaran, dan sebagainya.) dan untuk membeli ElastiCache Node Cadangan.

Sumber Daya Tambahan

- Informasi tentang Node ElastiCache Cadangan dan bagaimana mereka dapat menghemat uang Anda dapat ditemukan di sini.
- Untuk informasi selengkapnya tentang rekomendasi ini, lihat Pertanyaan Pemeriksaan Optimasi Instans Cadangan di Trusted Advisor FAQ.
- Untuk penjelasan lebih rinci tentang bidang, lihat dokumentasi Cost Explorer

Kolom laporan

- Wilayah
- Rangkaian
- Jenis Simpul
- Deskripsi Produk
- Jumlah Node Cadangan yang disarankan untuk dibeli
- Pemanfaatan Node Cadangan Rata-rata yang Diharapkan
- Estimasi Tabungan dengan Rekomendasi (bulanan)
- Biaya di Muka dari Node Cadangan
- Perkiraan biaya Node Cadangan (bulanan)
- Perkiraan Biaya Sesuai Permintaan Pasca Pembelian Node Cadangan yang Direkomendasikan (bulanan)

- Estimasi Break Even (bulan)
- Periode Lookback (hari)
- Jangka waktu (tahun)

Optimasi Instans Cadangan OpenSearch Layanan Amazon

Deskripsi

Memeriksa penggunaan OpenSearch Layanan Amazon dan memberikan rekomendasi tentang pembelian Instans Cadangan. Rekomendasi ini ditawarkan untuk mengurangi biaya yang dikeluarkan dari penggunaan OpenSearch On-Demand. Kami membuat rekomendasi ini dengan menganalisis penggunaan On-Demand Anda selama 30 hari terakhir.

Kami menggunakan analisis ini untuk mensimulasikan setiap kombinasi reservasi dalam kategori penggunaan yang dihasilkan. Hal ini memungkinkan kami untuk merekomendasikan jumlah setiap jenis Instans Cadangan yang akan dibeli untuk memaksimalkan penghematan Anda. Cek ini mencakup rekomendasi berdasarkan opsi pembayaran di muka sebagian dengan komitmen 1 tahun atau 3 tahun.

Pemeriksaan ini tidak tersedia untuk akun yang ditautkan dalam penagihan gabungan. Rekomendasi untuk cek ini hanya tersedia untuk akun pembayaran.

ID pemeriksaan

`7ujm6yhn5t`

Kriteria Peringatan

Kuning: Mengoptimalkan pembelian Instans Cadangan OpenSearch Layanan Amazon dapat membantu mengurangi biaya.

Tindakan yang Direkomendasikan

Lihat halaman Cost Explorer untuk rekomendasi lebih rinci, opsi penyesuaian (misalnya periode lihat kembali, opsi pembayaran, dll.) dan untuk membeli Instans Cadangan OpenSearch Layanan Amazon.

Sumber Daya Tambahan

- Informasi tentang Instans Cadangan OpenSearch Layanan Amazon dan bagaimana mereka dapat menghemat uang Anda dapat ditemukan di sini.

- Untuk informasi selengkapnya tentang rekomendasi ini, lihat Pertanyaan Pemeriksaan Optimasi Instans Cadangan di Trusted Advisor FAQ.
- Untuk penjelasan lebih rinci tentang bidang, lihat dokumentasi Cost Explorer

Kolom laporan

- Wilayah
- Kelas instans
- Ukuran Instans
- Jumlah Instans Cadangan yang disarankan untuk dibeli
- Pemanfaatan Instans Cadangan Rata-rata yang Diharapkan
- Estimasi Tabungan dengan Rekomendasi (bulanan)
- Biaya di Muka untuk Instans Cadangan
- Perkiraan biaya Instans Cadangan (bulanan)
- Perkiraan Biaya Sesuai Permintaan Pasca Rekomendasi Pembelian Instans Cadangan (bulanan)
- Estimasi Break Even (bulan)
- Periode Lookback (hari)
- Jangka waktu (tahun)

Amazon RDS Idle DB Instances

Deskripsi

Memeriksa konfigurasi Amazon Relational Database Service (Amazon RDS) untuk setiap instans database (DB) yang tampak menganggur.

Jika instans DB tidak memiliki koneksi untuk jangka waktu yang lama, Anda dapat menghapus instance untuk mengurangi biaya. Instans DB dianggap menganggur jika instance tidak memiliki koneksi dalam 7 hari terakhir. Jika penyimpanan persisten diperlukan untuk data pada instance, Anda dapat menggunakan opsi berbiaya lebih rendah seperti mengambil dan mempertahankan snapshot DB. Snapshot DB yang dibuat secara manual dipertahankan sampai Anda menghapusnya.

ID pemeriksaan

`Ti39halfu8`

Kriteria Peringatan

Kuning: Instans DB aktif tidak memiliki koneksi dalam 7 hari terakhir.

Tindakan yang Direkomendasikan

Pertimbangkan untuk mengambil snapshot dari instans DB idle dan kemudian menghentikannya atau menghapusnya. Menghentikan instans DB menghilangkan beberapa biaya untuk itu, tetapi tidak menghilangkan biaya penyimpanan. Instans yang dihentikan menyimpan semua pencadangan otomatis berdasarkan periode retensi yang dikonfigurasi. Menghentikan instans DB biasanya menimbulkan biaya tambahan jika dibandingkan dengan menghapus instance dan kemudian hanya mempertahankan snapshot akhir. Lihat Menghentikan instans Amazon RDS sementara dan Menghapus Instans DB dengan Snapshot Akhir.

Sumber Daya Tambahan

Cadangkan dan Kembalikan

Kolom laporan

- Wilayah
- Nama Instans DB
- Multi-AZ
- Tipe Instans
- Penyimpanan Disediakan (GB)
- Hari Sejak Koneksi Terakhir
- Perkiraan Tabungan Bulanan (Sesuai Permintaan)

Optimasi Node Cadangan Amazon Redshift

Deskripsi

Memeriksa penggunaan Amazon Redshift Anda dan berikan rekomendasi tentang pembelian Node Cadangan untuk membantu mengurangi biaya yang dikeluarkan dari penggunaan Amazon Redshift On-Demand.

Kami membuat rekomendasi ini dengan menganalisis penggunaan On-Demand Anda selama 30 hari terakhir. Kami menggunakan analisis ini untuk mensimulasikan setiap kombinasi reservasi dalam kategori penggunaan yang dihasilkan. Ini memungkinkan kami mengidentifikasi jumlah terbaik dari setiap jenis Node Cadangan untuk dibeli untuk memaksimalkan penghematan

Anda. Cek ini mencakup rekomendasi berdasarkan opsi pembayaran di muka sebagian dengan komitmen 1 tahun atau 3 tahun.

Pemeriksaan ini tidak tersedia untuk akun yang ditautkan dalam penagihan gabungan. Rekomendasi untuk cek ini hanya tersedia untuk akun pembayaran.

ID pemeriksaan

`1qw23er45t`

Kriteria Peringatan

Kuning: Mengoptimalkan pembelian Amazon Redshift Reserved Nodes dapat membantu mengurangi biaya.

Tindakan yang Direkomendasikan

Lihat halaman Cost Explorer untuk rekomendasi lebih rinci, opsi penyesuaian (misalnya periode lihat kembali, opsi pembayaran, dll.) Dan untuk membeli Node Cadangan Amazon Redshift.

Sumber Daya Tambahan

- Informasi tentang Amazon Redshift Reserved Nodes dan bagaimana mereka dapat menghemat uang Anda dapat ditemukan di sini.
- Untuk informasi selengkapnya tentang rekomendasi ini, lihat Pertanyaan Pemeriksaan Optimasi Instans Cadangan di Trusted Advisor FAQ.
- Untuk penjelasan lebih rinci tentang bidang, lihat dokumentasi Cost Explorer

Kolom laporan

- Wilayah
- Rangkaian
- Jenis Simpul
- Jumlah Node Cadangan yang disarankan untuk dibeli
- Pemanfaatan Node Cadangan Rata-rata yang Diharapkan
- Estimasi Tabungan dengan Rekomendasi (bulanan)
- UpFront Biaya Node Cadangan
- Perkiraan biaya Node Cadangan (bulanan)
- Perkiraan Biaya Sesuai Permintaan Pasca Pembelian Node Cadangan yang Direkomendasikan (bulanan)
- Estimasi Break Even (bulan)

- Periode Lookback (hari)
- Jangka waktu (tahun)

Optimasi Instans Cadangan Amazon Relational Database Service (RDS)

Deskripsi

Memeriksa penggunaan RDS dan memberikan rekomendasi tentang pembelian Instans Cadangan untuk membantu mengurangi biaya yang dikeluarkan dari penggunaan RDS On-Demand.

Kami membuat rekomendasi ini dengan menganalisis penggunaan On-Demand Anda selama 30 hari terakhir. Kami menggunakan analisis ini untuk mensimulasikan setiap kombinasi reservasi dalam kategori penggunaan yang dihasilkan. Hal ini memungkinkan kami mengidentifikasi jumlah terbaik dari setiap jenis Instans Cadangan untuk dibeli guna memaksimalkan penghematan Anda. Cek ini mencakup rekomendasi berdasarkan opsi pembayaran di muka sebagian dengan komitmen 1 tahun atau 3 tahun.

Pemeriksaan ini tidak tersedia untuk akun yang ditautkan dalam penagihan gabungan. Rekomendasi untuk cek ini hanya tersedia untuk akun pembayaran.

ID pemeriksaan

`1qazXsw23e`

Kriteria Peringatan

Kuning: Mengoptimalkan pembelian Instans Cadangan Amazon RDS dapat membantu mengurangi biaya.

Tindakan yang Direkomendasikan

Lihat halaman Cost Explorer untuk rekomendasi lebih rinci, opsi penyesuaian (misalnya periode lihat kembali, opsi pembayaran, dll.) dan untuk membeli Instans Cadangan Amazon RDS.

Sumber Daya Tambahan

- Informasi tentang Instans Cadangan Amazon RDS dan bagaimana mereka dapat menghemat uang Anda dapat ditemukan di sini.
- Untuk informasi selengkapnya tentang rekomendasi ini, lihat Pertanyaan Pemeriksaan Optimasi Instans Cadangan di Trusted Advisor FAQ.
- Untuk penjelasan lebih rinci tentang bidang, lihat dokumentasi Cost Explorer

Kolom laporan

- Wilayah
- Rangkaian
- Tipe Instans
- Model Lisensi
- Edisi Basis Data
- Mesin basis data
- Opsi Deployment
- Jumlah Instans Cadangan yang disarankan untuk dibeli
- Pemanfaatan Instans Cadangan Rata-rata yang Diharapkan
- Estimasi Tabungan dengan Rekomendasi (bulanan)
- Biaya di Muka untuk Instans Cadangan
- Perkiraan biaya Instans Cadangan (bulanan)
- Perkiraan Biaya Sesuai Permintaan Pasca Rekomendasi Pembelian Instans Cadangan (bulanan)
- Estimasi Break Even (bulan)
- Periode Lookback (hari)
- Jangka waktu (tahun)

Amazon Route 53 Set Rekor Sumber Daya Latensi

Deskripsi

Memeriksa set rekaman latensi Amazon Route 53 yang dikonfigurasi secara tidak efisien.

Untuk mengizinkan Amazon Route 53 merutekan kueri ke Wilayah AWS dengan latensi jaringan terendah, Anda harus membuat kumpulan catatan sumber daya latensi untuk nama domain tertentu (seperti example.com) di Wilayah yang berbeda. Jika Anda hanya membuat satu catatan sumber daya latensi yang ditetapkan untuk nama domain, semua kueri dirutekan ke satu Wilayah, dan Anda membayar ekstra untuk perutean berbasis latensi tanpa mendapatkan manfaatnya.

Zona yang di-host yang dibuat oleh AWS layanan tidak akan muncul di hasil pemeriksaan Anda.

ID pemeriksaan

`51fC20e7I2`

Kriteria Peringatan

Kuning: Hanya satu set catatan sumber daya latensi yang dikonfigurasi untuk nama domain tertentu.

Tindakan yang Direkomendasikan

Jika Anda memiliki sumber daya di beberapa wilayah, pastikan untuk menentukan kumpulan data sumber daya latensi untuk setiap wilayah. Lihat Perutean Berbasis Latensi.

Jika Anda memiliki sumber daya hanya dalam satuWilayah AWS, pertimbangkan untuk membuat sumber daya di lebih dari satu Wilayah AWS dan tentukan kumpulan catatan sumber daya latensi untuk masing-masing sumber daya; lihat Perutean Berbasis Latensi.

Jika Anda tidak ingin menggunakan beberapaWilayah AWS, Anda harus menggunakan kumpulan catatan sumber daya sederhana. Lihat Bekerja dengan Kumpulan Rekaman Sumber Daya.

Sumber Daya Tambahan

- Panduan Pengembang Amazon Route 53
- Harga Amazon Route 53

Kolom laporan

- Nama Zona yang Dihosting
- ID Zona yang Dihosting
- Nama Set Catatan Sumber Daya
- Jenis Set Rekaman Sumber Daya

Kebijakan Siklus Hidup Bucket Amazon S3 Dikonfigurasi

Deskripsi

Memeriksa apakah bucket Amazon S3 memiliki kebijakan siklus hidup yang dikonfigurasi. Kebijakan siklus hidup Amazon S3 memastikan bahwa objek Amazon S3 di dalam bucket disimpan dengan hemat biaya sepanjang siklus hidupnya. Ini penting untuk memenuhi persyaratan peraturan untuk penyimpanan dan penyimpanan data. Konfigurasi kebijakan adalah seperangkat aturan yang menentukan tindakan yang diterapkan oleh layanan Amazon S3 ke sekelompok objek. Kebijakan siklus hidup memungkinkan Anda mengotomatiskan transisi objek ke kelas penyimpanan berbiaya lebih rendah atau menghapusnya seiring bertambahnya usia. Misalnya, Anda dapat mentransisikan objek ke penyimpanan IA standar Amazon S3 30 hari setelah pembuatan, atau ke Amazon S3 Glacier setelah 1 tahun.

Anda juga dapat menentukan kedaluwarsa objek sehingga Amazon S3 menghapus objek atas nama Anda setelah jangka waktu tertentu.

Anda dapat menyesuaikan konfigurasi cek menggunakan parameter dalam AWS Config aturan Anda

Untuk informasi selengkapnya, lihat Mengelola siklus hidup penyimpanan Anda.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

```
c18d2gz100
```

Sumber

```
AWS Config Managed Rule: s3-lifecycle-policy-check
```

Kriteria Peringatan

Kuning: Bucket Amazon S3 tidak memiliki kebijakan siklus hidup yang dikonfigurasi.

Tindakan yang Direkomendasikan

Pastikan Anda memiliki kebijakan siklus hidup yang dikonfigurasi di bucket Amazon S3.

Jika organisasi Anda tidak memiliki kebijakan retensi, pertimbangkan untuk menggunakan Amazon S3 Intelligent-Tiering untuk mengoptimalkan biaya.

Untuk informasi tentang cara menentukan kebijakan siklus hidup Amazon S3, lihat Menyetel konfigurasi siklus hidup di bucket.

Untuk informasi tentang Tingkat Cerdas Amazon S3, lihat kelas penyimpanan Tingkat Cerdas Amazon S3

Sumber Daya Tambahan

Menyetel konfigurasi siklus hidup pada bucket

Contoh konfigurasi Siklus Hidup S3

Kolom laporan

- Status
- Wilayah
- Sumber daya
- AWS ConfigAturan
- Parameter Masukan

Konfigurasi Batalkan Unggahan Multipart Amazon S3 Tidak Lengkap

Deskripsi

Memeriksa apakah setiap bucket Amazon S3 dikonfigurasi dengan aturan siklus hidup untuk membatalkan unggahan multibagian yang tetap tidak lengkap setelah 7 hari. Disarankan menggunakan aturan siklus hidup untuk membatalkan unggahan yang tidak lengkap ini dan menghapus penyimpanan terkait.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan satu kali atau beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

`c1cj39rr6v`

Kriteria Peringatan

Kuning: Bucket konfigurasi siklus hidup tidak berisi aturan siklus hidup untuk membatalkan semua unggahan multibagian yang tetap tidak lengkap setelah 7 hari.

Tindakan yang Direkomendasikan

Tinjau konfigurasi siklus hidup untuk bucket tanpa aturan siklus hidup yang akan membersihkan semua unggahan multibagian yang tidak lengkap. Unggahan yang tidak selesai setelah 24 jam

tidak mungkin selesai. Klik di sini untuk mengikuti petunjuk untuk membuat aturan siklus hidup. Disarankan agar ini diterapkan pada semua benda di ember Anda. Jika Anda perlu menerapkan tindakan siklus hidup lainnya ke objek yang dipilih di bucket, Anda dapat memiliki beberapa aturan dengan filter berbeda. Periksa dasbor lensa penyimpanan atau hubungi ListMultipartUpload API untuk informasi lebih lanjut.

Sumber Daya Tambahan

Membuat konfigurasi siklus hidup

Menemukan dan Menghapus Unggahan Multipart yang Tidak Lengkap untuk Menurunkan Biaya Amazon S3

Mengunggah dan menyalin objek menggunakan unggahan multipart

Elemen konfigurasi siklus hidup

Elemen untuk menggambarkan tindakan siklus hidup

Konfigurasi siklus hidup untuk membatalkan unggahan multipart

Kolom laporan

- Status
- Wilayah
- Nama Bucket
- ARN Bucket
- Aturan siklus hidup untuk menghapus MPU yang tidak lengkap
- Hari Setelah Inisiasi
- Waktu Terakhir Diperbarui

Bucket berkemampuan versi Amazon S3 tanpa kebijakan siklus hidup yang dikonfigurasi

Deskripsi

Memeriksa apakah bucket berkemampuan versi Amazon S3 memiliki kebijakan siklus hidup yang dikonfigurasi..

Untuk informasi selengkapnya, lihat Mengelola siklus hidup penyimpanan Anda.

Anda dapat menentukan nama bucket yang ingin Anda periksa menggunakan parameter BucketNames dalam aturan Anda. AWS Config

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

```
c18d2gz171
```

Sumber

```
AWS Config Managed Rule: s3-version-lifecycle-policy-check
```

Kriteria Peringatan

Kuning: Bucket berkemampuan versi Amazon S3 dengan tidak memiliki kebijakan siklus hidup yang dikonfigurasi.

Tindakan yang Direkomendasikan

Konfigurasikan kebijakan siklus hidup untuk bucket Amazon S3 Anda untuk mengelola objek sehingga disimpan secara efektif sepanjang siklus hidupnya.

Untuk informasi selengkapnya, lihat Menyetel konfigurasi siklus hidup pada bucket.

Sumber Daya Tambahan

Mengelola siklus hidup penyimpanan

Menyetel konfigurasi siklus hidup pada bucket

Kolom laporan

- Status
- Wilayah
- Sumber daya
- AWS ConfigAturan
- Parameter Input

- Waktu Terakhir Diperbarui

Fungsi AWS Lambda dengan Waktu Habis Berlebihan

Deskripsi

Memeriksa fungsi Lambda dengan tingkat batas waktu tinggi yang dapat mengakibatkan biaya tinggi.

Lambda mengenakan biaya berdasarkan waktu berjalan dan jumlah permintaan untuk fungsi Anda. Batas waktu fungsi menghasilkan kesalahan yang dapat menyebabkan percobaan ulang. Mencoba kembali fungsi akan dikenakan biaya permintaan dan waktu pengoperasian tambahan.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

`L4dfs2Q3C3`

Kriteria Peringatan

Kuning: Fungsi di mana > 10% pemanggilan berakhir dengan kesalahan karena batas waktu pada hari tertentu dalam 7 hari terakhir.

Tindakan yang Direkomendasikan

Periksa pencatatan fungsi dan jejak sinar-X untuk menentukan kontributor durasi fungsi tinggi. Terapkan logging dalam kode Anda di bagian yang relevan, seperti sebelum atau sesudah panggilan API atau koneksi database. Secara default, batas waktu klien AWS SDK mungkin lebih lama dari durasi fungsi yang dikonfigurasi. Sesuaikan klien koneksi API dan SDK untuk mencoba lagi atau gagal dalam batas waktu fungsi. Jika durasi yang diharapkan lebih lama dari batas waktu yang dikonfigurasi, Anda dapat meningkatkan pengaturan batas waktu untuk fungsi tersebut. Untuk informasi selengkapnya, lihat Memantau dan memecahkan masalah aplikasi Lambda.

Sumber Daya Tambahan

- Pemantauan dan pemecahan masalah aplikasi Lambda

- Fungsi Lambda Coba Kembali SDK Timeout
- Menggunakan AWS Lambda dengan AWS X-Ray
- Mengakses CloudWatch log Amazon untuk AWS Lambda
- Aplikasi Contoh Prosesor Kesalahan untuk AWS Lambda

Kolom laporan

- Status
- Wilayah
- Fungsi ARN
- Tingkat Batas Waktu Harian Maks
- Tanggal Tarif Batas Waktu Harian Maks
- Rata-rata Tarif Timeout Harian
- Pengaturan Batas Waktu Fungsi (milidetik)
- Biaya Komputasi Harian yang Hilang
- Rata-rata Pemanggilan Harian
- Pemanggilan Hari Ini
- Tingkat Batas Waktu Hari Ini
- Waktu Terakhir Diperbarui

Fungsi AWS Lambda dengan Tingkat Eror Tinggi

Deskripsi

Memeriksa fungsi Lambda dengan tingkat kesalahan tinggi yang dapat mengakibatkan biaya lebih tinggi.

Biaya Lambda didasarkan pada jumlah permintaan dan waktu berjalan agregat untuk fungsi Anda. Kesalahan fungsi dapat menyebabkan percobaan ulang yang menimbulkan biaya tambahan.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

L4dfs2Q3C2

Kriteria Peringatan

Kuning: Fungsi di mana > 10% pemanggilan berakhir dengan kesalahan pada hari tertentu dalam 7 hari terakhir.

Tindakan yang Direkomendasikan

Pertimbangkan pedoman berikut untuk mengurangi kesalahan. Kesalahan fungsi mencakup kesalahan yang dikembalikan oleh kode fungsi dan kesalahan yang dikembalikan oleh runtime fungsi.

Untuk membantu Anda memecahkan masalah kesalahan Lambda, Lambda terintegrasi dengan layanan seperti Amazon dan. CloudWatch AWS X-Ray Anda dapat menggunakan kombinasi log, metrik, alarm, dan penelusuran X-Ray untuk mendeteksi dan mengidentifikasi masalah dengan cepat dalam kode fungsi, API, atau sumber daya lain yang mendukung aplikasi Anda. Untuk informasi selengkapnya, lihat Memantau dan memecahkan masalah aplikasi Lambda.

Untuk informasi selengkapnya tentang penanganan error dengan runtime tertentu, lihat Penanganan kesalahan dan percobaan ulang otomatis. AWS Lambda

Untuk pemecahan masalah tambahan, lihat Memecahkan masalah di Lambda.

Anda juga dapat memilih dari ekosistem alat pemantauan dan observabilitas yang disediakan oleh AWS Lambda mitra. Untuk informasi selengkapnya, lihat AWS LambdaMitra.

Sumber Daya Tambahan

- Penanganan Kesalahan dan Percobaan Ulang Otomatis di AWS Lambda
- Pemantauan dan Pemecahan Masalah Aplikasi Lambda
- Fungsi Lambda Coba Kembali SDK Timeout
- Memecahkan masalah di Lambda
- Kesalahan Pemanggilan API
- Aplikasi Contoh Prosesor Kesalahan untuk AWS Lambda

Kolom laporan

- Status

- Wilayah
- Fungsi ARN
- Tingkat Kesalahan Harian Maks
- Tanggal untuk Tingkat Kesalahan Maks
- Rata-rata Tingkat Kesalahan Harian
- Biaya Komputasi Harian yang Hilang
- Rata-rata Pemanggilan Harian
- Pemanggilan Hari Ini

  Tingkat Kesalahan Hari Ini
- Waktu Terakhir Diperbarui

AWS Lambdafungsi yang disediakan secara berlebihan untuk ukuran memori

Deskripsi

Memeriksa AWS Lambda fungsi yang dipanggil setidaknya sekali selama periode lookback. Pemeriksaan ini memberi tahu Anda jika ada fungsi Lambda Anda yang disediakan secara berlebihan untuk ukuran memori. Bila Anda memiliki fungsi Lambda yang disediakan secara berlebihan untuk ukuran memori, Anda membayar sumber daya yang tidak digunakan. Meskipun beberapa skenario dapat menghasilkan pemanfaatan yang rendah berdasarkan desain, Anda sering dapat menurunkan biaya dengan mengubah konfigurasi memori fungsi Lambda Anda. Perkiraan penghematan bulanan dihitung dengan menggunakan tingkat penggunaan saat ini untuk fungsi Lambda.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

`COr6dfpM05`

Kriteria Peringatan

Kuning: Fungsi Lambda yang disediakan secara berlebihan untuk ukuran memori selama periode lookback. Untuk menentukan apakah fungsi Lambda terlalu disediakan, kami mempertimbangkan semua metrik default CloudWatch untuk fungsi tersebut. Algoritma yang digunakan untuk mengidentifikasi fungsi Lambda yang disediakan secara berlebihan untuk ukuran memori mengikuti praktik terbaik. AWS Algoritma diperbarui ketika pola baru telah diidentifikasi.

Tindakan yang Direkomendasikan

Pertimbangkan untuk mengurangi ukuran memori fungsi Lambda Anda.

Untuk informasi selengkapnya, lihat Ikut serta AWS Compute Optimizer untuk Trusted Advisor cek.

Kolom laporan

- Status
- Wilayah
- Nama Fungsi
- Versi Fungsi
- Ukuran Memori (MB)
- Ukuran Memori yang Direkomendasikan (MB)
- Periode Lookback (hari)
- Peluang Tabungan (%)
- Perkiraan Tabungan Bulanan
- Estimasi Mata Uang Tabungan Bulanan
- Waktu Terakhir Diperbarui

AWS Well-Architectedmasalah risiko tinggi untuk optimalisasi biaya

Deskripsi

Memeriksa masalah risiko tinggi (HRI) untuk beban kerja Anda di pilar pengoptimalan biaya. Pemeriksaan ini didasarkan pada AWS-Well Architected ulasan Anda. Hasil pemeriksaan Anda tergantung pada apakah Anda menyelesaikan evaluasi beban kerja denganAWS Well-Architected.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

`Wxdfp4B1L1`

Kriteria Peringatan

- Merah: Setidaknya satu masalah risiko tinggi aktif diidentifikasi dalam pilar optimasi biaya untuk AWS Well-Architected.
- Hijau: Tidak ada masalah risiko tinggi aktif yang terdeteksi dalam pilar optimasi biaya untuk AWS Well-Architected.

Tindakan yang Direkomendasikan

AWSWell-Architected mendeteksi masalah risiko tinggi selama evaluasi beban kerja Anda. Masalah-masalah ini menghadirkan peluang untuk mengurangi risiko dan menghemat uang. Masuk ke alat AWSWell-Architected untuk meninjau jawaban Anda dan mengambil tindakan untuk menyelesaikan masalah aktif Anda.

Kolom laporan

- Status
- Wilayah
- Beban Kerja ARN
- Nama Beban Kerja
- Nama Pengulas
- Jenis Beban Kerja
- Tanggal Mulai Beban Kerja
- Beban Kerja Tanggal Modifikasi Terakhir
- Jumlah HRI yang diidentifikasi untuk Optimalisasi Biaya
- Jumlah HRI yang diselesaikan untuk Optimalisasi Biaya
- Jumlah pertanyaan yang dijawab untuk Optimalisasi Biaya

- Jumlah total pertanyaan dalam pilar Optimasi Biaya
- Waktu Terakhir Diperbarui

Penyeimbang Beban Idle

Deskripsi

Memeriksa konfigurasi Elastic Load Balancing Anda untuk penyeimbang beban yang menganggur.

Setiap penyeimbang beban yang dikonfigurasi akan dikenakan biaya. Jika penyeimbang beban tidak memiliki instance back-end terkait, atau jika lalu lintas jaringan sangat terbatas, penyeimbang beban tidak digunakan secara efektif. Pemeriksaan ini saat ini hanya memeriksa jenis Classic Load Balancer dalam layanan ELB. Tidak termasuk jenis ELB lainnya (Application Load Balancer, Network Load Balancer).

ID pemeriksaan

`hjLMh88uM8`

Kriteria Peringatan

- Kuning: Load balancer tidak memiliki instans back-end aktif.
- Kuning: Penyeimbang beban tidak memiliki instance back-end yang sehat.
- Kuning: Penyeimbang beban memiliki kurang dari 100 permintaan per hari selama 7 hari terakhir.

Tindakan yang Direkomendasikan

Jika penyeimbang beban Anda tidak memiliki instans back-end aktif, pertimbangkan untuk mendaftarkan instans atau menghapus penyeimbang beban Anda. Lihat Mendaftarkan Instans Amazon EC2 Anda dengan Load Balancer atau Hapus Load Balancer Anda.

Jika load balancer Anda tidak memiliki instans back-end yang sehat, lihat Memecahkan Masalah Elastic Load Balancing: Health Check Configuration.

Jika penyeimbang beban Anda memiliki jumlah permintaan yang rendah, pertimbangkan untuk menghapus penyeimbang beban Anda. Lihat Menghapus Load Balancer Anda.

Sumber Daya Tambahan

- Mengelola Load Balancer

- Memecahkan Masalah Elastic Load Balancing

Kolom laporan

- Wilayah
- Nama Load Balancer
- Alasan
- Perkiraan Tabungan Bulanan

Instans Amazon EC2 Penggunaan Rendah

Deskripsi

Memeriksa instans Amazon Elastic Compute Cloud (Amazon EC2) yang berjalan kapan saja selama 14 hari terakhir. Pemeriksaan ini memberi tahu Anda jika penggunaan CPU harian adalah 10% atau kurang dan I/O jaringan adalah 5 MB atau kurang selama setidaknya 4 hari.

Instans yang berjalan menghasilkan biaya penggunaan per jam. Meskipun beberapa skenario dapat menghasilkan pemanfaatan yang rendah berdasarkan desain, Anda sering dapat menurunkan biaya dengan mengelola jumlah dan ukuran instans Anda.

Perkiraan penghematan bulanan dihitung dengan menggunakan tingkat penggunaan saat ini untuk Instans Sesuai Permintaan dan perkiraan jumlah hari instans mungkin kurang dimanfaatkan. Penghematan aktual akan bervariasi jika Anda menggunakan Instans Cadangan atau Instans Spot, atau jika instans tidak berjalan selama sehari penuh. Untuk mendapatkan data pemanfaatan harian, unduh laporan untuk pemeriksaan ini.

ID pemeriksaan

`Qch7DwouX1`

Kriteria Peringatan

Kuning: Sebuah instance memiliki 10% atau kurang penggunaan CPU rata-rata harian dan 5 MB atau kurang jaringan I/O pada setidaknya 4 dari 14 hari sebelumnya.

Tindakan yang Direkomendasikan

Pertimbangkan untuk menghentikan atau menghentikan instance yang memiliki pemanfaatan rendah, atau skala jumlah instance dengan menggunakan Auto Scaling. Untuk informasi selengkapnya, lihat Menghentikan dan Memulai Instance Anda, Menghentikan Instans Anda, dan Apa itu Auto Scaling?

Sumber Daya Tambahan

- Pemantauan Amazon EC2
- Metadata Instance dan Data Pengguna
- Panduan CloudWatch Pengguna Amazon
- Panduan Pengembang Auto Scaling

Kolom laporan

- Wilayah/AZ
- ID instans
- Nama Instance
- Tipe Instans
- Perkiraan Tabungan Bulanan
- Pemanfaatan CPU Rata-rata 14 hari
- Jaringan I/O Rata-rata 14 Hari
- Jumlah Hari Pemanfaatan Rendah

Savings Plan

Deskripsi

Memeriksa penggunaan Amazon EC2, Fargate, dan Lambda selama 30 hari terakhir dan memberikan rekomendasi pembelian Savings Plan. Rekomendasi ini memungkinkan Anda untuk berkomitmen pada jumlah penggunaan yang konsisten yang diukur dalam dolar per jam untuk jangka waktu satu atau tiga tahun dengan imbalan tarif diskon.

Ini bersumber dari AWS Cost Explorer, yang bisa mendapatkan informasi rekomendasi lebih rinci. Anda juga dapat membeli paket tabungan melalui Cost Explorer. Rekomendasi ini harus dianggap sebagai alternatif untuk rekomendasi RI Anda. Kami menyarankan Anda bertindak berdasarkan satu set rekomendasi saja. Bertindak pada kedua set dapat menyebabkan komitmen berlebihan.

Pemeriksaan ini tidak tersedia untuk akun yang ditautkan dalam penagihan gabungan. Rekomendasi untuk cek ini hanya tersedia untuk akun pembayaran.

ID pemeriksaan

`vZ2c2W1srf`

Kriteria Peringatan

Kuning: Mengoptimalkan pembelian Savings Plans dapat membantu mengurangi biaya.

Tindakan yang Direkomendasikan

Lihat halaman Cost Explorer untuk rekomendasi yang lebih detail dan disesuaikan serta untuk membeli Savings Plans.

Sumber Daya Tambahan

- Panduan Pengguna Savings Plan
- FAQ Savings Plans

Kolom laporan

- Jenis Savings Plan
- Opsi pembayaran
- Biaya dimuka
- Komitmen per jam untuk membeli
- Perkiraan pemanfaatan rata-rata
- Perkiraan penghematan bulanan
- Perkiraan persentase penghematan
- Jangka Waktu (Tahun)
- Periode Lookback (Hari)

Alamat IP Elastis yang Tidak Terkait

Deskripsi

Memeriksa alamat IP Elastis (EIP) yang tidak terkait dengan instans Amazon Elastic Compute Cloud (Amazon EC2) yang sedang berjalan.

EIP adalah alamat IP statis yang dirancang untuk komputasi awan dinamis. Tidak seperti alamat IP statis tradisional, EIP menutupi kegagalan instance atau Availability Zone dengan memetakan ulang alamat IP publik ke instance lain di akun Anda. Biaya nominal dikenakan untuk EIP yang tidak terkait dengan instance yang sedang berjalan.

ID pemeriksaan

`Z4AUBRNSmz`

Kriteria Peringatan

Kuning: Alamat IP Elastis (EIP) yang dialokasikan tidak terkait dengan instans Amazon EC2 yang sedang berjalan.

Tindakan yang Direkomendasikan

Kaitkan EIP dengan instance aktif yang sedang berjalan, atau lepaskan EIP yang tidak terkait. Untuk informasi selengkapnya, lihat Mengaitkan Alamat IP Elastis dengan Instans Berjalan yang Berbeda dan Melepaskan Alamat IP Elastis.

Sumber Daya Tambahan

Alamat IP Elastis

Kolom laporan

- Wilayah
- Alamat IP

Volume Amazon EBS yang Kurang Digunakan

Deskripsi

Memeriksa konfigurasi volume Amazon Elastic Block Store (Amazon EBS) dan memperingatkan ketika volume tampaknya kurang dimanfaatkan.

Biaya dimulai saat volume dibuat. Jika volume tetap tidak terikat atau memiliki aktivitas tulis yang sangat rendah (tidak termasuk volume boot) untuk jangka waktu tertentu, volume tersebut kurang dimanfaatkan. Kami menyarankan Anda menghapus volume yang kurang dimanfaatkan untuk mengurangi biaya.

ID pemeriksaan

`DAvU99Dc4C`

Kriteria Peringatan

Kuning: Volume tidak terikat atau memiliki kurang dari 1 IOPS per hari selama 7 hari terakhir.

Tindakan yang Direkomendasikan

Pertimbangkan untuk membuat snapshot dan menghapus volume untuk mengurangi biaya. Untuk informasi selengkapnya, lihat Membuat Snapshot Amazon EBS dan Menghapus Volume Amazon EBS.

Sumber Daya Tambahan

- Toko Blok Elastis Amazon (Amazon EBS)
- Memantau Status Volume Anda

Kolom laporan

- Wilayah
- ID Volume
- Nama Volume
- Jenis Volume
- Ukuran Volume
- Biaya Penyimpanan Bulanan
- ID Cuplikan
- Nama Snapshot
- Umur Snapshot

> **Note**
>
> Jika Anda memilih akun AndaAWS Compute Optimizer, kami sarankan Anda menggunakan pemeriksaan volume Amazon EBS yang disediakan secara berlebihan. Untuk informasi selengkapnya, lihat Ikut serta AWS Compute Optimizer untuk Trusted Advisor cek.

Cluster Pergeseran Merah Amazon yang Kurang Digunakan

Deskripsi

Memeriksa konfigurasi Amazon Redshift Anda untuk cluster yang tampaknya kurang dimanfaatkan.

Jika klaster Amazon Redshift tidak memiliki koneksi untuk jangka waktu yang lama, atau menggunakan CPU dalam jumlah rendah, Anda dapat menggunakan opsi berbiaya lebih rendah seperti perampingan cluster, atau mematikan cluster dan mengambil snapshot akhir. Snapshot akhir dipertahankan bahkan setelah Anda menghapus klaster Anda.

ID pemeriksaan

`G31sQ1E9U`

Kriteria Peringatan

- Kuning: Cluster yang sedang berjalan belum memiliki koneksi dalam 7 hari terakhir.
- Kuning: Cluster yang berjalan memiliki kurang dari 5% pemanfaatan CPU rata-rata di seluruh cluster selama 99% dari 7 hari terakhir.

Tindakan yang Direkomendasikan

Pertimbangkan untuk mematikan cluster dan mengambil snapshot terakhir, atau perampingan cluster. Lihat Mematikan dan Menghapus Cluster dan Mengubah Ukuran Cluster.

Sumber Daya Tambahan

Panduan CloudWatch Pengguna Amazon

Kolom laporan

- Status
- Wilayah
- Klaster
- Tipe Instans
- Alasan
- Perkiraan Tabungan Bulanan

Kinerja

Tingkatkan kinerja layanan Anda dengan memeriksa kuota layanan Anda (sebelumnya disebut sebagai batas), sehingga Anda dapat memanfaatkan throughput yang disediakan, memantau instance yang digunakan secara berlebihan, dan mendeteksi sumber daya yang tidak digunakan.

Anda dapat menggunakan pemeriksaan berikut untuk kategori kinerja.

Periksa nama

- Cluster Amazon Aurora DB kurang disediakan untuk beban kerja baca
- Auto Scaling Amazon DynamoDB Tidak Diaktifkan
- Optimasi Amazon EBS Tidak Diaktifkan
- Konfigurasi Lampiran Volume IOPS (SSD) Amazon EBS
- Volume Amazon EBS yang kurang disediakan
- Grup Auto Scaling Amazon EC2 Tidak Terkait dengan Template Peluncuran

- Optimasi Throughput Amazon EC2 ke EBS
- Jenis Virtualisasi EC2 adalah Paravirtual
- Batas Keras Memori Amazon ECS
- Optimasi Mode Throughput Amazon EFS
- Parameter autovacuum Amazon RDS dimatikan
- Cluster Amazon RDS DB hanya mendukung volume hingga 64 TiB
- Instans Amazon RDS DB di cluster dengan kelas instans heterogen
- Instans Amazon RDS DB di cluster dengan ukuran instans heterogen
- Parameter memori Amazon RDS DB menyimpang dari default
- Amazon RDS enable_indexonlyscan parameter dimatikan
- Parameter Amazon RDS enable_indexscan dimatikan
- Parameter Amazon RDS general_logging diaktifkan
- Parameter Amazon RDS InnoDB_CHANGE_Buffering menggunakan kurang dari nilai optimal
- Parameter Amazon RDS innodb_open_files rendah
- Parameter Amazon RDS innodb_stats_persistent dimatikan
- Instans Amazon RDS kurang disediakan untuk kapasitas sistem
- Volume magnetik Amazon RDS sedang digunakan
- Grup parameter Amazon RDS tidak menggunakan halaman besar
- Parameter cache kueri Amazon RDS diaktifkan
- Pembaruan kelas instans sumber daya Amazon RDS diperlukan
- Sumber daya Amazon RDS pembaruan versi utama diperlukan
- Sumber daya Amazon RDS menggunakan akhir edisi mesin dukungan di bawah lisensi yang disertakan
- Amazon Route 53 Alias Resource Record Set
- AWS Lambda fungsi yang kurang disediakan untuk ukuran memori
- AWS Lambda Fungsi tanpa Batas Konkurensi Dikonfigurasi
- AWS Well-Architectedmasalah risiko tinggi untuk kinerja
- CloudFront Nama Domain Alternatif
- CloudFront Optimasi Pengiriman Konten
- CloudFront Penerusan Header dan Rasio Hit Cache

- Instans Amazon EC2 Pemanfaatan Tinggi

Cluster Amazon Aurora DB kurang disediakan untuk beban kerja baca

Deskripsi

Memeriksa apakah klaster Amazon Aurora DB memiliki sumber daya untuk mendukung beban kerja baca.

ID pemeriksaan

`c1qf5bt038`

Kriteria Peringatan

Kuning:

Peningkatan pembacaan basis data: Beban database tinggi dan database membaca lebih banyak baris daripada menulis atau memperbarui baris.

Tindakan yang Direkomendasikan

Sebaiknya Anda menyetel kueri untuk mengurangi beban database atau menambahkan instans DB pembaca ke cluster DB Anda dengan kelas dan ukuran instans yang sama dengan instans DB penulis di cluster. Konfigurasi saat ini memiliki setidaknya satu instans DB dengan beban database yang terus menerus tinggi yang sebagian besar disebabkan oleh operasi baca. Distribusikan operasi ini dengan menambahkan instans DB lain ke cluster dan mengarahkan beban kerja baca ke titik akhir read-only cluster DB.

Sumber Daya Tambahan

Cluster Aurora DB memiliki satu titik akhir pembaca untuk koneksi hanya-baca. Endpoint ini menggunakan load balancing untuk mengelola kueri yang berkontribusi paling besar terhadap pemuatan basis data di cluster DB Anda. Titik akhir pembaca mengarahkan pernyataan ini ke Aurora Read Replicas dan mengurangi beban pada instance utama. Titik akhir pembaca juga menskalakan kapasitas untuk menangani kueri SELECT bersamaan dengan jumlah Aurora Read Replicas di cluster.

Untuk informasi selengkapnya, lihat Menambahkan Replika Aurora ke Cluster DB serta Mengelola kinerja dan penskalaan untuk klaster Aurora DB.

Laporkan kolom

- Status

- Wilayah
- Sumber Daya
- Peningkatan pembacaan basis data (hitungan)
- Periode deteksi terakhir
- Waktu Terakhir Diperbarui

Auto Scaling Amazon DynamoDB Tidak Diaktifkan

Deskripsi

Memeriksa apakah tabel Amazon DynamoDB dan indeks sekunder global telah mengaktifkan penskalaan otomatis atau sesuai permintaan.

Penskalaan otomatis Amazon DynamoDB menggunakan layanan Application Auto Scaling untuk secara dinamis menyesuaikan kapasitas throughput yang disediakan atas nama Anda sebagai respons terhadap pola lalu lintas yang sebenarnya. Layanan ini memungkinkan tabel atau indeks sekunder global meningkatkan kapasitas baca dan tulis tersedia untuk menangani peningkatan lalu lintas yang mendadak, tanpa throttling. Ketika beban kerja berkurang, Application Auto Scaling dapat menurunkan throughput agar Anda tidak membayar kapasitas tersedia yang tidak terpakai.

Anda dapat menyesuaikan konfigurasi cek menggunakan parameter dalam AWS Config aturan Anda.

Untuk informasi selengkapnya, lihat Mengelola kapasitas throughput secara otomatis dengan penskalaan otomatis DynamoDB.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

`c18d2gz136`

Sumber

AWS Config Aturan Terkelola: dynamodb-autoscaling-enabled

Kriteria Peringatan

Kuning: Penskalaan otomatis tidak diaktifkan untuk tabel DynamoDB dan/atau indeks sekunder global Anda.

Tindakan yang Direkomendasikan

Kecuali Anda sudah memiliki mekanisme untuk secara otomatis menskalakan throughput yang disediakan dari tabel DynamoDB Anda dan/atau indeks sekunder global berdasarkan persyaratan beban kerja Anda, pertimbangkan untuk mengaktifkan penskalaan otomatis untuk tabel Amazon DynamoDB Anda.

Untuk informasi selengkapnya, lihat Menggunakan AWS Management Console dengan DynamoDB auto scalingp.

Sumber Daya Tambahan

Mengelola kapasitas throughput secara otomatis dengan penskalaan otomatis DynamoDB

Laporkan kolom

- Status
- Wilayah
- Sumber Daya
- AWS Config Aturan
- Parameter Input
- Waktu Terakhir Diperbarui

Optimasi Amazon EBS Tidak Diaktifkan

Deskripsi

Memeriksa apakah pengoptimalan Amazon EBS diaktifkan untuk instans Amazon EC2 Anda.

Instans Amazon EBS yang dioptimalkan menggunakan tumpukan konfigurasi yang dioptimalkan dan menyediakan kapasitas tambahan khusus untuk Amazon EBS I/O. Pengoptimalan ini

memberikan kinerja terbaik untuk volume Amazon EBS Anda dengan meminimalkan perselisihan antara Amazon EBS I/O dan lalu lintas lain dari instans Anda..

Untuk informasi selengkapnya, lihat Instans yang dioptimalkan Amazon EBS.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

`c18d2gz142`

Sumber

AWS Config Aturan Terkelola: ebs-optimized-instance

Kriteria Peringatan

Kuning: Optimasi Amazon EBS tidak diaktifkan pada instans Amazon EC2 yang didukung.

Tindakan yang Direkomendasikan

Aktifkan pengoptimalan Amazon EBS pada instans yang didukung.

Untuk informasi selengkapnya, lihat Mengaktifkan pengoptimalan EBS saat peluncuran.

Sumber Daya Tambahan

Amazon EBS — Instans yang dioptimalkan

Laporkan kolom

- Status
- Wilayah
- Sumber Daya
- AWS Config Aturan
- Parameter Input
- Waktu Terakhir Diperbarui

Konfigurasi Lampiran Volume IOPS (SSD) Amazon EBS

Deskripsi

Memeriksa volume IOPS (SSD) yang disediakan yang dilampirkan ke instans Amazon Elastic Compute Cloud (Amazon EC2) Amazon EBS yang dapat dioptimalkan yang tidak dioptimalkan oleh EBS.

Volume IOPS (SSD) yang disediakan di Amazon Elastic Block Store (Amazon EBS) dirancang untuk memberikan kinerja yang diharapkan hanya jika dipasang ke instans yang dioptimalkan EBS.

ID pemeriksaan

`PPkZrjsH2q`

Kriteria Peringatan

Kuning: Instans Amazon EC2 yang dapat dioptimalkan EBS memiliki volume IOPS (SSD) Terpasang tetapi instancenya tidak dioptimalkan oleh EBS.

Tindakan yang Direkomendasikan

Buat instance baru yang dioptimalkan EBS, lepaskan volume, dan pasang kembali volume ke instance baru Anda. Untuk informasi selengkapnya, lihat Instans yang dioptimalkan Amazon EBS dan Melampirkan Volume Amazon EBS ke Instance.

Sumber Daya Tambahan

- Jenis Volume Amazon EBS
- Kinerja Volume Amazon EBS

Laporkan kolom

- Status
- Wilayah/AZ
- ID Volume
- Nama Volume
- Lampiran Volume
- ID Instans
- Tipe Instans
- EBS Dioptimalkan

Volume Amazon EBS yang kurang disediakan

Deskripsi

Memeriksa volume Amazon Elastic Block Store (Amazon EBS) yang berjalan kapan saja selama periode lookback. Pemeriksaan ini memberi tahu Anda jika ada volume EBS yang kurang disediakan untuk beban kerja Anda. Pemanfaatan tinggi yang konsisten dapat menunjukkan kinerja yang optimal dan stabil, tetapi juga dapat menunjukkan bahwa aplikasi tidak memiliki sumber daya yang cukup.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

`COr6dfpM04`

Kriteria Peringatan

Kuning: Volume EBS yang kurang disediakan selama periode lookback. Untuk menentukan apakah volume kurang disediakan, kami mempertimbangkan semua CloudWatch metrik default (termasuk IOPS dan throughput). Algoritma yang digunakan untuk mengidentifikasi volume EBS yang kurang disediakan mengikuti praktik terbaik. AWS Algoritma diperbarui ketika pola baru telah diidentifikasi.

Tindakan yang Direkomendasikan

Pertimbangkan peningkatan volume yang memiliki pemanfaatan tinggi.

Untuk informasi selengkapnya, lihat Ikut serta AWS Compute Optimizer untuk Trusted Advisor cek.

Laporkan kolom

- Status
- Wilayah
- ID Volume
- Jenis Volume

- Ukuran Volume (GB)
- Volume Baseline IOPS
- Volume Burst IOPS
- Throughput Volume Burst
- Jenis Volume yang Direkomendasikan
- Ukuran Volume yang Direkomendasikan (GB)
- IOPS Dasar Volume yang Direkomendasikan
- Volume Burst IOPS yang Direkomendasikan
- Throughput Dasar Volume yang Direkomendasikan
- Throughput Volume Burst yang Direkomendasikan
- Periode Lookback (hari)
- Risiko Kinerja
- Waktu Terakhir Diperbarui

Grup Auto Scaling Amazon EC2 Tidak Terkait dengan Template Peluncuran

Deskripsi

Memeriksa apakah grup Auto Scaling Amazon EC2 dibuat dari templat peluncuran Amazon EC2.

Gunakan templat peluncuran untuk membuat grup Auto Scaling Amazon EC2 untuk memastikan akses ke fitur dan peningkatan grup Auto Scaling terbaru. Misalnya, pembuatan versi dan beberapa jenis instance.

Untuk informasi selengkapnya, lihat Meluncurkan templat.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

`c18d2gz102`

Sumber

AWS Config Aturan Terkelola: autoscaling-launch-template

Kriteria Peringatan

Kuning: Grup Auto Scaling Amazon EC2 tidak terkait dengan templat peluncuran yang valid.

Tindakan yang Direkomendasikan

Gunakan template peluncuran Amazon EC2 untuk membuat grup Auto Scaling Amazon EC2 Anda.

Untuk informasi selengkapnya, lihat Membuat template peluncuran untuk grup Auto Scaling.

Sumber Daya Tambahan

- Luncurkan template
- Buat template peluncuran

Laporkan kolom

- Status
- Wilayah
- Sumber Daya
- AWS Config Aturan
- Parameter Input
- Waktu Terakhir Diperbarui

Optimasi Throughput Amazon EC2 ke EBS

Deskripsi

Memeriksa volume Amazon EBS yang kinerjanya mungkin dipengaruhi oleh kemampuan throughput maksimum instans Amazon EC2 yang dilampirkan.

Untuk mengoptimalkan kinerja, Anda harus memastikan bahwa throughput maksimum instans Amazon EC2 lebih besar daripada throughput maksimum agregat volume EBS terlampir. Pemeriksaan ini menghitung total throughput volume EBS untuk setiap periode lima menit pada hari sebelumnya (berdasarkan Coordinated Universal Time (UTC)) untuk setiap instans yang dioptimalkan EBS dan memberi tahu Anda jika penggunaan di lebih dari setengah periode tersebut lebih besar dari 95% dari throughput maksimum instans EC2.

ID pemeriksaan

Bh2xRR2FGH

Kriteria Peringatan

Kuning: Pada hari sebelumnya (UTC), throughput agregat (megabit/detik) dari volume EBS yang melekat pada instans EC2 melebihi 95% dari throughput yang dipublikasikan antara instance dan volume EBS lebih dari 50% dari waktu.

Tindakan yang Direkomendasikan

Bandingkan throughput maksimum volume Amazon EBS Anda (lihat Jenis Volume Amazon EBS) dengan throughput maksimum instans Amazon EC2 yang dilampirkan. Lihat Jenis Instance yang Mendukung Optimasi EBS.

Pertimbangkan untuk melampirkan volume Anda ke instans yang mendukung throughput yang lebih tinggi ke Amazon EBS untuk kinerja optimal.

Sumber Daya Tambahan

- Jenis Volume Amazon EBS
- Instans Amazon EBS yang Dioptimalkan
- Memantau Status Volume Anda
- Melampirkan Volume Amazon EBS ke Instance
- Melepaskan Volume Amazon EBS dari Instance
- Menghapus Volume Amazon EBS

Laporkan kolom

- Status
- Wilayah
- ID Instans
- Tipe Instans
- Waktu Dekat Maksimum

Jenis Virtualisasi EC2 adalah Paravirtual

Deskripsi

Memeriksa apakah jenis virtualisasi instans Amazon EC2 adalah paravirtual.

Ini adalah praktik terbaik bahwa Anda menggunakan instance Hardware Virtual Machine (HVM) alih-alih instance paravirtual, jika memungkinkan. Ini karena peningkatan virtualisasi HVM dan ketersediaan driver PV untuk AMI HVM, yang telah menutup kesenjangan kinerja yang secara historis ada antara tamu PV dan HVM. Penting untuk dicatat bahwa jenis instans generasi saat ini tidak mendukung AMI PV. Oleh karena itu, memilih jenis instance HVM memberikan kinerja dan kompatibilitas terbaik dengan perangkat keras modern.

Untuk informasi selengkapnya, lihat Jenis virtualisasi Linux AMI.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

`c18d2gz148`

Sumber

AWS Config Aturan Terkelola: ec2-paravirtual-instance-check

Kriteria Peringatan

Kuning: Jenis virtualisasi instans Amazon EC2 bersifat paravirtual.

Tindakan yang Direkomendasikan

Gunakan virtualisasi HVM untuk instans Amazon EC2 Anda, dan gunakan jenis instans yang kompatibel.

Untuk informasi tentang memilih jenis virtualisasi yang sesuai, lihat Kompatibilitas untuk mengubah jenis instance.

Sumber Daya Tambahan

Kompatibilitas untuk mengubah jenis instance

Laporkan kolom

- Status
- Wilayah

- Sumber Daya
- AWS Config Aturan
- Parameter Input
- Waktu Terakhir Diperbarui

Batas Keras Memori Amazon ECS

Deskripsi

Memeriksa apakah definisi tugas Amazon ECS memiliki batas memori yang ditetapkan untuk definisi wadahnya. Jumlah total memori yang disediakan untuk semua kontainer dalam tugas harus lebih rendah dari nilai memori tugas.

Untuk informasi lebih lanjut, lihat Definisi kontainer.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

`c18d2gz176`

Sumber

AWS Config Aturan Terkelola: ecs-task-definition-memory -hard-limit

Kriteria Peringatan

Kuning: Batas keras memori Amazon ECS tidak diatur.

Tindakan yang Direkomendasikan

Alokasikan memori untuk tugas Amazon ECS Anda agar tidak kehabisan memori. Jika penampung Anda mencoba melebihi memori yang ditentukan, maka penampung akan dihentikan.

Untuk informasi selengkapnya, lihat Bagaimana cara mengalokasikan memori ke tugas di Amazon ECS? .

Sumber Daya Tambahan

Reservasi cluster

Laporkan kolom

- Status
- Wilayah
- Sumber Daya
- AWS Config Aturan
- Parameter Input
- Waktu Terakhir Diperbarui

Optimasi Mode Throughput Amazon EFS

Deskripsi

Memeriksa apakah sistem file Amazon EFS pelanggan saat ini dikonfigurasi untuk menggunakan mode Bursting Throughput.

Sistem file dalam mode Bursting Throughput EFS [1] memberikan tingkat throughput dasar yang konsisten (50 Kib/s per GiB data dalam penyimpanan EFS Standard), dan menggunakan model kredit untuk memberikan tingkat kinerja “burst throughput” yang lebih tinggi ketika “kredit burst” tersedia. Ketika Anda menghabiskan kredit burst Anda, kinerja sistem file Anda dibatasi ke tingkat dasar yang lebih rendah ini, yang dapat mengakibatkan kelambatan, batas waktu, atau bentuk dampak kinerja lainnya untuk pengguna akhir atau aplikasi Anda.

ID pemeriksaan

`c1dfprch02`

Kriteria Peringatan

- Kuning: Sistem file menggunakan mode throughput Bursting.

Tindakan yang Direkomendasikan

Untuk memungkinkan pengguna dan aplikasi Anda mencapai throughput yang diinginkan, kami sarankan Anda memperbarui konfigurasi sistem file Anda ke mode Elastic Throughput [2]. Saat dalam mode Elastic Throughput, sistem file Anda dapat mencapai throughput baca hingga 10 Gib/s atau throughput tulis 3 Gib/dtk — tergantung pada Wilayah AWS [3], dan Anda hanya membayar throughput yang Anda gunakan. Harap dicatat bahwa Anda dapat memperbarui

konfigurasi sistem file Anda untuk beralih antara mode throughput Elastic dan Bursting sesuai permintaan, dan Sistem File dalam mode Throughput Elastis akan dikenakan biaya tambahan untuk transfer data [4].

Sumber Daya Tambahan

- [1] Mode Throughput Kinerja Amazon EFS
- [2] Mode Throughput Elastis Kinerja Amazon EFS
- [3] Kuota dan Batas Amazon EFS
- [4] Harga Amazon EFS

Laporkan kolom

- Status
- Wilayah
- ID Sistem Berkas EFS
- Mode throughput
- Waktu Terakhir Diperbarui

Parameter autovacuum Amazon RDS dimatikan

Deskripsi

Parameter autovacuum dimatikan untuk instans DB Anda. Mematikan autovacuum meningkatkan tabel dan indeks kembung dan berdampak pada kinerja.

Kami menyarankan Anda mengaktifkan autovacuum di grup parameter DB Anda.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

> **Note**
>
> Ketika instans DB atau kluster DB dihentikan, Anda dapat melihat rekomendasi Amazon RDS Trusted Advisor selama 3 hingga 5 hari. Setelah lima hari, rekomendasi tidak

tersedia di Trusted Advisor. Untuk melihat rekomendasi, buka konsol Amazon RDS, lalu pilih Rekomendasi.
Jika Anda menghapus instans DB atau kluster DB, maka rekomendasi yang terkait dengan instans atau cluster tersebut tidak tersedia di Trusted Advisor atau konsol manajemen Amazon RDS.

ID pemeriksaan

`c1qf5bt025`

Kriteria Peringatan

Kuning: Grup parameter DB memiliki autovacuum dimatikan.

Tindakan yang Direkomendasikan

Aktifkan parameter autovacuum di grup parameter DB Anda.

Sumber Daya Tambahan

Database PostgreSQL membutuhkan pemeliharaan berkala yang dikenal sebagai penyedot debu. Autovacuum di PostgreSQL mengotomatiskan menjalankan perintah VACCUUM dan ANALYSIS. Proses ini mengumpulkan statistik tabel dan menghapus baris mati. Ketika autovacuum dimatikan, peningkatan tabel, indeks kembung, statistik basi akan berdampak pada kinerja database.

Untuk informasi selengkapnya, lihat Memahami autovacuum di Amazon RDS untuk lingkungan PostgreSQL.

Laporkan kolom

- Status
- Wilayah
- Sumber Daya
- Nama Parameter
- Nilai yang Direkomendasikan
- Waktu Terakhir Diperbarui

Cluster Amazon RDS DB hanya mendukung volume hingga 64 TiB

Deskripsi

Cluster DB Anda mendukung volume hingga 64 TiB. Versi mesin terbaru mendukung volume hingga 128 TiB. Kami menyarankan Anda meningkatkan versi mesin cluster DB Anda ke versi terbaru untuk mendukung volume hingga 128 TiB.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

> **Note**
>
> Ketika instans DB atau kluster DB dihentikan, Anda dapat melihat rekomendasi Amazon RDS Trusted Advisor selama 3 hingga 5 hari. Setelah lima hari, rekomendasi tidak tersedia di Trusted Advisor. Untuk melihat rekomendasi, buka konsol Amazon RDS, lalu pilih Rekomendasi.
> Jika Anda menghapus instans DB atau kluster DB, maka rekomendasi yang terkait dengan instans atau cluster tersebut tidak tersedia di Trusted Advisor atau konsol manajemen Amazon RDS.

ID pemeriksaan

`c1qf5bt017`

Kriteria Peringatan

Kuning: Cluster DB memiliki dukungan untuk volume hanya hingga 64 TiB.

Tindakan yang Direkomendasikan

Tingkatkan versi mesin cluster DB Anda untuk mendukung volume hingga 128 TiB.

Sumber Daya Tambahan

Ketika Anda meningkatkan aplikasi Anda pada satu cluster Amazon Aurora DB, Anda mungkin tidak mencapai batas jika batas penyimpanan 128 TiB. Batas penyimpanan yang meningkat membantu menghindari penghapusan data atau pemisahan database di beberapa instance.

Untuk informasi selengkapnya, lihat batas ukuran Amazon Aurora.

Laporkan kolom

- Status
- Wilayah
- Sumber Daya
- Nama Mesin
- Versi Mesin Saat Ini
- Nilai yang Direkomendasikan
- Waktu Terakhir Diperbarui

Instans Amazon RDS DB di cluster dengan kelas instans heterogen

Deskripsi

Kami menyarankan Anda menggunakan kelas dan ukuran instans DB yang sama untuk semua instans DB di cluster DB Anda.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

> **Note**
>
> Ketika instans DB atau kluster DB dihentikan, Anda dapat melihat rekomendasi Amazon RDS Trusted Advisor selama 3 hingga 5 hari. Setelah lima hari, rekomendasi tidak tersedia di Trusted Advisor. Untuk melihat rekomendasi, buka konsol Amazon RDS, lalu pilih Rekomendasi.

Jika Anda menghapus instans DB atau kluster DB, maka rekomendasi yang terkait dengan instans atau cluster tersebut tidak tersedia di Trusted Advisor atau konsol manajemen Amazon RDS.

ID pemeriksaan

`c1qf5bt009`

Kriteria Peringatan

Merah: Cluster DB memiliki instance DB dengan kelas instance heterogen.

Tindakan yang Direkomendasikan

Gunakan kelas dan ukuran instance yang sama untuk semua instans DB di cluster DB Anda.

Sumber Daya Tambahan

Ketika instans DB di cluster DB Anda menggunakan kelas atau ukuran instans DB yang berbeda, mungkin ada ketidakseimbangan dalam beban kerja untuk instans DB. Selama failover, salah satu instance DB pembaca berubah menjadi instance DB penulis. Jika instans DB menggunakan kelas dan ukuran instans DB yang sama, beban kerja dapat diseimbangkan untuk instans DB di cluster DB Anda.

Untuk informasi lebih lanjut, lihat Replika Aurora.

Laporkan kolom

- Status
- Wilayah
- Sumber Daya
- Nilai yang Direkomendasikan
- Nama Mesin
- Waktu Terakhir Diperbarui

Instans Amazon RDS DB di cluster dengan ukuran instans heterogen

Deskripsi

Kami menyarankan Anda menggunakan kelas dan ukuran instans DB yang sama untuk semua instans DB di cluster DB Anda.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

> **Note**
>
> Ketika instans DB atau kluster DB dihentikan, Anda dapat melihat rekomendasi Amazon RDS Trusted Advisor selama 3 hingga 5 hari. Setelah lima hari, rekomendasi tidak tersedia di Trusted Advisor. Untuk melihat rekomendasi, buka konsol Amazon RDS, lalu pilih Rekomendasi.
> Jika Anda menghapus instans DB atau kluster DB, maka rekomendasi yang terkait dengan instans atau cluster tersebut tidak tersedia di Trusted Advisor atau konsol manajemen Amazon RDS.

ID pemeriksaan

`c1qf5bt008`

Kriteria Peringatan

Merah: Cluster DB memiliki instans DB dengan ukuran instans heterogen.

Tindakan yang Direkomendasikan

Gunakan kelas dan ukuran instance yang sama untuk semua instans DB di cluster DB Anda.

Sumber Daya Tambahan

Ketika instans DB di cluster DB Anda menggunakan kelas atau ukuran instans DB yang berbeda, mungkin ada ketidakseimbangan dalam beban kerja untuk instans DB. Selama failover, salah satu instance DB pembaca berubah menjadi instance DB penulis. Jika instans DB menggunakan kelas dan ukuran instans DB yang sama, beban kerja dapat diseimbangkan untuk instans DB di cluster DB Anda.

Untuk informasi lebih lanjut, lihat Replika Aurora.

Laporkan kolom

- Status

- Wilayah
- Sumber Daya
- Nilai yang Direkomendasikan
- Nama Mesin
- Waktu Terakhir Diperbarui

Parameter memori Amazon RDS DB menyimpang dari default

Deskripsi

Parameter memori instans DB berbeda secara signifikan dari nilai default. Pengaturan ini dapat memengaruhi kinerja dan menyebabkan kesalahan.

Kami menyarankan Anda mengatur ulang parameter memori khusus untuk instans DB ke nilai defaultnya di grup parameter DB.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

> **Note**
>
> Ketika instans DB atau kluster DB dihentikan, Anda dapat melihat rekomendasi Amazon RDS Trusted Advisor selama 3 hingga 5 hari. Setelah lima hari, rekomendasi tidak tersedia di Trusted Advisor. Untuk melihat rekomendasi, buka konsol Amazon RDS, lalu pilih Rekomendasi.
> Jika Anda menghapus instans DB atau kluster DB, maka rekomendasi yang terkait dengan instans atau cluster tersebut tidak tersedia di Trusted Advisor atau konsol manajemen Amazon RDS.

ID pemeriksaan

```
c1qf5bt020
```

Kriteria Peringatan

Kuning: Grup parameter DB memiliki parameter memori yang sangat berbeda dari nilai default.

Tindakan yang Direkomendasikan

Setel ulang parameter memori ke nilai defaultnya.

Sumber Daya Tambahan

Untuk mengetahui informasi selengkapnya, lihat Praktik terbaik untuk mengonfigurasi parameter untuk Amazon RDS for MySQL, bagian 1: Parameter yang terkait dengan performa.

Laporkan kolom

- Status
- Wilayah
- Sumber Daya
- Nama Parameter
- Nilai yang Direkomendasikan
- Waktu Terakhir Diperbarui

Amazon RDS enable_indexonlyscan parameter dimatikan

Deskripsi

Perencana kueri atau pengoptimal tidak dapat menggunakan jenis paket pemindaian khusus indeks saat dimatikan.

Kami menyarankan Anda mengatur nilai parameter enable_indexonlyscan ke 1.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

> **Note**
>
> Ketika instans DB atau kluster DB dihentikan, Anda dapat melihat rekomendasi Amazon RDS Trusted Advisor selama 3 hingga 5 hari. Setelah lima hari, rekomendasi tidak tersedia di Trusted Advisor. Untuk melihat rekomendasi, buka konsol Amazon RDS, lalu pilih Rekomendasi.
> Jika Anda menghapus instans DB atau kluster DB, maka rekomendasi yang terkait dengan instans atau cluster tersebut tidak tersedia di Trusted Advisor atau konsol manajemen Amazon RDS.

ID pemeriksaan

`c1qf5bt028`

Kriteria Peringatan

Kuning: Grup parameter DB memiliki parameter enable_indexonlyscan dimatikan.

Tindakan yang Direkomendasikan

Setel parameter enable_indexonlyscan ke 1.

Sumber Daya Tambahan

Saat Anda mematikan parameter enable_indexonlyscan, ini mencegah perencana kueri memilih rencana eksekusi yang optimal. Perencana kueri menggunakan jenis rencana yang berbeda, seperti pemindaian indeks yang dapat meningkatkan biaya kueri dan waktu eksekusi. Indeks hanya jenis rencana pemindaian mengambil data tanpa mengakses data tabel.

Untuk informasi selengkapnya, lihat enable_indexonlyscan (boolean) di situs dokumentasi PostgreSQL.

Laporkan kolom

- Status
- Wilayah
- Sumber Daya
- Nama Parameter
- Nilai yang Direkomendasikan

- Waktu Terakhir Diperbarui

Parameter Amazon RDS enable_indexscan dimatikan

Deskripsi

Perencana kueri atau pengoptimal tidak dapat menggunakan jenis rencana pemindaian indeks saat dimatikan.

Kami menyarankan Anda mengatur nilai parameter enable_indexscan ke 1.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

> **Note**
>
> Ketika instans DB atau kluster DB dihentikan, Anda dapat melihat rekomendasi Amazon RDS Trusted Advisor selama 3 hingga 5 hari. Setelah lima hari, rekomendasi tidak tersedia di Trusted Advisor. Untuk melihat rekomendasi, buka konsol Amazon RDS, lalu pilih Rekomendasi.
> Jika Anda menghapus instans DB atau kluster DB, maka rekomendasi yang terkait dengan instans atau cluster tersebut tidak tersedia di Trusted Advisor atau konsol manajemen Amazon RDS.

ID pemeriksaan

`c1qf5bt029`

Kriteria Peringatan

Kuning: Grup parameter DB memiliki parameter enable_indexscan dimatikan.

Tindakan yang Direkomendasikan

Setel parameter enable_indexscan ke 1.

Sumber Daya Tambahan

Saat Anda mematikan parameter enable_indexscan, ini mencegah perencana kueri memilih rencana eksekusi yang optimal. Perencana kueri menggunakan jenis rencana yang berbeda, seperti pemindaian indeks yang dapat meningkatkan biaya kueri dan waktu eksekusi.

Untuk informasi selengkapnya, lihat enable_indexscan (boolean) di situs dokumentasi PostgreSQL.

Laporkan kolom

- Status
- Wilayah
- Sumber Daya
- Nama Parameter
- Nilai yang Direkomendasikan
- Waktu Terakhir Diperbarui

Parameter Amazon RDS general_logging diaktifkan

Deskripsi

Pencatatan umum diaktifkan untuk instans DB Anda. Pengaturan ini berguna saat memecahkan masalah database. Namun, menyalakan logging umum meningkatkan jumlah operasi I/O dan ruang penyimpanan yang dialokasikan, yang dapat mengakibatkan pertengkaran dan penurunan kinerja.

Periksa persyaratan Anda untuk penggunaan logging umum. Kami menyarankan Anda mengatur nilai parameter general_logging ke 0.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

> **Note**
>
> Ketika instans DB atau kluster DB dihentikan, Anda dapat melihat rekomendasi Amazon RDS Trusted Advisor selama 3 hingga 5 hari. Setelah lima hari, rekomendasi tidak tersedia di Trusted Advisor. Untuk melihat rekomendasi, buka konsol Amazon RDS, lalu pilih Rekomendasi.
> Jika Anda menghapus instans DB atau kluster DB, maka rekomendasi yang terkait dengan instans atau cluster tersebut tidak tersedia di Trusted Advisor atau konsol manajemen Amazon RDS.

ID pemeriksaan

`c1qf5bt037`

Kriteria Peringatan

Kuning: Grup parameter DB mengaktifkan general_logging.

Tindakan yang Direkomendasikan

Periksa persyaratan Anda untuk penggunaan logging umum. Jika tidak wajib, kami sarankan Anda untuk mengatur nilai parameter general_logging ke 0.

Sumber Daya Tambahan

Log kueri umum diaktifkan ketika nilai parameter general_logging adalah 1. Log query umum berisi catatan operasi server database. Server menulis informasi ke log ini ketika klien terhubung atau memutuskan sambungan dan log berisi setiap pernyataan SQL yang diterima dari klien. Log kueri umum berguna ketika Anda mencurigai adanya kesalahan pada klien dan Anda ingin menemukan informasi yang akan dikirim klien ke server database.

Untuk informasi selengkapnya, lihat Ikhtisar RDS untuk log database MySQL.

Laporkan kolom

- Status
- Wilayah
- Sumber Daya
- Nama Parameter
- Nilai yang Direkomendasikan
- Waktu Terakhir Diperbarui

Parameter Amazon RDS InnoDB_CHANGE_Buffering menggunakan kurang dari nilai optimal

Deskripsi

Perubahan buffering memungkinkan instance MySQL DB untuk menunda beberapa penulisan, yang diperlukan untuk mempertahankan indeks sekunder. Fitur ini berguna di lingkungan dengan disk lambat. Konfigurasi buffering perubahan sedikit meningkatkan kinerja DB tetapi menyebabkan penundaan pemulihan kerusakan dan waktu shutdown yang lama selama peningkatan.

Kami menyarankan Anda mengatur nilai parameter innodb_change_buffering ke NONE.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

> **Note**
>
> Ketika instans DB atau kluster DB dihentikan, Anda dapat melihat rekomendasi Amazon RDS Trusted Advisor selama 3 hingga 5 hari. Setelah lima hari, rekomendasi tidak tersedia di Trusted Advisor. Untuk melihat rekomendasi, buka konsol Amazon RDS, lalu pilih Rekomendasi.
> Jika Anda menghapus instans DB atau kluster DB, maka rekomendasi yang terkait dengan instans atau cluster tersebut tidak tersedia di Trusted Advisor atau konsol manajemen Amazon RDS.

ID pemeriksaan

`c1qf5bt021`

Kriteria Peringatan

Kuning: Grup parameter DB memiliki parameter innodb_change_buffering yang disetel ke nilai optimal rendah.

Tindakan yang Direkomendasikan

Setel nilai parameter innodb_change_buffering ke NONE di grup parameter DB Anda.

Sumber Daya Tambahan

Untuk mengetahui informasi selengkapnya, lihat Praktik terbaik untuk mengonfigurasi parameter untuk Amazon RDS for MySQL, bagian 1: Parameter yang terkait dengan performa.

Laporkan kolom

- Status
- Wilayah
- Sumber Daya
- Nama Parameter
- Nilai yang Direkomendasikan
- Waktu Terakhir Diperbarui

Parameter Amazon RDS innodb_open_files rendah

Deskripsi

Parameter innodb_open_files mengontrol jumlah file yang dapat dibuka InnoDB pada satu waktu. InnoDB membuka semua log dan file tablespace sistem saat mysqld berjalan.

Instans DB Anda memiliki nilai rendah untuk jumlah maksimum file yang dapat dibuka InnoDB pada satu waktu. Kami menyarankan Anda mengatur parameter innodb_open_files ke nilai minimum 65.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

> **Note**
>
> Ketika instans DB atau kluster DB dihentikan, Anda dapat melihat rekomendasi Amazon RDS Trusted Advisor selama 3 hingga 5 hari. Setelah lima hari, rekomendasi tidak

tersedia di Trusted Advisor. Untuk melihat rekomendasi, buka konsol Amazon RDS, lalu pilih Rekomendasi.
Jika Anda menghapus instans DB atau kluster DB, maka rekomendasi yang terkait dengan instans atau cluster tersebut tidak tersedia di Trusted Advisor atau konsol manajemen Amazon RDS.

ID pemeriksaan

`c1qf5bt033`

Kriteria Peringatan

Kuning: Grup parameter DB memiliki pengaturan file terbuka InnoDB salah dikonfigurasi.

Tindakan yang Direkomendasikan

Setel parameter innodb_open_files ke nilai minimum 65.

Sumber Daya Tambahan

Parameter innodb_open_files mengontrol jumlah file yang dapat dibuka InnoDB pada satu waktu. InnoDB menyimpan semua file log dan file tablespace sistem terbuka saat mysqld berjalan. InnoDB juga perlu membuka beberapa file.ibd, jika model file-per-table penyimpanan digunakan. Ketika pengaturan innodb_open_files rendah, itu berdampak pada kinerja database dan server mungkin gagal memulai.

Untuk informasi selengkapnya, lihat Opsi Startup InnoDB dan Variabel Sistem - innodb_open_files di situs dokumentasi. MySql

Kolom laporan

- Status
- Wilayah
- Sumber Daya
- Nama Parameter
- Nilai yang Direkomendasikan
- Waktu Terakhir Diperbarui

Parameter Amazon RDS innodb_stats_persistent dimatikan

Deskripsi

Instans DB Anda tidak dikonfigurasi untuk mempertahankan statistik InnoDB ke disk. Ketika statistik tidak disimpan, mereka dihitung ulang setiap kali instance restart dan tabel diakses. Hal ini menyebabkan variasi dalam rencana eksekusi query. Anda dapat memodifikasi nilai parameter global ini di tingkat tabel.

Kami menyarankan Anda menyetel nilai parameter innodb_stats_persistent ke ON.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

> **Note**
>
> Ketika instans DB atau kluster DB dihentikan, Anda dapat melihat rekomendasi Amazon RDS Trusted Advisor selama 3 hingga 5 hari. Setelah lima hari, rekomendasi tidak tersedia di Trusted Advisor. Untuk melihat rekomendasi, buka konsol Amazon RDS, lalu pilih Rekomendasi.
> Jika Anda menghapus instans DB atau kluster DB, maka rekomendasi yang terkait dengan instans atau cluster tersebut tidak tersedia di Trusted Advisor atau konsol manajemen Amazon RDS.

ID pemeriksaan

`c1qf5bt032`

Kriteria Peringatan

Kuning: Grup parameter DB memiliki statistik pengoptimal yang tidak disimpan ke disk.

Tindakan yang Direkomendasikan

Setel nilai parameter innodb_stats_persistent ke ON.

Sumber Daya Tambahan

Jika parameter innodb_stats_persistent disetel ke ON, maka statistik pengoptimal dipertahankan saat instance dimulai ulang. Ini meningkatkan stabilitas rencana eksekusi dan kinerja kueri yang konsisten. Anda dapat mengubah persistensi statistik global di tingkat tabel dengan menggunakan klausa STATS_PERSISTENT saat Anda membuat atau mengubah tabel.

Untuk mengetahui informasi selengkapnya, lihat Praktik terbaik untuk mengonfigurasi parameter untuk Amazon RDS for MySQL, bagian 1: Parameter yang terkait dengan performa.

Kolom laporan

- Status
- Wilayah
- Sumber Daya
- Nama Parameter
- Nilai yang Direkomendasikan
- Waktu Terakhir Diperbarui

Instans Amazon RDS kurang disediakan untuk kapasitas sistem

Deskripsi

Memeriksa apakah instans Amazon RDS atau instans Amazon Aurora DB memiliki kapasitas sistem yang diperlukan untuk beroperasi.

ID pemeriksaan

`c1qf5bt039`

Kriteria Peringatan

Kuning:

Pembunuhan di luar memori: Ketika proses pada host database dihentikan karena pengurangan memori di tingkat OS, penghitung Out Of Memory (OOM) membunuh penghitung meningkat.

Pertukaran berlebihan: nilai metrik os.memory.swap.in dan os.memory.swap.out tinggi.

Tindakan yang Direkomendasikan

Kami menyarankan Anda menyetel kueri Anda untuk menggunakan lebih sedikit memori atau menggunakan jenis instans DB dengan memori yang dialokasikan lebih tinggi. Ketika instance kehabisan memori, ini berdampak pada kinerja database.

Sumber Daya Tambahan

O ut-of-memory kill terdeteksi: kernel Linux memanggil Out of Memory (OOM) Killer ketika proses yang berjalan pada host membutuhkan lebih dari memori yang tersedia secara fisik dari sistem operasi. Dalam hal ini, OOM Killer meninjau semua proses yang berjalan, dan menghentikan satu atau lebih proses, untuk membebaskan memori sistem dan menjaga sistem tetap berjalan.

Swapping terdeteksi: Ketika memori tidak cukup pada host database, sistem operasi mengirimkan beberapa halaman minimum yang digunakan ke disk di ruang swap. Proses pembongkaran ini berdampak pada kinerja database.

Untuk informasi selengkapnya, lihat Jenis Instans Amazon RDS dan Penskalaan instans Amazon RDS Anda.

Kolom laporan

- Status
- Wilayah
- Sumber Daya
- O ut-of-memory membunuh (menghitung)
- Pertukaran berlebihan (hitung)
- Periode deteksi terakhir
- Waktu Terakhir Diperbarui

Volume magnetik Amazon RDS sedang digunakan

Deskripsi

Instans DB Anda menggunakan penyimpanan magnetik. Penyimpanan magnetik tidak disarankan untuk sebagian besar instans DB. Pilih jenis penyimpanan yang berbeda: General Purpose (SSD) atau Provisioned IOPS.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

> **Note**
>
> Ketika instans DB atau kluster DB dihentikan, Anda dapat melihat rekomendasi Amazon RDS Trusted Advisor selama 3 hingga 5 hari. Setelah lima hari, rekomendasi tidak tersedia di Trusted Advisor. Untuk melihat rekomendasi, buka konsol Amazon RDS, lalu pilih Rekomendasi.
> Jika Anda menghapus instans DB atau kluster DB, maka rekomendasi yang terkait dengan instans atau cluster tersebut tidak tersedia di Trusted Advisor atau konsol manajemen Amazon RDS.

ID pemeriksaan

`c1qf5bt000`

Kriteria Peringatan

Kuning: Sumber daya Amazon RDS menggunakan penyimpanan magnetik.

Tindakan yang Direkomendasikan

Pilih jenis penyimpanan yang berbeda: General Purpose (SSD) atau Provisioned IOPS.

Sumber Daya Tambahan

Penyimpanan magnetik adalah jenis penyimpanan generasi sebelumnya. General Purpose (SSD) atau Provisioned IOPS adalah jenis penyimpanan yang direkomendasikan untuk kebutuhan penyimpanan baru. Jenis penyimpanan ini memberikan kinerja yang lebih tinggi dan konsisten, serta opsi ukuran penyimpanan yang ditingkatkan.

Untuk informasi selengkapnya, lihat Volume generasi sebelumnya.

Kolom laporan

- Status
- Wilayah

- Sumber Daya
- Nilai yang Direkomendasikan
- Nama Mesin
- Waktu Terakhir Diperbarui

Grup parameter Amazon RDS tidak menggunakan halaman besar

Deskripsi

Halaman besar dapat meningkatkan skalabilitas database, tetapi instans DB Anda tidak menggunakan halaman besar. Kami menyarankan Anda mengatur nilai parameter use_large_pages ke HANYA di grup parameter DB untuk instance DB Anda.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

> **Note**
>
> Ketika instans DB atau kluster DB dihentikan, Anda dapat melihat rekomendasi Amazon RDS Trusted Advisor selama 3 hingga 5 hari. Setelah lima hari, rekomendasi tidak tersedia di Trusted Advisor. Untuk melihat rekomendasi, buka konsol Amazon RDS, lalu pilih Rekomendasi.
> Jika Anda menghapus instans DB atau kluster DB, maka rekomendasi yang terkait dengan instans atau cluster tersebut tidak tersedia di Trusted Advisor atau konsol manajemen Amazon RDS.

ID pemeriksaan

`c1qf5bt024`

Kriteria Peringatan

Kuning: Grup parameter DB tidak menggunakan halaman besar.

Tindakan yang Direkomendasikan

Tetapkan nilai parameter use_large_pages ke HANYA di grup parameter DB Anda.

Sumber Daya Tambahan

Untuk informasi selengkapnya, lihat Menghidupkan HugePages RDS untuk instance Oracle.

Kolom laporan

- Status
- Wilayah
- Sumber Daya
- Nama Parameter
- Nilai yang Direkomendasikan
- Waktu Terakhir Diperbarui

Parameter cache kueri Amazon RDS diaktifkan

Deskripsi

Ketika perubahan mengharuskan cache kueri Anda dibersihkan, instans DB Anda akan tampak macet. Cache kueri tidak bermanfaat untuk sebagian besar beban kerja. Cache kueri dihapus dari MySQL versi 8.0. Kami menyarankan Anda mengatur parameter query_cache_type ke 0.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

> **Note**
>
> Ketika instans DB atau kluster DB dihentikan, Anda dapat melihat rekomendasi Amazon RDS Trusted Advisor selama 3 hingga 5 hari. Setelah lima hari, rekomendasi tidak tersedia di Trusted Advisor. Untuk melihat rekomendasi, buka konsol Amazon RDS, lalu pilih Rekomendasi.

Jika Anda menghapus instans DB atau kluster DB, maka rekomendasi yang terkait dengan instans atau cluster tersebut tidak tersedia di Trusted Advisor atau konsol manajemen Amazon RDS.

ID pemeriksaan

`c1qf5bt022`

Kriteria Peringatan

Kuning: Grup parameter DB mengaktifkan cache kueri.

Tindakan yang Direkomendasikan

Setel nilai parameter query_cache_type ke 0 di grup parameter DB Anda.

Sumber Daya Tambahan

Untuk mengetahui informasi selengkapnya, lihat Praktik terbaik untuk mengonfigurasi parameter untuk Amazon RDS for MySQL, bagian 1: Parameter yang terkait dengan performa.

Kolom laporan

- Status
- Wilayah
- Sumber Daya
- Nama Parameter
- Nilai yang Direkomendasikan
- Waktu Terakhir Diperbarui

Pembaruan kelas instans sumber daya Amazon RDS diperlukan

Deskripsi

Database Anda menjalankan kelas instans DB generasi sebelumnya. Kami telah mengganti kelas instans DB dari generasi sebelumnya dengan kelas instans DB dengan biaya, kinerja, atau keduanya yang lebih baik. Kami menyarankan Anda menjalankan instans DB Anda dengan kelas instans DB dari generasi yang lebih baru.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

> **Note**
>
> Ketika instans DB atau kluster DB dihentikan, Anda dapat melihat rekomendasi Amazon RDS Trusted Advisor selama 3 hingga 5 hari. Setelah lima hari, rekomendasi tidak tersedia di Trusted Advisor. Untuk melihat rekomendasi, buka konsol Amazon RDS, lalu pilih Rekomendasi.
> Jika Anda menghapus instans DB atau kluster DB, maka rekomendasi yang terkait dengan instans atau cluster tersebut tidak tersedia di Trusted Advisor atau konsol manajemen Amazon RDS.

ID pemeriksaan

`c1qf5bt015`

Kriteria Peringatan

Merah: Instans DB menggunakan akhir dari kelas instans DB dukungan.

Tindakan yang Direkomendasikan

Tingkatkan ke kelas instans DB terbaru.

Sumber Daya Tambahan

Untuk informasi selengkapnya, lihat Mesin DB yang didukung untuk kelas instans DB.

Kolom laporan

- Status
- Wilayah
- Sumber Daya
- Kelas Instans DB
- Nilai yang Direkomendasikan

- Nama Mesin
- Waktu Terakhir Diperbarui

Sumber daya Amazon RDS pembaruan versi utama diperlukan

Deskripsi

Database dengan versi utama saat ini untuk mesin DB tidak akan didukung. Kami menyarankan Anda meningkatkan ke versi utama terbaru yang mencakup fungsionalitas dan peningkatan baru.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

> **Note**
>
> Ketika instans DB atau kluster DB dihentikan, Anda dapat melihat rekomendasi Amazon RDS Trusted Advisor selama 3 hingga 5 hari. Setelah lima hari, rekomendasi tidak tersedia di Trusted Advisor. Untuk melihat rekomendasi, buka konsol Amazon RDS, lalu pilih Rekomendasi.
> Jika Anda menghapus instans DB atau kluster DB, maka rekomendasi yang terkait dengan instans atau cluster tersebut tidak tersedia di Trusted Advisor atau konsol manajemen Amazon RDS.

ID pemeriksaan

`c1qf5bt014`

Kriteria Peringatan

Merah: Sumber daya RDS menggunakan versi utama dukungan akhir.

Tindakan yang Direkomendasikan

Tingkatkan ke versi utama terbaru untuk mesin DB.

Sumber Daya Tambahan

Amazon RDS merilis versi baru untuk mesin database yang didukung untuk memelihara database Anda dengan versi terbaru. Versi baru yang dirilis mungkin termasuk perbaikan bug, peningkatan keamanan, dan perbaikan lainnya untuk mesin database. Anda dapat meminimalkan waktu henti yang diperlukan untuk peningkatan instans DB dengan menggunakan penerapan biru/hijau.

Untuk informasi selengkapnya, lihat sumber daya berikut:

- Memutakhirkan versi mesin instans DB
- Pembaruan Amazon Aurora
- Menggunakan Amazon RDS Blue/Green Deployment untuk pembaruan database

Kolom laporan

- Status
- Wilayah
- Sumber Daya
- Nama Mesin
- Versi Mesin Saat Ini
- Nilai yang Direkomendasikan
- Waktu Terakhir Diperbarui

Sumber daya Amazon RDS menggunakan akhir edisi mesin dukungan di bawah lisensi yang disertakan

Deskripsi

Kami menyarankan Anda meningkatkan versi utama ke versi mesin terbaru yang didukung oleh Amazon RDS untuk melanjutkan dukungan lisensi saat ini. Versi mesin database Anda tidak akan didukung dengan lisensi saat ini.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

> **Note**
>
> Ketika instans DB atau kluster DB dihentikan, Anda dapat melihat rekomendasi Amazon RDS Trusted Advisor selama 3 hingga 5 hari. Setelah lima hari, rekomendasi tidak tersedia di Trusted Advisor. Untuk melihat rekomendasi, buka konsol Amazon RDS, lalu pilih Rekomendasi.
> Jika Anda menghapus instans DB atau kluster DB, maka rekomendasi yang terkait dengan instans atau cluster tersebut tidak tersedia di Trusted Advisor atau konsol manajemen Amazon RDS.

ID pemeriksaan

`c1qf5bt016`

Kriteria Peringatan

Merah: Sumber daya Amazon RDS menggunakan akhir edisi mesin dukungan di bawah model yang disertakan lisensi.

Tindakan yang Direkomendasikan

Kami menyarankan Anda meningkatkan database Anda ke versi terbaru yang didukung di Amazon RDS untuk terus menggunakan model berlisensi.

Sumber Daya Tambahan

Untuk informasi selengkapnya, lihat Upgrade versi utama Oracle.

Kolom laporan

- Status
- Wilayah
- Sumber Daya
- Nama Mesin
- Versi Mesin Saat Ini
- Nilai yang Direkomendasikan
- Nama Mesin
- Waktu Terakhir Diperbarui

Amazon Route 53 Alias Resource Record Set

Deskripsi

Memeriksa kumpulan catatan sumber daya yang dapat diubah menjadi kumpulan catatan sumber daya alias untuk meningkatkan kinerja dan menghemat uang.

Kumpulan rekaman sumber daya alias merutekan kueri DNS ke AWS sumber daya (misalnya, penyeimbang beban Elastic Load Balancing atau bucket Amazon S3) atau ke kumpulan rekaman sumber daya Route 53 lainnya. Saat Anda menggunakan kumpulan catatan sumber daya alias, Route 53 merutekan kueri DNS Anda ke AWS sumber daya secara gratis.

Zona yang di-host yang dibuat oleh AWS layanan tidak akan muncul di hasil pemeriksaan Anda.

ID pemeriksaan

`B913Ef6fb4`

Kriteria Peringatan

- Kuning: Kumpulan catatan sumber daya adalah CNAME ke situs web Amazon S3.
- Kuning: Kumpulan catatan sumber daya adalah CNAME ke CloudFront distribusi Amazon.
- Kuning: Rekaman sumber daya adalah CNAME ke penyeimbang beban Elastic Load Balancing.

Tindakan yang Direkomendasikan

Ganti set rekaman sumber daya CNAME yang terdaftar dengan kumpulan catatan sumber daya alias; lihat Memilih Antara Kumpulan Rekaman Sumber Daya Alias dan Non-Alias.

Anda juga perlu mengubah jenis rekaman dari CNAME ke A atau AAAA, tergantung pada sumber daya. AWS Lihat Nilai yang Anda Tentukan Saat Membuat atau Mengedit Kumpulan Rekaman Sumber Daya Amazon Route 53.

Sumber Daya Tambahan

Perutean Kueri ke Sumber Daya AWS

Kolom laporan

- Status
- Nama Zona yang Dihosting
- ID Zona yang Dihosting
- Nama Set Catatan Sumber Daya

- Jenis Set Rekaman Sumber Daya
- Pengidentifikasi Set Rekaman Sumber Daya
- Target Alias

AWS Lambda fungsi yang kurang disediakan untuk ukuran memori

Deskripsi

Memeriksa AWS Lambda fungsi yang dipanggil setidaknya sekali selama periode lookback. Pemeriksaan ini memberi tahu Anda jika ada fungsi Lambda Anda yang kurang disediakan untuk ukuran memori. Ketika Anda memiliki fungsi Lambda yang kurang disediakan untuk ukuran memori, fungsi-fungsi ini membutuhkan waktu lebih lama untuk diselesaikan.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

`C0r6dfpM06`

Kriteria Peringatan

Kuning: Fungsi Lambda yang kurang disediakan untuk ukuran memori selama periode lookback. Untuk menentukan apakah fungsi Lambda kurang disediakan, kami mempertimbangkan semua metrik default untuk fungsi tersebut. CloudWatch Algoritma yang digunakan untuk mengidentifikasi fungsi Lambda yang kurang disediakan untuk ukuran memori mengikuti praktik terbaik. AWS Algoritma diperbarui ketika pola baru telah diidentifikasi.

Tindakan yang Direkomendasikan

Pertimbangkan untuk meningkatkan ukuran memori fungsi Lambda Anda.

Untuk informasi selengkapnya, lihat Ikut serta AWS Compute Optimizer untuk Trusted Advisor cek.

Kolom laporan

- Status

- Wilayah
- Nama Fungsi
- Versi Fungsi
- Ukuran Memori (MB)
- Ukuran Memori yang Direkomendasikan (MB)
- Periode Lookback (hari)
- Risiko Kinerja
- Waktu Terakhir Diperbarui

AWS Lambda Fungsi tanpa Batas Konkurensi Dikonfigurasi

Deskripsi

Memeriksa apakah AWS Lambda fungsi dikonfigurasi dengan batas eksekusi bersamaan tingkat fungsi.

Konkurensi adalah jumlah permintaan dalam penerbangan yang ditangani oleh fungsi AWS Lambda Anda secara bersamaan. Untuk setiap permintaan bersamaan, Lambda menyediakan instance terpisah dari lingkungan eksekusi Anda.

Anda dapat menentukan batas konkurensi minimum dan maksimum menggunakan parameter konkurensi LimitLow dan ConcurrencyLimittinggi dalam aturan Anda AWS Config .

Untuk informasi selengkapnya, lihat Penskalaan fungsi Lambda.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

`c18d2gz181`

Sumber

AWS Config Aturan Terkelola: lambda-concurrency-check

Kriteria Peringatan

Kuning: Fungsi Lambda tidak memiliki batas konkurensi yang dikonfigurasi.

Tindakan yang Direkomendasikan

Pastikan fungsi Lambda Anda telah dikonfigurasi secara konkurensi. Batas konkurensi untuk fungsi Lambda Anda membantu memastikan bahwa fungsi Anda memproses permintaan dengan andal dan dapat diprediksi. Batas konkurensi mengurangi risiko fungsi Anda kewalahan karena lonjakan lalu lintas yang tiba-tiba.

Untuk informasi selengkapnya, lihat Mengonfigurasi konkurensi cadangan.

Sumber Daya Tambahan

- Penskalaan fungsi Lambda
- Mengkonfigurasi konkurensi cadangan

Kolom laporan

- Status
- Wilayah
- Sumber Daya
- AWS Config Aturan
- Parameter Input
- Waktu Terakhir Diperbarui

AWS Well-Architectedmasalah risiko tinggi untuk kinerja

Deskripsi

Memeriksa masalah risiko tinggi (HRI) untuk beban kerja Anda di pilar kinerja. Pemeriksaan ini didasarkan pada AWS-Well Architected ulasan Anda. Hasil pemeriksaan Anda tergantung pada apakah Anda menyelesaikan evaluasi beban kerja denganAWS Well-Architected.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

`Wxdfp4B1L2`

Kriteria Peringatan

- Merah: Setidaknya satu masalah risiko tinggi aktif diidentifikasi dalam pilar kinerja untuk AWS Well-Architected.
- Hijau: Tidak ada masalah risiko tinggi aktif yang terdeteksi di pilar kinerja untuk AWS Well-Architected.

Tindakan yang Direkomendasikan

AWS Well-Architected mendeteksi masalah risiko tinggi selama evaluasi beban kerja Anda. Masalah-masalah ini menghadirkan peluang untuk mengurangi risiko dan menghemat uang. Masuk ke alat AWS Well-Architected untuk meninjau jawaban Anda dan mengambil tindakan untuk menyelesaikan masalah aktif Anda.

Kolom laporan

- Status
- Wilayah
- Beban Kerja ARN
- Nama Beban Kerja
- Nama Peninjau
- Jenis Beban Kerja
- Tanggal Mulai Beban Kerja
- Beban Kerja Tanggal Modifikasi Terakhir
- Jumlah HRI yang diidentifikasi untuk Kinerja
- Jumlah HRI yang diselesaikan untuk Kinerja
- Jumlah pertanyaan yang dijawab untuk Kinerja
- Jumlah total pertanyaan di pilar Kinerja
- Waktu Terakhir Diperbarui

CloudFront Nama Domain Alternatif

Deskripsi

Memeriksa CloudFront distribusi Amazon untuk nama domain alternatif (CNAMES) yang salah mengonfigurasi pengaturan DNS.

Jika CloudFront distribusi menyertakan nama domain alternatif, konfigurasi DNS untuk domain harus merutekan kueri DNS ke distribusi tersebut.

> **Note**
>
> Pemeriksaan ini mengasumsikan Amazon Route 53 DNS dan CloudFront distribusi Amazon dikonfigurasi dalam hal yang sama. Akun AWS Dengan demikian, daftar peringatan mungkin menyertakan sumber daya yang berfungsi seperti yang diharapkan karena pengaturan DNS di luar ini. Akun AWS

ID pemeriksaan

`N420c450f2`

Kriteria Peringatan

- Kuning: CloudFront Distribusi menyertakan nama domain alternatif, tetapi konfigurasi DNS tidak diatur dengan benar dengan catatan CNAME atau catatan sumber daya alias Amazon Route 53.
- Kuning: CloudFront Distribusi mencakup nama domain alternatif, tetapi tidak Trusted Advisor dapat mengevaluasi konfigurasi DNS karena terlalu banyak pengalihan.
- Kuning: CloudFront Distribusi mencakup nama domain alternatif, tetapi tidak Trusted Advisor dapat mengevaluasi konfigurasi DNS karena alasan lain, kemungkinan besar karena batas waktu.

Tindakan yang Direkomendasikan

Memperbarui konfigurasi DNS untuk merutekan kueri DNS ke CloudFront distribusi; lihat Menggunakan Nama Domain Alternatif (CNames).

Jika Anda menggunakan Amazon Route 53 sebagai layanan DNS, lihat Merutekan Lalu Lintas ke Distribusi CloudFront Web Amazon dengan Menggunakan Nama Domain Anda. Jika waktu cek habis, coba segarkan cek.

Sumber Daya Tambahan

Panduan CloudFront Pengembang Amazon

Kolom laporan

- Status
- ID Distribusi
- Nama Domain Distribusi
- Nama Domain Alternatif
- Alasan

CloudFront Optimasi Pengiriman Konten

Deskripsi

Memeriksa kasus di mana transfer data dari bucket Amazon Simple Storage Service (Amazon S3) dapat dipercepat dengan menggunakan CloudFront Amazon, AWS layanan pengiriman konten global.

Ketika Anda mengonfigurasi CloudFront untuk mengirimkan konten Anda, permintaan untuk konten Anda secara otomatis dirutekan ke lokasi tepi terdekat tempat konten di-cache. Perutean ini memungkinkan konten dikirimkan ke pengguna Anda dengan kinerja terbaik. Rasio data yang ditransfer tinggi dibandingkan dengan data yang disimpan dalam bucket menunjukkan bahwa Anda bisa mendapatkan keuntungan dari menggunakan Amazon CloudFront untuk mengirimkan data.

ID pemeriksaan

`796d6f3D83`

Kriteria Peringatan

- Kuning: Jumlah data yang ditransfer keluar dari bucket ke pengguna Anda oleh permintaan GET dalam 30 hari sebelum cek setidaknya 25 kali lebih besar dari jumlah rata-rata data yang disimpan dalam bucket.
- Merah: Jumlah data yang ditransfer keluar dari bucket ke pengguna Anda oleh permintaan GET dalam 30 hari sebelum cek setidaknya 10 TB dan setidaknya 25 kali lebih besar dari jumlah rata-rata data yang disimpan dalam bucket.

Tindakan yang Direkomendasikan

Pertimbangkan CloudFront untuk menggunakan untuk kinerja yang lebih baik. Lihat Detail CloudFront Produk Amazon.

Jika data yang ditransfer adalah 10 TB per bulan atau lebih, lihat CloudFront Harga Amazon untuk menjelajahi kemungkinan penghematan biaya.

Sumber Daya Tambahan

- Panduan CloudFront Pengembang Amazon
- AWS Studi Kasus: PBS

Kolom laporan

- Status
- Wilayah
- Nama Bucket
- Penyimpanan S3 (GB)
- Transfer Data Keluar (GB)
- Rasio Transfer ke Penyimpanan

CloudFront Penerusan Header dan Rasio Hit Cache

Deskripsi

Memeriksa header permintaan HTTP yang CloudFront saat ini menerima dari klien dan meneruskan ke server asal Anda.

Beberapa header, seperti tanggal, atau agen pengguna, secara signifikan mengurangi rasio hit cache (proporsi permintaan yang disajikan dari cache CloudFront tepi). Ini meningkatkan beban pada asal Anda dan mengurangi kinerja, karena CloudFront harus meneruskan lebih banyak permintaan ke asal Anda.

ID pemeriksaan

`N415c450f2`

Kriteria Peringatan

Kuning: Satu atau beberapa header permintaan yang CloudFront diteruskan ke asal Anda mungkin secara signifikan mengurangi rasio hit cache Anda.

Tindakan yang Direkomendasikan

Pertimbangkan apakah header permintaan memberikan manfaat yang cukup untuk membenarkan efek negatif pada rasio hit cache. Jika asal Anda mengembalikan objek yang sama terlepas dari nilai header yang diberikan, sebaiknya Anda tidak mengonfigurasi CloudFront untuk meneruskan header tersebut ke asal. Untuk informasi selengkapnya, lihat Mengonfigurasi CloudFront ke Objek Cache Berdasarkan Header Permintaan.

Sumber Daya Tambahan

- Meningkatkan Proporsi Permintaan yang Dilayani dari Cache CloudFront Edge
- CloudFront Laporan Statistik Cache
- Header dan Perilaku Permintaan HTTP CloudFront

Kolom laporan

- ID Distribusi
- Nama Domain Distribusi
- Pola Jalur Perilaku Cache
- Header

Instans Amazon EC2 Pemanfaatan Tinggi

Deskripsi

Memeriksa instans Amazon Elastic Compute Cloud (Amazon EC2) yang berjalan kapan saja selama 14 hari terakhir. Peringatan dikirim jika penggunaan CPU harian lebih besar dari 90% pada empat hari atau lebih.

Pemanfaatan tinggi yang konsisten dapat menunjukkan kinerja yang optimal dan stabil. Namun, ini juga dapat menunjukkan bahwa suatu aplikasi tidak memiliki sumber daya yang cukup. Untuk mendapatkan data pemanfaatan CPU harian, unduh laporan untuk pemeriksaan ini.

ID pemeriksaan

`ZRxQlPsb6c`

Kriteria Peringatan

Kuning: Sebuah instance memiliki lebih dari 90% penggunaan CPU rata-rata harian setidaknya pada 4 dari 14 hari sebelumnya.

Tindakan yang Direkomendasikan

Pertimbangkan untuk menambahkan lebih banyak contoh. Untuk informasi tentang penskalaan jumlah instans berdasarkan permintaan, lihat Apa itu Auto Scaling?

Sumber Daya Tambahan

- Pemantauan Amazon EC2
- Metadata Instance dan Data Pengguna
- Panduan CloudWatch Pengguna Amazon
- Panduan Pengguna Penskalaan Otomatis Amazon EC2

Kolom laporan

- Wilayah/AZ
- ID Instans
- Tipe Instans
- Nama Instance
- Pemanfaatan CPU Rata-Rata 14 Hari
- Jumlah Hari Lebih dari 90% Pemanfaatan CPU

Keamanan

Anda dapat menggunakan pemeriksaan berikut untuk kategori keamanan.

> **Note**
>
> Jika Anda mengaktifkan Security Hub untuk Anda Akun AWS, Anda dapat melihat temuan Anda di Trusted Advisor konsol. Untuk informasi, lihat MelihatAWS Security Hub kontrol diAWS Trusted Advisor.
> Anda dapat melihat semua kontrol dalam standar keamanan Praktik Terbaik Keamanan AWS Dasar kecuali untuk kontrol yang memiliki Kategori: Pulih> Ketahanan. Untuk daftar kontrol yang didukung, lihat Kontrol Praktik Terbaik Keamanan AWS Dasar di Panduan AWS Security Hub Pengguna.

Periksa nama

- Periode Retensi Grup CloudWatch Log Amazon

- Instans Amazon EC2 dengan dukungan akhir Microsoft SQL Server
- Instans Amazon EC2 dengan dukungan akhir Microsoft Windows Server
- Instans Amazon EC2 dengan dukungan standar Ubuntu LTS akhir
- Klien Amazon EFS tidak menggunakan data-in-transit enkripsi
- Cuplikan Publik Amazon EBS
- Enkripsi penyimpanan Amazon RDS Aurora dimatikan
- Diperlukan peningkatan versi minor mesin Amazon RDS
- Cuplikan Publik Amazon RDS
- Risiko Akses Grup Keamanan Amazon RDS
- Enkripsi penyimpanan Amazon RDS dimatikan
- Amazon Route 53 tidak cocok dengan catatan CNAME yang menunjuk langsung ke bucket S3
- Amazon Route 53 Kumpulan Rekaman Sumber Daya MX dan Kerangka Kebijakan Pengirim
- Izin Bucket Amazon S3
- Log Akses Amazon S3Server Diaktifkan
- Koneksi Peering VPC Amazon dengan Resolusi DNS Dinonaktifkan
- AWS Backup Vault Tanpa Kebijakan Berbasis Sumber Daya untuk Mencegah Penghapusan Poin Pemulihan
- AWS CloudTrail Penebangan
- AWS Lambda Fungsi Menggunakan Runtime yang Tidak Digunakan Lagi
- AWS Well-Architectedmasalah risiko tinggi untuk keamanan
- CloudFrontSertifikat SSL Kustom di Toko Sertifikat IAM
- CloudFront Sertifikat SSL di Server Asal
- ELB Listener Keamanan
- Grup Keamanan ELB
- Exposed Access Keys
- Rotasi Kunci Akses IAM
- Kebijakan Kata Sandi IAM
- MFA pada Akun Root
- Grup Keamanan — Port Tertentu Tidak Dibatasi

- Grup Keamanan — Akses Tidak Terbatas

Periode Retensi Grup CloudWatch Log Amazon

Deskripsi

Memeriksa apakah periode penyimpanan grup CloudWatch log Amazon disetel ke 365 hari atau nomor tertentu lainnya.

Secara default, log disimpan tanpa batas waktu dan tidak pernah kedaluwarsa. Namun, Anda dapat menyesuaikan kebijakan penyimpanan untuk setiap grup log untuk mematuhi peraturan industri atau persyaratan hukum untuk periode tertentu.

Anda dapat menentukan waktu penyimpanan minimum dan nama grup log menggunakan parameter LogGroupNama dan MinRetentionWaktu dalam AWS Config aturan Anda.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

```
c18d2gz186
```

Sumber

```
AWS Config Managed Rule: cw-loggroup-retention-period-check
```

Kriteria Peringatan

Kuning: Periode retensi grup CloudWatch log Amazon kurang dari jumlah hari minimum yang diinginkan.

Tindakan yang Direkomendasikan

Konfigurasikan periode penyimpanan lebih dari 365 hari untuk data log Anda yang disimpan di CloudWatch Log Amazon untuk memenuhi persyaratan kepatuhan.

Untuk informasi selengkapnya, lihat Mengubah penyimpanan data CloudWatch log di Log.

Sumber Daya Tambahan

Mengubah retensi CloudWatch log

Kolom laporan

- Status
- Wilayah
- Sumber Daya
- AWS Config Aturan
- Parameter Input
- Waktu Terakhir Diperbarui

Instans Amazon EC2 dengan dukungan akhir Microsoft SQL Server

Deskripsi

Memeriksa instans Amazon Elastic Compute Cloud (Amazon EC2) versi SQL Server yang berjalan dalam 24 jam terakhir. Pemeriksaan ini memberi tahu Anda jika versi sudah dekat atau telah mencapai akhir dukungan. Setiap versi SQL Server menawarkan 10 tahun dukungan, termasuk 5 tahun dukungan mainstream dan 5 tahun dukungan diperpanjang. Setelah dukungan berakhir, versi SQL Server tidak akan menerima pembaruan keamanan reguler. Menjalankan aplikasi dengan versi SQL Server yang tidak didukung dapat membawa risiko keamanan atau kepatuhan.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

`Qsdfp3A4L3`

Kriteria Peringatan

- Merah: Instans EC2 memiliki versi SQL Server yang mencapai akhir dukungan.

- Kuning: Instans EC2 memiliki versi SQL Server yang akan mencapai akhir dukungan dalam 12 bulan.

Tindakan yang Direkomendasikan

Untuk memodernisasi beban kerja SQL Server Anda, pertimbangkan refactoring ke database asli seperti Amazon Aurora. AWS Cloud Untuk informasi selengkapnya, lihat Memodernisasi Beban Kerja Windows dengan. AWS

Untuk beralih ke database yang dikelola sepenuhnya, pertimbangkan replatforming ke Amazon Relational Database Service (Amazon RDS). Untuk informasi selengkapnya, lihat Amazon RDS for SQL Server.

Untuk memutakhirkan SQL Server Anda di Amazon EC2, pertimbangkan untuk menggunakan runbook otomatisasi untuk menyederhanakan pemutakhiran Anda. Untuk informasi lebih lanjut, lihat dokumentasi AWS Systems Manager.

Jika Anda tidak dapat memutakhirkan SQL Server di Amazon EC2, pertimbangkan Program Migrasi Akhir Dukungan (EMP) untuk Windows Server. Untuk informasi lebih lanjut, lihat Situs Web EMP.

Sumber Daya Tambahan

- Bersiaplah untuk dukungan akhir SQL Server dengan AWS
- Microsoft SQL Server aktif AWS

Kolom laporan

- Status
- Wilayah
- ID Instans
- Versi SQL Server
- Support Siklus
- Akhir dari Support
- Waktu Terakhir Diperbarui

Instans Amazon EC2 dengan dukungan akhir Microsoft Windows Server

Deskripsi

Pemeriksaan ini memberi tahu Anda jika versi sudah dekat atau telah mencapai akhir dukungan. Setiap versi Windows Server menawarkan dukungan selama 10 tahun. Ini termasuk 5 tahun dukungan arus utama dan 5 tahun dukungan diperpanjang. Setelah dukungan berakhir, versi Windows Server tidak akan menerima pembaruan keamanan reguler. Jika Anda menjalankan aplikasi dengan versi Windows Server yang tidak didukung, Anda berisiko keamanan atau kepatuhan aplikasi ini.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

`Qsdfp3A4L4`

Kriteria Peringatan

- Merah: Instans EC2 memiliki versi Windows Server yang mencapai akhir dukungan (Windows Server 2003, 2003 R2, 2008, dan 2008 R2).
- Kuning: Instans EC2 memiliki versi Windows Server yang akan mencapai akhir dukungan dalam waktu kurang dari 18 bulan (Windows Server 2012 dan 2012 R2).

Tindakan yang Direkomendasikan

Untuk memodernisasi beban kerja Windows Server Anda, pertimbangkan berbagai opsi yang tersedia di Modernisasi Beban Kerja Windows dengan. AWS

Untuk memutakhirkan beban kerja Windows Server agar berjalan pada versi Windows Server yang lebih baru, Anda dapat menggunakan runbook otomatisasi. Untuk informasi selengkapnya, lihat dokumentasi AWS Systems Manager.

Silakan ikuti serangkaian langkah di bawah ini:

- Tingkatkan versi Windows Server

- Berhenti keras dan mulai saat meningkatkan
- Jika menggunakan EC2config, silakan bermigrasi ke EC2launch

Kolom laporan

- Status
- Wilayah
- ID Instans
- Versi Server Windows
- Support Siklus
- Akhir dari Support
- Waktu Terakhir Diperbarui

Instans Amazon EC2 dengan dukungan standar Ubuntu LTS akhir

Deskripsi

Pemeriksaan ini memberi tahu Anda jika versi sudah dekat atau telah mencapai akhir dukungan standar. Penting untuk mengambil tindakan - baik dengan bermigrasi ke LTS berikutnya atau meningkatkan ke Ubuntu Pro. Setelah dukungan berakhir, mesin LTS 18.04 Anda tidak akan menerima pembaruan keamanan apa pun. Dengan langganan Ubuntu Pro, penerapan Ubuntu 18.04 LTS Anda dapat menerima Expanded Security Maintenance (ESM) hingga 2028. Kerentanan keamanan yang tetap tidak ditambal membuka sistem Anda untuk peretas dan potensi pelanggaran besar.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

`c1dfprch15`

Kriteria Peringatan

Merah: Instans Amazon EC2 memiliki versi Ubuntu yang mencapai akhir dukungan standar (Ubuntu 18.04 LTS, 18.04.1 LTS, 18.04.2 LTS, 18.04.3 LTS, 18.04.4 LTS, 18.04.5 LTS, dan 18.04.6 LTS).

Kuning: Instans Amazon EC2 memiliki versi Ubuntu yang akan mencapai akhir dukungan standar dalam waktu kurang dari 6 bulan (Ubuntu 20.04 LTS, 20.04.1 LTS, 20.04.2 LTS, 20.04.3 LTS, 20.04.4 LTS, 20.04.5 LTS, dan 20.04.6 LTS).

Hijau: Semua instans Amazon EC2 sesuai.

Tindakan yang Direkomendasikan

Untuk memutakhirkan instance Ubuntu 18.04 LTS ke versi LTS yang didukung, ikuti langkah-langkah yang disebutkan dalam artikel ini. Untuk memutakhirkan instance Ubuntu 18.04 LTS ke Ubuntu Pro, kunjungi AWS License Manager konsol dan ikuti langkah-langkah yang disebutkan dalam panduan pengguna.AWS License Manager Anda juga dapat merujuk ke blog Ubuntu yang menunjukkan demo langkah demi langkah untuk meningkatkan instance Ubuntu ke Ubuntu Pro.

Sumber Daya Tambahan

Untuk informasi tentang harga, hubungi AWS Support.

Kolom laporan

- Status
- Wilayah
- Versi Ubuntu Lts
- Tanggal Akhir Dukungan yang Diharapkan
- ID Instans
- Support Siklus
- Waktu Terakhir Diperbarui

Klien Amazon EFS tidak menggunakan data-in-transit enkripsi

Deskripsi

Memeriksa apakah sistem file Amazon EFS dipasang menggunakan data-in-transit enkripsi. AWS merekomendasikan agar pelanggan menggunakan data-in-transit enkripsi untuk semua aliran

data untuk melindungi data dari paparan yang tidak disengaja atau akses yang tidak sah. Amazon EFS merekomendasikan klien menggunakan pengaturan pemasangan '-o tls' menggunakan helper mount Amazon EFS untuk mengenkripsi data dalam perjalanan menggunakan TLS v1.2.

ID pemeriksaan

`c1dfpnchv1`

Kriteria Peringatan

Kuning: Satu atau lebih klien NFS untuk sistem file Amazon EFS Anda tidak menggunakan pengaturan pemasangan yang disarankan yang menyediakan data-in-transit enkripsi.

Hijau: Semua klien NFS untuk sistem file Amazon EFS Anda menggunakan pengaturan pemasangan yang disarankan yang menyediakan data-in-transit enkripsi.

Tindakan yang Direkomendasikan

Untuk memanfaatkan fitur data-in-transit enkripsi di Amazon EFS, sebaiknya Anda memasang ulang sistem file menggunakan helper mount Amazon EFS dan pengaturan pemasangan yang disarankan.

> **Note**
>
> Beberapa distribusi Linux tidak menyertakan versi stunnel yang mendukung fitur TLS secara default. Jika Anda menggunakan distribusi Linux yang tidak didukung (lihat distribusi yang didukung di sini), sebaiknya Anda memutakhirkannya sebelum melakukan remounting dengan pengaturan pemasangan yang disarankan.

Sumber Daya Tambahan

- Mengenkripsi data dalam perjalanan

Kolom laporan

- Status
- Wilayah
- ID Sistem Berkas EFS
- AZ dengan Koneksi Tidak Terenkripsi
- Waktu Terakhir Diperbarui

Cuplikan Publik Amazon EBS

Deskripsi

Memeriksa pengaturan izin untuk snapshot volume Amazon Elastic Block Store (Amazon EBS) Anda dan memberi tahu Anda jika ada snapshot yang dapat diakses publik.

Saat Anda membuat snapshot publik, Anda memberi semua Akun AWS dan pengguna akses ke semua data pada snapshot. Untuk membagikan snapshot hanya dengan pengguna atau akun tertentu, tandai snapshot sebagai pribadi. Kemudian, tentukan pengguna atau akun yang ingin Anda bagikan data snapshot. Perhatikan bahwa jika Anda mengaktifkan Blokir Akses Publik dalam mode 'blokir semua berbagi', maka snapshot publik Anda tidak dapat diakses publik dan tidak muncul di hasil pemeriksaan ini.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul.

ID pemeriksaan

`ePs02jT06w`

Kriteria Peringatan

Merah: Snapshot volume EBS dapat diakses publik.

Tindakan yang Direkomendasikan

Kecuali Anda yakin ingin membagikan semua data dalam snapshot dengan semua Akun AWS dan pengguna, ubah izin: tandai snapshot sebagai pribadi, lalu tentukan akun yang ingin Anda berikan izin. Untuk informasi selengkapnya, lihat Berbagi Snapshot Amazon EBS. Gunakan Blokir Akses Publik untuk Snapshot EBS untuk mengontrol pengaturan yang memungkinkan akses publik ke data Anda. Pemeriksaan ini tidak dapat dikecualikan dari tampilan di Trusted Advisor konsol.

Untuk mengubah izin snapshot Anda secara langsung, gunakan runbook di konsol. AWS Systems Manager Untuk informasi selengkapnya, lihat `AWSSupport-ModifyEBSSnapshotPermission`.

Sumber Daya Tambahan

- Cuplikan Amazon EBS

Kolom laporan

- Status
- Wilayah
- ID Volume
- ID Cuplikan
- Deskripsi

Enkripsi penyimpanan Amazon RDS Aurora dimatikan

Deskripsi

Amazon RDS mendukung enkripsi saat istirahat untuk semua mesin database dengan menggunakan kunci yang Anda kelola. AWS Key Management Service Pada instans DB aktif dengan enkripsi Amazon RDS, data yang disimpan saat istirahat di penyimpanan dienkripsi, mirip dengan pencadangan otomatis, replika baca, dan snapshot.

Jika enkripsi tidak diaktifkan saat membuat cluster Aurora DB, maka Anda harus mengembalikan snapshot yang didekripsi ke cluster DB terenkripsi.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

> **Note**
>
> Ketika instans DB atau cluster DB dihentikan, Anda dapat melihat rekomendasi Amazon RDS Trusted Advisor selama 3 hingga 5 hari. Setelah lima hari, rekomendasi tidak tersedia di Trusted Advisor. Untuk melihat rekomendasi, buka konsol Amazon RDS, lalu pilih Rekomendasi.

Jika Anda menghapus instans DB atau kluster DB, maka rekomendasi yang terkait dengan instans atau cluster tersebut tidak tersedia di Trusted Advisor atau konsol manajemen Amazon RDS.

ID pemeriksaan

`c1qf5bt005`

Kriteria Peringatan

Merah: Sumber daya Amazon RDS Aurora tidak mengaktifkan enkripsi.

Tindakan yang Direkomendasikan

Aktifkan enkripsi data saat istirahat untuk cluster DB Anda.

Sumber Daya Tambahan

Anda dapat mengaktifkan enkripsi saat membuat instans DB atau menggunakan solusi untuk mengaktifkan enkripsi pada instans DB aktif. Anda tidak dapat memodifikasi cluster DB yang didekripsi ke cluster DB terenkripsi. Namun, Anda dapat mengembalikan snapshot yang didekripsi ke cluster DB terenkripsi. Saat Anda memulihkan dari snapshot yang didekripsi, Anda harus menentukan kunci. AWS KMS

Untuk informasi selengkapnya, lihat Mengenkripsi sumber daya Amazon Aurora.

Kolom laporan

- Status
- Wilayah
- Resouce
- Nama Mesin
- Waktu Terakhir Diperbarui

Diperlukan peningkatan versi minor mesin Amazon RDS

Deskripsi

Sumber daya database Anda tidak menjalankan versi mesin DB minor terbaru. Versi minor terbaru berisi perbaikan keamanan terbaru dan peningkatan lainnya.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

> **Note**
>
> Ketika instans DB atau cluster DB dihentikan, Anda dapat melihat rekomendasi Amazon RDS Trusted Advisor selama 3 hingga 5 hari. Setelah lima hari, rekomendasi tidak tersedia di Trusted Advisor. Untuk melihat rekomendasi, buka konsol Amazon RDS, lalu pilih Rekomendasi.
> Jika Anda menghapus instans DB atau kluster DB, maka rekomendasi yang terkait dengan instans atau cluster tersebut tidak tersedia di Trusted Advisor atau konsol manajemen Amazon RDS.

ID pemeriksaan

`c1qf5bt003`

Kriteria Peringatan

Merah: Sumber daya Amazon RDS tidak menjalankan versi mesin DB minor terbaru.

Tindakan yang Direkomendasikan

Tingkatkan ke versi mesin terbaru.

Sumber Daya Tambahan

Kami menyarankan Anda memelihara database Anda dengan versi minor mesin DB terbaru karena versi ini mencakup perbaikan keamanan dan fungsionalitas terbaru. Upgrade versi minor DB engine hanya berisi perubahan yang kompatibel dengan versi minor sebelumnya dari versi utama yang sama dari mesin DB.

Untuk informasi selengkapnya, lihat Memutakhirkan versi mesin instans DB.

Kolom laporan

- Status
- Wilayah

- Resouce
- Nama Mesin
- Versi Mesin Saat Ini
- Nilai yang Direkomendasikan
- Waktu Terakhir Diperbarui

Cuplikan Publik Amazon RDS

Deskripsi

Memeriksa pengaturan izin untuk snapshot DB Amazon Relational Database Service (Amazon RDS) Anda dan memberi tahu Anda jika ada snapshot yang ditandai sebagai publik.

Saat Anda membuat snapshot publik, Anda memberi semua Akun AWS dan pengguna akses ke semua data pada snapshot. Jika Anda ingin berbagi snapshot hanya dengan pengguna atau akun tertentu, tandai snapshot sebagai pribadi. Kemudian, tentukan pengguna atau akun yang ingin Anda bagikan data snapshot.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul.

ID pemeriksaan

`rSs93HQwa1`

Kriteria Peringatan

Merah: Snapshot Amazon RDS ditandai sebagai publik.

Tindakan yang Direkomendasikan

Kecuali Anda yakin ingin membagikan semua data dalam snapshot dengan semua Akun AWS dan pengguna, ubah izin: tandai snapshot sebagai pribadi, lalu tentukan akun yang ingin Anda berikan izin. Untuk informasi selengkapnya, lihat Berbagi Snapshot DB atau Snapshot Cluster DB. Pemeriksaan ini tidak dapat dikecualikan dari tampilan di Trusted Advisor konsol.

Untuk mengubah izin snapshot Anda secara langsung, Anda dapat menggunakan runbook di konsol. AWS Systems Manager Untuk informasi selengkapnya, lihat `AWSSupport-ModifyRDSSnapshotPermission`.

Sumber Daya Tambahan

Mencadangkan dan Memulihkan Instans Amazon RDS DB

Kolom laporan

- Status
- Wilayah
- Instans DB atau ID Cluster
- ID Cuplikan

Risiko Akses Grup Keamanan Amazon RDS

Deskripsi

Memeriksa konfigurasi grup keamanan untuk Amazon Relational Database Service (Amazon RDS) dan memperingatkan ketika aturan grup keamanan memberikan akses yang terlalu permisif ke database Anda. Konfigurasi yang disarankan untuk aturan grup keamanan adalah mengizinkan akses hanya dari grup keamanan Amazon Elastic Compute Cloud (Amazon EC2) tertentu atau dari alamat IP tertentu.

ID pemeriksaan

`nNauJisYIT`

Kriteria Peringatan

- Kuning: Aturan grup keamanan DB merujuk pada grup keamanan Amazon EC2 yang memberikan akses global pada salah satu port ini: 20, 21, 22, 1433, 1434, 3306, 3389, 4333, 5432, 5500.
- Kuning: Aturan grup keamanan DB memberikan akses ke lebih dari satu alamat IP (akhiran aturan CIDR bukan /0 atau/32).
- Merah: Aturan grup keamanan DB memberikan akses global (akhiran aturan CIDR adalah /0).

Tindakan yang Direkomendasikan

Tinjau aturan grup keamanan Anda dan batasi akses ke alamat IP resmi atau rentang IP. Untuk mengedit grup keamanan, gunakan AuthorizeDB SecurityGroup Ingress API atau file. AWS Management Console Untuk informasi selengkapnya, lihat Bekerja dengan Grup Keamanan DB.

Sumber Daya Tambahan

- Grup Keamanan Amazon RDS
- Perutean Antar Domain Tanpa Kelas
- Daftar nomor port TCP dan UDP

Kolom laporan

- Status
- Wilayah
- Nama Grup Keamanan RDS
- Aturan Masuk
- Alasan

Enkripsi penyimpanan Amazon RDS dimatikan

Deskripsi

Amazon RDS mendukung enkripsi saat istirahat untuk semua mesin database dengan menggunakan kunci yang Anda kelola. AWS Key Management Service Pada instans DB aktif dengan enkripsi Amazon RDS, data yang disimpan saat istirahat di penyimpanan dienkripsi, mirip dengan pencadangan otomatis, replika baca, dan snapshot.

Jika enkripsi tidak diaktifkan saat membuat instans DB, maka Anda harus mengembalikan salinan terenkripsi dari snapshot yang didekripsi sebelum Anda mengaktifkan enkripsi.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

> **Note**
>
> Ketika instans DB atau cluster DB dihentikan, Anda dapat melihat rekomendasi Amazon RDS Trusted Advisor selama 3 hingga 5 hari. Setelah lima hari, rekomendasi tidak tersedia di Trusted Advisor. Untuk melihat rekomendasi, buka konsol Amazon RDS, lalu pilih Rekomendasi.

Jika Anda menghapus instans DB atau kluster DB, maka rekomendasi yang terkait dengan instans atau cluster tersebut tidak tersedia di Trusted Advisor atau konsol manajemen Amazon RDS.

ID pemeriksaan

`c1qf5bt006`

Kriteria Peringatan

Merah: Sumber daya Amazon RDS tidak mengaktifkan enkripsi.

Tindakan yang Direkomendasikan

Aktifkan enkripsi data saat istirahat untuk instans DB Anda.

Sumber Daya Tambahan

Anda dapat mengenkripsi instans DB hanya ketika Anda membuat instans DB. Untuk mengenkripsi instans DB aktif yang ada:

Buat salinan terenkripsi dari instans DB asli

1. Buat snapshot instans DB Anda.
2. Buat salinan terenkripsi dari snapshot yang dibuat pada langkah 1.
3. Kembalikan instance DB dari snapshot terenkripsi.

Untuk informasi selengkapnya, lihat sumber daya berikut:

- Mengenkripsi sumber daya Amazon RDS
- Menyalin snapshot DB

Kolom laporan

- Status
- Wilayah
- Resouce
- Nama Mesin
- Waktu Terakhir Diperbarui

Amazon Route 53 tidak cocok dengan catatan CNAME yang menunjuk langsung ke bucket S3

Deskripsi

Memeriksa Zona Dihosting Amazon Route 53 dengan catatan CNAME yang mengarah langsung ke nama host bucket Amazon S3 dan peringatan jika CNAME Anda tidak cocok dengan nama bucket S3 Anda.

ID pemeriksaan

`c1ng44jvbm`

Kriteria Peringatan

Merah: Amazon Route 53 Hosted Zone memiliki catatan CNAME yang menunjuk ke nama host bucket S3 yang tidak cocok.

Hijau: Tidak ada catatan CNAME yang tidak cocok yang ditemukan di Zona Dihosting Amazon Route 53 Anda.

Tindakan yang Direkomendasikan

Saat mengarahkan catatan CNAME ke nama host bucket S3, Anda harus memastikan ada bucket yang cocok untuk catatan CNAME atau alias yang Anda konfigurasikan. Dengan melakukan ini, Anda menghindari risiko catatan CNAME Anda dipalsukan. Anda juga mencegah AWS pengguna yang tidak sah menghosting konten web yang salah atau berbahaya dengan domain Anda.

Untuk menghindari mengarahkan catatan CNAME langsung ke nama host bucket S3, pertimbangkan untuk menggunakan kontrol akses asal (OAC) untuk mengakses aset web bucket S3 Anda melalui Amazon. CloudFront

Untuk informasi selengkapnya tentang mengaitkan CNAME dengan nama host bucket Amazon S3, lihat Menyesuaikan URL Amazon S3 dengan catatan CNAME.

Sumber Daya Tambahan

- Cara mengaitkan nama host dengan bucket Amazon S3
- Membatasi akses ke asal Amazon S3 dengan CloudFront

Kolom laporan

- Status
- ID Zona yang Dihosting

- Zona yang Dihosting ARN
- Mencocokkan Catatan CNAME
- Catatan CNAME yang tidak cocok
- Waktu Terakhir Diperbarui

Amazon Route 53 Kumpulan Rekaman Sumber Daya MX dan Kerangka Kebijakan Pengirim

Deskripsi

Untuk setiap kumpulan rekaman sumber daya MX, periksa apakah kumpulan catatan sumber daya TXT atau SPF berisi catatan SPF yang valid. Catatan harus dimulai dengan "`v=spf1`". Catatan SPF menentukan server yang berwenang untuk mengirim email untuk domain Anda, yang membantu mendeteksi dan menghentikan spoofing alamat email dan untuk mengurangi spam. Route 53 merekomendasikan agar Anda menggunakan catatan TXT alih-alih catatan SPF. Trusted Advisor melaporkan pemeriksaan ini berwarna hijau selama setiap set catatan sumber daya MX memiliki setidaknya satu catatan SPF atau TXT.

ID pemeriksaan

`c9D319e7sG`

Kriteria Peringatan

Kuning: Kumpulan catatan sumber daya MX tidak memiliki catatan sumber daya TXT atau SPF yang berisi nilai SPF yang valid.

Tindakan yang Direkomendasikan

Untuk setiap kumpulan rekaman sumber daya MX, buat kumpulan catatan sumber daya TXT yang berisi nilai SPF yang valid. Untuk informasi selengkapnya, lihat Kerangka Kebijakan Pengirim: Sintaks Rekaman SPF dan Membuat Kumpulan Rekaman Sumber Daya Dengan Menggunakan Konsol Amazon Route 53.

Sumber Daya Tambahan

- Kerangka Kebijakan Pengirim
- Rekor MX

Kolom laporan

- Nama Zona yang Dihosting

- ID Zona yang Dihosting
- Nama Set Rekaman Sumber Daya
- Status

Izin Bucket Amazon S3

Deskripsi

Memeriksa bucket di Amazon Simple Storage Service (Amazon S3) yang memiliki izin akses terbuka, atau yang memungkinkan akses ke pengguna yang diautentikasi. AWS

Pemeriksaan ini memeriksa izin bucket eksplisit, serta kebijakan bucket yang mungkin mengganti izin tersebut. Memberikan izin akses daftar ke semua pengguna untuk bucket Amazon S3 tidak disarankan. Izin ini dapat menyebabkan pengguna yang tidak diinginkan mencantumkan objek di bucket pada frekuensi tinggi, yang dapat menghasilkan biaya yang lebih tinggi dari yang diharapkan. Izin yang memberikan akses unggah dan hapus ke semua orang dapat menyebabkan kerentanan keamanan di bucket Anda.

ID pemeriksaan

`Pfx0RwqBli`

Kriteria Peringatan

- Kuning: Bucket ACL memungkinkan akses Daftar untuk Semua Orang atau Pengguna Terautentikasi. AWS
- Kuning: Kebijakan bucket memungkinkan segala jenis akses terbuka.
- Kuning: Kebijakan Bucket memiliki pernyataan yang memberikan akses publik. Blokir akses publik dan lintas akun ke bucket yang memiliki pengaturan kebijakan publik diaktifkan dan telah membatasi akses hanya ke pengguna yang berwenang dari akun tersebut hingga pernyataan publik dihapus.
- Kuning: Trusted Advisor tidak memiliki izin untuk memeriksa kebijakan, atau kebijakan tidak dapat dievaluasi karena alasan lain.
- Merah: Bucket ACL memungkinkan akses unggah dan hapus untuk Semua Orang atau Pengguna Terautentikasi. AWS

Tindakan yang Direkomendasikan

Jika bucket memungkinkan akses terbuka, tentukan apakah akses terbuka benar-benar diperlukan. Jika tidak, perbarui izin bucket untuk membatasi akses ke pemilik atau pengguna

tertentu. Gunakan Amazon S3 Blokir Akses Publik untuk mengontrol pengaturan yang memungkinkan akses publik ke data Anda. Lihat Menyetel Bucket dan Izin Akses Objek.

Sumber Daya Tambahan

Mengelola Izin Akses ke Sumber Daya Amazon S3 Anda

Kolom laporan

- Status
- Nama wilayah
- Parameter API Wilayah
- Nama Bucket
- ACL Memungkinkan Daftar
- ACL Memungkinkan Upload/Delete
- Kebijakan Memungkinkan Akses

Log Akses Amazon S3Server Diaktifkan

Deskripsi

Memeriksa konfigurasi logging bucket Amazon Simple Storage Service.

Saat pencatatan akses server diaktifkan, log akses terperinci dikirimkan setiap jam ke bucket yang Anda pilih. Catatan log akses berisi rincian tentang setiap permintaan, seperti jenis permintaan, sumber daya yang ditentukan dalam permintaan, dan waktu dan tanggal permintaan diproses. Secara default, pencatatan bucket tidak diaktifkan. Anda harus mengaktifkan pencatatan jika ingin melakukan audit keamanan atau mempelajari lebih lanjut tentang pengguna dan pola penggunaan.

Ketika logging awalnya diaktifkan, konfigurasi secara otomatis divalidasi. Namun, modifikasi future dapat mengakibatkan kegagalan logging. Pemeriksaan ini memeriksa izin bucket Amazon S3 eksplisit. Cara terbaik adalah menggunakan kebijakan bucket untuk mengontrol izin bucket, namun ACL juga dapat digunakan.

ID pemeriksaan

`c1fd6b96l4`

Kriteria Peringatan

- Kuning: Bucket tidak mengaktifkan pencatatan akses server.

- Kuning: Izin bucket target tidak menyertakan akun root, jadi Trusted Advisor tidak dapat memeriksanya.
- Merah: Ember target tidak ada.
- Merah: Ember target dan ember sumber memiliki pemilik yang berbeda.
- Merah: Pengirim log tidak memiliki izin menulis untuk bucket target.
- Hijau: Bucket mengaktifkan pencatatan akses server, target ada, dan izin untuk menulis ke target ada

Tindakan yang Direkomendasikan

Aktifkan pencatatan ember untuk sebagian besar ember. Lihat Mengaktifkan Pencatatan Menggunakan Konsol dan Mengaktifkan Pencatatan Secara Terprogram.

Jika izin bucket target tidak menyertakan akun root dan Anda Trusted Advisor ingin memeriksa status logging, tambahkan akun root sebagai penerima hibah. Lihat Mengedit Izin Bucket.

Jika bucket target tidak ada, pilih bucket yang sudah ada sebagai target atau buat bucket baru dan pilih bucket tersebut. Lihat Mengelola Bucket Logging.

Jika target dan sumber memiliki pemilik yang berbeda, ubah bucket target menjadi bucket yang memiliki pemilik yang sama dengan bucket sumber. Lihat Mengelola Bucket Logging.

Jika pengirim log tidak memiliki izin menulis untuk target (Tulis tidak diaktifkan), berikan izin Unggah/Hapus ke grup Pengiriman Log. Disarankan menggunakan kebijakan bucket melalui ACL. Lihat Mengedit Izin Bucket dan Izin untuk Pengiriman Log.

Sumber Daya Tambahan

Bekerja dengan ember

Pencatatan akses server

Format log akses server

Menghapus file log

Kolom laporan

- Status
- Wilayah
- ARN Sumber Daya

- Nama Bucket
- Nama Target
- Target Ada
- Pemilik yang sama
- Menulis Diaktifkan
- Alasan
- Waktu Terakhir Diperbarui

Koneksi Peering VPC Amazon dengan Resolusi DNS Dinonaktifkan

Deskripsi

Memeriksa apakah koneksi peering VPC Anda mengaktifkan resolusi DNS untuk vPC akseptor dan pemohon.

Resolusi DNS untuk koneksi peering VPC memungkinkan resolusi nama host DNS publik ke alamat IPv4 pribadi saat ditanyakan dari VPC Anda. Hal ini memungkinkan penggunaan nama DNS untuk komunikasi antara sumber daya dalam VPC peered. Resolusi DNS dalam koneksi peering VPC Anda membuat pengembangan dan manajemen aplikasi lebih sederhana dan tidak terlalu rawan kesalahan, dan memastikan bahwa sumber daya selalu berkomunikasi secara pribadi melalui koneksi peering VPC.

Anda dapat menentukan ID VPC, menggunakan parameter VPCIDS dalam aturan Anda. AWS Config

Untuk informasi selengkapnya, lihat Mengaktifkan resolusi DNS untuk koneksi peering VPC.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

`c18d2gz124`

Sumber

AWS Config Managed Rule: vpc-peering-dns-resolution-check

Kriteria Peringatan

Kuning: Resolusi DNS tidak diaktifkan untuk akseptor dan VPC pemohon dalam koneksi peering VPC.

Tindakan yang Direkomendasikan

Aktifkan resolusi DNS untuk koneksi peering VPC Anda.

Sumber Daya Tambahan

- Ubah opsi koneksi peering VPC
- Atribut DNS di VPC Anda

Kolom laporan

- Status
- Wilayah
- Sumber Daya
- AWS Config Aturan
- Parameter Input
- Waktu Terakhir Diperbarui

AWS Backup Vault Tanpa Kebijakan Berbasis Sumber Daya untuk Mencegah Penghapusan Poin Pemulihan

Deskripsi

Memeriksa apakah AWS Backup vault memiliki kebijakan berbasis sumber daya terlampir yang mencegah penghapusan titik pemulihan.

Kebijakan berbasis sumber daya mencegah penghapusan titik pemulihan yang tidak terduga, yang memungkinkan Anda untuk menerapkan kontrol akses dengan hak istimewa paling sedikit terhadap data cadangan Anda.

Anda dapat menentukan AWS Identity and Access Management ARN yang Anda tidak ingin aturan untuk memeriksa ArnList parameter utama AWS Config aturan Anda.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

`c18d2gz152`

Sumber

`AWS Config Managed Rule: backup-recovery-point-manual-deletion-disabled`

Kriteria Peringatan

Kuning: Ada AWS Backup brankas yang tidak memiliki kebijakan berbasis sumber daya untuk mencegah penghapusan titik pemulihan.

Tindakan yang Direkomendasikan

Buat kebijakan berbasis sumber daya untuk AWS Backup brankas Anda untuk mencegah penghapusan titik pemulihan yang tidak terduga.

Kebijakan harus menyertakan pernyataan “Tolak” dengan PutBackupVaultAccessPolicy izin cadangan: DeleteRecovery Point, backup: UpdateRecoveryPointLifecycle, dan backup:.

Untuk informasi selengkapnya, lihat Menetapkan kebijakan akses pada brankas cadangan.

Kolom laporan

- Status
- Wilayah
- Sumber Daya
- AWS Config Aturan
- Parameter Input
- Waktu Terakhir Diperbarui

AWS CloudTrail Penebangan

Deskripsi

Memeriksa penggunaan Anda AWS CloudTrail. CloudTrail memberikan peningkatan visibilitas ke aktivitas Anda Akun AWS dengan merekam informasi tentang panggilan AWS API yang dilakukan di akun. Anda dapat menggunakan log ini untuk menentukan, misalnya, tindakan apa yang telah dilakukan pengguna tertentu selama periode waktu tertentu, atau pengguna mana yang telah mengambil tindakan pada sumber daya tertentu selama periode waktu tertentu.

Karena CloudTrail mengirimkan file log ke bucket Amazon Simple Storage Service (Amazon S3) Simple Storage Service (Amazon S3), CloudTrail harus memiliki izin menulis untuk bucket. Jika jejak berlaku untuk semua Wilayah (default saat membuat jejak baru), jejak akan muncul beberapa kali dalam Trusted Advisor laporan.

ID pemeriksaan

`vjafUGJ9H0`

Kriteria Peringatan

- Kuning: CloudTrail melaporkan kesalahan pengiriman log untuk jejak.
- Merah: Jejak belum dibuat untuk suatu Wilayah, atau penebangan dimatikan untuk jalan setapak.

Tindakan yang Direkomendasikan

Untuk membuat jejak dan mulai masuk dari konsol, buka AWS CloudTrail konsol.

Untuk memulai logging, lihat Menghentikan dan Memulai Logging untuk Jejak.

Jika Anda menerima kesalahan pengiriman log, periksa untuk memastikan bahwa bucket ada dan kebijakan yang diperlukan dilampirkan ke bucket. Lihat Kebijakan Bucket Amazon S3.

Sumber Daya Tambahan

- AWS CloudTrail Panduan Pengguna
- Wilayah yang didukung
- Layanan yang Didukung

Kolom laporan

- Status

- Wilayah
- Nama Jejak
- Status Pencatatan
- Nama Bucket
- Tanggal Pengiriman Terakhir

AWS Lambda Fungsi Menggunakan Runtime yang Tidak Digunakan Lagi

Deskripsi

Memeriksa fungsi Lambda yang versi $LATEST dikonfigurasi untuk menggunakan runtime yang mendekati penghentian, atau tidak digunakan lagi. Runtime yang tidak digunakan lagi tidak memenuhi syarat untuk pembaruan keamanan atau dukungan teknis

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

Versi fungsi Lambda yang diterbitkan tidak dapat diubah, yang berarti mereka dapat dipanggil tetapi tidak diperbarui. Hanya `$LATEST` versi untuk fungsi Lambda yang dapat diperbarui. Untuk informasi selengkapnya, lihat Versi fungsi Lambda.

ID pemeriksaan

`L4dfs2Q4C5`

Kriteria Peringatan

- Merah: Versi $LATEST fungsi dikonfigurasi untuk menggunakan runtime yang sudah usang.
- Kuning: Versi $LATEST fungsi berjalan pada runtime yang akan usang dalam 180 hari.

Tindakan yang Direkomendasikan

Jika Anda memiliki fungsi yang berjalan pada runtime yang mendekati penghentian, Anda harus mempersiapkan migrasi ke runtime yang didukung. Untuk informasi selengkapnya, lihat Kebijakan dukungan Runtime.

Kami menyarankan Anda menghapus versi fungsi sebelumnya yang tidak lagi Anda gunakan.

Sumber Daya Tambahan

Runtime Lambda

Kolom laporan

- Status
- Wilayah
- Fungsi ARN
- Waktu Aktif
- Hari ke Deprecation
- Tanggal penghentian
- Rata-rata Pemanggilan Harian
- Waktu Terakhir Diperbarui

AWS Well-Architectedmasalah risiko tinggi untuk keamanan

Deskripsi

Memeriksa masalah risiko tinggi (HRI) untuk beban kerja Anda di pilar keamanan. Pemeriksaan ini didasarkan pada AWS-Well Architected ulasan Anda. Hasil pemeriksaan Anda tergantung pada apakah Anda menyelesaikan evaluasi beban kerja denganAWS Well-Architected.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

`Wxdfp4B1L3`

Kriteria Peringatan

- Merah: Setidaknya satu masalah risiko tinggi aktif diidentifikasi dalam pilar keamanan untuk AWS Well-Architected.

- Hijau: Tidak ada masalah risiko tinggi aktif yang terdeteksi di pilar keamanan untuk AWS Well-Architected.

Tindakan yang Direkomendasikan

AWS Well-Architected mendeteksi masalah risiko tinggi selama evaluasi beban kerja Anda. Masalah-masalah ini menghadirkan peluang untuk mengurangi risiko dan menghemat uang. Masuk ke alat AWS Well-Architected untuk meninjau jawaban Anda dan mengambil tindakan untuk menyelesaikan masalah aktif Anda.

Kolom laporan

- Status
- Wilayah
- Beban Kerja ARN
- Nama Beban Kerja
- Nama Pengulas
- Jenis Beban Kerja
- Tanggal Mulai Beban Kerja
- Beban Kerja Tanggal Modifikasi Terakhir
- Jumlah HRI yang diidentifikasi untuk Keamanan
- Jumlah HRI yang diselesaikan untuk Keamanan
- Jumlah pertanyaan untuk Keamanan
- Jumlah total pertanyaan di pilar Keamanan
- Waktu Terakhir Diperbarui

CloudFrontSertifikat SSL Kustom di Toko Sertifikat IAM

Deskripsi

Memeriksa sertifikat SSL untuk nama domain CloudFront alternatif di toko sertifikat IAM. Pemeriksaan ini memberi tahu Anda jika sertifikat kedaluwarsa, akan segera kedaluwarsa, menggunakan enkripsi yang sudah ketinggalan zaman, atau tidak dikonfigurasi dengan benar untuk distribusi.

Ketika sertifikat khusus untuk nama domain alternatif kedaluwarsa, browser yang menampilkan CloudFront konten Anda mungkin menampilkan pesan peringatan tentang keamanan situs web

Anda. Sertifikat yang dienkripsi dengan menggunakan algoritma hashing SHA-1 tidak digunakan lagi oleh browser web seperti Chrome dan Firefox.

Sertifikat harus berisi nama domain yang cocok dengan Nama Domain Asal atau nama domain di header host permintaan penampil. Jika tidak cocok, CloudFront mengembalikan kode status HTTP 502 (gateway buruk) ke pengguna. Untuk informasi lebih lanjut, lihat Menggunakan Nama Domain Alternatif dan HTTPS.

ID pemeriksaan

`N425c450f2`

Kriteria Peringatan

- Merah: Sertifikat SSL khusus kedaluwarsa.
- Kuning: Sertifikat SSL khusus kedaluwarsa dalam tujuh hari ke depan.
- Kuning: Sertifikat SSL khusus dienkripsi dengan menggunakan algoritma hashing SHA-1.
- Kuning: Satu atau beberapa nama domain alternatif dalam distribusi tidak muncul baik di bidang Nama Umum atau bidang Nama Alternatif Subjek dari sertifikat SSL kustom.

Tindakan yang Direkomendasikan

Perpanjang sertifikat yang kedaluwarsa atau sertifikat yang akan kedaluwarsa.

Ganti sertifikat yang dienkripsi dengan menggunakan algoritma hashing SHA-1 dengan sertifikat yang dienkripsi dengan menggunakan algoritma hashing SHA-256.

Ganti sertifikat dengan sertifikat yang berisi nilai yang berlaku di bidang Nama Umum atau Nama Domain Alternatif Subjek.

Sumber Daya Tambahan

Menggunakan Koneksi HTTPS untuk Mengakses Objek Anda

Kolom laporan

- Status
- ID Distribusi
- Nama Domain Distribusi
- Nama Sertifikat
- Alasan

CloudFront Sertifikat SSL di Server Asal

Deskripsi

Memeriksa server asal Anda untuk sertifikat SSL yang kedaluwarsa, akan kedaluwarsa, hilang, atau yang menggunakan enkripsi usang. Jika sertifikat memiliki salah satu masalah ini, CloudFront menanggapi permintaan untuk konten Anda dengan kode status HTTP 502, Bad Gateway.

Sertifikat yang dienkripsi dengan menggunakan algoritma hashing SHA-1 tidak digunakan lagi oleh browser web seperti Chrome dan Firefox. Bergantung pada jumlah sertifikat SSL yang telah Anda kaitkan dengan CloudFront distribusi Anda, pemeriksaan ini mungkin menambahkan beberapa sen per bulan ke tagihan Anda dengan penyedia hosting web Anda, misalnya, AWS jika Anda menggunakan Amazon EC2 atau Elastic Load Balancing sebagai asal distribusi Anda. CloudFront Pemeriksaan ini tidak memvalidasi rantai sertifikat asal atau otoritas sertifikat Anda. Anda dapat memeriksanya di CloudFront konfigurasi Anda.

ID pemeriksaan

`N430c450f2`

Kriteria Peringatan

- Merah: Sertifikat SSL pada asal Anda telah kedaluwarsa atau tidak ada.
- Kuning: Sertifikat SSL tentang asal Anda kedaluwarsa dalam tiga puluh hari ke depan.
- Kuning: Sertifikat SSL pada asal Anda dienkripsi dengan menggunakan algoritma hashing SHA-1.
- Kuning: Sertifikat SSL pada asal Anda tidak dapat ditemukan. Koneksi mungkin gagal karena batas waktu, atau masalah koneksi HTTPS lainnya.

Tindakan yang Direkomendasikan

Perpanjang sertifikat asal Anda jika telah kedaluwarsa atau akan kedaluwarsa.

Tambahkan sertifikat jika tidak ada.

Ganti sertifikat yang dienkripsi dengan menggunakan algoritma hashing SHA-1 dengan sertifikat yang dienkripsi dengan menggunakan algoritma hashing SHA-256.

Sumber Daya Tambahan

Menggunakan Nama Domain Alternatif dan HTTPS

Kolom laporan

- Status
- ID Distribusi
- Nama Domain Distribusi
- Asal
- Alasan

ELB Listener Keamanan

Deskripsi

Memeriksa penyeimbang beban dengan pendengar yang tidak menggunakan konfigurasi keamanan yang disarankan untuk komunikasi terenkripsi. AWS merekomendasikan penggunaan protokol aman (HTTPS atau SSL), kebijakan up-to-date keamanan, serta sandi dan protokol yang aman.

Saat Anda menggunakan protokol aman untuk koneksi front-end (client to load balancer), permintaan dienkripsi antara klien Anda dan penyeimbang beban, yang menciptakan lingkungan yang lebih aman. Elastic Load Balancing menyediakan kebijakan keamanan yang telah ditentukan sebelumnya dengan sandi dan protokol yang mematuhi praktik terbaik keamanan. AWS Versi baru dari kebijakan yang telah ditetapkan dirilis saat konfigurasi baru tersedia.

ID pemeriksaan

`a2sEc6ILx`

Kriteria Peringatan

- Kuning: Load balancer tidak memiliki pendengar yang menggunakan protokol aman (HTTPS atau SSL).
- Kuning: Pendengar penyeimbang beban menggunakan kebijakan keamanan SSL yang telah ditentukan sebelumnya.
- Kuning: Pendengar penyeimbang beban menggunakan sandi atau protokol yang tidak direkomendasikan.
- Merah: Pendengar penyeimbang beban menggunakan sandi atau protokol yang tidak aman.

Tindakan yang Direkomendasikan

Jika lalu lintas ke penyeimbang beban Anda harus aman, gunakan protokol HTTPS atau SSL untuk koneksi front-end.

Tingkatkan penyeimbang beban Anda ke versi terbaru dari kebijakan keamanan SSL yang telah ditentukan sebelumnya.

Gunakan hanya cipher dan protokol yang direkomendasikan.

Untuk informasi selengkapnya, lihat Konfigurasi Pendengar untuk Elastic Load Balancing.

Sumber Daya Tambahan

- Konfigurasi Pendengar Referensi Cepat
- Perbarui Konfigurasi Negosiasi SSL Load Balancer Anda
- Konfigurasi Negosiasi SSL untuk Elastic Load Balancing
- Tabel Kebijakan Keamanan SSL

Kolom laporan

- Status
- Wilayah
- Nama Load Balancer
- Port Load Balancer
- Alasan

Grup Keamanan ELB

Deskripsi

Memeriksa penyeimbang beban yang dikonfigurasi dengan grup keamanan yang hilang, atau grup keamanan yang memungkinkan akses ke port yang tidak dikonfigurasi untuk penyeimbang beban.

Jika grup keamanan yang terkait dengan penyeimbang beban dihapus, penyeimbang beban tidak akan berfungsi seperti yang diharapkan. Jika grup keamanan memungkinkan akses ke port yang tidak dikonfigurasi untuk penyeimbang beban, risiko kehilangan data atau serangan berbahaya meningkat.

ID pemeriksaan

`xSqX82fQu`

Kriteria Peringatan

- Kuning: Aturan masuk grup keamanan VPC Amazon yang terkait dengan penyeimbang beban memungkinkan akses ke port yang tidak ditentukan dalam konfigurasi pendengar penyeimbang beban.
- Merah: Grup keamanan yang terkait dengan penyeimbang beban tidak ada.

Tindakan yang Direkomendasikan

Konfigurasikan aturan grup keamanan untuk membatasi akses hanya ke port dan protokol yang ditentukan dalam konfigurasi pendengar penyeimbang beban, ditambah protokol ICMP untuk mendukung Path MTU Discovery. Lihat Pendengar untuk Classic Load Balancer dan Grup Keamanan Anda untuk Load Balancer di VPC.

Jika grup keamanan hilang, terapkan grup keamanan baru ke penyeimbang beban. Buat aturan grup keamanan yang membatasi akses hanya ke port dan protokol yang ditentukan dalam konfigurasi pendengar penyeimbang beban. Lihat Grup Keamanan untuk Load Balancer di VPC.

Sumber Daya Tambahan

- Panduan Pengguna Elastic Load Balancing
- Konfigurasikan Classic Load Balancer Anda

Kolom laporan

- Status
- Wilayah
- Nama Load Balancer
- ID Grup Keamanan
- Alasan

Exposed Access Keys

Deskripsi

Memeriksa repositori kode populer untuk kunci akses yang telah diekspos ke publik dan untuk penggunaan Amazon Elastic Compute Cloud (Amazon EC2) yang tidak teratur yang mungkin merupakan hasil dari kunci akses yang disusupi.

Kunci akses terdiri dari ID kunci akses dan kunci akses rahasia yang sesuai. Kunci akses yang terbuka menimbulkan risiko keamanan bagi akun Anda dan pengguna lain, dapat menyebabkan

biaya berlebihan dari aktivitas atau penyalahgunaan yang tidak sah, dan melanggar Perjanjian AWS Pelanggan.

Jika kunci akses Anda terbuka, segera ambil tindakan untuk mengamankan akun Anda. Untuk melindungi akun Anda dari biaya yang berlebihan, batasi AWS sementara kemampuan Anda untuk membuat beberapa AWS sumber daya. Ini tidak membuat akun Anda aman. Ini hanya membatasi sebagian penggunaan tidak sah yang dapat dikenakan biaya.

> **Note**
>
> Pemeriksaan ini tidak menjamin identifikasi kunci akses yang terbuka atau instans EC2 yang disusupi. Anda pada akhirnya bertanggung jawab atas keselamatan dan keamanan kunci akses dan AWS sumber daya Anda.
> Hasil untuk pemeriksaan ini disegarkan secara otomatis, dan permintaan penyegaran tidak diizinkan. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

Jika tenggat waktu ditampilkan untuk kunci akses, AWS dapat menangguhkan Anda Akun AWS jika penggunaan yang tidak sah tidak dihentikan pada tanggal tersebut. Jika Anda yakin ada peringatan yang salah, hubungi AWS Support.

Informasi yang ditampilkan Trusted Advisor mungkin tidak mencerminkan status terbaru akun Anda. Tidak ada kunci akses terbuka yang ditandai sebagai diselesaikan sampai semua kunci akses yang terbuka pada akun telah diselesaikan. Sinkronisasi data ini bisa memakan waktu hingga satu minggu.

ID pemeriksaan

`12Fnkpl8Y5`

Kriteria Peringatan

- Merah: Berpotensi dikompromikan - AWS telah mengidentifikasi ID kunci akses dan kunci akses rahasia terkait yang telah terpapar di Internet dan mungkin telah disusupi (digunakan).
- Red: Exposed — AWS telah mengidentifikasi ID kunci akses dan kunci akses rahasia terkait yang telah terpapar di Internet.
- Merah: Diduga - Penggunaan Amazon EC2 yang tidak teratur menunjukkan bahwa kunci akses mungkin telah dikompromikan, tetapi belum diidentifikasi sebagai terpapar di Internet.

Tindakan yang Direkomendasikan

Hapus kunci akses yang terpengaruh sesegera mungkin. Jika kunci dikaitkan dengan pengguna IAM, lihat Mengelola Kunci Akses untuk Pengguna IAM.

Periksa akun Anda untuk penggunaan yang tidak sah. Masuk ke AWS Management Consoledan periksa setiap konsol layanan untuk sumber daya yang mencurigakan. Berikan perhatian khusus untuk menjalankan instans Amazon EC2, permintaan Instans Spot, kunci akses, dan pengguna IAM. Anda juga dapat memeriksa penggunaan keseluruhan pada konsol Billing and Cost Management.

Sumber Daya Tambahan

- Praktik Terbaik untuk Mengelola Kunci AWS Akses
- AWS Pedoman Audit Keamanan

Kolom laporan

- Access key ID
- Nama Pengguna (IAM atau Root)
- Jenis Penipuan
- ID Kasus
- Waktu Diperbarui
- Lokasi
- Batas waktu
- Penggunaan (USD per Hari)

Rotasi Kunci Akses IAM

Deskripsi

Memeriksa kunci akses IAM aktif yang belum diputar dalam 90 hari terakhir.

Ketika Anda memutar kunci akses Anda secara teratur, Anda mengurangi kemungkinan bahwa kunci yang dikompromikan dapat digunakan tanpa sepengetahuan Anda untuk mengakses sumber daya. Untuk keperluan pemeriksaan ini, tanggal dan waktu rotasi terakhir adalah ketika kunci akses dibuat atau yang terbaru diaktifkan. Nomor kunci akses dan tanggal berasal dari `access_key_1_last_rotated` dan `access_key_2_last_rotated` informasi dalam laporan kredensi IAM terbaru.

Karena frekuensi regenerasi laporan kredensyal dibatasi, penyegaran pemeriksaan ini mungkin tidak mencerminkan perubahan terbaru. Untuk informasi selengkapnya, lihat Mendapatkan Laporan Kredensi untuk Anda Akun AWS.

Untuk membuat dan memutar kunci akses, pengguna harus memiliki izin yang sesuai. Untuk informasi selengkapnya, lihat Mengizinkan Pengguna Mengelola Kata Sandi, Kunci Akses, dan Kunci SSH Mereka Sendiri.

ID pemeriksaan

`DqdJqYeRm5`

Kriteria Peringatan

- Hijau: Kunci akses aktif dan telah diputar dalam 90 hari terakhir.
- Kuning: Kunci akses aktif dan telah diputar dalam 2 tahun terakhir, tetapi lebih dari 90 hari yang lalu.
- Merah: Kunci akses aktif dan belum diputar dalam 2 tahun terakhir.

Tindakan yang Direkomendasikan

Putar tombol akses secara teratur. Lihat Memutar Kunci Akses dan Mengelola Kunci Akses untuk Pengguna IAM.

Sumber Daya Tambahan

- Praktik Terbaik IAM
- Cara memutar tombol akses untuk pengguna IAM

Kolom laporan

- Status
- Pengguna IAM
- Access key
- Kunci Terakhir Diputar
- Alasan

Kebijakan Kata Sandi IAM

Deskripsi

Memeriksa kebijakan kata sandi untuk akun Anda dan memperingatkan saat kebijakan kata sandi tidak diaktifkan, atau jika persyaratan konten kata sandi belum diaktifkan.

Persyaratan konten kata sandi meningkatkan keamanan AWS lingkungan Anda secara keseluruhan dengan menegakkan pembuatan kata sandi pengguna yang kuat. Saat Anda membuat atau mengubah kebijakan kata sandi, perubahan diberlakukan segera untuk pengguna baru tetapi tidak mengharuskan pengguna yang ada untuk mengubah kata sandi mereka.

ID pemeriksaan

`Yw2K9puPzl`

Kriteria Peringatan

- Kuning: Kebijakan kata sandi diaktifkan, tetapi setidaknya satu persyaratan konten tidak diaktifkan.
- Merah: Tidak ada kebijakan kata sandi yang diaktifkan.

Tindakan yang Direkomendasikan

Jika beberapa persyaratan konten tidak diaktifkan, pertimbangkan untuk mengaktifkannya. Jika tidak ada kebijakan kata sandi yang diaktifkan, buat dan konfigurasikan satu. Lihat Menyetel Kebijakan Kata Sandi Akun untuk Pengguna IAM.

Sumber Daya Tambahan

Mengelola Kata Sandi

Kolom laporan

- Kebijakan Kata Sandi
- Huruf besar
- Huruf kecil
- Jumlah
- Bukan alfanumerik

MFA pada Akun Root

Deskripsi

Memeriksa akun root dan memperingatkan jika otentikasi multi-faktor (MFA) tidak diaktifkan.

Untuk meningkatkan keamanan, kami menyarankan Anda melindungi akun Anda dengan menggunakan MFA, yang mengharuskan pengguna untuk memasukkan kode otentikasi unik

dari perangkat keras MFA atau perangkat virtual mereka saat berinteraksi dengan dan situs web terkait. AWS Management Console

ID pemeriksaan

`7DAFEmoDos`

Kriteria Peringatan

Merah: MFA tidak diaktifkan pada akun root.

Tindakan yang Direkomendasikan

Masuk ke akun root Anda dan aktifkan perangkat MFA. Lihat Memeriksa Status MFA dan Menyiapkan Perangkat MFA.

Sumber Daya Tambahan

Menggunakan Perangkat Multi-Factor Authentication (MFA) dengan AWS

Grup Keamanan — Port Tertentu Tidak Dibatasi

Deskripsi

Memeriksa grup keamanan untuk aturan yang memungkinkan akses tidak terbatas (0.0.0.0/0) ke port tertentu.

Akses tidak terbatas meningkatkan peluang untuk aktivitas berbahaya (peretasan, denial-of-service serangan, kehilangan data). Port dengan risiko tertinggi ditandai merah, dan port dengan risiko lebih kecil ditandai kuning. Port yang ditandai hijau biasanya digunakan oleh aplikasi yang memerlukan akses tidak terbatas, seperti HTTP dan SMTP.

Jika Anda sengaja mengonfigurasi grup keamanan Anda dengan cara ini, sebaiknya gunakan langkah-langkah keamanan tambahan untuk mengamankan infrastruktur Anda (seperti tabel IP).

> **Note**
>
> Pemeriksaan ini hanya mengevaluasi grup keamanan yang Anda buat dan aturan masuknya untuk alamat IPv4. Grup keamanan AWS Directory Service yang dibuat oleh ditandai sebagai merah atau kuning, tetapi mereka tidak menimbulkan risiko keamanan dan dapat diabaikan atau dikecualikan dengan aman. Untuk informasi lebih lanjut, lihat Trusted Advisor FAQ.

> **Note**
>
> Pemeriksaan ini tidak menyertakan kasus penggunaan ketika daftar awalan terkelola pelanggan memberikan akses ke 0.0.0.0/0 dan digunakan sebagai sumber dengan grup keamanan.

ID pemeriksaan

`HCP4007jGY`

Kriteria Peringatan

- Hijau: Akses ke port 80, 25, 443, atau 465 tidak dibatasi.
- Merah: Akses ke port 20, 21, 1433, 1434, 3306, 3389, 4333, 5432, atau 5500 tidak dibatasi.
- Kuning: Akses ke port lain tidak dibatasi.

Tindakan yang Direkomendasikan

Batasi akses hanya ke alamat IP yang membutuhkannya. Untuk membatasi akses ke alamat IP tertentu, atur akhiran ke /32 (misalnya, 192.0.2.10/32). Pastikan untuk menghapus aturan yang terlalu permisif setelah membuat aturan yang lebih ketat.

Sumber Daya Tambahan

- Grup Keamanan Amazon EC2

  Daftar nomor port TCP dan UDP
- Perutean Antar Domain Tanpa Kelas

Kolom laporan

- Status
- Wilayah
- Nama Grup Keamanan
- ID Grup Keamanan
- Protokol
- Dari Port
- Ke Pelabuhan

Grup Keamanan — Akses Tidak Terbatas

Deskripsi

Memeriksa grup keamanan untuk aturan yang memungkinkan akses tidak terbatas ke sumber daya.

Akses tidak terbatas meningkatkan peluang untuk aktivitas berbahaya (peretasan, denial-of-service serangan, kehilangan data).

> **Note**
>
> Pemeriksaan ini hanya mengevaluasi grup keamanan yang Anda buat dan aturan masuknya untuk alamat IPv4. Grup keamanan AWS Directory Service yang dibuat oleh ditandai sebagai merah atau kuning, tetapi mereka tidak menimbulkan risiko keamanan dan dapat diabaikan atau dikecualikan dengan aman. Untuk informasi lebih lanjut, lihat Trusted Advisor FAQ.

> **Note**
>
> Pemeriksaan ini tidak menyertakan kasus penggunaan ketika daftar awalan terkelola pelanggan memberikan akses ke 0.0.0.0/0 dan digunakan sebagai sumber dengan grup keamanan.

ID pemeriksaan

`1iG5NDGVre`

Kriteria Peringatan

Merah: Aturan grup keamanan memiliki alamat IP sumber dengan akhiran /0 untuk port selain 25, 80, atau 443.

Tindakan yang Direkomendasikan

Batasi akses hanya ke alamat IP yang membutuhkannya. Untuk membatasi akses ke alamat IP tertentu, atur akhiran ke /32 (misalnya, 192.0.2.10/32). Pastikan untuk menghapus aturan yang terlalu permisif setelah membuat aturan yang lebih ketat.

Sumber Daya Tambahan

- Grup Keamanan Amazon EC2
- Perutean Antar Domain Tanpa Kelas

Kolom laporan

- Status
- Wilayah
- Nama Grup Keamanan
- ID Grup Keamanan
- Protokol
- Dari Port
- Ke Pelabuhan
- Rentang IP

Toleransi kesalahan

Anda dapat menggunakan pemeriksaan berikut untuk kategori toleransi kesalahan.

Periksa nama

- ALB Multi-AZ
- Amazon Aurora MySQL cluster backtracking tidak diaktifkan
- Aksesibilitas Instans Amazon Aurora DB
- Failover CloudFront Asal Amazon
- Amazon Comprehend Risiko Akses Titik Akhir
- Cluster AZ Tunggal Amazon DocumentDB
- Pemulihan Amazon oint-in-time DynamoDB P
- Tabel Amazon DynamoDB Tidak Termasuk dalam Paket Cadangan
- Amazon EBS Tidak Termasuk dalam Paket AWS Backup
- Cuplikan Amazon EBS
- Auto Scaling Amazon EC2 tidak mengaktifkan Pemeriksaan Kesehatan ELB
- Grup Auto Scaling Amazon EC2 memiliki Rebalancing Kapasitas Diaktifkan
- Auto Scaling Amazon EC2 tidak digunakan di beberapa AZ atau tidak memenuhi jumlah minimum AZ

- Saldo Zona Ketersediaan Amazon EC2
- Pemantauan Terperinci Amazon EC2 Tidak Diaktifkan
- Driver Amazon ECS AWS Logs dalam mode pemblokiran
- Layanan Amazon ECS menggunakan satu AZ
- Strategi penempatan Multi-AZ Amazon ECS
- Amazon EFS Tidak Ada Redundansi Target Mount
- Amazon EFS tidak ada dalam AWS Backup Rencana
- Cluster Amazon ElastiCache Multi-AZ
- Cadangan ElastiCache Otomatis Amazon Redis Cluster
- Amazon MemoryDB kluster Multi-AZ
- Broker MSK Amazon menghosting terlalu banyak partisi
- Domain Amazon OpenSearch Service dengan kurang dari tiga node data
- Cadangan Amazon RDS
- Cluster Amazon RDS DB memiliki satu instans DB
- Cluster Amazon RDS DB dengan semua instans di Availability Zone yang sama
- Cluster Amazon RDS DB dengan semua instans pembaca di Availability Zone yang sama
- Pemantauan Peningkatan Instans Amazon RDS DB tidak diaktifkan
- Instans Amazon RDS DB memiliki penyimpanan autoscaling dimatikan
- Instans Amazon RDS DB tidak menggunakan penerapan Multi-AZ
- Amazon RDS DiskQueueDepth
- Amazon RDS FreeStorageSpace
- Parameter log_output Amazon RDS diatur ke tabel
- Amazon RDS innodb_default_row_format pengaturan parameter tidak aman
- Amazon RDS innodb_flush_log_at_trx_commit parameter bukan 1
- Parameter Amazon RDS max_user_connections rendah
- Amazon RDS Multi-AZ
- Amazon RDS Tidak Dalam Rencana AWS Backup
- Replika Baca Amazon RDS terbuka dalam mode yang dapat ditulis
- Pencadangan otomatis sumber daya Amazon RDS dimatikan
- Parameter Amazon RDS sync_binlog dimatikan

- RDS DB Cluster tidak mengaktifkan replikasi Multi-AZ
- Instans Siaga Multi-AZ RDS Tidak Diaktifkan
- Amazon RDS ReplicaLag
- Parameter Amazon RDS synchronous_commit dimatikan
- Cuplikan otomatis klaster Amazon Redshift
- Amazon Route 53 Menghapus Pemeriksaan Kesehatan
- Rekor Sumber Daya Failover Amazon Route 53
- Amazon Route 53 Set Rekor Sumber Daya TTL Tinggi
- Delegasi Server Nama Amazon Route 53
- Amazon Route 53 Resolver Redundansi Zona Ketersediaan Titik Akhir
- Pencatatan Bucket Amazon S3
- Replikasi Bucket Amazon S3 Tidak Diaktifkan
- Versi Bucket Amazon S3
- Penyeimbang Beban Aplikasi, Jaringan, dan Gateway Tidak Mencakup Beberapa Zona Ketersediaan
- Auto Scaling IP tersedia di Subnet
- Pemeriksaan Kesehatan Grup Auto Scaling
- Sumber Daya Grup Auto Scaling
- AWS CloudHSM cluster yang menjalankan instance HSM dalam satu AZ
- AWS Direct Connect Ketahanan Lokasi
- AWS Lambda fungsi tanpa antrian huruf mati yang dikonfigurasi
- AWS Lambda Tentang Tujuan Acara Kegagalan
- Fungsi AWS Lambda berkemampuan VPC tanpa Redundansi Multi-AZ
- AWS Resilience Hub Pemeriksaan Komponen Aplikasi
- AWS Resilience Hub kebijakan dilanggar
- AWS Resilience Hub skor ketahanan
- AWS Resilience Hub usia penilaian
- AWS Site-to-Site VPN memiliki setidaknya satu terowongan dalam status DOWN
- AWS Well-Architectedmasalah risiko tinggi untuk keandalan
- Classic Load Balancer tidak memiliki beberapa AZ yang dikonfigurasi

- ELB Connection Draining
- Optimalisasi Penyeimbang Beban
- NAT Gateway AZ Kemerdekaan
- Penyeimbang Beban Jaringan Cross Load Balancing
- NLB - Sumber daya yang menghadap Internet di subnet pribadi
- NLB Multi-AZ
- Jumlah Wilayah AWS dalam set replikasi Manajer Insiden
- Pemeriksaan Aplikasi AZ Tunggal
- Antarmuka jaringan titik akhir antarmuka VPC di beberapa AZ
- Redundansi Terowongan VPN
- Redundansi Zona Ketersediaan ActiveMQ
- Redundansi Zona Ketersediaan RabbitMQ

ALB Multi-AZ

Deskripsi

Memeriksa apakah Application Load Balancer Anda dikonfigurasi untuk menggunakan lebih dari satu Availability Zone (AZ). AZ adalah lokasi berbeda yang terisolasi dari kegagalan di zona lain. Konfigurasikan penyeimbang beban Anda di beberapa AZ di Wilayah yang sama untuk membantu meningkatkan ketersediaan beban kerja Anda.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

`c1dfprch08`

Kriteria Peringatan

Kuning: ALB ada dalam satu AZ.

Hijau: ALB memiliki dua atau lebih AZ.

Tindakan yang Direkomendasikan

Pastikan penyeimbang beban Anda dikonfigurasi dengan setidaknya dua Availability Zone.

Untuk informasi selengkapnya, lihat Availability Zone untuk Application Load Balancer Anda.

Sumber Daya Tambahan

Untuk informasi selengkapnya, lihat dokumentasi berikut ini:

- Bagaimana Elastic Load Balancing bekerja
- Wilayah, Availability Zone, dan Local Zones

Kolom laporan

- Status
- Wilayah
- Nama ALB
- Aturan ALB
- ALB ARN
- Jumlah AZ
- Waktu Terakhir Diperbarui

Amazon Aurora MySQL cluster backtracking tidak diaktifkan

Deskripsi

Memeriksa apakah kluster MySQL Amazon Aurora telah mengaktifkan backtracking.

Amazon Aurora MySQL cluster backtracking adalah fitur yang memungkinkan Anda mengembalikan cluster Aurora DB ke titik waktu sebelumnya tanpa membuat cluster baru. Ini memungkinkan Anda untuk memutar kembali database Anda ke titik waktu tertentu dalam periode retensi, tanpa perlu memulihkan dari snapshot.

Anda dapat menyesuaikan jendela waktu backtracking (jam) dalam BacktrackWindowInHoursparameter AWS Config aturan.

Untuk informasi selengkapnya, lihat Menelusuri balik klaster Aurora DB.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

`c18d2gz131`

Sumber

`AWS Config Managed Rule: aurora-mysql-backtracking-enabled`

Kriteria Peringatan

Kuning: Amazon Aurora MySQL cluster backtracking tidak diaktifkan.

Tindakan yang Direkomendasikan

Aktifkan backtracking untuk cluster MySQL Amazon Aurora Anda.

Untuk informasi selengkapnya, lihat Menelusuri balik klaster Aurora DB.

Sumber Daya Tambahan

Melacak kembali klaster Aurora DB

Kolom laporan

- Status
- Wilayah
- Sumber Daya
- AWS Config Aturan
- Parameter Input
- Waktu Terakhir Diperbarui

Aksesibilitas Instans Amazon Aurora DB

Deskripsi

Memeriksa kasus di mana kluster Amazon Aurora DB memiliki instans pribadi dan publik.

Ketika instance utama Anda gagal, replika dapat dipromosikan ke instance utama. Jika replika itu bersifat pribadi, pengguna yang hanya memiliki akses publik tidak akan lagi dapat terhubung ke database setelah failover. Kami merekomendasikan bahwa semua instans DB dalam sebuah cluster memiliki aksesibilitas yang sama.

ID pemeriksaan

`xuy7H1avtl`

Kriteria Peringatan

Kuning: Instans dalam cluster Aurora DB memiliki aksesibilitas yang berbeda (campuran publik dan pribadi).

Tindakan yang Direkomendasikan

Ubah `Publicly Accessible` pengaturan instance di cluster DB sehingga semuanya bersifat publik atau pribadi. Untuk detailnya, lihat petunjuk untuk instance MySQL di Memodifikasi Instans DB Menjalankan Mesin Database MySQL.

Sumber Daya Tambahan

Toleransi Kesalahan untuk Cluster Aurora DB

Kolom laporan

- Status
- Wilayah
- Klaster
- Instans DB Publik
- Instans DB Pribadi
- Alasan

Failover CloudFront Asal Amazon

Deskripsi

Memeriksa apakah grup asal dikonfigurasi untuk distribusi yang menyertakan dua asal di Amazon CloudFront.

Untuk informasi selengkapnya, lihat Mengoptimalkan ketersediaan tinggi dengan failover CloudFront asal.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

`c18d2gz112`

Sumber

`AWS Config Managed Rule: cloudfront-origin-failover-enabled`

Kriteria Peringatan

Kuning: Failover CloudFront asal Amazon tidak diaktifkan.

Tindakan yang Direkomendasikan

Pastikan Anda mengaktifkan fitur failover asal untuk CloudFront distribusi Anda untuk membantu memastikan ketersediaan konten Anda yang tinggi bagi pengguna akhir. Ketika Anda mengaktifkan fitur ini, lalu lintas secara otomatis diarahkan ke server asal cadangan jika server asal utama tidak tersedia. Ini meminimalkan potensi downtime dan memastikan ketersediaan konten Anda secara berkelanjutan.

Kolom laporan

- Status
- Wilayah
- Sumber Daya
- AWS Config Aturan
- Parameter Input
- Waktu Terakhir Diperbarui

Amazon Comprehend Risiko Akses Titik Akhir

Deskripsi

Memeriksa izin kunci AWS Key Management Service (AWS KMS) untuk titik akhir di mana model yang mendasarinya dienkripsi dengan menggunakan kunci yang dikelola pelanggan. Jika kunci

yang dikelola pelanggan dinonaktifkan, atau kebijakan kunci diubah untuk mengubah izin yang diizinkan untuk Amazon Comprehend, ketersediaan titik akhir mungkin terpengaruh.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

`Cm24dfsM13`

Kriteria Peringatan

Merah: Kunci yang dikelola pelanggan dinonaktifkan atau kebijakan kunci diubah untuk mengubah izin yang diizinkan untuk akses Amazon Comprehend.

Tindakan yang Direkomendasikan

Jika kunci yang dikelola pelanggan dinonaktifkan, kami sarankan Anda mengaktifkannya. Untuk informasi selengkapnya, lihat Mengaktifkan kunci. Jika kebijakan kunci diubah dan Anda ingin tetap menggunakan titik akhir, sebaiknya Anda memperbarui kebijakan AWS KMS kunci. Untuk informasi selengkapnya, lihat Mengubah kebijakan utama.

Sumber Daya Tambahan

AWS KMS Izin

Kolom laporan

- Status
- Wilayah
- Titik akhir ARN
- Model ARN
- KMS KeyId
- Waktu Terakhir Diperbarui

Cluster AZ Tunggal Amazon DocumentDB

Deskripsi

Memeriksa apakah ada cluster Amazon DocumentDB yang dikonfigurasi sebagai Single-AZ.

Menjalankan beban kerja Amazon DocumentDB dalam arsitektur single-AZ tidak cukup untuk beban kerja yang sangat kritis dan dapat memakan waktu hingga 10 menit untuk pulih dari kegagalan komponen. Pelanggan harus menerapkan instance replika di zona ketersediaan tambahan untuk memastikan ketersediaan selama pemeliharaan, kegagalan instans, kegagalan komponen, atau kegagalan zona ketersediaan.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan satu kali atau beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

`c15vnddn2x`

Kriteria Peringatan

Kuning: Cluster Amazon DocumentDB memiliki instance di kurang dari tiga zona ketersediaan.

Hijau: Cluster Amazon DocumentDB memiliki instance di tiga zona ketersediaan.

Tindakan yang Direkomendasikan

Jika aplikasi Anda memerlukan ketersediaan tinggi, ubah instans DB Anda untuk mengaktifkan Multi-AZ menggunakan instance replika. Lihat Ketersediaan dan Replikasi Tinggi Amazon DocumentDB

Sumber Daya Tambahan

Memahami Toleransi Kesalahan Cluster Amazon DocumentDB

Wilayah dan Zona Ketersediaan

Kolom laporan

- Status
- Wilayah
- Zona Ketersediaan
- Pengidentifikasi Cluster DB
- DB Kluster ARN
- Waktu Terakhir Diperbarui

Pemulihan Amazon oint-in-time DynamoDB P

Deskripsi

Memeriksa apakah pemulihan waktu point-in diaktifkan untuk tabel Amazon DynamoDB Anda.

Poin-in-time-recovery membantu melindungi tabel DynamoDB Anda dari operasi tulis atau penghapusan yang tidak disengaja. Dengan point-in time-recovery, Anda tidak perlu khawatir tentang membuat, memelihara, atau menjadwalkan backup sesuai permintaan. Poin-in-time-recovery mengembalikan tabel ke titik waktu mana pun selama 35 hari terakhir. DynamoDB memelihara cadangan tambahan tabel Anda.

Untuk informasi selengkapnya, lihat oint-in-time pemulihan P untuk DynamoDB.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

```
c18d2gz138
```

Sumber

```
AWS Config Managed Rule: dynamodb-pitr-enabled
```

Kriteria Peringatan

Kuning: oint-in-time Pemulihan P tidak diaktifkan untuk tabel DynamoDB Anda.

Tindakan yang Direkomendasikan

Aktifkan point-in-time pemulihan di Amazon DynamoDB untuk terus mencadangkan data tabel Anda.

Untuk informasi selengkapnya, lihat oint-in-time Pemulihan P: Cara kerjanya.

Sumber Daya Tambahan

oint-in-time Pemulihan P untuk DynamoDB

Laporkan kolom

- Status
- Wilayah
- Sumber Daya
- AWS Config Aturan
- Parameter Input
- Waktu Terakhir Diperbarui

Tabel Amazon DynamoDB Tidak Termasuk dalam Paket Cadangan

Deskripsi

Memeriksa apakah tabel Amazon DynamoDB adalah bagian dari rencana. AWS Backup

AWS Backup menyediakan backup tambahan untuk tabel DynamoDB yang menangkap perubahan yang dibuat sejak backup terakhir. Menyertakan tabel DynamoDB dalam AWS Backup rencana membantu melindungi data Anda dari skenario kehilangan data yang tidak disengaja dan mengotomatiskan proses pencadangan. Ini memberikan solusi cadangan yang andal dan dapat diskalakan untuk tabel DynamoDB Anda, membantu memastikan bahwa data berharga Anda terlindungi dan tersedia untuk pemulihan sesuai kebutuhan.

Untuk informasi selengkapnya, lihat Membuat cadangan tabel DynamoDB dengan AWS Backup

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

```
c18d2gz107
```

Sumber

```
AWS Config Managed Rule: dynamodb-in-backup-plan
```

Kriteria Peringatan

Kuning: Tabel Amazon DynamoDB tidak termasuk dalam paket. AWS Backup

Tindakan yang Direkomendasikan

Pastikan tabel Amazon DynamoDB Anda adalah bagian dari rencana. AWS Backup

Sumber Daya Tambahan

Backup terjadwal

Apa itu AWS Backup?

Membuat paket cadangan menggunakan konsol AWS Backup

Laporkan kolom

- Status
- Wilayah
- Sumber Daya
- AWS Config Aturan
- Parameter Input
- Waktu Terakhir Diperbarui

Amazon EBS Tidak Termasuk dalam Paket AWS Backup

Deskripsi

Memeriksa apakah volume Amazon EBS ada dalam paket cadangan untuk AWS Backup.

Sertakan volume Amazon EBS dalam AWS Backup rencana untuk mengotomatiskan pencadangan reguler untuk data yang disimpan pada volume tersebut. Ini melindungi Anda dari kehilangan data, membuat manajemen data lebih mudah, dan memungkinkan pemulihan data bila

diperlukan. Rencana cadangan membantu memastikan bahwa data Anda aman dan Anda dapat memenuhi waktu pemulihan dan tujuan titik (RTO/RPO) untuk aplikasi dan layanan Anda.

Untuk informasi selengkapnya, lihat Membuat paket cadangan

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

`c18d2gz106`

Sumber

`AWS Config Managed Rule: ebs-in-backup-plan`

Kriteria Peringatan

Kuning: Volume Amazon EBS tidak termasuk dalam AWS Backup paket.

Tindakan yang Direkomendasikan

Pastikan volume Amazon EBS Anda adalah bagian dari AWS Backup rencana.

Sumber Daya Tambahan

Membuat paket cadangan menggunakan AWS Backup konsol

Apa itu AWS Backup?

Memulai 3: Buat cadangan terjadwal

Laporkan kolom

- Status
- Wilayah
- Sumber Daya
- AWS Config Aturan
- Parameter Input

- Waktu Terakhir Diperbarui

Cuplikan Amazon EBS

Deskripsi

Memeriksa usia snapshot untuk volume Amazon Elastic Block Store (Amazon EBS) Anda (tersedia atau sedang digunakan).

Meskipun volume Amazon EBS direplikasi, kegagalan dapat terjadi. Snapshot disimpan ke Amazon Simple Storage Service (Amazon S3) Simple Storage Service (Amazon S3) untuk penyimpanan dan pemulihan yang tahan lama. point-in-time

ID pemeriksaan

`H7IgTzjTYb`

Kriteria Peringatan

- Kuning: Snapshot volume terbaru berusia antara 7 dan 30 hari.
- Merah: Snapshot volume terbaru berusia lebih dari 30 hari.
- Merah: Volume tidak memiliki snapshot.

Tindakan yang Direkomendasikan

Buat snapshot mingguan atau bulanan volume Anda. Untuk informasi selengkapnya, lihat Membuat Snapshot Amazon EBS.

Sumber Daya Tambahan

Toko Blok Elastis Amazon (Amazon EBS)

Laporkan kolom

- Status
- Wilayah
- ID Volume
- Nama Volume
- ID Cuplikan
- Nama Snapshot
- Umur Snapshot

- Lampiran Volume
- Alasan

Auto Scaling Amazon EC2 tidak mengaktifkan Pemeriksaan Kesehatan ELB

Deskripsi

Memeriksa apakah grup Auto Scaling Amazon EC2 yang terkait dengan Classic Load Balancer menggunakan pemeriksaan kesehatan Elastic Load Balancing. Pemeriksaan kesehatan default untuk grup Auto Scaling hanya pemeriksaan status Amazon EC2. Jika sebuah instance gagal memeriksa status ini, itu ditandai tidak sehat dan dihentikan. Auto Scaling Amazon EC2 meluncurkan instans pengganti baru. Pemeriksaan kesehatan Elastic Load Balancing secara berkala memantau instans Amazon EC2 untuk mendeteksi dan menghentikan instans yang tidak sehat, lalu meluncurkan instans baru.

Untuk informasi selengkapnya, lihat Pemeriksaan kesehatan Tambahkan Elastic Load Balancing.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

```
c18d2gz104
```

Sumber

```
AWS Config Managed Rule: autoscaling-group-elb-healthcheck-required
```

Kriteria Peringatan

Kuning: Grup Auto Scaling Amazon EC2 yang terpasang pada Classic Load Balancer belum mengaktifkan pemeriksaan kesehatan Elastic Load Balancing.

Tindakan yang Direkomendasikan

Pastikan grup Auto Scaling Anda yang terkait dengan Classic Load Balancer menggunakan pemeriksaan kesehatan Elastic Load Balancing.

Pemeriksaan kesehatan Elastic Load Balancing melaporkan jika load balancer sehat dan tersedia untuk menangani permintaan. Ini memastikan ketersediaan tinggi untuk aplikasi Anda.

Untuk informasi selengkapnya, lihat Menambahkan pemeriksaan kesehatan Menambahkan Elastic Load Balancing ke grup Auto Scaling

Laporkan kolom

- Status
- Wilayah
- Sumber Daya
- AWS Config Aturan
- Parameter Input
- Waktu Terakhir Diperbarui

Grup Auto Scaling Amazon EC2 memiliki Rebalancing Kapasitas Diaktifkan

Deskripsi

Memeriksa apakah Penyeimbangan Kembali Kapasitas diaktifkan untuk grup Auto Scaling Amazon EC2 yang menggunakan beberapa jenis instans.

Mengonfigurasi grup Auto Scaling Amazon EC2 dengan penyeimbangan kembali kapasitas membantu memastikan instans Amazon EC2 didistribusikan secara merata di seluruh Availability Zone, terlepas dari jenis instans dan opsi pembelian. Ini menggunakan kebijakan pelacakan target yang terkait dengan grup, seperti pemanfaatan CPU atau lalu lintas jaringan.

Untuk informasi selengkapnya, lihat grup Auto Scaling dengan beberapa jenis instans dan opsi pembelian.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

```
AWS Config c18d2gz103
```

Sumber

AWS Config Aturan Terkelola: autoscaling-capacity-rebalancing

Kriteria Peringatan

Kuning: Penyeimbangan kembali kapasitas grup Auto Scaling Amazon EC2 tidak diaktifkan.

Tindakan yang Direkomendasikan

Pastikan penyeimbangan kembali kapasitas diaktifkan untuk grup Auto Scaling Amazon EC2 yang menggunakan beberapa jenis instans.

Untuk informasi selengkapnya, lihat Mengaktifkan Penyeimbangan Kembali Kapasitas (konsol)

Laporkan kolom

- Status
- Wilayah
- Sumber Daya
- AWS Config Aturan
- Parameter Input
- Waktu Terakhir Diperbarui

Auto Scaling Amazon EC2 tidak digunakan di beberapa AZ atau tidak memenuhi jumlah minimum AZ

Deskripsi

Memeriksa apakah grup Auto Scaling Amazon EC2 diterapkan di beberapa Availability Zone, atau jumlah minimum Availability Zone yang ditentukan. Terapkan instans Amazon EC2 di beberapa Availability Zone untuk memastikan ketersediaan tinggi.

Anda dapat menyesuaikan jumlah minimum Availability Zone menggunakan AvailibilityZones parameter min dalam AWS Config aturan Anda.

Untuk informasi selengkapnya, lihat grup Auto Scaling dengan beberapa jenis instans dan opsi pembelian.

ID pemeriksaan

`c18d2gz101`

Sumber

```
AWS Config Managed Rule: autoscaling-multiple-az
```

Kriteria Peringatan

Merah: Grup Auto Scaling Amazon EC2 tidak memiliki beberapa AZ yang dikonfigurasi, atau tidak memenuhi jumlah minimum AZ yang ditentukan.

Tindakan yang Direkomendasikan

Pastikan grup Auto Scaling Amazon EC2 Anda dikonfigurasi dengan beberapa AZ. Terapkan instans Amazon EC2 di beberapa Availability Zone untuk memastikan ketersediaan tinggi.

Sumber Daya Tambahan

Buat grup Auto Scaling menggunakan template peluncuran

Membuat grup Auto Scaling menggunakan konfigurasi peluncuran

Laporkan kolom

- Status
- Wilayah
- Sumber Daya
- AWS Config Aturan
- Parameter Input
- Waktu Terakhir Diperbarui

Saldo Zona Ketersediaan Amazon EC2

Deskripsi

Memeriksa distribusi instans Amazon Elastic Compute Cloud (Amazon EC2) di seluruh Availability Zone di suatu Wilayah.

Availability Zone adalah lokasi berbeda yang terisolasi dari kegagalan di Availability Zone lainnya. Ini memungkinkan konektivitas jaringan latensi rendah yang murah antara Availability Zones di Wilayah yang sama. Dengan meluncurkan instans di beberapa Availability Zone di Region yang sama, Anda dapat membantu melindungi aplikasi Anda dari satu titik kegagalan.

ID pemeriksaan

```
wuy7G1zxql
```

Kriteria Peringatan

- Kuning: Wilayah ini memiliki instance di beberapa zona, tetapi distribusinya tidak merata (perbedaan antara jumlah instans tertinggi dan terendah di Availability Zone yang digunakan lebih besar dari 20%).
- Merah: Wilayah hanya memiliki instance di satu Availability Zone.

Tindakan yang Direkomendasikan

Seimbangkan instans Amazon EC2 Anda secara merata di beberapa Availability Zone. Anda dapat melakukan ini dengan meluncurkan instance secara manual atau dengan menggunakan Auto Scaling untuk melakukannya secara otomatis. Untuk informasi selengkapnya, lihat Meluncurkan Instance Anda dan Memuat Saldo Grup Auto Scaling Anda.

Sumber Daya Tambahan

Panduan Pengguna Penskalaan Otomatis Amazon EC2

Laporkan kolom

- Status
- Wilayah
- Zona sebuah Instans
- Zona b Contoh
- Zona c Contoh
- Zona e Instans
- Zona f Contoh
- Alasan

Pemantauan Terperinci Amazon EC2 Tidak Diaktifkan

Deskripsi

Memeriksa apakah pemantauan terperinci diaktifkan untuk instans Amazon EC2 Anda.

Pemantauan terperinci Amazon EC2 memberikan metrik yang lebih sering, diterbitkan pada interval satu menit, alih-alih interval lima menit yang digunakan dalam pemantauan dasar Amazon EC2. Mengaktifkan pemantauan terperinci untuk Amazon EC2 membantu Anda mengelola sumber daya Amazon EC2 dengan lebih baik, sehingga Anda dapat menemukan tren dan mengambil tindakan lebih cepat.

Untuk informasi selengkapnya, lihat Pemantauan dasar dan pemantauan terperinci.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

`AWS Config c18d2gz144`

Sumber

AWS Config Aturan Terkelola: ec2-instance-detailed-monitoring-enabled

Kriteria Peringatan

Kuning: Pemantauan terperinci tidak diaktifkan untuk instans Amazon EC2.

Tindakan yang Direkomendasikan

Aktifkan pemantauan terperinci untuk instans Amazon EC2 Anda untuk meningkatkan frekuensi data metrik Amazon EC2 dipublikasikan ke Amazon CloudWatch (dari interval 5 menit hingga 1 menit).

Laporkan kolom

- Status
- Wilayah
- Sumber Daya
- AWS Config Aturan
- Parameter Input
- Waktu Terakhir Diperbarui

Driver Amazon ECS AWS Logs dalam mode pemblokiran

Deskripsi

Memeriksa definisi tugas Amazon ECS yang dikonfigurasi dengan driver logging AWS Log dalam mode pemblokiran. Driver yang dikonfigurasi dalam mode pemblokiran berisiko ketersediaan sistem.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan satu kali atau beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

`c1dvkm4z6b`

Kriteria Peringatan

Kuning: Mode parameter konfigurasi pencatatan driver awslogs diatur ke pemblokiran atau hilang. Parameter mode yang hilang menunjukkan konfigurasi pemblokiran default.

Hijau: Definisi tugas Amazon ECS tidak menggunakan driver awslogs atau driver awslogs dikonfigurasi dalam mode non-pemblokiran.

Tindakan yang Direkomendasikan

Untuk mengurangi risiko ketersediaan, pertimbangkan untuk mengubah konfigurasi driver AWS Log definisi tugas dari pemblokiran menjadi non-pemblokiran. Dengan mode non-pemblokiran, Anda harus menetapkan nilai untuk max-buffer-size parameter. Untuk informasi selengkapnya dan panduan tentang parameter konfigurasi, lihat. Lihat Mencegah kehilangan log dengan mode non-pemblokiran di driver AWS log kontainer Log

Sumber Daya Tambahan

Menggunakan driver AWS log log

Memilih opsi pencatatan kontainer untuk menghindari tekanan balik

Mencegah kehilangan log dengan mode non-pemblokiran di driver AWS log kontainer Log

Laporkan kolom

- Status
- Wilayah
- Definisi Tugas ARN
- Nama Definisi Kontainer
- Waktu Terakhir Diperbarui

Layanan Amazon ECS menggunakan satu AZ

Deskripsi

Memeriksa apakah konfigurasi layanan Anda menggunakan Availability Zone (AZ) tunggal.

AZ adalah lokasi berbeda yang terisolasi dari kegagalan di zona lain. Ini mendukung konektivitas jaringan latensi rendah yang murah antara AZ dalam hal yang sama. Wilayah AWS Dengan meluncurkan instans di beberapa AZ di Wilayah yang sama, Anda dapat membantu melindungi aplikasi Anda dari satu titik kegagalan.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

`c1z7dfpz01`

Kriteria Peringatan

- Kuning: Layanan Amazon ECS menjalankan semua tugas dalam satu AZ.
- Hijau: Layanan Amazon ECS menjalankan tugas di setidaknya dua AZ yang berbeda.

Tindakan yang Direkomendasikan

Buat setidaknya satu tugas lagi untuk layanan di AZ yang berbeda.

Sumber Daya Tambahan

Kapasitas dan ketersediaan Amazon ECS

Laporkan kolom

- Status
- Wilayah
- Nama Cluster ECS/Nama Layanan ECS
- Jumlah Availability Zone
- Waktu Terakhir Diperbarui

Strategi penempatan Multi-AZ Amazon ECS

Deskripsi

Memeriksa apakah layanan Amazon ECS Anda menggunakan strategi penempatan spread berdasarkan Availability Zone (AZ). Strategi ini mendistribusikan tugas di seluruh Availability Zone secara bersamaan Wilayah AWS dan dapat membantu melindungi aplikasi Anda dari satu titik kegagalan.

Untuk tugas yang berjalan sebagai bagian dari layanan Amazon ECS, spread adalah strategi penempatan tugas default.

Pemeriksaan ini juga memverifikasi bahwa spread adalah strategi pertama atau satu-satunya dalam daftar strategi penempatan yang diaktifkan.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

`c1z7dfpz02`

Kriteria Peringatan

- Kuning: Penyebaran berdasarkan zona ketersediaan dinonaktifkan atau bukan strategi pertama dalam daftar strategi penempatan yang diaktifkan untuk layanan Amazon ECS Anda.

- Hijau: Spread by availability zone adalah strategi pertama dalam daftar strategi penempatan yang diaktifkan atau satu-satunya strategi penempatan yang diaktifkan untuk layanan Amazon ECS Anda.

Tindakan yang Direkomendasikan

Aktifkan strategi penempatan tugas spread untuk mendistribusikan tugas di beberapa AZ. Verifikasi bahwa spread by availability zone adalah strategi pertama untuk semua strategi penempatan tugas yang diaktifkan atau satu-satunya strategi yang digunakan. Jika Anda memilih untuk mengelola penempatan AZ, Anda dapat menggunakan layanan cermin di AZ lain untuk mengurangi risiko ini.

Sumber Daya Tambahan

Strategi penempatan tugas Amazon ECS

Laporkan kolom

- Status
- Wilayah
- Nama Cluster ECS/Nama Layanan ECS
- Spread Task Placement Strategy Diaktifkan dan Diterapkan dengan Benar
- Waktu Terakhir Diperbarui

Amazon EFS Tidak Ada Redundansi Target Mount

Deskripsi

Memeriksa apakah target pemasangan ada di beberapa Availability Zone untuk sistem file Amazon EFS.

Availability Zone adalah lokasi berbeda yang terisolasi dari kegagalan di zona lain. Dengan membuat target mount di beberapa Availability Zone yang terpisah secara geografis dalam Wilayah AWS, Anda dapat mencapai tingkat ketersediaan dan daya tahan tertinggi untuk sistem file Amazon EFS Anda.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

`c1dfprch01`

Kriteria Peringatan

- Kuning: Sistem file memiliki 1 target pemasangan yang dibuat dalam satu Availability Zone.

  Hijau: Sistem file memiliki 2 atau lebih target mount yang dibuat di beberapa Availability Zone.

Tindakan yang Direkomendasikan

Untuk sistem file EFS yang menggunakan kelas penyimpanan One Zone, kami sarankan Anda membuat sistem file baru yang menggunakan kelas penyimpanan Standar dengan memulihkan cadangan ke sistem file baru. Kemudian buat target mount di beberapa Availability Zone.

Untuk sistem file EFS yang menggunakan kelas penyimpanan Standar, kami sarankan Anda membuat target pemasangan di beberapa Availability Zone.

Sumber Daya Tambahan

- Mengelola target pemasangan menggunakan konsol Amazon EFS
- Kuota dan Batas Amazon EFS

Laporkan kolom

- Status
- Wilayah
- ID Sistem Berkas EFS
- Jumlah target pemasangan
- Jumlah AZ
- Waktu Terakhir Diperbarui

Amazon EFS tidak ada dalam AWS Backup Rencana

Deskripsi

Memeriksa apakah sistem file Amazon EFS disertakan dalam paket cadangan dengan AWS Backup.

AWS Backup adalah layanan pencadangan terpadu yang dirancang untuk menyederhanakan pembuatan, migrasi, pemulihan, dan penghapusan cadangan, sambil memberikan pelaporan dan audit yang lebih baik.

Untuk informasi selengkapnya, lihat Mencadangkan sistem file Amazon EFS Anda.

ID pemeriksaan

```
c18d2gz117
```

Sumber

```
AWS Config Managed Rule: EFS_IN_BACKUP_PLAN
```

Kriteria Peringatan

Merah: Amazon EFS tidak termasuk dalam AWS Backup paket.

Tindakan yang Direkomendasikan

Pastikan sistem file Amazon EFS Anda disertakan dalam AWS Backup paket Anda untuk melindungi dari kehilangan data yang tidak disengaja atau korupsi data.

Sumber Daya Tambahan

Mencadangkan sistem file Amazon EFS Anda

Amazon EFS Backup dan Restore menggunakan AWS Backup.

Laporkan kolom

- Status
- Wilayah
- Sumber Daya
- AWS Config Aturan
- Parameter Input
- Waktu Terakhir Diperbarui

Cluster Amazon ElastiCache Multi-AZ

Deskripsi

Memeriksa ElastiCache klaster yang diterapkan dalam satu Availability Zone (AZ). Pemeriksaan ini memberi tahu Anda jika Multi-AZ tidak aktif di cluster.

Penerapan di beberapa AZ meningkatkan ketersediaan ElastiCache klaster dengan mereplikasi secara asinkron ke replika hanya-baca di AZ yang berbeda. Ketika pemeliharaan klaster yang direncanakan terjadi, atau node primer tidak tersedia, ElastiCache secara otomatis mempromosikan replika ke primer. Failover ini memungkinkan operasi penulisan klaster untuk dilanjutkan, dan tidak memerlukan administrator untuk campur tangan.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

`ECHdfsQ402`

Kriteria Peringatan

- Hijau: Multi-AZ aktif di cluster.
- Kuning: Multi-AZ tidak aktif di cluster.

Tindakan yang Direkomendasikan

Buat setidaknya satu replika per pecahan, dalam AZ yang berbeda dari yang primer.

Sumber Daya Tambahan

Untuk informasi selengkapnya, lihat Meminimalkan waktu henti ElastiCache untuk Redis dengan Multi-AZ.

Laporkan kolom

- Status
- Wilayah
- Nama Klaster

- Waktu Terakhir Diperbarui

Cadangan ElastiCache Otomatis Amazon Redis Cluster

Deskripsi

Memeriksa apakah klaster Amazon ElastiCache untuk Redis mengaktifkan pencadangan otomatis dan jika periode retensi snapshot di atas batas default yang ditentukan atau 15 hari. Saat pencadangan otomatis diaktifkan, ElastiCache buat cadangan cluster setiap hari.

Anda dapat menentukan batas retensi snapshot yang Anda inginkan menggunakan RetentionPeriod parameter snapshot aturan Anda AWS Config .

Untuk informasi selengkapnya, lihat Backup dan restore ElastiCache untuk Redis.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

```
c18d2gz178
```

Sumber

```
AWS Config Managed Rule: elasticache-redis-cluster-automatic-backup-check
```

Kriteria Peringatan

Merah: Amazon ElastiCache untuk kluster Redis tidak mengaktifkan cadangan otomatis atau periode retensi snapshot di bawah batas.

Tindakan yang Direkomendasikan

Pastikan bahwa klaster Amazon ElastiCache untuk Redis mengaktifkan pencadangan otomatis dan periode retensi snapshot berada di atas batas default yang ditentukan atau 15 hari. Backup otomatis dapat membantu mencegah kehilangan data. Jika terjadi kegagalan, Anda dapat membuat klaster baru, memulihkan data Anda dari backup terakhir.

Untuk informasi selengkapnya, lihat Backup dan restore ElastiCache untuk Redis.

Sumber Daya Tambahan

Untuk informasi selengkapnya, lihat Menjadwalkan pencadangan otomatis.

Laporkan kolom

- Status
- Wilayah
- Nama Klaster
- Waktu Terakhir Diperbarui

Amazon MemoryDB kluster Multi-AZ

Deskripsi

Memeriksa klaster MemoryDB yang diterapkan dalam satu Availability Zone (AZ). Pemeriksaan ini memberi tahu Anda jika Multi-AZ tidak aktif di cluster.

Penerapan di beberapa AZ meningkatkan ketersediaan cluster MemoryDB dengan mereplikasi secara asinkron ke replika hanya-baca di AZ yang berbeda. Ketika pemeliharaan cluster yang direncanakan terjadi, atau node primer tidak tersedia, MemoryDB secara otomatis mempromosikan replika ke primer. Failover ini memungkinkan operasi penulisan klaster untuk dilanjutkan, dan tidak memerlukan administrator untuk campur tangan.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

`MDBdfsQ401`

Kriteria Peringatan

- Hijau: Multi-AZ aktif di cluster.
- Kuning: Multi-AZ tidak aktif di cluster.

Tindakan yang Direkomendasikan

Buat setidaknya satu replika per pecahan, dalam AZ yang berbeda dari yang primer.

Sumber Daya Tambahan

Untuk informasi selengkapnya, lihat Meminimalkan waktu henti di MemoryDB dengan Multi-AZ.

Laporkan kolom

- Status
- Wilayah
- Nama Klaster
- Waktu Terakhir Diperbarui

Broker MSK Amazon menghosting terlalu banyak partisi

Deskripsi

Memeriksa bahwa broker dari Cluster Streaming Terkelola untuk Kafka (MSK) tidak memiliki lebih dari jumlah partisi yang disarankan yang ditetapkan.

ID pemeriksaan

`Cmsvnj8vf1`

Kriteria Peringatan

- Merah: Broker MSK Anda telah mencapai atau melampaui 100% dari batas partisi maksimum yang disarankan
- Kuning: MSK Anda telah mencapai 80% dari batas partisi maksimum yang disarankan

Tindakan yang Direkomendasikan

Ikuti praktik terbaik yang direkomendasikan MSK untuk menskalakan Kluster MSK Anda atau menghapus partisi yang tidak terpakai.

Sumber Daya Tambahan

- Ukuran kanan Cluster Anda

Laporkan kolom

- Status
- Wilayah
- ARN klaster

- ID Pialang
- Jumlah Partisi

Domain Amazon OpenSearch Service dengan kurang dari tiga node data

Deskripsi

Memeriksa apakah domain OpenSearch Layanan Amazon dikonfigurasi dengan setidaknya tiga node data dan ZoneAwarenessEnabled benar. Dengan ZoneAwarenessEnabled diaktifkan, Amazon OpenSearch Service memastikan bahwa setiap pecahan utama dan replika yang sesuai dialokasikan di Availability Zone yang berbeda.

Untuk informasi selengkapnya, lihat Mengonfigurasi domain Multi-AZ di Layanan Amazon OpenSearch .

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

```
c18d2gz183
```

Sumber

```
AWS Config Managed Rule: opensearch-data-node-fault-tolerance
```

Kriteria Peringatan

Kuning: Domain Amazon OpenSearch Service dikonfigurasi dengan kurang dari tiga node data.

Tindakan yang Direkomendasikan

Pastikan domain Amazon OpenSearch Service dikonfigurasi dengan minimal tiga node data. Konfigurasikan domain Multi-AZ untuk meningkatkan ketersediaan kluster OpenSearch Layanan Amazon dengan mengalokasikan node dan mereplikasi data di tiga Availability Zone dalam Wilayah yang sama. Ini mencegah kehilangan data dan meminimalkan waktu henti jika terjadi kegagalan node atau pusat data (AZ).

Untuk informasi selengkapnya, lihat Meningkatkan ketersediaan untuk OpenSearch Layanan Amazon dengan menerapkan di tiga Availability Zone.

Sumber Daya Tambahan

- Tingkatkan ketersediaan untuk OpenSearch Layanan Amazon dengan menerapkan di tiga Availability Zone

Laporkan kolom

- Status
- Wilayah
- Sumber Daya
- AWS Config Aturan
- Parameter Input
- Waktu Terakhir Diperbarui

Cadangan Amazon RDS

Deskripsi

Memeriksa pencadangan otomatis instans Amazon RDS DB.

Secara default, backup diaktifkan dengan periode retensi satu hari. Cadangan mengurangi risiko kehilangan data yang tidak terduga dan memungkinkan pemulihan. point-in-time

ID pemeriksaan

`opQPADkZvH`

Kriteria Peringatan

Merah: Instans DB memiliki periode retensi cadangan yang disetel ke 0 hari.

Tindakan yang Direkomendasikan

Atur periode retensi untuk pencadangan instans DB otomatis menjadi 1 hingga 35 hari sesuai dengan persyaratan aplikasi Anda. Lihat Bekerja Dengan Pencadangan Otomatis.

Sumber Daya Tambahan

Memulai dengan Amazon RDS

Laporkan kolom

- Status

- Wilayah/AZ
- Instans DB
- ID VPC
- Periode Retensi Cadangan

Cluster Amazon RDS DB memiliki satu instans DB

Deskripsi

Tambahkan setidaknya instans DB lain ke cluster DB untuk meningkatkan ketersediaan dan kinerja.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

> **Note**
>
> Ketika instans DB atau kluster DB dihentikan, Anda dapat melihat rekomendasi Amazon RDS Trusted Advisor selama 3 hingga 5 hari. Setelah lima hari, rekomendasi tidak tersedia di Trusted Advisor. Untuk melihat rekomendasi, buka konsol Amazon RDS, lalu pilih Rekomendasi.
> Jika Anda menghapus instans DB atau kluster DB, maka rekomendasi yang terkait dengan instans atau cluster tersebut tidak tersedia di Trusted Advisor atau konsol manajemen Amazon RDS.

ID pemeriksaan

```
c1qf5bt011
```

Kriteria Peringatan

Kuning: Cluster DB hanya memiliki satu instans DB.

Tindakan yang Direkomendasikan

Tambahkan instance DB pembaca ke cluster DB.

Sumber Daya Tambahan

Dalam konfigurasi saat ini, satu instance DB digunakan untuk operasi baca dan tulis. Anda dapat menambahkan instans DB lain untuk memungkinkan redistribusi baca dan opsi failover.

Untuk informasi selengkapnya, lihat Ketersediaan tinggi untuk Amazon Aurora.

Laporkan kolom

- Status
- Wilayah
- Sumber Daya
- Nama Mesin
- Kelas Instans DB
- Waktu Terakhir Diperbarui

Cluster Amazon RDS DB dengan semua instans di Availability Zone yang sama

Deskripsi

Cluster DB saat ini berada dalam satu Availability Zone. Gunakan beberapa Availability Zone untuk meningkatkan ketersediaan.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

> **Note**
>
> Ketika instans DB atau kluster DB dihentikan, Anda dapat melihat rekomendasi Amazon RDS Trusted Advisor selama 3 hingga 5 hari. Setelah lima hari, rekomendasi tidak tersedia di Trusted Advisor. Untuk melihat rekomendasi, buka konsol Amazon RDS, lalu pilih Rekomendasi.

Jika Anda menghapus instans DB atau kluster DB, maka rekomendasi yang terkait dengan instans atau cluster tersebut tidak tersedia di Trusted Advisor atau konsol manajemen Amazon RDS.

ID pemeriksaan

`c1qf5bt007`

Kriteria Peringatan

Kuning: Cluster DB memiliki semua instance di Availability Zone yang sama.

Tindakan yang Direkomendasikan

Tambahkan instans DB ke beberapa Availability Zone di cluster DB Anda.

Sumber Daya Tambahan

Kami menyarankan Anda menambahkan instans DB ke beberapa Availability Zone dalam cluster DB. Menambahkan instans DB ke beberapa Availability Zone meningkatkan ketersediaan cluster DB Anda.

Untuk informasi selengkapnya, lihat Ketersediaan tinggi untuk Amazon Aurora.

Laporkan kolom

- Status
- Wilayah
- Sumber Daya
- Nama Mesin
- Waktu Terakhir Diperbarui

Cluster Amazon RDS DB dengan semua instans pembaca di Availability Zone yang sama

Deskripsi

Klaster DB Anda memiliki semua instans pembaca di Zona Ketersediaan yang sama. Kami menyarankan Anda mendistribusikan instans Pembaca di beberapa Availability Zone di cluster DB Anda.

Distribusi meningkatkan ketersediaan database, dan meningkatkan waktu respons dengan mengurangi latensi jaringan antara klien dan database.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

> **Note**
>
> Ketika instans DB atau kluster DB dihentikan, Anda dapat melihat rekomendasi Amazon RDS Trusted Advisor selama 3 hingga 5 hari. Setelah lima hari, rekomendasi tidak tersedia di Trusted Advisor. Untuk melihat rekomendasi, buka konsol Amazon RDS, lalu pilih Rekomendasi.
> Jika Anda menghapus instans DB atau kluster DB, maka rekomendasi yang terkait dengan instans atau cluster tersebut tidak tersedia di Trusted Advisor atau konsol manajemen Amazon RDS.

ID pemeriksaan

`c1qf5bt018`

Kriteria Peringatan

Merah: Cluster DB memiliki instance pembaca di Availability Zone yang sama.

Tindakan yang Direkomendasikan

Mendistribusikan instance pembaca di beberapa Availability Zone.

Sumber Daya Tambahan

Availability Zones (AZ) adalah lokasi yang berbeda satu sama lain untuk memberikan isolasi jika terjadi pemadaman di setiap AWS Wilayah. Sebaiknya Anda mendistribusikan instans utama dan instans pembaca di cluster DB Anda di beberapa AZ untuk meningkatkan ketersediaan cluster DB Anda. Anda dapat membuat klaster Multi-AZ menggunakan AWS Management Console, AWS CLI, atau Amazon RDS API saat membuat klaster. Anda dapat memodifikasi cluster Aurora yang

ada ke cluster multi-AZ dengan menambahkan instance pembaca baru dan menentukan AZ yang berbeda.

Untuk informasi selengkapnya, lihat Ketersediaan tinggi untuk Amazon Aurora.

Laporkan kolom

- Status
- Wilayah
- Sumber Daya
- Nama Mesin
- Waktu Terakhir Diperbarui

Pemantauan Peningkatan Instans Amazon RDS DB tidak diaktifkan

Deskripsi

Memeriksa apakah instans Amazon RDS DB Anda telah mengaktifkan Enhanced Monitoring.

Amazon RDS Enhanced Monitoring menyediakan metrik secara real time untuk sistem operasi (OS) tempat instans DB Anda berjalan. Semua metrik sistem dan informasi proses untuk instans Amazon RDS DB Anda dapat dilihat di konsol Amazon RDS. Dan, Anda dapat menyesuaikan dasbor. Dengan Enhanced Monitoring, Anda memiliki visibilitas status operasi instans Amazon RDS dalam waktu dekat, sehingga Anda dapat merespons masalah operasional lebih cepat.

Anda dapat menentukan interval pemantauan yang Anda inginkan menggunakan parameter MonitoringInterval aturan Anda. AWS Config

Untuk informasi selengkapnya, lihat Ikhtisar Metrik Pemantauan yang Ditingkatkan dan OS di Pemantauan yang Ditingkatkan.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

```
c18d2gz158
```

Sumber

```
AWS Config Managed Rule: rds-enhanced-monitoring-enabled
```

Kriteria Peringatan

Kuning: Instans Amazon RDS DB Anda tidak mengaktifkan Enhanced Monitoring atau tidak dikonfigurasi dengan interval yang diinginkan.

Tindakan yang Direkomendasikan

Aktifkan Pemantauan yang Ditingkatkan untuk instans Amazon RDS DB Anda untuk meningkatkan visibilitas status operasi instans Amazon RDS Anda.

Untuk informasi selengkapnya, lihat Memantau metrik OS dengan Enhanced Monitoring.

Sumber Daya Tambahan

Metrik OS dalam Pemantauan yang Ditingkatkan

Laporkan kolom

- Status
- Wilayah
- Sumber Daya
- AWS Config Aturan
- Parameter Input
- Waktu Terakhir Diperbarui

Instans Amazon RDS DB memiliki penyimpanan autoscaling dimatikan

Deskripsi

Penskalaan otomatis penyimpanan Amazon RDS tidak diaktifkan untuk instans DB Anda. Ketika ada peningkatan beban kerja database, penskalaan otomatis RDS Storage secara otomatis menskalakan kapasitas penyimpanan dengan nol waktu henti.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

> **Note**
>
> Ketika instans DB atau kluster DB dihentikan, Anda dapat melihat rekomendasi Amazon RDS Trusted Advisor selama 3 hingga 5 hari. Setelah lima hari, rekomendasi tidak tersedia di Trusted Advisor. Untuk melihat rekomendasi, buka konsol Amazon RDS, lalu pilih Rekomendasi.
> Jika Anda menghapus instans DB atau kluster DB, maka rekomendasi yang terkait dengan instans atau cluster tersebut tidak tersedia di Trusted Advisor atau konsol manajemen Amazon RDS.

ID pemeriksaan

`c1qf5bt013`

Kriteria Peringatan

Merah: Instans DB tidak mengaktifkan penskalaan otomatis penyimpanan.

Tindakan yang Direkomendasikan

Aktifkan penskalaan otomatis penyimpanan Amazon RDS dengan ambang penyimpanan maksimum yang ditentukan.

Sumber Daya Tambahan

Penskalaan otomatis penyimpanan Amazon RDS secara otomatis menskalakan kapasitas penyimpanan tanpa waktu henti saat beban kerja database meningkat. Penskalaan otomatis penyimpanan memantau penggunaan penyimpanan dan secara otomatis meningkatkan kapasitas saat penggunaan mendekati kapasitas penyimpanan yang disediakan. Anda dapat menentukan batas maksimum penyimpanan yang dapat dialokasikan Amazon RDS ke instans DB. Tidak ada biaya tambahan untuk penyimpanan autoscaling. Anda hanya membayar untuk sumber daya Amazon RDS yang dialokasikan ke instans DB Anda. Kami menyarankan Anda mengaktifkan penskalaan otomatis penyimpanan Amazon RDS.

Untuk informasi selengkapnya, lihat Mengelola kapasitas secara otomatis dengan penskalaan otomatis penyimpanan Amazon RDS.

Laporkan kolom

- Status
- Wilayah
- Sumber Daya
- Nilai yang Direkomendasikan
- Nama Mesin
- Waktu Terakhir Diperbarui

Instans Amazon RDS DB tidak menggunakan penerapan Multi-AZ

Deskripsi

Sebaiknya gunakan deployment Multi-AZ. Deployment multi-AZ meningkatkan ketersediaan dan durabilitas instans DB.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

> **Note**
>
> Ketika instans DB atau kluster DB dihentikan, Anda dapat melihat rekomendasi Amazon RDS Trusted Advisor selama 3 hingga 5 hari. Setelah lima hari, rekomendasi tidak tersedia di Trusted Advisor. Untuk melihat rekomendasi, buka konsol Amazon RDS, lalu pilih Rekomendasi.
> Jika Anda menghapus instans DB atau kluster DB, maka rekomendasi yang terkait dengan instans atau cluster tersebut tidak tersedia di Trusted Advisor atau konsol manajemen Amazon RDS.

ID pemeriksaan

`c1qf5bt019`

Kriteria Peringatan

Kuning: Instans DB tidak menggunakan penerapan Multi-AZ.

Tindakan yang Direkomendasikan

Siapkan Multi-AZ untuk instans DB yang terkena dampak.

Sumber Daya Tambahan

Dalam penerapan Multi-AZ Amazon RDS, Amazon RDS secara otomatis membuat instance database utama dan mereplikasi data ke instance di zona ketersediaan yang berbeda. Ketika mendeteksi kegagalan, Amazon RDS secara otomatis gagal ke instance siaga tanpa intervensi manual.

Untuk informasi selengkapnya, silakan lihat Harga .

Laporkan kolom

- Status
- Wilayah
- Sumber Daya
- Nama Mesin
- Waktu Terakhir Diperbarui

Amazon RDS DiskQueueDepth

Deskripsi

Pemeriksaan untuk melihat apakah CloudWatch metrik DiskQueueDepth menunjukkan bahwa jumlah penulisan antrian ke penyimpanan database Instans RDS telah berkembang ke tingkat di mana penyelidikan operasional harus disarankan.

ID pemeriksaan

`Cmsvnj8db3`

Kriteria Peringatan

- Merah: DiskQueueDepth CloudWatch metrik telah melebihi 10

- Kuning: DiskQueueDepth CloudWatch metrik lebih besar dari 5 tetapi kurang dari atau sama dengan 10
- Hijau: DiskQueueDepth CloudWatch metrik kurang dari atau sama dengan 5

Tindakan yang Direkomendasikan

Pertimbangkan untuk pindah ke instance dan volume penyimpanan yang mendukung karakteristik baca/tulis.

Laporkan kolom

- Status
- Wilayah
- DB Contoh ARN
- DiskQueueDepth Metrik

Amazon RDS FreeStorageSpace

Deskripsi

Memeriksa untuk melihat apakah FreeStorageSpace CloudWatch metrik untuk instance database RDS telah meningkat di atas ambang batas yang wajar secara operasional.

ID pemeriksaan

`Cmsvnj8db2`

Kriteria Peringatan

- Merah: FreeStorageSpace telah mencapai/melebihi 90% dari total kapasitas
- Kuning: FreeStorageSpace antara 80% dan 90% dari total kapasitas
- Hijau: FreeStorageSpace kurang dari 80% dari total kapasitas

Tindakan yang Direkomendasikan

Tingkatkan ruang penyimpanan untuk instans database RDS yang kehabisan penyimpanan gratis menggunakan Amazon RDS Management Console, Amazon RDS API, atau AWS Command Line Interface.

Laporkan kolom

- Status
- Wilayah

- DB Contoh ARN
- FreeStorageSpace Metrik (MB)
- Penyimpanan yang Dialokasikan Instans DB (MB)
- Penyimpanan Instans DB Digunakan Persen

Parameter log_output Amazon RDS diatur ke tabel

Deskripsi

Ketika log_output diatur ke TABLE, lebih banyak penyimpanan digunakan daripada ketika log_output diatur ke FILE. Kami menyarankan Anda mengatur parameter ke FILE, untuk menghindari mencapai batas ukuran penyimpanan.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

> **Note**
>
> Ketika instans DB atau kluster DB dihentikan, Anda dapat melihat rekomendasi Amazon RDS Trusted Advisor selama 3 hingga 5 hari. Setelah lima hari, rekomendasi tidak tersedia di Trusted Advisor. Untuk melihat rekomendasi, buka konsol Amazon RDS, lalu pilih Rekomendasi.
> Jika Anda menghapus instans DB atau kluster DB, maka rekomendasi yang terkait dengan instans atau cluster tersebut tidak tersedia di Trusted Advisor atau konsol manajemen Amazon RDS.

ID pemeriksaan

`c1qf5bt023`

Kriteria Peringatan

Kuning: Grup parameter DB memiliki parameter log_output diatur ke TABLE.

Tindakan yang Direkomendasikan

Tetapkan nilai parameter log_output ke FILE di grup parameter DB Anda.

Sumber Daya Tambahan

Untuk informasi selengkapnya, lihat file log database MySQL.

Laporkan kolom

- Status
- Wilayah
- Sumber Daya
- Nama Parameter
- Nilai yang Direkomendasikan
- Waktu Terakhir Diperbarui

Amazon RDS innodb_default_row_format pengaturan parameter tidak aman

Deskripsi

Instans DB Anda mengalami masalah yang diketahui: Tabel yang dibuat dalam versi MySQL yang lebih rendah dari 8.0.26 dengan row_format disetel ke COMPACT atau REDUNDANT tidak dapat diakses dan tidak dapat dipulihkan ketika indeks melebihi 767 byte.

Kami menyarankan Anda mengatur nilai parameter innodb_default_row_format ke DYNAMIC.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

> **Note**
>
> Ketika instans DB atau kluster DB dihentikan, Anda dapat melihat rekomendasi Amazon RDS Trusted Advisor selama 3 hingga 5 hari. Setelah lima hari, rekomendasi tidak tersedia di Trusted Advisor. Untuk melihat rekomendasi, buka konsol Amazon RDS, lalu pilih Rekomendasi.

Jika Anda menghapus instans DB atau kluster DB, maka rekomendasi yang terkait dengan instans atau cluster tersebut tidak tersedia di Trusted Advisor atau konsol manajemen Amazon RDS.

ID pemeriksaan

`c1qf5bt036`

Kriteria Peringatan

Merah: Grup parameter DB memiliki pengaturan tidak aman untuk parameter innodb_default_row_format.

Tindakan yang Direkomendasikan

Setel parameter innodb_default_row_format ke DYNAMIC.

Sumber Daya Tambahan

Ketika tabel dibuat dengan versi MySQL lebih rendah dari 8.0.26 dengan row_format disetel ke COMPACT atau REDUNDANT, membuat indeks dengan key prefix yang lebih pendek dari 767 byte tidak diberlakukan. Setelah database dimulai ulang, tabel ini tidak dapat diakses atau dipulihkan.

Untuk informasi selengkapnya, lihat Perubahan di MySQL 8.0.26 (2021-07-20, Ketersediaan Umum) n di situs web dokumentasi MySQL.

Laporkan kolom

- Status
- Wilayah
- Sumber Daya
- Nama Parameter
- Nilai yang Direkomendasikan
- Waktu Terakhir Diperbarui

Amazon RDS innodb_flush_log_at_trx_commit parameter bukan 1

Deskripsi

Nilai parameter innodb_flush_log_at_trx_commit dari instance DB Anda bukanlah nilai yang aman. Parameter ini mengontrol persistensi operasi commit ke disk.

Kami menyarankan Anda mengatur parameter innodb_flush_log_at_trx_commit ke 1.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

> **Note**
>
> Ketika instans DB atau kluster DB dihentikan, Anda dapat melihat rekomendasi Amazon RDS Trusted Advisor selama 3 hingga 5 hari. Setelah lima hari, rekomendasi tidak tersedia di Trusted Advisor. Untuk melihat rekomendasi, buka konsol Amazon RDS, lalu pilih Rekomendasi.
> Jika Anda menghapus instans DB atau kluster DB, maka rekomendasi yang terkait dengan instans atau cluster tersebut tidak tersedia di Trusted Advisor atau konsol manajemen Amazon RDS.

ID pemeriksaan

`c1qf5bt030`

Kriteria Peringatan

Kuning: Grup parameter DB memiliki innodb_flush_log_at_trx_commit disetel ke selain 1.

Tindakan yang Direkomendasikan

Setel nilai parameter innodb_flush_log_at_trx_commit ke 1

Sumber Daya Tambahan

Transaksi database tahan lama ketika buffer log disimpan ke penyimpanan yang tahan lama. Namun, menyimpan ke disk berdampak pada kinerja. Bergantung pada nilai yang ditetapkan

untuk parameter innodb_flush_log_at_trx_commit, perilaku bagaimana log ditulis dan disimpan ke disk dapat bervariasi.

- Ketika nilai parameter adalah 1, log ditulis dan disimpan ke disk setelah setiap transaksi yang dilakukan.
- Ketika nilai parameter adalah 0, log ditulis dan disimpan ke disk sekali per detik.
- Ketika nilai parameter adalah 2, log ditulis setelah setiap transaksi dilakukan dan disimpan ke disk sekali per detik. Data bergerak dari buffer memori InnoDB ke cache sistem operasi yang juga ada di memori.

> **Note**
>
> Ketika nilai parameter bukan 1, InnoDB tidak menjamin properti ACID. Transaksi terakhir untuk detik terakhir mungkin hilang ketika database mogok.

Untuk mengetahui informasi selengkapnya, lihat Praktik terbaik untuk mengonfigurasi parameter untuk Amazon RDS for MySQL, bagian 1: Parameter yang terkait dengan performa.

Laporkan kolom

- Status
- Wilayah
- Sumber Daya
- Nama Parameter
- Nilai yang Direkomendasikan
- Waktu Terakhir Diperbarui

Parameter Amazon RDS max_user_connections rendah

Deskripsi

Instans DB Anda memiliki nilai rendah untuk jumlah maksimum koneksi simultan untuk setiap akun basis data.

Sebaiknya atur parameter max_user_connections ke angka yang lebih besar dari 5.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

> **Note**
>
> Ketika instans DB atau kluster DB dihentikan, Anda dapat melihat rekomendasi Amazon RDS Trusted Advisor selama 3 hingga 5 hari. Setelah lima hari, rekomendasi tidak tersedia di Trusted Advisor. Untuk melihat rekomendasi, buka konsol Amazon RDS, lalu pilih Rekomendasi.
> Jika Anda menghapus instans DB atau kluster DB, maka rekomendasi yang terkait dengan instans atau cluster tersebut tidak tersedia di Trusted Advisor atau konsol manajemen Amazon RDS.

ID pemeriksaan

`c1qf5bt034`

Kriteria Peringatan

Kuning: Grup parameter DB memiliki max_user_connections yang salah dikonfigurasi.

Tindakan yang Direkomendasikan

Tingkatkan nilai parameter max_user_connections ke angka yang lebih besar dari 5.

Sumber Daya Tambahan

Pengaturan max_user_connections mengontrol jumlah maksimum koneksi simultan yang diizinkan untuk akun pengguna MySQL. Mencapai batas koneksi ini menyebabkan kegagalan dalam operasi administrasi instans Amazon RDS, seperti pencadangan, penambalan, dan perubahan parameter.

Untuk informasi selengkapnya, lihat Mengatur Batas Sumber Daya Akun di situs web dokumentasi MySQL.

Kolom laporan

- Status

- Wilayah
- Sumber Daya
- Nama Parameter
- Nilai yang Direkomendasikan
- Waktu Terakhir Diperbarui

Amazon RDS Multi-AZ

Deskripsi

Memeriksa instans DB yang digunakan dalam satu Availability Zone (AZ).

Penerapan multi-AZ meningkatkan ketersediaan database dengan mereplikasi secara sinkron ke instance siaga di Availability Zone yang berbeda. Selama pemeliharaan database yang direncanakan, atau kegagalan instans DB atau Availability Zone, Amazon RDS secara otomatis gagal ke siaga. Failover ini memungkinkan operasi database dilanjutkan dengan cepat tanpa intervensi administratif. Karena Amazon RDS tidak mendukung penyebaran Multi-AZ untuk Microsoft SQL Server, pemeriksaan ini tidak memeriksa instance SQL Server.

ID pemeriksaan

`f2iK5R6Dep`

Kriteria Peringatan

Kuning: Instans DB digunakan dalam satu Availability Zone.

Tindakan yang Direkomendasikan

Jika aplikasi Anda memerlukan ketersediaan tinggi, ubah instans DB Anda untuk mengaktifkan penerapan Multi-AZ. Lihat Ketersediaan Tinggi (Multi-AZ).

Sumber Daya Tambahan

Wilayah dan Zona Ketersediaan

Kolom laporan

- Status
- Wilayah/AZ
- Instans DB

- ID VPC
- Multi-AZ

Amazon RDS Tidak Dalam Rencana AWS Backup

Deskripsi

Memeriksa apakah instans Amazon RDS DB Anda disertakan dalam paket cadangan di. AWS Backup

AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya yang memudahkan untuk memusatkan dan mengotomatiskan pencadangan data di seluruh layanan. AWS

Menyertakan instans Amazon RDS DB Anda dalam rencana cadangan penting untuk kewajiban kepatuhan terhadap peraturan, pemulihan bencana, kebijakan bisnis untuk perlindungan data, dan tujuan kelangsungan bisnis.

Untuk informasi selengkapnya, lihat Apa itu AWS Backup? .

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

```
c18d2gz159
```

Sumber

```
AWS Config Managed Rule: rds-in-backup-plan
```

Kriteria Peringatan

Kuning: Instans Amazon RDS DB tidak disertakan dalam paket cadangan dengan AWS Backup.

Tindakan yang Direkomendasikan

Sertakan instans Amazon RDS DB Anda dalam paket cadangan dengan. AWS Backup

Untuk informasi selengkapnya, lihat Cadangan dan Pemulihan Amazon RDS Menggunakan AWS Backup.

Sumber Daya Tambahan

Menetapkan sumber daya ke rencana cadangan

Kolom laporan

- Status
- Wilayah
- Sumber Daya
- AWS Config Aturan
- Parameter Input
- Waktu Terakhir Diperbarui

Replika Baca Amazon RDS terbuka dalam mode yang dapat ditulis

Deskripsi

Instans DB Anda memiliki replika baca dalam mode yang dapat ditulis, yang memungkinkan pembaruan dari klien.

Kami menyarankan Anda mengatur parameter read_only ke TrueIfReplica sehingga replika baca tidak dalam mode yang dapat ditulis.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

> **Note**
>
> Ketika instans DB atau kluster DB dihentikan, Anda dapat melihat rekomendasi Amazon RDS Trusted Advisor selama 3 hingga 5 hari. Setelah lima hari, rekomendasi tidak tersedia di Trusted Advisor. Untuk melihat rekomendasi, buka konsol Amazon RDS, lalu pilih Rekomendasi.

Jika Anda menghapus instans DB atau kluster DB, maka rekomendasi yang terkait dengan instans atau cluster tersebut tidak tersedia di Trusted Advisor atau konsol manajemen Amazon RDS.

ID pemeriksaan

`c1qf5bt035`

Kriteria Peringatan

Kuning: Grup parameter DB mengaktifkan mode yang dapat ditulis untuk replika baca.

Tindakan yang Direkomendasikan

Setel nilai parameter read_only ke TrueIf Replica.

Sumber Daya Tambahan

Parameter read_only mengontrol izin tulis dari klien ke instance database. Nilai default untuk parameter ini adalah TrueIfReplica. Untuk contoh replika, TrueIfReplica menetapkan nilai read_only ke ON (1) dan menonaktifkan aktivitas penulisan apa pun dari klien. Untuk instance master/writer, TrueIfReplica menetapkan nilai ke OFF (0) dan mengaktifkan aktivitas tulis dari klien untuk instance tersebut. Ketika replika baca dibuka dalam mode yang dapat ditulis, data yang disimpan dalam instance ini dapat menyimpang dari instance utama yang menyebabkan kesalahan replikasi.

Untuk informasi selengkapnya, lihat Praktik terbaik untuk mengonfigurasi parameter Amazon RDS for MySQL, bagian 2: Parameter yang terkait dengan replikasi di situs web dokumentasi MySQL.

Kolom laporan

- Status
- Wilayah
- Sumber Daya
- Nama Parameter
- Nilai yang Direkomendasikan
- Waktu Terakhir Diperbarui

Pencadangan otomatis sumber daya Amazon RDS dimatikan

Deskripsi

Pencadangan otomatis dinonaktifkan pada sumber daya DB Anda. Pencadangan otomatis memungkinkan point-in-time pemulihan instans DB Anda.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

> **Note**
>
> Ketika instans DB atau kluster DB dihentikan, Anda dapat melihat rekomendasi Amazon RDS Trusted Advisor selama 3 hingga 5 hari. Setelah lima hari, rekomendasi tidak tersedia di Trusted Advisor. Untuk melihat rekomendasi, buka konsol Amazon RDS, lalu pilih Rekomendasi.
> Jika Anda menghapus instans DB atau kluster DB, maka rekomendasi yang terkait dengan instans atau cluster tersebut tidak tersedia di Trusted Advisor atau konsol manajemen Amazon RDS.

ID pemeriksaan

`c1qf5bt001`

Kriteria Peringatan

Merah: Sumber daya Amazon RDS tidak mengaktifkan pencadangan otomatis

Tindakan yang Direkomendasikan

Aktifkan pencadangan otomatis dengan periode retensi hingga 14 hari.

Sumber Daya Tambahan

Pencadangan otomatis memungkinkan point-in-time pemulihan instans DB Anda. Kami merekomendasikan untuk mengaktifkan cadangan otomatis. Saat Anda mengaktifkan

pencadangan otomatis untuk instans DB, Amazon RDS secara otomatis melakukan pencadangan penuh data Anda setiap hari selama jendela pencadangan pilihan Anda. Cadangan menangkap log transaksi ketika ada pembaruan untuk instans DB Anda. Anda mendapatkan penyimpanan cadangan hingga ukuran penyimpanan instans DB Anda tanpa biaya tambahan.

Untuk informasi selengkapnya, lihat sumber daya berikut:

- Mengaktifkan backup otomatis
- Mengungkap biaya penyimpanan cadangan Amazon RDS

Kolom laporan

- Status
- Wilayah
- Sumber Daya
- Nilai yang Direkomendasikan
- Nama Mesin
- Waktu Terakhir Diperbarui

Parameter Amazon RDS sync_binlog dimatikan

Deskripsi

Sinkronisasi log biner ke disk tidak diberlakukan sebelum komit transaksi diakui dalam instans DB Anda.

Kami menyarankan Anda mengatur nilai parameter sync_binlog ke 1.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

> **Note**
>
> Ketika instans DB atau kluster DB dihentikan, Anda dapat melihat rekomendasi Amazon RDS Trusted Advisor selama 3 hingga 5 hari. Setelah lima hari, rekomendasi tidak

tersedia di Trusted Advisor. Untuk melihat rekomendasi, buka konsol Amazon RDS, lalu pilih Rekomendasi.
Jika Anda menghapus instans DB atau kluster DB, maka rekomendasi yang terkait dengan instans atau cluster tersebut tidak tersedia di Trusted Advisor atau konsol manajemen Amazon RDS.

ID pemeriksaan

`c1qf5bt031`

Kriteria Peringatan

Kuning: Grup parameter DB memiliki logging biner sinkron dimatikan.

Tindakan yang Direkomendasikan

Setel parameter sync_binlog ke 1.

Sumber Daya Tambahan

Parameter sync_binlog mengontrol bagaimana MySQL mendorong log biner ke disk. Ketika nilai parameter ini diatur ke 1, itu menyalakan sinkronisasi log biner ke disk sebelum transaksi dilakukan. Ketika nilai parameter ini diatur ke 0, itu mematikan sinkronisasi log biner ke disk. Biasanya, MySQL server bergantung pada sistem operasi untuk mendorong log biner ke disk secara teratur mirip dengan file lain. Nilai parameter sync_binlog yang disetel ke 0 dapat meningkatkan kinerja. Namun, selama kegagalan daya atau crash sistem operasi, server kehilangan semua transaksi yang dilakukan yang tidak disinkronkan ke log biner.

Untuk informasi selengkapnya, lihat Praktik terbaik untuk mengonfigurasi parameter Amazon RDS for MySQL, bagian 2: Parameter yang terkait dengan replikasi.

Kolom laporan

- Status
- Wilayah
- Sumber Daya
- Nama Parameter
- Nilai yang Direkomendasikan
- Waktu Terakhir Diperbarui

RDS DB Cluster tidak mengaktifkan replikasi Multi-AZ

Deskripsi

Memeriksa apakah kluster Amazon RDS DB Anda mengaktifkan replikasi Multi-AZ.

Klaster basis data Multi-AZ memiliki satu instans basis data penulis dan dua instans basis data pembaca dalam tiga Zona Ketersediaan terpisah. Klaster DB Multi-AZ menyediakan ketersediaan tinggi, peningkatan kapasitas untuk beban kerja baca, dan latensi yang lebih rendah jika dibandingkan dengan deployment Multi-AZ.

Untuk informasi selengkapnya, lihat Membuat klaster DB multi-AZ.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

```
c18d2gz161
```

Sumber

```
AWS Config Managed Rule: rds-cluster-multi-az-enabled
```

Kriteria Peringatan

Kuning: Cluster Amazon RDS DB Anda tidak memiliki replikasi Multi-AZ yang dikonfigurasi

Tindakan yang Direkomendasikan

Aktifkan penerapan klaster DB multi-AZ saat Anda membuat klaster Amazon RDS DB.

Untuk informasi selengkapnya, lihat Membuat klaster DB multi-AZ.

Sumber Daya Tambahan

Penerapan cluster DB multi-AZ

Kolom laporan

- Status
- Wilayah

- Sumber Daya
- AWS Config Aturan
- Parameter Input
- Waktu Terakhir Diperbarui

Instans Siaga Multi-AZ RDS Tidak Diaktifkan

Deskripsi

Memeriksa apakah instans Amazon RDS DB Anda memiliki replika siaga Multi-AZ yang dikonfigurasi.

Amazon RDS Multi-AZ menyediakan ketersediaan dan daya tahan tinggi untuk instans database dengan mereplikasi data ke replika siaga di Availability Zone yang berbeda. Ini memberikan failover otomatis, meningkatkan kinerja, dan meningkatkan daya tahan data. Dalam deployment instans DB Multi-AZ, Amazon RDS akan otomatis menyediakan dan mempertahankan replika siaga yang sinkron di Zona Ketersediaan yang berbeda. Instans DB primer direplikasi secara sinkron di seluruh Zona Ketersediaan ke replika siaga untuk memberikan redundansi data dan meminimalkan lonjakan latensi selama pencadangan sistem. Menjalankan instans DB dengan ketersediaan tinggi meningkatkan ketersediaan selama pemeliharaan sistem yang direncanakan. Hal ini juga dapat membantu melindungi basis data Anda terhadap kegagalan instans DB dan gangguan Zona Ketersediaan.

Untuk informasi selengkapnya, lihat Penerapan instans DB multi-AZ.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

```
c18d2gz156
```

Sumber

```
AWS Config Managed Rule: rds-multi-az-support
```

Kriteria Peringatan

Kuning: Instans Amazon RDS DB tidak memiliki replika Multi-AZ yang dikonfigurasi.

Tindakan yang Direkomendasikan

Aktifkan penerapan multi-AZ saat Anda membuat instans Amazon RDS DB.

Pemeriksaan ini tidak dapat dikecualikan dari tampilan di Trusted Advisor konsol.

Sumber Daya Tambahan

Penerapan instans DB multi-AZ

Kolom laporan

- Status
- Wilayah
- Sumber Daya
- AWS Config Aturan
- Parameter Input
- Waktu Terakhir Diperbarui

Amazon RDS ReplicaLag

Deskripsi

Memeriksa untuk melihat apakah ReplicaLag CloudWatch metrik untuk instance database RDS telah meningkat di atas ambang batas operasional yang wajar selama seminggu terakhir.

ReplicaLag metrik mengukur jumlah detik replika baca berada di belakang instance utama. Kelambatan replikasi terjadi ketika pembaruan asinkron yang dibuat ke replika baca tidak dapat mengikuti pembaruan yang terjadi pada instance database utama. Jika terjadi kegagalan pada instance utama, data dapat hilang dari replika baca jika ReplicaLag berada di atas ambang batas yang wajar secara operasional.

ID pemeriksaan

`Cmsvnj8db1`

Kriteria Peringatan

- Merah: ReplicaLag metrik melebihi 60 detik setidaknya sekali selama seminggu.

- Kuning: ReplicaLag metrik melebihi 10 detik setidaknya sekali selama seminggu.
- Hijau: ReplicaLag kurang dari 10 detik.

Tindakan yang Direkomendasikan

Ada beberapa kemungkinan penyebab ReplicaLag untuk meningkat melampaui tingkat yang aman secara operasional. Misalnya, hal ini dapat disebabkan oleh contoh replika yang baru saja diganti/diluncurkan dari cadangan yang lebih lama dan replika ini membutuhkan waktu yang cukup lama untuk “mengejar” instance database utama dan transaksi langsung. Ini ReplicaLag mungkin berkurang seiring waktu saat terjadi pengejaran. Contoh lain adalah kecepatan transaksi yang dapat dicapai pada instance database utama lebih tinggi daripada proses replikasi atau infrastruktur replika yang dapat dicocokkan. Ini ReplicaLag dapat tumbuh seiring waktu karena replikasi gagal mengimbangi kinerja basis data utama. Akhirnya, beban kerja mungkin meledak selama periode yang berbeda dari hari/bulan/dll. yang mengakibatkan sesekali tertinggal. ReplicaLag Tim Anda harus menyelidiki kemungkinan akar penyebab yang berkontribusi tinggi ReplicaLag untuk database, dan mungkin mengubah jenis instance database atau karakteristik lain dari beban kerja untuk memastikan kontinuitas data pada replika sesuai dengan kebutuhan Anda.

Sumber Daya Tambahan

- Bekerja dengan replika baca untuk Amazon RDS for PostgreSQL
- Bekerja dengan replikasi MySQL di Amazon RDS
- Bekerja dengan replika baca MySQL

Kolom laporan

- Status
- Wilayah
- DB Contoh ARN
- ReplicaLag Metrik

Parameter Amazon RDS synchronous_commit dimatikan

Deskripsi

Ketika parameter synchronous_commit dimatikan, data dapat hilang dalam kerusakan database. Daya tahan database berisiko.

Kami menyarankan Anda mengaktifkan parameter synchronous_commit.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

> **Note**
>
> Ketika instans DB atau kluster DB dihentikan, Anda dapat melihat rekomendasi Amazon RDS Trusted Advisor selama 3 hingga 5 hari. Setelah lima hari, rekomendasi tidak tersedia di Trusted Advisor. Untuk melihat rekomendasi, buka konsol Amazon RDS, lalu pilih Rekomendasi.
> Jika Anda menghapus instans DB atau kluster DB, maka rekomendasi yang terkait dengan instans atau cluster tersebut tidak tersedia di Trusted Advisor atau konsol manajemen Amazon RDS.

ID pemeriksaan

`c1qf5bt026`

Kriteria Peringatan

Merah: Grup parameter DB memiliki parameter synchronous_commit dimatikan.

Tindakan yang Direkomendasikan

Aktifkan parameter synchronous_commit di grup parameter DB Anda.

Sumber Daya Tambahan

Parameter synchronous_commit mendefinisikan penyelesaian proses Write-Ahead Logging (WAL) sebelum server database mengirimkan notifikasi yang berhasil ke klien. Komit ini disebut sebagai komit asinkron karena klien mengakui komit sebelum WAL menyimpan transaksi dalam disk. Jika parameter synchronous_commit dimatikan, maka transaksi dapat hilang, daya tahan instans DB mungkin terganggu, dan data mungkin hilang saat database mogok.

Untuk informasi selengkapnya, lihat file log database MySQL.

Kolom laporan

- Status

- Wilayah
- Sumber Daya
- Nama Parameter
- Nilai yang Direkomendasikan
- Waktu Terakhir Diperbarui

Cuplikan otomatis klaster Amazon Redshift

Deskripsi

Memeriksa apakah snapshot otomatis diaktifkan untuk klaster Amazon Redshift Anda.

Amazon Redshift secara otomatis mengambil snapshot tambahan yang melacak perubahan pada cluster sejak snapshot otomatis sebelumnya. Snapshot otomatis menyimpan semua data yang diperlukan untuk memulihkan cluster dari snapshot. Untuk menonaktifkan snapshot otomatis, atur periode retensi ke nol. Anda tidak dapat menonaktifkan snapshot otomatis untuk tipe node RA3.

Anda dapat menentukan periode retensi minimum dan maksimum yang Anda inginkan menggunakan parameter MinRetentionMaxRetentionPeriode dan Periode AWS Config aturan Anda.

Cuplikan dan cadangan Amazon Redshift

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

```
c18d2gz135
```

Sumber

```
AWS Config Managed Rule: redshift-backup-enabled
```

Kriteria Peringatan

Merah: Amazon Redshift tidak memiliki snapshot otomatis yang dikonfigurasi dalam periode retensi yang diinginkan.

Tindakan yang Direkomendasikan

Pastikan snapshot otomatis diaktifkan untuk cluster Amazon Redshift Anda.

Untuk informasi selengkapnya, lihat Mengelola snapshot menggunakan konsol.

Sumber Daya Tambahan

Cuplikan dan cadangan Amazon Redshift

Untuk informasi selengkapnya, lihat Menggunakan cadangan.

Kolom laporan

- Status
- Wilayah
- Sumber Daya
- AWS Config Aturan
- Parameter Input
- Waktu Terakhir Diperbarui

Amazon Route 53 Menghapus Pemeriksaan Kesehatan

Deskripsi

Memeriksa kumpulan catatan sumber daya yang terkait dengan pemeriksaan kesehatan yang telah dihapus.

Route 53 tidak mencegah Anda menghapus pemeriksaan kesehatan yang terkait dengan satu atau lebih kumpulan catatan sumber daya. Jika Anda menghapus pemeriksaan kesehatan tanpa memperbarui kumpulan catatan sumber daya terkait, perutean kueri DNS untuk konfigurasi failover DNS Anda tidak akan berfungsi sebagaimana dimaksud.

Zona yang di-host yang dibuat oleh AWS layanan tidak akan muncul di hasil pemeriksaan Anda.

ID pemeriksaan

`Cb877eB72b`

Kriteria Peringatan

Kuning: Kumpulan catatan sumber daya dikaitkan dengan pemeriksaan kesehatan yang telah dihapus.

Tindakan yang Direkomendasikan

Buat pemeriksaan kesehatan baru dan kaitkan dengan kumpulan catatan sumber daya. Lihat Membuat, Memperbarui, dan Menghapus Pemeriksaan Kesehatan dan Menambahkan Pemeriksaan Kesehatan ke Kumpulan Rekaman Sumber Daya.

Sumber Daya Tambahan

- Amazon Route 53 Pemeriksaan Kesehatan dan DNS Failover
- Cara Kerja Pemeriksaan Kesehatan dalam Konfigurasi Amazon Route 53 Sederhana

Kolom laporan

- Nama Zona yang Dihosting
- ID Zona yang Dihosting
- Nama Set Catatan Sumber Daya
- Jenis Set Rekaman Sumber Daya
- Pengidentifikasi Set Rekaman Sumber Daya

Rekor Sumber Daya Failover Amazon Route 53

Deskripsi

Memeriksa kumpulan catatan sumber daya failover Amazon Route 53 yang memiliki kesalahan konfigurasi.

Ketika pemeriksaan kesehatan Amazon Route 53 menentukan bahwa sumber daya utama tidak sehat, Amazon Route 53 merespons kueri dengan kumpulan catatan sumber daya cadangan sekunder. Anda harus membuat kumpulan catatan sumber daya primer dan sekunder yang dikonfigurasi dengan benar agar failover berfungsi.

Zona yang di-host yang dibuat oleh AWS layanan tidak akan muncul di hasil pemeriksaan Anda.

ID pemeriksaan

`b73EEdD790`

Kriteria Peringatan

- Kuning: Kumpulan catatan sumber daya failover primer tidak memiliki kumpulan catatan sumber daya sekunder yang sesuai.
- Kuning: Kumpulan catatan sumber daya failover sekunder tidak memiliki kumpulan catatan sumber daya primer yang sesuai.
- Kuning: Kumpulan catatan sumber daya primer dan sekunder yang memiliki nama yang sama dikaitkan dengan pemeriksaan kesehatan yang sama.

Tindakan yang Direkomendasikan

Jika kumpulan sumber daya failover hilang, buat kumpulan catatan sumber daya yang sesuai. Lihat Membuat Kumpulan Rekaman Sumber Daya Failover.

Jika kumpulan catatan sumber daya Anda dikaitkan dengan pemeriksaan kesehatan yang sama, buat pemeriksaan kesehatan terpisah untuk masing-masing pemeriksaan kesehatan. Lihat Membuat, Memperbarui, dan Menghapus Pemeriksaan Kesehatan.

Sumber Daya Tambahan

Amazon Route 53 Pemeriksaan Kesehatan dan DNS Failover

Kolom laporan

- Nama Zona yang Dihosting
- ID Zona yang Dihosting
- Nama Set Catatan Sumber Daya
- Jenis Set Rekaman Sumber Daya
- Alasan

Amazon Route 53 Set Rekor Sumber Daya TTL Tinggi

Deskripsi

Memeriksa kumpulan catatan sumber daya yang dapat memperoleh manfaat dari memiliki nilai time-to-live (TTL) yang lebih rendah.

TTL adalah jumlah detik yang set catatan sumber daya di-cache oleh resolver DNS. Saat Anda menentukan TTL yang panjang, penyelesai DNS membutuhkan waktu lebih lama untuk meminta catatan DNS yang diperbarui, yang dapat menyebabkan penundaan yang tidak perlu dalam

mengalihkan lalu lintas. Misalnya, TTL yang panjang menciptakan penundaan antara saat DNS Failover mendeteksi kegagalan endpoint, dan ketika merespons dengan mengalihkan lalu lintas.

Zona yang di-host yang dibuat oleh AWS layanan tidak akan muncul di hasil pemeriksaan Anda.

ID pemeriksaan

`C056F80cR3`

Kriteria Peringatan

- Kuning: Kumpulan catatan sumber daya yang kebijakan peruteannya adalah Failover memiliki TTL lebih dari 60 detik.
- Kuning: Catatan sumber daya yang ditetapkan dengan pemeriksaan kesehatan terkait memiliki TTL lebih dari 60 detik.

Tindakan yang Direkomendasikan

Masukkan nilai TTL 60 detik untuk kumpulan catatan sumber daya yang terdaftar. Untuk informasi selengkapnya, lihat Bekerja dengan Kumpulan Rekaman Sumber Daya.

Sumber Daya Tambahan

Amazon Route 53 Pemeriksaan Kesehatan dan DNS Failover

Kolom laporan

- Status
- Nama Zona yang Dihosting
- ID Zona yang Dihosting
- Nama Set Catatan Sumber Daya
- Jenis Set Rekaman Sumber Daya
- ID Set Catatan Sumber Daya
- TTL

Delegasi Server Nama Amazon Route 53

Deskripsi

Memeriksa zona yang dihosting Amazon Route 53 yang registrar domain atau DNS Anda tidak menggunakan server nama Route 53 yang benar.

Saat Anda membuat zona yang dihosting, Route 53 menetapkan kumpulan delegasi empat server nama. *Nama-nama server ini adalah ns- ### .awsdns- ## .com, .net, .org, dan .co.uk, di mana ### dan ## biasanya mewakili nomor yang berbeda.* Sebelum Route 53 dapat merutekan kueri DNS untuk domain Anda, Anda harus memperbarui konfigurasi server nama registrar Anda untuk menghapus server nama yang ditetapkan oleh pencatat. Kemudian, Anda harus menambahkan keempat server nama di set delegasi Route 53. Untuk ketersediaan maksimum, Anda harus menambahkan keempat server nama Route 53.

Zona yang di-host yang dibuat oleh AWS layanan tidak akan muncul di hasil pemeriksaan Anda.

ID pemeriksaan

`cF171Db240`

Kriteria Peringatan

Kuning: Zona yang di-host dimana registrar untuk domain Anda tidak menggunakan keempat server nama Route 53 dalam kumpulan delegasi.

Tindakan yang Direkomendasikan

Tambahkan atau perbarui catatan server nama dengan registrar Anda atau dengan layanan DNS saat ini untuk domain Anda untuk menyertakan keempat server nama dalam kumpulan delegasi Route 53 Anda. Untuk menemukan nilai ini, lihat Mendapatkan Server Nama untuk Zona yang Dihosting. Untuk informasi tentang menambahkan atau memperbarui catatan server nama, lihat Membuat dan Memigrasi Domain dan Subdomain ke Amazon Route 53.

Sumber Daya Tambahan

Bekerja dengan Zona yang Dihosting

Kolom laporan

- Nama Zona yang Dihosting
- ID Zona yang Dihosting
- Jumlah Delegasi Server Nama yang Digunakan

Amazon Route 53 Resolver Redundansi Zona Ketersediaan Titik Akhir

Deskripsi

Memeriksa untuk melihat apakah konfigurasi layanan Anda memiliki alamat IP yang ditentukan dalam setidaknya dua Availability Zones (AZ) untuk redundansi. AZ adalah lokasi berbeda yang

terisolasi dari kegagalan di zona lain. Dengan menentukan alamat IP di beberapa AZ di Wilayah yang sama, Anda dapat membantu melindungi aplikasi Anda dari satu titik kegagalan.

ID pemeriksaan

`Chrv231ch1`

Kriteria Peringatan

- Kuning: Alamat IP hanya ditentukan dalam satu AZ
- Hijau: Alamat IP ditentukan dalam setidaknya dua AZ

Tindakan yang Direkomendasikan

Tentukan alamat IP di setidaknya dua Availability Zone untuk redundansi.

Sumber Daya Tambahan

- Jika memerlukan lebih dari satu titik akhir antarmuka jaringan elastis agar tersedia setiap saat, kami sarankan Anda menambahkan setidaknya satu antarmuka jaringan melebihi kebutuhan, untuk memastikan Anda memiliki kapasitas tambahan yang tersedia untuk menangani kemungkinan lonjakan lalu lintas. Antarmuka jaringan tambahan juga memastikan ketersediaan selama operasi layanan seperti pemeliharaan atau peningkatan.
- Ketersediaan tinggi untuk titik akhir Resolver

Kolom laporan

- Status
- Wilayah
- ARN Sumber Daya
- Jumlah AZ

Pencatatan Bucket Amazon S3

Deskripsi

Memeriksa konfigurasi logging bucket Amazon Simple Storage Service (Amazon S3).

Saat pencatatan akses server diaktifkan, log akses terperinci dikirimkan setiap jam ke bucket yang Anda pilih. Catatan log akses berisi rincian tentang setiap permintaan, seperti jenis permintaan, sumber daya yang ditentukan dalam permintaan, dan waktu dan tanggal permintaan diproses. Secara default, pencatatan bucket tidak diaktifkan. Anda harus mengaktifkan pencatatan jika

ingin melakukan audit keamanan atau mempelajari lebih lanjut tentang pengguna dan pola penggunaan.

Ketika logging awalnya diaktifkan, konfigurasi secara otomatis divalidasi. Namun, modifikasi future dapat mengakibatkan kegagalan logging. Pemeriksaan ini memeriksa izin bucket Amazon S3 eksplisit, tetapi pemeriksaan ini tidak memeriksa kebijakan bucket terkait yang mungkin mengesampingkan izin bucket.

ID pemeriksaan

`BueAdJ7NrP`

Kriteria Peringatan

- Kuning: Bucket tidak mengaktifkan pencatatan akses server.
- Kuning: Izin bucket target tidak menyertakan akun root, jadi Trusted Advisor tidak dapat memeriksanya.
- Merah: Ember target tidak ada.
- Merah: Ember target dan ember sumber memiliki pemilik yang berbeda.
- Merah: Pengirim log tidak memiliki izin menulis untuk bucket target.

Tindakan yang Direkomendasikan

Aktifkan pencatatan ember untuk sebagian besar ember. Lihat Mengaktifkan Pencatatan Menggunakan Konsol dan Mengaktifkan Pencatatan Secara Terprogram.

Jika izin bucket target tidak menyertakan akun root dan Anda Trusted Advisor ingin memeriksa status logging, tambahkan akun root sebagai penerima hibah. Lihat Mengedit Izin Bucket.

Jika bucket target tidak ada, pilih bucket yang sudah ada sebagai target atau buat bucket baru dan pilih bucket tersebut. Lihat Mengelola Bucket Logging.

Jika target dan sumber memiliki pemilik yang berbeda, ubah bucket target menjadi bucket yang memiliki pemilik yang sama dengan bucket sumber. Lihat Mengelola Bucket Logging.

Jika pengirim log tidak memiliki izin menulis untuk target (tulis tidak diaktifkan), berikan izin Unggah/Hapus ke grup Pengiriman Log. Lihat Mengedit Izin Bucket.

Sumber Daya Tambahan

- Bekerja dengan Bucket
- Pencatatan Akses Server

- Format Log Akses Server
- Menghapus File Log

Kolom laporan

- Status
- Wilayah
- Nama Bucket
- Nama Target
- Target Ada
- Pemilik yang sama
- Menulis Diaktifkan
- Alasan

Replikasi Bucket Amazon S3 Tidak Diaktifkan

Deskripsi

Memeriksa apakah bucket Amazon S3 Anda memiliki aturan replikasi yang diaktifkan untuk Replikasi Lintas Wilayah, Replikasi Wilayah Sama, atau keduanya.

Replikasi adalah penyalinan objek secara otomatis dan asinkron di seluruh ember di Wilayah yang sama atau berbeda. AWS Replikasi menyalin objek yang baru dibuat dan pembaruan objek dari bucket sumber ke bucket atau bucket tujuan. Gunakan replikasi bucket Amazon S3 untuk membantu meningkatkan ketahanan dan kepatuhan aplikasi dan penyimpanan data Anda.

Untuk informasi selengkapnya, lihat Mereplikasi objek.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

`c18d2gz119`

Sumber

```
AWS Config Managed Rule: s3-bucket-replication-enabled
```

Kriteria Peringatan

Kuning: Aturan replikasi bucket Amazon S3 tidak diaktifkan untuk Replikasi Lintas Wilayah, Replikasi Wilayah Sama, atau keduanya.

Tindakan yang Direkomendasikan

Aktifkan aturan replikasi bucket Amazon S3 untuk meningkatkan ketahanan dan kepatuhan aplikasi dan penyimpanan data Anda.

Untuk informasi selengkapnya, lihat Melihat pekerjaan cadangan dan titik pemulihan dan Menyiapkan replikasi.

Sumber Daya Tambahan

Walkthroughs: Contoh untuk mengonfigurasi replikasi

Kolom laporan

- Status
- Wilayah
- Sumber Daya
- AWS Config Aturan
- Parameter Input
- Waktu Terakhir Diperbarui

Versi Bucket Amazon S3

Deskripsi

Memeriksa bucket Amazon Simple Storage Service yang tidak mengaktifkan versi, atau versi ditangguhkan.

Saat pembuatan versi diaktifkan, Anda dapat dengan mudah memulihkan dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi. Pembuatan versi memungkinkan Anda untuk mempertahankan, mengambil, dan memulihkan versi objek apa pun yang disimpan dalam ember.

Anda dapat menggunakan aturan siklus hidup untuk mengelola semua versi objek Anda, serta biaya terkait, dengan secara otomatis mengarsipkan objek ke kelas penyimpanan Glacier. Aturan juga dapat dikonfigurasi untuk menghapus versi objek Anda setelah periode waktu tertentu. Anda juga dapat meminta otentikasi multi-faktor (MFA) untuk setiap penghapusan objek atau perubahan konfigurasi pada bucket Anda.

Pembuatan versi tidak dapat dinonaktifkan setelah diaktifkan. Namun, itu dapat ditangguhkan, yang mencegah versi objek baru dibuat. Menggunakan versi dapat meningkatkan biaya Anda untuk Amazon S3, karena Anda membayar untuk penyimpanan beberapa versi objek.

ID pemeriksaan

`R365s2Qddf`

Kriteria Peringatan

- Hijau: Pembuatan versi diaktifkan untuk bucket.
- Kuning: Pembuatan versi tidak diaktifkan untuk bucket.
- Kuning: Versi ditangguhkan untuk ember.

Tindakan yang Direkomendasikan

Aktifkan pembuatan versi bucket di sebagian besar bucket untuk mencegah penghapusan atau penimpaan yang tidak disengaja. Lihat Menggunakan Pembuatan Versi dan Mengaktifkan Versi Secara Terprogram.

Jika pembuatan versi bucket ditangguhkan, pertimbangkan untuk mengaktifkan kembali pembuatan versi. Untuk informasi tentang bekerja dengan objek dalam bucket yang ditangguhkan versi, lihat Mengelola Objek dalam Bucket yang Ditangguhkan Versi.

Saat pembuatan versi diaktifkan atau ditangguhkan, Anda dapat menentukan aturan konfigurasi siklus hidup untuk menandai versi objek tertentu sebagai kedaluwarsa atau menghapus versi objek yang tidak diperlukan secara permanen. Untuk informasi lebih lanjut, lihat Manajemen Siklus Aktif Objek.

MFA Delete memerlukan otentikasi tambahan saat status pembuatan versi bucket diubah atau saat versi objek dihapus. Ini mengharuskan pengguna untuk memasukkan kredensyal dan kode dari perangkat otentikasi yang disetujui. Untuk informasi lebih lanjut, lihat Penghapusan MFA.

Sumber Daya Tambahan

Bekerja dengan Bucket

Kolom laporan

- Status
- Wilayah
- Nama Bucket
- Penentuan Versi
- MFA Hapus Diaktifkan

Penyeimbang Beban Aplikasi, Jaringan, dan Gateway Tidak Mencakup Beberapa Zona Ketersediaan

Deskripsi

Memeriksa Apakah penyeimbang beban Anda (Application, Network, dan Gateway Load Balancer) dikonfigurasi dengan subnet di beberapa Availability Zone.

Anda dapat menentukan Availability Zone minimum yang diinginkan dalam AvailabilityZones parameter min AWS Config aturan Anda.

Untuk informasi selengkapnya, lihat Availability Zone untuk Application Load Balancer, Availability Zones - Network Load Balancers, dan Create a Gateway Load Balancer.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

```
c18d2gz169
```

Sumber

```
AWS Config Managed Rule: elbv2-multiple-az
```

Kriteria Peringatan

Kuning: Application, Network, atau Gateway Load Balancers dikonfigurasi dengan subnet di kurang dari dua Availability Zone.

Tindakan yang Direkomendasikan

Konfigurasikan Application, Network, dan Gateway Load Balancer Anda dengan subnet di beberapa Availability Zone.

Sumber Daya Tambahan

Availability Zone untuk Application Load Balancer Anda

Zona Ketersediaan (Elastic Load Balancing)

Buat Load Balancer Gateway

Kolom laporan

- Status
- Wilayah
- Sumber Daya
- AWS Config Aturan
- Parameter Input
- Waktu Terakhir Diperbarui

Auto Scaling IP tersedia di Subnet

Deskripsi

Memeriksa bahwa IP yang tersedia cukup tetap ada di antara Subnet yang ditargetkan. Memiliki IP yang cukup tersedia untuk digunakan akan membantu ketika Grup Auto Scaling mencapai ukuran maksimumnya dan perlu meluncurkan instance tambahan.

ID pemeriksaan

`Cjxm268ch1`

Kriteria Peringatan

- Merah: Jumlah maksimum instance dan alamat IP yang dapat dibuat oleh ASG melebihi jumlah alamat IP yang tersisa di subnet yang dikonfigurasi.
- Hijau: Ada cukup alamat IP yang tersedia untuk skala yang tersisa di ASG.

Tindakan yang Direkomendasikan

Meningkatkan jumlah alamat IP yang tersedia

Kolom laporan

- Status
- Wilayah
- ARN Sumber Daya
- Contoh maksimum yang dapat dibuat
- Jumlah instans yang tersedia

Pemeriksaan Kesehatan Grup Auto Scaling

Deskripsi

Memeriksa konfigurasi pemeriksaan kesehatan untuk grup Auto Scaling.

Jika Elastic Load Balancing digunakan untuk grup Auto Scaling, konfigurasi yang disarankan adalah mengaktifkan pemeriksaan kesehatan Elastic Load Balancing. Jika pemeriksaan kesehatan Elastic Load Balancing tidak digunakan, Auto Scaling hanya dapat bertindak atas kesehatan instans Amazon Elastic Compute Cloud (Amazon EC2). Auto Scaling tidak akan bertindak pada aplikasi yang berjalan pada instance.

ID pemeriksaan

`CLOG40CDO8`

Kriteria Peringatan

- Kuning: Grup Auto Scaling memiliki penyeimbang beban terkait, tetapi pemeriksaan kesehatan Elastic Load Balancing tidak diaktifkan.
- Kuning: Grup Auto Scaling tidak memiliki penyeimbang beban terkait, tetapi pemeriksaan kesehatan Elastic Load Balancing diaktifkan.

Tindakan yang Direkomendasikan

Jika grup Auto Scaling memiliki penyeimbang beban terkait, tetapi pemeriksaan kesehatan Elastic Load Balancing tidak diaktifkan, lihat Menambahkan Pemeriksaan Kesehatan Elastic Load Balancing ke Grup Auto Scaling Anda.

Jika pemeriksaan kesehatan Elastic Load Balancing diaktifkan, tetapi tidak ada penyeimbang beban yang terkait dengan grup Auto Scaling, lihat Mengatur Aplikasi Berskala Otomatis dan Beban Seimbang.

Sumber Daya Tambahan

Panduan Pengguna Penskalaan Otomatis Amazon EC2

Kolom laporan

- Status
- Wilayah
- Nama Grup Auto Scaling
- Load Balancer Terkait
- Pemeriksaan Kondisi

Sumber Daya Grup Auto Scaling

Deskripsi

Memeriksa ketersediaan sumber daya yang terkait dengan konfigurasi peluncuran dan grup Auto Scaling Anda.

Grup Auto Scaling yang mengarah ke sumber daya yang tidak tersedia tidak dapat meluncurkan instans Amazon Elastic Compute Cloud (Amazon EC2) baru. Jika dikonfigurasi dengan benar, Auto Scaling menyebabkan jumlah instans Amazon EC2 meningkat dengan mulus selama lonjakan permintaan, dan berkurang secara otomatis selama jeda permintaan. Grup Auto Scaling dan konfigurasi peluncuran yang mengarah ke sumber daya yang tidak tersedia tidak beroperasi sebagaimana dimaksud.

ID pemeriksaan

`8CNsSllI5v`

Kriteria Peringatan

- Merah: Grup Auto Scaling dikaitkan dengan penyeimbang beban yang dihapus.
- Merah: Konfigurasi peluncuran dikaitkan dengan Gambar Mesin Amazon (AMI) yang dihapus.

Tindakan yang Direkomendasikan

Jika penyeimbang beban telah dihapus, buat penyeimbang beban baru atau grup target lalu kaitkan ke grup Auto Scaling, atau buat grup Auto Scaling baru tanpa penyeimbang beban. Untuk informasi tentang membuat grup Auto Scaling baru dengan penyeimbang beban baru, lihat Mengatur Aplikasi Berskala Otomatis dan Beban Seimbang. Untuk informasi tentang membuat

grup Auto Scaling baru tanpa penyeimbang beban, lihat Membuat Grup Auto Scaling di Memulai Auto Scaling Menggunakan Konsol.

Jika AMI telah dihapus, buat template peluncuran baru atau luncurkan versi template menggunakan AMI yang valid dan kaitkan dengan grup Auto Scaling. Lihat Membuat Konfigurasi Peluncuran di Memulai Auto Scaling Menggunakan Konsol.

Sumber Daya Tambahan

- Pemecahan Masalah Auto Scaling: Amazon EC2 AMI
- Pemecahan Masalah Auto Scaling: Konfigurasi Load Balancer
- Panduan Pengguna Penskalaan Otomatis Amazon EC2

Kolom laporan

- Status
- Wilayah
- Nama Grup Auto Scaling
- Jenis Peluncuran
- Jenis Sumber Daya
- Nama Sumber Daya

AWS CloudHSM cluster yang menjalankan instance HSM dalam satu AZ

Deskripsi

Memeriksa klaster Anda yang menjalankan instance HSM dalam satu Availability Zone (AZ). Pemeriksaan ini memberi tahu Anda jika cluster Anda berisiko tidak memiliki cadangan terbaru.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

```
hc0dfs7601
```

Kriteria Peringatan

- Kuning: Cluster CloudHSM menjalankan semua instance HSM dalam satu Availability Zone selama lebih dari 1 jam.
- Hijau: Cluster CloudHSM menjalankan semua instance HSM di setidaknya dua Availability Zone yang berbeda.

Tindakan yang Direkomendasikan

Buat setidaknya satu instance lagi untuk cluster di Availability Zone yang berbeda.

Sumber Daya Tambahan

Praktik terbaik untuk AWS CloudHSM

Kolom laporan

- Status
- Wilayah
- ID Klaster
- Jumlah Instans HSM
- Waktu Terakhir Diperbarui

AWS Direct Connect Ketahanan Lokasi

Deskripsi

Memeriksa ketahanan yang AWS Direct Connect digunakan untuk menghubungkan lokal Anda ke setiap gateway Direct Connect atau gateway pribadi virtual.

Pemeriksaan ini memberi tahu Anda jika gateway Direct Connect atau gateway pribadi virtual tidak dikonfigurasi dengan antarmuka virtual di setidaknya dua lokasi Direct Connect yang berbeda. Kurangnya ketahanan lokasi dapat mengakibatkan downtime yang tidak terduga selama pemeliharaan, pemotongan serat, kegagalan perangkat, atau kegagalan lokasi total.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul.

> **Note**
>
> Direct Connect diimplementasikan dengan Transit Gateway menggunakan gateway Direct Connect.

ID pemeriksaan

`c1dfpnchv2`

Kriteria Peringatan

Merah: Gateway Direct Connect atau gateway pribadi virtual dikonfigurasi dengan satu atau beberapa antarmuka virtual pada satu perangkat Direct Connect.

Kuning: Gateway Direct Connect atau gateway pribadi virtual dikonfigurasi dengan antarmuka virtual di beberapa perangkat Direct Connect dalam satu lokasi Direct Connect.

Hijau: Gateway Direct Connect atau gateway pribadi virtual dikonfigurasi dengan antarmuka virtual di dua atau lebih lokasi Direct Connect yang berbeda.

Tindakan yang Direkomendasikan

Untuk membangun ketahanan lokasi Direct Connect, Anda dapat mengonfigurasi gateway Direct Connect atau gateway pribadi virtual untuk terhubung ke setidaknya dua lokasi Direct Connect yang berbeda. Untuk informasi lebih lanjut, lihat Rekomendasi AWS Direct Connect Ketahanan.

Sumber Daya Tambahan

AWS Direct Connect Rekomendasi Ketahanan

AWS Direct Connect Tes Failover

Kolom laporan

- Status
- Wilayah
- Waktu Terakhir Diperbarui
- Status Ketahanan
- Lokasi
- ID Koneksi
- ID Gerbang

AWS Lambda fungsi tanpa antrian huruf mati yang dikonfigurasi

Deskripsi

Memeriksa apakah suatu AWS Lambda fungsi dikonfigurasi dengan antrian huruf mati.

Antrian huruf mati adalah fitur AWS Lambda yang memungkinkan Anda menangkap dan menganalisis peristiwa yang gagal, menyediakan cara untuk menangani peristiwa tersebut sesuai dengan itu. Kode Anda mungkin memunculkan pengecualian, waktu habis, atau kehabisan memori, yang mengakibatkan eksekusi asinkron fungsi Lambda Anda gagal. Antrian surat mati menyimpan pesan dari pemanggilan yang gagal, menyediakan cara untuk menangani pesan dan memecahkan masalah kegagalan.

Anda dapat menentukan sumber daya antrian huruf mati yang ingin Anda periksa menggunakan parameter DlQarns dalam aturan Anda. AWS Config

Untuk informasi selengkapnya, lihat Antrian surat mati.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

```
c18d2gz182
```

Sumber

```
AWS Config Managed Rule: lambda-dlq-check
```

Kriteria Peringatan

Kuning: AWS Lambda fungsi tidak memiliki antrian huruf mati yang dikonfigurasi.

Tindakan yang Direkomendasikan

Pastikan AWS Lambda fungsi Anda memiliki antrian huruf mati yang dikonfigurasi untuk mengontrol penanganan pesan untuk semua pemanggilan asinkron yang gagal.

Untuk informasi selengkapnya, lihat Antrian surat mati.

Sumber Daya Tambahan

- Desain Aplikasi Tanpa Server yang Kuat dengan AWS Lambda Dead Letter Queues

Kolom laporan

- Status
- Wilayah
- Sumber Daya
- AWS Config Aturan
- Parameter Input
- Waktu Terakhir Diperbarui

AWS Lambda Tentang Tujuan Acara Kegagalan

Deskripsi

Memeriksa apakah fungsi Lambda di akun Anda memiliki tujuan acara On Failure atau Dead Letter Queue (DLQ) yang dikonfigurasi untuk pemanggilan asinkron, sehingga catatan dari pemanggilan yang gagal dapat dialihkan ke tujuan untuk penyelidikan atau pemrosesan lebih lanjut.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

`c1dfprch05`

Kriteria Peringatan

- Kuning: Fungsi tidak memiliki tujuan acara On Failure atau DLQ yang dikonfigurasi.

Tindakan yang Direkomendasikan

Harap siapkan tujuan acara On Failure atau DLQ untuk fungsi Lambda Anda untuk mengirim pemanggilan yang gagal bersama dengan detail lainnya ke salah satu layanan AWS tujuan yang tersedia untuk debugging atau pemrosesan lebih lanjut.

Sumber Daya Tambahan

- Doa Asinkron
- AWS Lambda Tentang Destinasi Acara Kegagalan

Kolom laporan

- Status
- Wilayah
- Fungsi dengan versi yang ditandai.
- Permintaan async hari ini turun persentase
- Permintaan async hari ini
- Permintaan async harian rata-rata turun persentase
- Permintaan async harian rata-rata
- Waktu Terakhir Diperbarui

Fungsi AWS Lambda berkemampuan VPC tanpa Redundansi Multi-AZ

Deskripsi

Memeriksa versi $LATEST dari fungsi Lambda berkemampuan VPC yang rentan terhadap gangguan layanan di satu Availability Zone. Ini adalah praktik terbaik bahwa fungsi berkemampuan VPC terhubung ke beberapa Availability Zone untuk ketersediaan tinggi.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

`L4dfs2Q4C6`

Kriteria Peringatan

Kuning: Versi $LATEST dari fungsi Lambda berkemampuan VPC terhubung ke subnet dalam satu Availability Zone.

Tindakan yang Direkomendasikan

Saat mengonfigurasi fungsi untuk akses ke VPC Anda, pilih subnet di beberapa Availability Zone untuk memastikan ketersediaan tinggi.

Sumber Daya Tambahan

- Mengkonfigurasi fungsi Lambda untuk mengakses sumber daya di VPC
- Ketahanan di AWS Lambda

Kolom laporan

- Status
- Wilayah
- Fungsi ARN
- ID VPC
- Rata-rata Pemanggilan harian
- Waktu Terakhir Diperbarui

AWS Resilience Hub Pemeriksaan Komponen Aplikasi

Deskripsi

Memeriksa apakah Komponen Aplikasi (AppComponent) dalam aplikasi Anda tidak dapat dipulihkan. Jika AppComponent tidak pulih dalam kasus peristiwa gangguan, Anda mungkin mengalami kehilangan data yang tidak diketahui dan downtime sistem.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul.

ID pemeriksaan

`RH23stmM04`

Kriteria Peringatan

Merah: AppComponent tidak dapat dipulihkan.

Tindakan yang Direkomendasikan

Untuk memastikan bahwa Anda dapat AppComponent dipulihkan, tinjau dan terapkan rekomendasi ketahanan, dan kemudian jalankan penilaian baru. Untuk informasi selengkapnya tentang meninjau rekomendasi ketahanan, lihat Sumber Daya Tambahan.

Sumber Daya Tambahan

Meninjau rekomendasi ketahanan

AWS Resilience Hub konsep

AWS Resilience Hub Panduan Pengguna

Kolom laporan

- Status
- Wilayah
- Nama Aplikasi
- AppComponent Nama
- Waktu Terakhir Diperbarui

AWS Resilience Hub kebijakan dilanggar

Deskripsi

Memeriksa Resilience Hub untuk aplikasi yang tidak memenuhi tujuan waktu pemulihan (RTO) dan tujuan titik pemulihan (RPO) yang ditentukan oleh kebijakan. Pemeriksaan memberi tahu Anda jika aplikasi Anda tidak memenuhi tujuan RTO dan RPO yang telah Anda tetapkan untuk aplikasi di Resilience Hub.

> **Note**
>
> Hasil untuk pemeriksaan ini disegarkan secara otomatis, dan permintaan penyegaran tidak diizinkan. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

`RH23stmM02`

Kriteria Peringatan

- Hijau: Aplikasi ini memiliki kebijakan dan memenuhi tujuan RTO dan RPO.
- Kuning: Aplikasi belum dinilai.
- Merah: Aplikasi ini memiliki kebijakan tetapi tidak memenuhi tujuan RTO dan RPO.

Tindakan yang Direkomendasikan

Masuk ke konsol Resilience Hub dan tinjau rekomendasi agar aplikasi Anda memenuhi tujuan RTO dan RPO.

Sumber Daya Tambahan

Konsep Resilience Hub

Kolom laporan

- Status
- Wilayah
- Nama Aplikasi
- Waktu Terakhir Diperbarui

AWS Resilience Hub skor ketahanan

Deskripsi

Memeriksa apakah Anda telah menjalankan penilaian untuk aplikasi Anda di Resilience Hub. Pemeriksaan ini memberi tahu Anda jika skor ketahanan Anda di bawah nilai tertentu.

> **Note**
>
> Hasil untuk pemeriksaan ini disegarkan secara otomatis, dan permintaan penyegaran tidak diizinkan. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

`RH23stmM01`

Kriteria Peringatan

- Hijau: Aplikasi Anda memiliki skor ketahanan 70 atau lebih.

- Kuning: Aplikasi Anda memiliki skor ketahanan 40 hingga 69.
- Kuning: Aplikasi belum dinilai.
- Merah: Aplikasi Anda memiliki skor ketahanan kurang dari 40.

Tindakan yang Direkomendasikan

Masuk ke konsol Resilience Hub dan jalankan penilaian untuk aplikasi Anda. Tinjau rekomendasi untuk meningkatkan skor ketahanan.

Sumber Daya Tambahan

Konsep Resilience Hub

Kolom laporan

- Status
- Wilayah
- Nama Aplikasi
- Skor Ketahanan Aplikasi
- Waktu Terakhir Diperbarui

AWS Resilience Hub usia penilaian

Deskripsi

Memeriksa berapa lama sejak Anda terakhir menjalankan penilaian aplikasi. Pemeriksaan ini memberi tahu Anda jika Anda belum menjalankan penilaian aplikasi selama beberapa hari tertentu.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

`RH23stmM03`

Kriteria Peringatan

- Hijau: Penilaian aplikasi Anda berjalan dalam 30 hari terakhir.
- Kuning: Penilaian aplikasi Anda belum berjalan dalam 30 hari terakhir.

Tindakan yang Direkomendasikan

Masuk ke konsol Resilience Hub dan jalankan penilaian untuk aplikasi Anda.

Sumber Daya Tambahan

Konsep Resilience Hub

Kolom laporan

- Status
- Wilayah
- Nama Aplikasi
- Hari Sejak Penilaian Terakhir Berlangsung
- Waktu Jalankan Penilaian Terakhir
- Waktu Terakhir Diperbarui

AWS Site-to-Site VPN memiliki setidaknya satu terowongan dalam status DOWN

Deskripsi

Memeriksa jumlah terowongan yang aktif untuk masing-masing AWS Site-to-Site VPN s Anda.

VPN harus memiliki dua terowongan yang dikonfigurasi setiap saat. Ini memberikan redundansi jika terjadi pemadaman atau pemeliharaan perangkat yang direncanakan di titik akhir AWS. Untuk beberapa perangkat keras, hanya satu terowongan yang aktif dalam satu waktu. Jika VPN tidak memiliki terowongan aktif, biaya untuk VPN mungkin masih berlaku.

Untuk informasi lebih lanjut, lihat Apa yang dimaksud dengan AWS Site-to-Site VPN?

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

```
c18d2gz123
```

Sumber

```
AWS Config Managed Rule: vpc-vpn-2-tunnels-up
```

Kriteria Peringatan

Kuning: Sebuah Site-to-Site VPN memiliki setidaknya satu terowongan DOWN.

Tindakan yang Direkomendasikan

Pastikan bahwa dua terowongan dikonfigurasi untuk koneksi VPN. Dan, jika perangkat keras Anda mendukungnya, pastikan kedua terowongan aktif. Jika Anda tidak lagi memerlukan koneksi VPN, hapus untuk menghindari biaya.

Untuk informasi selengkapnya, lihat perangkat gateway pelanggan Anda dan konten yang tersedia di Pusat Pengetahuan AWS.

Sumber Daya Tambahan

- AWS Site-to-Site VPN Panduan Pengguna
- Menambahkan Gateway Pribadi Virtual ke VPC Anda

Kolom laporan

- Status
- Wilayah
- Sumber Daya
- AWS Config Aturan
- Parameter Input
- Waktu Terakhir Diperbarui

AWS Well-Architectedmasalah risiko tinggi untuk keandalan

Deskripsi

Memeriksa masalah risiko tinggi (HRI) untuk beban kerja Anda di pilar keandalan. Pemeriksaan ini didasarkan pada AWS-Well Architected ulasan Anda. Hasil pemeriksaan Anda tergantung pada apakah Anda menyelesaikan evaluasi beban kerja denganAWS Well-Architected.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

`Wxdfp4B1L4`

Kriteria Peringatan

- Merah: Setidaknya satu masalah risiko tinggi aktif diidentifikasi dalam pilar keandalan untuk AWS Well-Architected.
- Hijau: Tidak ada masalah risiko tinggi aktif yang terdeteksi di pilar keandalan untuk AWS Well-Architected.

Tindakan yang Direkomendasikan

AWS Well-Architected mendeteksi masalah risiko tinggi selama evaluasi beban kerja Anda. Masalah-masalah ini menghadirkan peluang untuk mengurangi risiko dan menghemat uang. Masuk ke alat AWS Well-Architected untuk meninjau jawaban Anda dan mengambil tindakan untuk menyelesaikan masalah aktif Anda.

Kolom laporan

- Status
- Wilayah
- Beban Kerja ARN
- Nama Beban Kerja
- Nama Pengulas
- Jenis Beban Kerja
- Tanggal Mulai Beban Kerja
- Beban Kerja Tanggal Modifikasi Terakhir
- Jumlah HRI yang diidentifikasi untuk Keandalan
- Jumlah HRI yang diselesaikan untuk Keandalan
- Jumlah pertanyaan yang dijawab untuk Keandalan

- Jumlah total pertanyaan di pilar Keandalan
- Waktu Terakhir Diperbarui

Classic Load Balancer tidak memiliki beberapa AZ yang dikonfigurasi

Deskripsi

Memeriksa apakah Classic Load Balancer mencakup beberapa Availability Zone (AZ).

Penyeimbang beban mendistribusikan lalu lintas aplikasi yang masuk di beberapa instans Amazon EC2 di beberapa Availability Zone. Secara default, penyeimbang beban mendistribusikan lalu lintas secara merata di seluruh Availability Zone yang Anda aktifkan untuk penyeimbang beban Anda. Jika satu Availability Zone mengalami pemadaman, maka node penyeimbang beban secara otomatis meneruskan permintaan ke instance terdaftar yang sehat di satu atau beberapa Availability Zone.

Anda dapat menyesuaikan jumlah minimum Availability Zone menggunakan AvailabilityZones parameter min dalam AWS Config aturan

Untuk informasi selengkapnya, lihat Apa itu Classic Load Balancer? .

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

```
c18d2gz154
```

Sumber

```
AWS Config Managed Rule: clb-multiple-az
```

Kriteria Peringatan

Kuning: Classic Load Balancer tidak memiliki konfigurasi Multi-AZ atau tidak memenuhi jumlah minimum AZ yang ditentukan.

Tindakan yang Direkomendasikan

Pastikan Classic Load Balancer Anda memiliki beberapa Availability Zone yang dikonfigurasi. Rentang penyeimbang beban Anda di beberapa AZ untuk memastikan bahwa Anda memiliki ketersediaan aplikasi yang tinggi.

Untuk informasi selengkapnya, lihat Tutorial: Membuat Classic Load Balancer.

Kolom laporan

- Status
- Wilayah
- Sumber Daya
- AWS Config Aturan
- Parameter Input
- Waktu Terakhir Diperbarui

ELB Connection Draining

Deskripsi

Memeriksa penyeimbang beban yang tidak mengaktifkan pengurasan koneksi.

Jika pengurasan koneksi tidak diaktifkan dan Anda membatalkan pendaftaran instans Amazon EC2 dari penyeimbang beban, penyeimbang beban menghentikan perutean lalu lintas ke instans tersebut dan menutup sambungan. Saat pengurasan koneksi diaktifkan, penyeimbang beban berhenti mengirim permintaan baru ke instance yang dideregistrasi tetapi membuat koneksi tetap terbuka untuk melayani permintaan aktif.

ID pemeriksaan

`7qGXsKIUw`

Kriteria Peringatan

Kuning: Pengurasan koneksi tidak diaktifkan untuk penyeimbang beban.

Tindakan yang Direkomendasikan

Aktifkan pengeringan koneksi untuk penyeimbang beban. Untuk informasi selengkapnya, lihat Connection Draining dan Aktifkan atau Nonaktifkan Connection Draining untuk Load Balancer Anda.

Sumber Daya Tambahan

Konsep Elastic Load Balancing

Kolom laporan

- Status
- Wilayah
- Nama Load Balancer
- Alasan

Optimalisasi Penyeimbang Beban

Deskripsi

Memeriksa konfigurasi penyeimbang beban Anda.

Untuk membantu meningkatkan tingkat toleransi kesalahan di Amazon Elastic Compute Cloud (Amazon EC2) saat menggunakan Elastic Load Balancing, sebaiknya jalankan jumlah instans yang sama di beberapa Availability Zone di suatu Wilayah. Penyeimbang beban yang dikonfigurasi akan dikenakan biaya, jadi ini juga merupakan pemeriksaan pengoptimalan biaya.

ID pemeriksaan

`iqdCTZKCUp`

Kriteria Peringatan

- Kuning: Penyeimbang beban diaktifkan untuk satu Availability Zone.
- Kuning: Penyeimbang beban diaktifkan untuk Availability Zone yang tidak memiliki instance aktif.
- Kuning: Instans Amazon EC2 yang terdaftar dengan penyeimbang beban didistribusikan secara tidak merata di seluruh Availability Zone. (Perbedaan antara jumlah instans tertinggi dan terendah di Availability Zone yang digunakan lebih dari 1, dan perbedaannya lebih dari 20% dari jumlah tertinggi.)

Tindakan yang Direkomendasikan

Pastikan penyeimbang beban Anda mengarah ke instans aktif dan sehat di setidaknya dua Availability Zone. Untuk informasi selengkapnya, lihat Menambahkan Availability Zone.

Jika penyeimbang beban Anda dikonfigurasi untuk Availability Zone tanpa instans yang sehat, atau jika ada ketidakseimbangan instans di seluruh Availability Zone, tentukan apakah semua

Availability Zone diperlukan. Hilangkan Availability Zone yang tidak perlu dan pastikan ada distribusi instans yang seimbang di seluruh Availability Zone yang tersisa. Untuk informasi selengkapnya, lihat Menghapus Availability Zone.

Sumber Daya Tambahan

- Zona dan Wilayah Ketersediaan
- Mengelola Load Balancer
- Praktik Terbaik dalam Mengevaluasi Elastic Load Balancing

Kolom laporan

- Status
- Wilayah
- Nama Load Balancer
- # Zona
- Zona sebuah Instans
- Zona b Contoh
- Zona c Contoh
- Zona d Contoh
- Zona e Instans
- Zona f Contoh
- Alasan

NAT Gateway AZ Kemerdekaan

Deskripsi

Memeriksa apakah Gateway NAT Anda dikonfigurasi dengan independensi Availability Zone (AZ).

NAT Gateway memungkinkan sumber daya di subnet pribadi Anda untuk terhubung dengan aman ke layanan di luar subnet menggunakan alamat IP NAT Gateway dan menjatuhkan lalu lintas masuk yang tidak diminta. Setiap Gateway NAT beroperasi dalam Availability Zone (AZ) yang ditunjuk dan dibangun dengan redundansi hanya di AZ tersebut. Oleh karena itu, sumber daya Anda di AZ tertentu harus menggunakan NAT Gateway di AZ yang sama sehingga potensi pemadaman Gateway NAT atau AZ-nya tidak memengaruhi sumber daya Anda di AZ lain.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

`c1dfptbg10`

Kriteria Peringatan

- Merah: Lalu lintas dari subnet Anda dalam satu AZ sedang dirutekan melalui NATGW di AZ yang berbeda.
- Hijau: Lalu lintas dari subnet Anda dalam satu AZ sedang dirutekan melalui NATGW di AZ yang sama.

Tindakan yang Direkomendasikan

Silakan periksa AZ subnet Anda dan rute lalu lintas melalui NAT Gateway di AZ yang sama.

Jika tidak ada NATGW di AZ, silakan buat satu dan kemudian rutekan lalu lintas subnet Anda melaluinya.

Jika Anda memiliki tabel rute yang sama yang terkait di seluruh subnet di AZ yang berbeda, simpan tabel rute ini terkait dengan subnet yang berada di AZ yang sama dengan NAT Gateway dan untuk subnet di AZ lainnya, harap kaitkan tabel rute terpisah dengan rute ke NAT Gateway di AZ lainnya ini.

Sebaiknya pilih jendela pemeliharaan untuk perubahan arsitektur di VPC Amazon Anda.

Sumber Daya Tambahan

- Cara membuat NAT Gateway
- Cara mengonfigurasi rute untuk kasus penggunaan NAT Gateway yang berbeda

Kolom laporan

- Status
- Wilayah
- Zona Ketersediaan NAT

- NAT ID
- Zona Ketersediaan Subnet
- ID Subnet
- ID Tabel Rute
- NAT ARN
- Waktu Terakhir Diperbarui

Penyeimbang Beban Jaringan Cross Load Balancing

Deskripsi

Memeriksa apakah penyeimbangan beban lintas zona diaktifkan pada Network Load Balancers.

Penyeimbangan beban lintas zona membantu menjaga pemerataan lalu lintas masuk di seluruh instans di Availability Zone yang berbeda. Hal ini mencegah penyeimbang beban merutekan semua lalu lintas ke instance di Availability Zone yang sama, yang dapat menyebabkan distribusi lalu lintas yang tidak merata dan potensi kelebihan beban. Fitur ini juga membantu keandalan aplikasi dengan secara otomatis merutekan lalu lintas ke instans sehat di Availability Zone lainnya jika terjadi kegagalan Availability Zone tunggal.

Untuk informasi selengkapnya, lihat Penyeimbangan beban lintas zona.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

```
c18d2gz105
```

Sumber

```
AWS Config Managed Rule: nlb-cross-zone-load-balancing-enabled
```

Kriteria Peringatan

- Kuning: Network Load Balancer tidak mengaktifkan penyeimbangan beban lintas zona.

Tindakan yang Direkomendasikan

Pastikan penyeimbangan beban lintas zona diaktifkan pada Network Load Balancer.

Sumber Daya Tambahan

Penyeimbangan beban lintas zona (Network Load Balancers)

Kolom laporan

- Status
- Wilayah
- Sumber Daya
- AWS Config Aturan
- Parameter Input
- Waktu Terakhir Diperbarui

NLB - Sumber daya yang menghadap Internet di subnet pribadi

Deskripsi

Memeriksa apakah Network Load Balancer (NLB) yang menghadap ke internet dikonfigurasi dengan subnet pribadi. Network Load Balancer (NLB) yang menghadap ke internet harus dikonfigurasi dalam subnet publik untuk menerima lalu lintas. Subnet publik didefinisikan sebagai subnet yang memiliki rute langsung ke gateway internet. Jika subnet dikonfigurasi sebagai pribadi, maka Availability Zone (AZ) tidak menerima lalu lintas, yang dapat menyebabkan masalah ketersediaan.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

`c1dfpnchv4`

Kriteria Peringatan

Merah: NLB dikonfigurasi dengan satu atau lebih subnet pribadi

Hijau: Tidak ada subnet pribadi yang dikonfigurasi untuk NLB yang menghadap ke internet

Tindakan yang Direkomendasikan

Konfirmasikan bahwa subnet yang dikonfigurasi dalam penyeimbang beban yang menghadap ke internet bersifat publik. Subnet publik didefinisikan sebagai subnet yang memiliki rute langsung ke gateway internet. Gunakan salah satu opsi berikut:

- Buat penyeimbang beban baru dan pilih subnet yang berbeda dengan rute langsung ke gateway internet.
- Ubah subnet yang saat ini dilampirkan ke penyeimbang beban dari pribadi ke publik. Untuk melakukan ini, ubah tabel rute dan kaitkan gateway internet.

Sumber Daya Tambahan

- Konfigurasikan penyeimbang beban dan pendengar
- Subnet untuk VPC Anda
- Kaitkan gateway dengan tabel rute

Kolom laporan

- Status
- Wilayah
- NLB Arn
- Nama NLB
- ID Subnet
- Skema NLB
- Jenis Subnet
- Waktu Terakhir Diperbarui

NLB Multi-AZ

Deskripsi

Memeriksa apakah Network Load Balancer Anda dikonfigurasi untuk menggunakan lebih dari satu Availability Zone (AZ). AZ adalah lokasi berbeda yang terisolasi dari kegagalan di zona lain.

Konfigurasikan penyeimbang beban Anda di beberapa AZ di Wilayah yang sama untuk membantu meningkatkan ketersediaan beban kerja Anda.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

`c1dfprch09`

Kriteria Peringatan

Kuning: NLB ada dalam satu AZ.

Hijau: NLB memiliki dua atau lebih AZ.

Tindakan yang Direkomendasikan

Pastikan penyeimbang beban Anda dikonfigurasi dengan setidaknya dua Availability Zone.

Sumber Daya Tambahan

Untuk informasi selengkapnya, lihat dokumentasi berikut ini:

- Zona Ketersediaan
- AWS Well-Architected - Menyebarkan beban kerja ke beberapa lokasi
- Wilayah dan Zona Ketersediaan

Kolom laporan

- Status
- Wilayah
- Jumlah AZ
- NLB ARN
- Nama NLB
- Waktu Terakhir Diperbarui

Jumlah Wilayah AWS dalam set replikasi Manajer Insiden

Deskripsi

Memeriksa apakah konfigurasi set replikasi Manajer Incident menggunakan lebih dari satu Wilayah AWS untuk mendukung failover dan respons regional. Untuk insiden yang dibuat oleh CloudWatch alarm atau EventBridge peristiwa, Manajer Insiden membuat insiden yang Wilayah AWS sama dengan aturan alarm atau peristiwa. Jika Manajer Insiden sementara tidak tersedia di Wilayah itu, sistem mencoba membuat insiden di Wilayah lain dalam kumpulan replikasi. Jika set replikasi hanya mencakup satu Wilayah, sistem gagal membuat catatan insiden sementara Manajer Insiden tidak tersedia.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

`cIdfp1js9r`

Kriteria Peringatan

- Hijau: Set replikasi berisi lebih dari satu Wilayah.
- Kuning: Set replikasi berisi satu Wilayah.

Tindakan yang Direkomendasikan

Tambahkan setidaknya satu Wilayah lagi ke set replikasi.

Sumber Daya Tambahan

Untuk informasi selengkapnya, lihat Manajemen insiden lintas wilayah.

Kolom laporan

- Status
- Multi-wilayah
- Set Replikasi

- Waktu Terakhir Diperbarui

Pemeriksaan Aplikasi AZ Tunggal

Deskripsi

Memeriksa pola jaringan jika lalu lintas jaringan keluar Anda merutekan melalui Availability Zone (AZ) tunggal.

AZ adalah lokasi berbeda yang terisolasi dari dampak apa pun di zona lain. Dengan menyebarkan layanan Anda di beberapa AZ, Anda membatasi radius ledakan kegagalan AZ.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

`c1dfptbg11`

Kriteria Peringatan

- Kuning: Aplikasi Anda dapat digunakan hanya dalam satu AZ berdasarkan pola jaringan keluar yang diamati. Jika ini benar dan aplikasi Anda mengharapkan ketersediaan tinggi, kami sarankan Anda menyediakan sumber daya aplikasi Anda dan menerapkan alur jaringan Anda untuk memanfaatkan beberapa Availability Zone.

Tindakan yang Direkomendasikan

Jika aplikasi Anda memerlukan ketersediaan tinggi, pertimbangkan untuk menerapkan arsitektur multi-AZ untuk ketersediaan yang lebih tinggi.

Kolom laporan

- Status
- Wilayah
- ID VPC
- Waktu Terakhir Diperbarui

Antarmuka jaringan titik akhir antarmuka VPC di beberapa AZ

Deskripsi

Memeriksa apakah titik akhir antarmuka AWS PrivateLink VPC Anda dikonfigurasi untuk menggunakan lebih dari satu Availability Zone (AZ). AZ adalah lokasi berbeda yang terisolasi dari kegagalan di zona lain. Ini mendukung konektivitas jaringan latensi rendah yang murah antara AZ di Wilayah yang sama. AWS Pilih subnet di beberapa AZ saat Anda membuat titik akhir antarmuka untuk membantu melindungi aplikasi Anda dari satu titik kegagalan.

> **Note**
>
> Pemeriksaan ini saat ini hanya mencakup titik akhir antarmuka.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

`c1dfprch10`

Kriteria Peringatan

Kuning: Titik akhir VPC ada dalam satu AZ.

Hijau: Titik akhir VPC setidaknya ada di dua AZ.

Tindakan yang Direkomendasikan

Pastikan titik akhir antarmuka VPC Anda dikonfigurasi dengan setidaknya dua Availability Zone.

Sumber Daya Tambahan

Untuk informasi selengkapnya, lihat dokumentasi berikut ini:

- Mengakses AWS layanan menggunakan antarmuka VPC endpoint
- Alamat IP pribadi dari antarmuka jaringan titik akhir

- AWS PrivateLink konsep
- Wilayah dan Zona Ketersediaan

Kolom laporan

- Status
- Wilayah
- ID Titik Akhir VPC
- Adalah Multi AZ
- Waktu Terakhir Diperbarui

Redundansi Terowongan VPN

Deskripsi

Memeriksa jumlah terowongan yang aktif untuk setiap VPN Anda.

VPN harus memiliki dua terowongan yang dikonfigurasi setiap saat. Ini memberikan redundansi jika terjadi pemadaman atau pemeliharaan perangkat yang direncanakan di titik akhir. AWS Untuk beberapa perangkat keras, hanya satu terowongan yang aktif dalam satu waktu. Jika VPN tidak memiliki terowongan aktif, biaya untuk VPN mungkin masih berlaku. Untuk informasi selengkapnya, lihat Panduan AWS Client VPN Administrator.

ID pemeriksaan

`S45wrEXrLz`

Kriteria Peringatan

- Kuning: VPN memiliki satu terowongan aktif (ini normal untuk beberapa perangkat keras).
- Kuning: VPN tidak memiliki terowongan aktif.

Tindakan yang Direkomendasikan

Pastikan bahwa dua terowongan dikonfigurasi untuk koneksi VPN Anda, dan keduanya aktif jika perangkat keras Anda mendukungnya. Jika Anda tidak lagi memerlukan koneksi VPN, Anda dapat menghapusnya untuk menghindari biaya. Untuk informasi selengkapnya, lihat Gateway Pelanggan Anda atau Menghapus koneksi VPN.

Sumber Daya Tambahan

- AWS Panduan Pengguna VPN Site-to-Site
- Menambahkan Gerbang Pribadi Virtual Perangkat Keras ke VPC Anda

Kolom laporan

- Status
- Wilayah
- ID VPN
- VPC
- Gerbang Pribadi Virtual
- Gateway pelanggan
- Terowongan Aktif
- Alasan

Redundansi Zona Ketersediaan ActiveMQ

Deskripsi

Memeriksa bahwa Amazon MQ untuk broker ActiveMQ dikonfigurasi untuk ketersediaan tinggi dengan broker aktif/siaga di beberapa Availability Zone.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

`c1t3k8mqv1`

Kriteria Peringatan

- Kuning: Amazon MQ untuk broker ActiveMQ dikonfigurasi dalam satu Availability Zone.

  Hijau: Amazon MQ untuk broker ActiveMQ dikonfigurasi di setidaknya dua Availability Zone.

Tindakan yang Direkomendasikan

Buat broker baru dengan mode penerapan aktif/siaga.

Sumber Daya Tambahan

- Membuat broker ActiveMQ

Kolom laporan

- Status
- Wilayah
- ID Pialang ActiveMQ
- Jenis Mesin Broker
- Mode Penerapan
- Waktu Terakhir Diperbarui

Redundansi Zona Ketersediaan RabbitMQ

Deskripsi

Memeriksa bahwa Amazon MQ untuk broker RabbitMQ dikonfigurasi untuk ketersediaan tinggi dengan instance cluster di beberapa Availability Zone.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

`c1t3k8mqv2`

Kriteria Peringatan

- Kuning: Amazon MQ untuk broker RabbitMQ dikonfigurasi dalam satu Availability Zone.

  Hijau: Amazon MQ untuk broker RabbitMQ dikonfigurasi di beberapa Availability Zone.

Tindakan yang Direkomendasikan

Buat broker baru dengan mode penyebaran cluster.

Sumber Daya Tambahan

- Membuat broker RabbitMQ

Kolom laporan

- Status

- Wilayah
- ID Pialang RabbitMQ
- Jenis Mesin Broker
- Mode Penerapan
- Waktu Terakhir Diperbarui

Batas layanan

Lihat pemeriksaan berikut untuk kategori batas layanan (juga dikenal sebagai kuota).

Semua cek dalam kategori ini memiliki deskripsi berikut:

Kriteria Peringatan

- Kuning: 80% dari batas tercapai.
- Merah: 100% dari batas tercapai.
- Biru: Trusted Advisor tidak dapat mengambil pemanfaatan atau batasan dalam satu atau lebih. Wilayah AWS

Tindakan yang Direkomendasikan

Jika Anda berharap melebihi batas layanan, minta peningkatan langsung dari konsol Service Quotas. Jika Service Quotas belum mendukung layanan Anda, Anda dapat membuat open case dukungan di Support Center.

Kolom laporan

- Status
- Layanan
- wilayah
- Batas Jumlah
- Penggunaan Saat Ini

> **Note**
>
> - Nilai didasarkan pada snapshot, sehingga penggunaan Anda saat ini mungkin berbeda. Kuota dan data penggunaan dapat memakan waktu hingga 24 jam untuk mencerminkan

perubahan apa pun. Dalam kasus di mana kuota baru-baru ini ditingkatkan, Anda mungkin untuk sementara melihat pemanfaatan yang melebihi kuota.

Periksa nama

- Grup Auto Scaling
- Konfigurasi Peluncuran Auto Scaling
- CloudFormation Tumpukan
- Kapasitas Baca DynamoDB
- Kapasitas Tulis DynamoDB
- Snapshot Aktif EBS
- Penyimpanan Volume Cold HDD (sc1) EBS
- Penyimpanan Volume General Purpose SSD (gp2) EBS
- Penyimpanan Volume General Purpose SSD (gp3) EBS
- Penyimpanan Volume Magnetis EBS (standar)
- IOPS Agregat Volume IOPS (SSD) yang Disediakan EBS
- Penyimpanan Volume Provisioned IOPS SSD (io1) EBS
- Penyimpanan Volume Provisioned IOPS SSD (io2) EBS
- Penyimpanan Volume Throughput Optimized HDD (st1) EBS
- Instans Sesuai Permintaan EC2
- Sewa Instans Cadangan EC2
- Alamat IP Elastis EC2-Klasik
- Alamat IP Elastis EC2-VPC
- Penyeimbang Beban Aplikasi ELB
- ELB Classic Load Balancer
- Penyeimbang Beban Jaringan ELB
- Grup IAM
- Profil Instans IAM
- Kebijakan IAM
- IAM Role
- Sertifikat Server IAM

- Pengguna IAM
- Pecahan Kinesis per Wilayah
- Penggunaan Penyimpanan Kode Lambda
- Grup Parameter Cluster RDS
- Peran Cluster RDS
- Cluster RDS
- Instans RDS DB
- Cuplikan Manual RDS DB
- Grup Parameter RDS DB
- Grup Keamanan RDS DB
- Langganan Acara RDS
- RDS Max Auths untuk Grup Keamanan
- Grup Opsi RDS
- RDS Baca Replika untuk Master
- Instans Cadangan RDS
- Grup Subnet RDS
- Subnet RDS untuk Grup Subnet
- Kuota Penyimpanan Total RDS
- Rute 53 Zona yang Dihosting
- Pemeriksaan Kesehatan Route 53 Max
- Rute 53 Set Delegasi yang Dapat Digunakan Kembali
- Kebijakan Lalu Lintas Route 53
- Contoh Kebijakan Lalu Lintas Route 53
- Kuota Pengiriman Harian SES
- VPC
- Gateway Internet VPC

Grup Auto Scaling

Deskripsi

Memeriksa penggunaan yang lebih dari 80% dari kuota Grup Auto Scaling.

ID pemeriksaan

`fW7HH0l7J9`

Sumber Daya Tambahan

Kuota Auto Scaling

Konfigurasi Peluncuran Auto Scaling

Deskripsi

Memeriksa penggunaan yang lebih dari 80% dari kuota konfigurasi peluncuran Auto Scaling.

ID pemeriksaan

`aW7HH0l7J9`

Sumber Daya Tambahan

Kuota Auto Scaling

CloudFormation Tumpukan

Deskripsi

Memeriksa penggunaan yang lebih dari 80% dari kuota CloudFormation tumpukan.

ID pemeriksaan

`gW7HH0l7J9`

Sumber Daya Tambahan

AWS CloudFormationkuota

Kapasitas Baca DynamoDB

Deskripsi

Memeriksa penggunaan yang lebih dari 80% dari batas throughput yang disediakan DynamoDB untuk pembacaan per. Akun AWS

ID pemeriksaan

`6gtQddfEw6`

Sumber Daya Tambahan

Kuota DynamoDB

Kapasitas Tulis DynamoDB

Deskripsi

Memeriksa penggunaan yang lebih dari 80% dari batas throughput yang disediakan DynamoDB untuk penulisan per. Akun AWS

ID pemeriksaan

`c5ftjdfkMr`

Sumber Daya Tambahan

Kuota DynamoDB

Snapshot Aktif EBS

Deskripsi

Memeriksa penggunaan yang lebih dari 80% dari kuota snapshot aktif EBS.

ID pemeriksaan

`eI7KK0l7J9`

Sumber Daya Tambahan

Batas Amazon EBS

Penyimpanan Volume Cold HDD (sc1) EBS

Deskripsi

Memeriksa penggunaan yang lebih dari 80% dari kuota penyimpanan volume EBS Cold HDD (sc1).

ID pemeriksaan

gH5CC0e3J9

Sumber Daya Tambahan

Batas Amazon EBS

Penyimpanan Volume General Purpose SSD (gp2) EBS

Deskripsi

Memeriksa penggunaan yang lebih dari 80% dari kuota penyimpanan volume EBS General Purpose SSD (gp2).

ID pemeriksaan

dH7RR0l6J9

Sumber Daya Tambahan

Batas Amazon EBS

Penyimpanan Volume General Purpose SSD (gp3) EBS

Deskripsi

Memeriksa penggunaan yang lebih dari 80% dari kuota penyimpanan volume EBS General Purpose SSD (gp3).

ID pemeriksaan

dH7RR0l6J3

Sumber Daya Tambahan

Batas Amazon EBS

Penyimpanan Volume Magnetis EBS (standar)

Deskripsi

Memeriksa penggunaan yang lebih dari 80% dari kuota penyimpanan volume EBS Magnetic (standar).

ID pemeriksaan

`cG7HH0l7J9`

Sumber Daya Tambahan

Batas Amazon EBS

IOPS Agregat Volume IOPS (SSD) yang Disediakan EBS

Deskripsi

Memeriksa penggunaan yang lebih dari 80% dari kuota IOPS agregat volume IOPS (SSD) EBS Provisioned.

ID pemeriksaan

`tV7YY0l7J9`

Sumber Daya Tambahan

Batas Amazon EBS

Penyimpanan Volume Provisioned IOPS SSD (io1) EBS

Deskripsi

Memeriksa penggunaan yang lebih dari 80% dari kuota penyimpanan volume EBS Provisioned IOPS SSD (io1).

ID pemeriksaan

`gI7MM0l7J9`

Sumber Daya Tambahan

Batas Amazon EBS

Penyimpanan Volume Provisioned IOPS SSD (io2) EBS

Deskripsi

Memeriksa penggunaan yang lebih dari 80% dari kuota penyimpanan volume EBS Provisioned IOPS SSD (io2).

ID pemeriksaan

`gI7MM0l7J2`

Sumber Daya Tambahan

Batas Amazon EBS

Penyimpanan Volume Throughput Optimized HDD (st1) EBS

Deskripsi

Memeriksa penggunaan yang lebih dari 80% dari kuota penyimpanan volume EBS Throughput Optimized HDD (st1).

ID pemeriksaan

`wH7DD0l3J9`

Sumber Daya Tambahan

Batas Amazon EBS

Instans Sesuai Permintaan EC2

Deskripsi

Memeriksa penggunaan yang lebih dari 80% dari kuota Instans Sesuai Permintaan EC2.

ID pemeriksaan

`0Xc6LMYG8P`

Sumber Daya Tambahan

Kuota Amazon EC2

Sewa Instans Cadangan EC2

Deskripsi

Memeriksa penggunaan yang lebih dari 80% dari kuota sewa Instans Cadangan EC2.

ID pemeriksaan

`iH7PP0l7J9`

Sumber Daya Tambahan

Kuota Amazon EC2

Alamat IP Elastis EC2-Klasik

Deskripsi

Memeriksa penggunaan yang lebih dari 80% dari kuota alamat IP Elastis EC2-Classic.

ID pemeriksaan

`aW9HH0l8J6`

Sumber Daya Tambahan

Kuota Amazon EC2

Alamat IP Elastis EC2-VPC

Deskripsi

Memeriksa penggunaan yang lebih dari 80% dari kuota alamat IP Elastic EC2-VPC.

ID pemeriksaan

`lN7RR0l7J9`

Sumber Daya Tambahan

Kuota IP VPC Elastis

Penyeimbang Beban Aplikasi ELB

Deskripsi

Cek penggunaan yang lebih dari 80% dari kuota ELB Application Load Balancers.

ID pemeriksaan

`EM8b3yLRTr`

Sumber Daya Tambahan

Kuota Elastic Load Balancing

ELB Classic Load Balancer

Deskripsi

Cek penggunaan yang lebih dari 80% dari kuota ELB Classic Load Balancers.

ID pemeriksaan

`iK7O00l7J9`

Sumber Daya Tambahan

Kuota Elastic Load Balancing

Penyeimbang Beban Jaringan ELB

Deskripsi

Cek penggunaan yang lebih dari 80% dari kuota ELB Network Load Balancers.

ID pemeriksaan

`8wIqYSt25K`

Sumber Daya Tambahan

Kuota Elastic Load Balancing

Grup IAM

Deskripsi

Cek penggunaan yang lebih dari 80% dari kuota grup IAM.

ID pemeriksaan

`sU7XX0l7J9`

Sumber Daya Tambahan

Kuota IAM

Profil Instans IAM

Deskripsi

Memeriksa penggunaan yang lebih dari 80% dari kuota profil instans IAM.

ID pemeriksaan

`nO7SS0l7J9`

Sumber Daya Tambahan

Kuota IAM

Kebijakan IAM

Deskripsi

Cek penggunaan yang lebih dari 80% dari kuota kebijakan IAM.

ID pemeriksaan

`pR7UU0l7J9`

Sumber Daya Tambahan

Kuota IAM

IAM Role

Deskripsi

Memeriksa penggunaan yang lebih dari 80% dari kuota peran IAM.

ID pemeriksaan

`oQ7TT0l7J9`

Sumber Daya Tambahan

Kuota IAM

Sertifikat Server IAM

Deskripsi

Memeriksa penggunaan yang lebih dari 80% dari kuota sertifikat server IAM.

ID pemeriksaan

`rT7WW0l7J9`

Sumber Daya Tambahan

Kuota IAM

Pengguna IAM

Deskripsi

Cek penggunaan yang lebih dari 80% dari kuota pengguna IAM.

ID pemeriksaan

`qS7VV0l7J9`

Sumber Daya Tambahan

Kuota IAM

Pecahan Kinesis per Wilayah

Deskripsi

Memeriksa penggunaan yang lebih dari 80% dari pecahan Kinesis per kuota Wilayah.

ID pemeriksaan

`bW7HH0l7J9`

Sumber Daya Tambahan

Kuota Kinesis

Penggunaan Penyimpanan Kode Lambda

Deskripsi

Memeriksa penggunaan penyimpanan kode yang lebih dari 80% dari batas akun.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

`c1dfprch07`

Kriteria Peringatan

- Kuning: 80% dari batas tercapai.

Tindakan yang Direkomendasikan

Harap identifikasi fungsi atau versi lambda yang tidak digunakan dan hapus untuk mengosongkan penyimpanan kode untuk akun Anda di wilayah tersebut. Jika Anda membutuhkan penyimpanan tambahan, silakan buat kasus dukungan di Support Center. Jika Anda berharap melebihi batas layanan, minta peningkatan langsung dari konsol Service Quotas. Jika Service Quotas belum mendukung layanan Anda, Anda dapat membuat open case dukungan di Support Center.

Sumber Daya Tambahan

- Penggunaan Penyimpanan Kode Lambda

Kolom laporan

- Status
- wilayah
- Fungsi ARN yang memenuhi syarat untuk sumber daya ini.
- Penggunaan penyimpanan kode fungsi MegaBytes dengan 2 desimal.
- Jumlah versi dalam fungsi
- Waktu Terakhir Diperbarui

Grup Parameter Cluster RDS

Deskripsi

Memeriksa penggunaan yang lebih dari 80% dari kuota kelompok parameter klaster RDS.

ID pemeriksaan

`jtlIMO3qZM`

Sumber Daya Tambahan

Kuota Amazon RDS

Peran Cluster RDS

Deskripsi

Memeriksa penggunaan yang lebih dari 80% dari kuota peran klaster RDS.

ID pemeriksaan

`7fuccf1Mx7`

Sumber Daya Tambahan

Kuota Amazon RDS

Cluster RDS

Deskripsi

Memeriksa penggunaan yang lebih dari 80% dari kuota klaster RDS.

ID pemeriksaan

`gjqMBn6pjz`

Sumber Daya Tambahan

Kuota Amazon RDS

Instans RDS DB

Deskripsi

Memeriksa penggunaan yang lebih dari 80% dari kuota instans RDS DB.

ID pemeriksaan

`XG0aXHpIEt`

Sumber Daya Tambahan

Kuota Amazon RDS

Cuplikan Manual RDS DB

Deskripsi

Memeriksa penggunaan yang lebih dari 80% dari kuota snapshot manual RDS DB.

ID pemeriksaan

`dV84wpqRUs`

Sumber Daya Tambahan

Kuota Amazon RDS

Grup Parameter RDS DB

Deskripsi

Memeriksa penggunaan yang lebih dari 80% dari kuota kelompok parameter RDS DB.

ID pemeriksaan

`jEECYg2YVU`

Sumber Daya Tambahan

Kuota Amazon RDS

Grup Keamanan RDS DB

Deskripsi

Memeriksa penggunaan yang lebih dari 80% dari kuota grup keamanan RDS DB.

ID pemeriksaan

`gfZAn3W7wl`

Sumber Daya Tambahan

Kuota Amazon RDS

Langganan Acara RDS

Deskripsi

Cek penggunaan yang lebih dari 80% dari kuota langganan acara RDS.

ID pemeriksaan

`keAhfbH5yb`

Sumber Daya Tambahan

Kuota Amazon RDS

RDS Max Auths untuk Grup Keamanan

Deskripsi

Memeriksa penggunaan yang lebih dari 80% dari RDS max auths per kuota grup keamanan.

ID pemeriksaan

`dBkuNCvqn5`

Sumber Daya Tambahan

Kuota Amazon RDS

Grup Opsi RDS

Deskripsi

Memeriksa penggunaan yang lebih dari 80% dari kuota grup opsi RDS.

ID pemeriksaan

`3Njm0DJQO9`

Sumber Daya Tambahan

Kuota Amazon RDS

RDS Baca Replika untuk Master

Deskripsi

Memeriksa penggunaan yang lebih dari 80% dari replika baca RDS per kuota master.

ID pemeriksaan

`pYW8UkYz2w`

Sumber Daya Tambahan

Kuota Amazon RDS

Instans Cadangan RDS

Deskripsi

Memeriksa penggunaan yang lebih dari 80% dari kuota Instans Cadangan RDS.

ID pemeriksaan

`UUDv0a5r34`

Sumber Daya Tambahan

Kuota Amazon RDS

Grup Subnet RDS

Deskripsi

Memeriksa penggunaan yang lebih dari 80% dari kuota grup subnet RDS.

ID pemeriksaan

`dYWBaXaaMM`

Sumber Daya Tambahan

Kuota Amazon RDS

Subnet RDS untuk Grup Subnet

Deskripsi

Memeriksa penggunaan yang lebih dari 80% dari subnet RDS per kuota grup subnet.

ID pemeriksaan

`jEhCtdJKOY`

Sumber Daya Tambahan

Kuota Amazon RDS

Kuota Penyimpanan Total RDS

Deskripsi

Cek penggunaan yang lebih dari 80% dari total kuota penyimpanan RDS.

ID pemeriksaan

`P1jhKWEmLa`

Sumber Daya Tambahan

Kuota Amazon RDS

Rute 53 Zona yang Dihosting

Deskripsi

Memeriksa penggunaan yang lebih dari 80% dari kuota zona yang dihosting Route 53 per akun.

ID pemeriksaan

`dx3xfcdfMr`

Sumber Daya Tambahan

Rute 53 kuota

Pemeriksaan Kesehatan Route 53 Max

Deskripsi

Cek penggunaan yang lebih dari 80% dari kuota cek kesehatan Route 53 per akun.

ID pemeriksaan

`ru4xfcdfMr`

Sumber Daya Tambahan

Rute 53 kuota

Rute 53 Set Delegasi yang Dapat Digunakan Kembali

Deskripsi

Memeriksa penggunaan yang lebih dari 80% dari delegasi Route 53 yang dapat digunakan kembali menetapkan kuota per akun.

ID pemeriksaan

`ty3xfcdfMr`

Sumber Daya Tambahan

Rute 53 kuota

Kebijakan Lalu Lintas Route 53

Deskripsi

Memeriksa penggunaan yang lebih dari 80% dari kuota kebijakan lalu lintas Route 53 per akun.

ID pemeriksaan

`dx3xfbjfMr`

Sumber Daya Tambahan

Rute 53 kuota

Contoh Kebijakan Lalu Lintas Route 53

Deskripsi

Memeriksa penggunaan yang lebih dari 80% dari kuota instans kebijakan lalu lintas Route 53 per akun.

ID pemeriksaan

`dx8afcdfMr`

Sumber Daya Tambahan

Rute 53 kuota

Kuota Pengiriman Harian SES

Deskripsi

Memeriksa penggunaan yang lebih dari 80% dari kuota pengiriman harian Amazon SES.

ID pemeriksaan

`hJ7NN0l7J9`

Sumber Daya Tambahan

Kuota Amazon SES

VPC

Deskripsi

Cek pemakaian yang lebih dari 80% dari kuota VPC.

ID pemeriksaan

`jL7PP0l7J9`

Sumber Daya Tambahan

Kuota VPC

Gateway Internet VPC

Deskripsi

Memeriksa penggunaan yang lebih dari 80% dari kuota gateway Internet VPC.

ID pemeriksaan

`kM7QQ0l7J9`

Sumber Daya Tambahan

Kuota VPC

Keunggulan Operasional

Anda dapat menggunakan cek berikut untuk kategori keunggulan operasional.

Periksa nama

- Amazon API Gateway Tidak Mencatat Log Eksekusi
- API REST Amazon API Gateway Tanpa Penelusuran Sinar-X Diaktifkan
- Log CloudFront Akses Amazon Dikonfigurasi
- Tindakan CloudWatch Alarm Amazon Dinonaktifkan
- Instans Amazon EC2 Tidak Dikelola oleh AWS Systems Manager
- Repositori Amazon ECR Dengan Kekekalan Tag Dinonaktifkan
- Cluster Amazon ECS dengan Wawasan Kontainer dinonaktifkan

- Pencatatan tugas Amazon ECS tidak diaktifkan
- Pencatatan OpenSearch Layanan Amazon CloudWatch tidak dikonfigurasi
- Instans Amazon RDS DB di cluster dengan grup parameter heterogen
- Amazon RDS Enhanced Monitoring dimatikan
- Amazon RDS Performance Insights dimatikan
- Parameter track_counts Amazon RDS dimatikan
- Pencatatan audit klaster Amazon Redshift
- Amazon S3 tidak mengaktifkan Pemberitahuan Acara
- Topik Amazon SNS Tidak Mencatat Status Pengiriman Pesan
- Amazon VPC Tanpa Log Aliran
- Aplikasi Load Balancer dan Classic Load Balancer Tanpa Akses Log Diaktifkan
- AWS CloudFormation Pemberitahuan Stack
- AWS CloudTrail pencatatan peristiwa data untuk objek dalam bucket S3
- AWS CodeBuild Pencatatan Proyek
- AWS CodeDeploy Rollback Otomatis dan Monitor Diaktifkan
- AWS CodeDeploy Lambda menggunakan konfigurasi penerapan all-at-once
- AWS Elastic Beanstalk Pelaporan Kesehatan yang Ditingkatkan Tidak Dikonfigurasi
- AWS Elastic Beanstalk dengan Pembaruan Platform Terkelola Dinonaktifkan
- AWS Fargate versi platform tidak terbaru
- AWS Systems Manager Asosiasi Manajer Negara dalam Status Tidak Patuh
- CloudTrail jejak tidak dikonfigurasi dengan Amazon Logs CloudWatch
- Perlindungan Penghapusan Elastic Load Balancing Tidak Diaktifkan untuk Load Balancer
- Pemeriksaan Perlindungan Penghapusan Cluster RDS DB
- Pemeriksaan Peningkatan Versi Kecil Otomatis Instans RDS DB

Amazon API Gateway Tidak Mencatat Log Eksekusi

Deskripsi

Memeriksa apakah Amazon API Gateway mengaktifkan CloudWatch Log pada tingkat logging yang diinginkan.

Aktifkan CloudWatch logging untuk metode REST WebSocket API atau rute API di Amazon API Gateway untuk mengumpulkan log eksekusi di CloudWatch Log untuk permintaan yang diterima oleh API Anda. Informasi yang terkandung dalam log eksekusi membantu mengidentifikasi dan memecahkan masalah yang terkait dengan API Anda.

Anda dapat menentukan ID level logging (ERROR, INFO) di parameter LoggingLevel dalam aturan. AWS Config

Lihat dokumentasi REST API atau WebSocket API untuk informasi selengkapnya tentang CloudWatch login di Amazon API Gateway.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

```
c18d2gz125
```

Sumber

```
AWS Config Managed Rule: api-gw-execution-logging-enabled
```

Kriteria Peringatan

Kuning: Pengaturan CloudWatch logging untuk pengumpulan log eksekusi tidak diaktifkan pada tingkat logging yang diinginkan untuk Amazon API Gateway.

Tindakan yang Direkomendasikan

Aktifkan CloudWatch logging untuk log eksekusi untuk API REST Amazon API Gateway atau WebSocket API dengan tingkat logging yang sesuai (ERROR, INFO).

Untuk informasi selengkapnya, lihat Membuat log alur

Sumber Daya Tambahan

- Menyiapkan CloudWatch logging untuk REST API di API Gateway
- Mengonfigurasi logging untuk API WebSocket

Kolom laporan

- Status
- Wilayah
- Sumber Daya
- AWS Config Aturan
- Parameter Input
- Waktu Terakhir Diperbarui

API REST Amazon API Gateway Tanpa Penelusuran Sinar-X Diaktifkan

Deskripsi

Memeriksa apakah API REST Amazon API Gateway telah diaktifkan AWS X-Ray penelusuran.

Aktifkan penelusuran X-Ray untuk REST API Anda agar API Gateway dapat mengambil sampel permintaan pemanggilan API dengan informasi pelacakan. Hal ini memungkinkan Anda memanfaatkan AWS X-Ray untuk melacak dan menganalisis permintaan saat mereka melakukan perjalanan melalui API API Gateway REST API Anda ke layanan hilir.

Untuk informasi selengkapnya, lihat Menelusuri permintaan pengguna ke REST API menggunakan X-Ray.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

```
c18d2gz126
```

Sumber

```
AWS Config Managed Rule: api-gw-xray-enabled
```

Kriteria Peringatan

Kuning: Penelusuran X-Ray tidak diaktifkan untuk API REST API Gateway API.

Tindakan yang Direkomendasikan

Aktifkan penelusuran X-Ray untuk API REST API Gateway API Anda.

Untuk informasi selengkapnya, lihat Menyiapkan AWS X-Ray dengan API REST API Gateway.

Sumber Daya Tambahan

- Menelusuri permintaan pengguna ke REST API menggunakan X-Ray
- Apa itu AWS X-Ray?

Kolom laporan

- Status
- Wilayah
- Sumber Daya
- AWS Config Aturan
- Parameter Input
- Waktu Terakhir Diperbarui

Log CloudFront Akses Amazon Dikonfigurasi

Deskripsi

Memeriksa apakah CloudFront distribusi Amazon dikonfigurasi untuk menangkap informasi dari log akses server Amazon S3. Log akses server Amazon S3 berisi informasi terperinci tentang setiap permintaan pengguna yang CloudFront diterima.

Anda dapat menyesuaikan nama bucket Amazon S3 untuk menyimpan log akses server, menggunakan BucketName parameter S3 dalam aturan Anda. AWS Config

Untuk informasi selengkapnya, lihat Mengkonfigurasi dan menggunakan log standar (log akses).

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

```
c18d2gz110
```

Sumber

```
AWS Config Managed Rule: cloudfront-accesslogs-enabled
```

Kriteria Peringatan

Kuning: Pencatatan CloudFront akses Amazon tidak diaktifkan

Tindakan yang Direkomendasikan

Pastikan Anda mengaktifkan pencatatan CloudFront akses untuk menangkap informasi terperinci tentang setiap permintaan pengguna yang CloudFront diterima.

Anda dapat mengaktifkan log standar saat membuat atau memperbarui distribusi.

Untuk informasi selengkapnya, lihat Nilai yang Anda tentukan saat membuat atau memperbarui distribusi.

Sumber Daya Tambahan

- Nilai yang Anda tentukan saat membuat atau memperbarui distribusi
- Mengkonfigurasi dan menggunakan log standar (log akses)

Kolom laporan

- Status
- Wilayah
- Sumber Daya
- AWS Config Aturan
- Parameter Input
- Waktu Terakhir Diperbarui

Tindakan CloudWatch Alarm Amazon Dinonaktifkan

Deskripsi

Memeriksa apakah tindakan CloudWatch alarm Amazon Anda dalam status dinonaktifkan.

Anda dapat menggunakan AWS CLI untuk mengaktifkan atau menonaktifkan fitur tindakan di alarm Anda. Atau, Anda dapat menonaktifkan atau mengaktifkan fitur tindakan secara terprogram menggunakan AWS SDK. Ketika fitur tindakan alarm dimatikan, CloudWatch tidak melakukan tindakan yang ditentukan dalam keadaan apa pun (OK, INSUFFICIENT_DATA, ALARM).

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

```
c18d2gz109
```

Sumber

```
AWS Config Managed Rule: cloudwatch-alarm-action-enabled-check
```

Kriteria Peringatan

Kuning: Tindakan CloudWatch alarm Amazon tidak diaktifkan. Tidak ada tindakan yang dilakukan dalam keadaan alarm apa pun.

Tindakan yang Direkomendasikan

Aktifkan tindakan di CloudWatch alarm Anda kecuali Anda memiliki alasan yang sah untuk menonaktifkannya, seperti untuk tujuan pengujian.

Jika CloudWatch alarm tidak lagi diperlukan, hapus untuk menghindari biaya yang tidak perlu.

Untuk informasi selengkapnya, lihat mengaktifkan tindakan alarm di Referensi AWS CLI Perintah dan func (*) di CloudWatch SDK EnableAlarmActions for Go API Reference. AWS

Kolom laporan

- Status
- Wilayah
- Sumber Daya
- AWS Config Aturan

- Parameter Input
- Waktu Terakhir Diperbarui

Instans Amazon EC2 Tidak Dikelola oleh AWS Systems Manager

Deskripsi

Memeriksa apakah instans Amazon EC2 di akun Anda dikelola oleh. AWS Systems Manager

Systems Manager membantu Anda memahami dan mengontrol status instans Amazon EC2 dan konfigurasi OS saat ini. Dengan Systems Manager, Anda dapat mengumpulkan konfigurasi perangkat lunak dan informasi inventaris tentang armada instans Anda, termasuk perangkat lunak yang diinstal pada mereka. Ini memungkinkan Anda untuk melacak konfigurasi sistem terperinci, tingkat patch OS, konfigurasi aplikasi, dan detail lainnya tentang penerapan Anda.

Untuk informasi selengkapnya, lihat Menyiapkan Systems Manager untuk instans EC2.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

```
c18d2gz145
```

Sumber

```
AWS Config Managed Rule: ec2-instance-managed-by-systems-manager
```

Kriteria Peringatan

Kuning: Instans Amazon EC2 tidak dikelola oleh Systems Manager.

Tindakan yang Direkomendasikan

Konfigurasikan instans Amazon EC2 agar dikelola oleh Systems Manager.

Pemeriksaan ini tidak dapat dikecualikan dari tampilan di Trusted Advisor konsol.

Untuk informasi selengkapnya, lihat Mengapa instans EC2 saya tidak ditampilkan sebagai node terkelola atau menampilkan status “Koneksi hilang” di Systems Manager? .

Sumber Daya Tambahan

Menyiapkan Systems Manager untuk instans EC2

Kolom laporan

- Status
- Wilayah
- Sumber Daya
- AWS Config Aturan
- Parameter Input
- Waktu Terakhir Diperbarui

Repositori Amazon ECR Dengan Kekekalan Tag Dinonaktifkan

Deskripsi

Memeriksa apakah repositori Amazon ECR pribadi mengaktifkan kekekalan tag gambar.

Aktifkan kekekalan tag gambar untuk repositori ECR Amazon pribadi untuk mencegah tag gambar ditimpa. Ini memungkinkan Anda mengandalkan tag deskriptif sebagai mekanisme yang andal untuk melacak dan mengidentifikasi gambar secara unik.Misalnya, jika kekekalan tag gambar diaktifkan, pengguna dapat menggunakan tag gambar dengan andal untuk mengkorelasikan versi gambar yang diterapkan dengan build yang menghasilkan gambar tersebut.

Untuk informasi selengkapnya, lihat Mutabilitas tag gambar.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

```
c18d2gz129
```

Sumber

`AWS Config Managed Rule: ecr-private-tag-immutability-enabled`

Kriteria Peringatan

Kuning: Repositori pribadi Amazon ECR tidak mengaktifkan kekekalan tag.

Tindakan yang Direkomendasikan

Aktifkan kekekalan tag gambar untuk repositori pribadi Amazon ECR Anda.

Untuk informasi selengkapnya, lihat Mutabilitas tag gambar.

Kolom laporan

- Status
- Wilayah
- Sumber Daya
- AWS Config Aturan
- Parameter Input
- Waktu Terakhir Diperbarui

Cluster Amazon ECS dengan Wawasan Kontainer dinonaktifkan

Deskripsi

Memeriksa apakah Amazon CloudWatch Container Insights diaktifkan untuk kluster Amazon ECS Anda.

CloudWatch Container Insights mengumpulkan, mengumpulkan, dan merangkum metrik dan log dari aplikasi dan layanan mikro dalam kontainer Anda. Metrik tersebut mencakup pemanfaatan sumber daya seperti CPU, memori, disk, dan jaringan.

Untuk informasi selengkapnya, lihat Amazon ECS CloudWatch Container Insights.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

```
c18d2gz173
```

Sumber

```
AWS Config Managed Rule: ecs-container-insights-enabled
```

Kriteria Peringatan

Kuning: Cluster Amazon ECS tidak mengaktifkan wawasan kontainer.

Tindakan yang Direkomendasikan

Aktifkan CloudWatch Wawasan Kontainer di kluster Amazon ECS Anda.

Untuk informasi selengkapnya, lihat Menggunakan Wawasan Kontainer.

Sumber Daya Tambahan

Wawasan CloudWatch Kontainer Amazon ECS

Kolom laporan

- Status
- Wilayah
- Sumber Daya
- AWS Config Aturan
- Parameter Input
- Waktu Terakhir Diperbarui

Pencatatan tugas Amazon ECS tidak diaktifkan

Deskripsi

Memeriksa apakah konfigurasi log disetel pada definisi tugas Amazon ECS yang aktif.

Memeriksa konfigurasi log dalam definisi tugas Amazon ECS Anda memastikan bahwa log yang dihasilkan oleh kontainer dikonfigurasi dan disimpan dengan benar. Ini membantu mengidentifikasi dan memecahkan masalah dengan lebih cepat, mengoptimalkan kinerja, dan memenuhi persyaratan kepatuhan.

Secara default, log yang diambil menunjukkan output perintah yang biasanya Anda lihat di terminal interaktif jika Anda menjalankan kontainer secara lokal. Driver awslogs meneruskan log ini dari Docker ke Amazon Logs. CloudWatch

Untuk informasi selengkapnya, lihat Menggunakan driver log awslogs.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

```
c18d2gz175
```

Sumber

```
AWS Config Managed Rule: ecs-task-definition-log-configuration
```

Kriteria Peringatan

Kuning: Definisi tugas Amazon ECS tidak memiliki konfigurasi logging.

Tindakan yang Direkomendasikan

Pertimbangkan untuk menentukan konfigurasi driver log dalam definisi kontainer untuk mengirim informasi CloudWatch log ke Log atau driver logging yang berbeda.

Untuk informasi lebih lanjut, lihat LogConfiguration.

Sumber Daya Tambahan

Pertimbangkan untuk menentukan konfigurasi driver log dalam definisi kontainer untuk mengirim informasi CloudWatch log ke Log atau driver logging yang berbeda.

Untuk informasi selengkapnya, lihat Contoh definisi tugas.

Kolom laporan

- Status
- Wilayah
- Sumber Daya

- AWS Config Aturan
- Parameter Input
- Waktu Terakhir Diperbarui

Pencatatan OpenSearch Layanan Amazon CloudWatch tidak dikonfigurasi

Deskripsi

Memeriksa apakah domain OpenSearch Layanan Amazon dikonfigurasi untuk mengirim log ke CloudWatch Log Amazon.

Log pemantauan sangat penting untuk menjaga keandalan, ketersediaan, dan kinerja OpenSearch Layanan.

Cari log lambat, pengindeksan log lambat, dan log kesalahan berguna untuk memecahkan masalah kinerja dan stabilitas beban kerja Anda. Log ini perlu diaktifkan untuk menangkap data.

Anda dapat menentukan jenis log mana yang ingin Anda filter (kesalahan, pencarian, indeks) menggunakan parameter LogTypes dalam AWS Config aturan Anda.

Untuk informasi selengkapnya, lihat Memantau domain OpenSearch Layanan Amazon.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

```
c18d2gz184
```

Sumber

```
AWS Config Managed Rule: opensearch-logs-to-cloudwatch
```

Kriteria Peringatan

Kuning: OpenSearch Layanan Amazon tidak memiliki konfigurasi logging dengan Amazon CloudWatch Logs

Tindakan yang Direkomendasikan

Konfigurasikan domain OpenSearch Layanan untuk mempublikasikan log ke CloudWatch Log.

Untuk informasi selengkapnya, lihat Mengaktifkan penerbitan log (konsol).

Sumber Daya Tambahan

- Memantau metrik kluster OpenSearch Layanan dengan Amazon CloudWatch

Kolom laporan

- Status
- Wilayah
- Sumber Daya
- AWS Config Aturan
- Parameter Input
- Waktu Terakhir Diperbarui

Instans Amazon RDS DB di cluster dengan grup parameter heterogen

Deskripsi

Kami merekomendasikan bahwa semua instance DB di cluster DB menggunakan grup parameter DB yang sama.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

> **Note**
>
> Ketika instans DB atau cluster DB dihentikan, Anda dapat melihat rekomendasi Amazon RDS Trusted Advisor selama 3 hingga 5 hari. Setelah lima hari, rekomendasi tidak tersedia di Trusted Advisor. Untuk melihat rekomendasi, buka konsol Amazon RDS, lalu pilih Rekomendasi.

Jika Anda menghapus instans DB atau kluster DB, maka rekomendasi yang terkait dengan instans atau cluster tersebut tidak tersedia di Trusted Advisor atau konsol manajemen Amazon RDS.

ID pemeriksaan

`c1qf5bt010`

Kriteria Peringatan

Kuning: Cluster DB memiliki instance DB dengan kelompok parameter heterogen.

Tindakan yang Direkomendasikan

Kaitkan instans DB dengan grup parameter DB yang terkait dengan instance penulis di cluster DB Anda.

Sumber Daya Tambahan

Ketika instans DB di cluster DB Anda menggunakan grup parameter DB yang berbeda, mungkin ada perilaku yang tidak konsisten selama masalah failover atau kompatibilitas antara instans DB di cluster DB Anda.

Untuk informasi selengkapnya, lihat Bekerja dengan grup parameter.

Kolom laporan

- Status
- Wilayah
- Sumber Daya
- Nilai yang Direkomendasikan
- Nama Mesin
- Waktu Terakhir Diperbarui

Amazon RDS Enhanced Monitoring dimatikan

Deskripsi

Sumber daya database Anda tidak mengaktifkan Enhanced Monitoring. Pemantauan yang Ditingkatkan menyediakan metrik sistem operasi waktu nyata untuk pemantauan dan pemecahan masalah.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

> **Note**
>
> Ketika instans DB atau cluster DB dihentikan, Anda dapat melihat rekomendasi Amazon RDS Trusted Advisor selama 3 hingga 5 hari. Setelah lima hari, rekomendasi tidak tersedia di Trusted Advisor. Untuk melihat rekomendasi, buka konsol Amazon RDS, lalu pilih Rekomendasi.
> Jika Anda menghapus instans DB atau kluster DB, maka rekomendasi yang terkait dengan instans atau cluster tersebut tidak tersedia di Trusted Advisor atau konsol manajemen Amazon RDS.

ID pemeriksaan

`c1qf5bt004`

Kriteria Peringatan

Kuning: Sumber daya Amazon RDS tidak mengaktifkan Enhanced Monitoring.

Tindakan yang Direkomendasikan

Aktifkan Pemantauan yang Ditingkatkan.

Sumber Daya Tambahan

Pemantauan yang Ditingkatkan untuk Amazon RDS memberikan visibilitas tambahan tentang kesehatan instans DB Anda. Kami menyarankan Anda mengaktifkan Enhanced Monitoring. Ketika opsi Enhanced Monitoring diaktifkan untuk instans DB Anda, opsi ini mengumpulkan metrik sistem operasi penting dan informasi proses.

Untuk informasi selengkapnya, lihat Memantau metrik OS dengan Enhanced Monitoring.

Kolom laporan

- Status
- Wilayah

- Sumber Daya
- Nilai yang Direkomendasikan
- Nama Mesin
- Waktu Terakhir Diperbarui

Amazon RDS Performance Insights dimatikan

Deskripsi

Amazon RDS Performance Insights memantau pemuatan instans DB untuk membantu Anda menganalisis dan menyelesaikan masalah performa database. Kami menyarankan Anda mengaktifkan Performance Insights.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

> **Note**
>
> Ketika instans DB atau cluster DB dihentikan, Anda dapat melihat rekomendasi Amazon RDS Trusted Advisor selama 3 hingga 5 hari. Setelah lima hari, rekomendasi tidak tersedia di Trusted Advisor. Untuk melihat rekomendasi, buka konsol Amazon RDS, lalu pilih Rekomendasi.
> Jika Anda menghapus instans DB atau kluster DB, maka rekomendasi yang terkait dengan instans atau cluster tersebut tidak tersedia di Trusted Advisor atau konsol manajemen Amazon RDS.

ID pemeriksaan

`c1qf5bt012`

Kriteria Peringatan

Kuning: Sumber daya Amazon RDS tidak mengaktifkan Performance Insights.

Tindakan yang Direkomendasikan

Mengaktifkan Wawasan Performa.

Sumber Daya Tambahan

Performance Insights menggunakan metode pengumpulan data ringan yang tidak memengaruhi kinerja aplikasi Anda. Performance Insights membantu Anda menilai beban database dengan cepat.

Untuk informasi selengkapnya, lihat Memantau pemuatan DB dengan Performance Insights di Amazon RDS.

Kolom laporan

- Status
- Wilayah
- Sumber Daya
- Nilai yang Direkomendasikan
- Nama Mesin
- Waktu Terakhir Diperbarui

Parameter track_counts Amazon RDS dimatikan

Deskripsi

Ketika parameter track_counts dimatikan, database tidak mengumpulkan statistik aktivitas database. Autovacuum membutuhkan statistik ini untuk berfungsi dengan benar.

Kami menyarankan Anda mengatur parameter track_counts ke 1

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

> **Note**
>
> Ketika instans DB atau cluster DB dihentikan, Anda dapat melihat rekomendasi Amazon RDS Trusted Advisor selama 3 hingga 5 hari. Setelah lima hari, rekomendasi tidak tersedia di Trusted Advisor. Untuk melihat rekomendasi, buka konsol Amazon RDS, lalu pilih Rekomendasi.
> Jika Anda menghapus instans DB atau kluster DB, maka rekomendasi yang terkait dengan instans atau cluster tersebut tidak tersedia di Trusted Advisor atau konsol manajemen Amazon RDS.

ID pemeriksaan

`c1qf5bt027`

Kriteria Peringatan

Kuning: Grup parameter DB memiliki parameter track_counts dimatikan.

Tindakan yang Direkomendasikan

Setel parameter track_counts ke 1

Sumber Daya Tambahan

Ketika parameter track_counts dimatikan, ia menonaktifkan pengumpulan statistik aktivitas database. Daemon autovacuum membutuhkan statistik yang dikumpulkan untuk mengidentifikasi tabel untuk autovacuum dan autoanalysis.

Untuk informasi selengkapnya, lihat Statistik Run-time untuk PostgreSQL di situs dokumentasi PostgreSQL.

Kolom laporan

- Status
- Wilayah
- Sumber Daya
- Nilai Parameter
- Nilai yang Direkomendasikan
- Waktu Terakhir Diperbarui

Pencatatan audit klaster Amazon Redshift

Deskripsi

Memeriksa apakah klaster Amazon Redshift Anda mengaktifkan pencatatan audit database. Amazon Redshift mencatat informasi tentang koneksi dan aktivitas pengguna di database Anda.

Anda dapat menentukan nama bucket Amazon S3 logging yang diinginkan agar sesuai dengan parameter BucketNames aturan Anda. AWS Config

Untuk informasi selengkapnya, lihat Pencatatan audit database.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

```
c18d2gz134
```

Sumber

```
AWS Config Managed Rule: redshift-audit-logging-enabled
```

Kriteria Peringatan

Kuning: Cluster Amazon Redshift menonaktifkan pencatatan audit basis data

Tindakan yang Direkomendasikan

Aktifkan pencatatan dan pemantauan untuk klaster Amazon Redshift Anda.

Untuk informasi selengkapnya, lihat Mengonfigurasi audit menggunakan konsol.

Sumber Daya Tambahan

Pencatatan dan pemantauan di Amazon Redshift

Kolom laporan

- Status
- Wilayah

- Sumber Daya
- AWS Config Aturan
- Parameter Input
- Waktu Terakhir Diperbarui

Amazon S3 tidak mengaktifkan Pemberitahuan Acara

Deskripsi

Memeriksa apakah Pemberitahuan Acara Amazon S3 diaktifkan atau dikonfigurasi dengan benar dengan tujuan atau jenis yang diinginkan.

Fitur Pemberitahuan Acara Amazon S3 mengirimkan pemberitahuan saat peristiwa tertentu terjadi di bucket Amazon S3 Anda. Amazon S3 dapat mengirim pesan notifikasi ke antrian Amazon SQS, topik Amazon SNS, dan fungsi. AWS Lambda

Anda dapat menentukan tujuan dan jenis acara yang Anda inginkan menggunakan parameter destinationArn dan EventTypes dari aturan Anda. AWS Config

Untuk informasi selengkapnya, lihat Pemberitahuan Acara Amazon S3.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

```
c18d2gz163
```

Sumber

```
AWS Config Managed Rule: s3-event-notifications-enabled
```

Kriteria Peringatan

Kuning: Amazon S3 tidak mengaktifkan Pemberitahuan Acara, atau tidak dikonfigurasi dengan desitnasi atau jenis yang diinginkan.

Tindakan yang Direkomendasikan

Konfigurasikan Notfiikasi Acara Amazon S3 untuk peristiwa objek dan bucket.

Untuk informasi selengkapnya, lihat Mengaktifkan dan mengonfigurasi notifikasi peristiwa menggunakan konsol Amazon S3.

Kolom laporan

- Status
- Wilayah
- Sumber Daya
- AWS Config Aturan
- Parameter Input
- Waktu Terakhir Diperbarui

Topik Amazon SNS Tidak Mencatat Status Pengiriman Pesan

Deskripsi

Memeriksa apakah topik Amazon SNS mengaktifkan pencatatan status pengiriman pesan.

Konfigurasikan topik Amazon SNS untuk mencatat status pengiriman pesan guna membantu memberikan wawasan operasional yang lebih baik. Misalnya, pencatatan pengiriman pesan memverifikasi apakah pesan dikirim ke titik akhir Amazon SNS tertentu. Dan, ini juga membantu mengidentifikasi respons yang dikirim dari titik akhir.

Untuk informasi selengkapnya, lihat status pengiriman pesan Amazon SNS.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

`c18d2gz121`

Sumber

`AWS Config Managed Rule: sns-topic-message-delivery-notification-enabled`

Kriteria Peringatan

Kuning: Pencatatan status pengiriman pesan tidak diaktifkan untuk topik Amazon SNS.

Tindakan yang Direkomendasikan

Aktifkan pencatatan status pengiriman pesan untuk topik SNS Anda.

Untuk informasi selengkapnya, lihat Mengonfigurasi pencatatan status pengiriman menggunakan AWS Management Console.

Kolom laporan

- Status
- Wilayah
- Sumber Daya
- AWS Config Aturan
- Parameter Input
- Waktu Terakhir Diperbarui

Amazon VPC Tanpa Log Aliran

Deskripsi

Memeriksa apakah Amazon Virtual Private Cloud Flow Log dibuat untuk VPC.

Anda dapat menentukan jenis lalu lintas menggunakan parameter TrafficType dalam aturan Anda. AWS Config

Untuk informasi selengkapnya, lihat Mencatat lalu lintas IP menggunakan Log Aliran VPC.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

```
c18d2gz122
```

Sumber

```
AWS Config Managed Rule: vpc-flow-logs-enabled
```

Kriteria Peringatan

Kuning: VPC tidak memiliki Amazon VPC Flow Logs.

Tindakan yang Direkomendasikan

Buat Log Aliran VPC untuk setiap VPC Anda.

Untuk informasi selengkapnya, lihat Membuat log alur

Kolom laporan

- Status
- Wilayah
- Sumber Daya
- AWS Config Aturan
- Parameter Input
- Waktu Terakhir Diperbarui

Aplikasi Load Balancer dan Classic Load Balancer Tanpa Akses Log Diaktifkan

Deskripsi

Memeriksa apakah Application Load Balancers dan Classic Load Balancers mengaktifkan akses logging.

Elastic Load Balancing memberikan log akses yang mengambil informasi mendetail tentang permintaan yang dikirim ke penyeimbang beban Anda. Setiap log berisi informasi, seperti waktu permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server. Anda dapat menggunakan log akses ini untuk menganalisis pola lalu lintas dan memecahkan masalah.

Log akses adalah fitur opsional Elastic Load Balancing yang dinonaktifkan secara default. Setelah mengaktifkan log akses untuk penyeimbang beban, Elastic Load Balancing menangkap log dan menyimpannya di bucket Amazon S3 yang Anda tentukan.

Anda dapat menentukan log akses Amazon S3 bucket yang ingin Anda periksa menggunakan BucketNames parameter s3 dalam aturan Anda. AWS Config

Untuk informasi selengkapnya, lihat Log akses untuk Application Load Balancer atau log Access untuk Classic Load Balancer Anda.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

```
c18d2gz167
```

Sumber

```
AWS Config Managed Rule: elb-logging-enabled
```

Kriteria Peringatan

Kuning: Fitur log akses tidak diaktifkan untuk Application Load Balancer atau Classic Load Balancer.

Tindakan yang Direkomendasikan

Aktifkan log akses untuk Application Load Balancers dan Classic Load Balancer Anda.

Untuk informasi selengkapnya, lihat Mengaktifkan log akses untuk Application Load Balancer atau Aktifkan log akses untuk Classic Load Balancer Anda.

Kolom laporan

- Status
- Wilayah
- Sumber Daya
- AWS Config Aturan
- Parameter Input
- Waktu Terakhir Diperbarui

AWS CloudFormation Pemberitahuan Stack

Deskripsi

Memeriksa apakah semua AWS CloudFormation tumpukan Anda menggunakan Amazon SNS untuk menerima pemberitahuan saat peristiwa terjadi.

Anda dapat mengonfigurasi pemeriksaan ini untuk mencari ARN topik Amazon SNS tertentu menggunakan parameter dalam aturan Anda. AWS Config

Untuk informasi selengkapnya, lihat Mengatur opsi AWS CloudFormation tumpukan.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

`c18d2gz111`

Sumber

`AWS Config Managed Rule: cloudformation-stack-notification-check`

Kriteria Peringatan

Kuning: Pemberitahuan acara Amazon SNS untuk AWS CloudFormation tumpukan Anda tidak diaktifkan.

Tindakan yang Direkomendasikan

Pastikan AWS CloudFormation tumpukan Anda menggunakan Amazon SNS untuk menerima notifikasi saat peristiwa terjadi.

Memantau peristiwa tumpukan membantu Anda merespons dengan cepat tindakan tidak sah yang dapat mengubah lingkungan Anda AWS .

Sumber Daya Tambahan

Bagaimana saya bisa menerima peringatan email ketika AWS CloudFormation stack saya memasuki status ROLLBACK_IN_PROGRESS?

Kolom laporan

- Status
- Wilayah
- Sumber Daya
- AWS Config Aturan
- Parameter Input
- Waktu Terakhir Diperbarui

AWS CloudTrail pencatatan peristiwa data untuk objek dalam bucket S3

Deskripsi

Memeriksa apakah setidaknya satu AWS CloudTrail jejak mencatat peristiwa data Amazon S3 untuk semua bucket Amazon S3 Anda.

Untuk informasi selengkapnya, lihat Mencatat panggilan API Amazon S3 menggunakan. AWS CloudTrail

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

```
c18d2gz166
```

Sumber

```
AWS Config Managed Rule: cloudtrail-s3-dataevents-enabled
```

Kriteria Peringatan

Kuning: pencatatan AWS CloudTrail peristiwa untuk bucket Amazon S3 tidak dikonfigurasi

Tindakan yang Direkomendasikan

Aktifkan pencatatan CloudTrail peristiwa untuk bucket dan objek Amazon S3 untuk melacak permintaan akses bucket target.

Untuk informasi selengkapnya, lihat Mengaktifkan pencatatan CloudTrail peristiwa untuk bucket dan objek S3.

Kolom laporan

- Status
- Wilayah
- Sumber Daya
- AWS Config Aturan
- Parameter Input
- Waktu Terakhir Diperbarui

AWS CodeBuild Pencatatan Proyek

Deskripsi

Memeriksa apakah lingkungan AWS CodeBuild proyek menggunakan logging. Opsi logging dapat berupa log di Amazon CloudWatch Log, atau dibangun di bucket Amazon S3 tertentu, atau keduanya. Mengaktifkan logging dalam CodeBuild proyek dapat memberikan beberapa manfaat seperti debugging dan audit.

Anda dapat menentukan nama bucket Amazon S3 atau grup CloudWatch Log untuk menyimpan log, menggunakan parameter s3 BucketNames atau Cloud WatchGroup Names dalam aturan Anda. AWS Config

Untuk informasi lebih lanjut, lihat Monitoring AWS CodeBuild.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

```
c18d2gz113
```

Sumber

```
AWS Config Managed Rule: codebuild-project-logging-enabled
```

Kriteria Peringatan

Kuning: pencatatan AWS CodeBuild proyek tidak diaktifkan.

Tindakan yang Direkomendasikan

Pastikan pencatatan diaktifkan di AWS CodeBuild proyek Anda. Pemeriksaan ini tidak dapat dikecualikan dari tampilan di AWS Trusted Advisor konsol.

Untuk informasi selengkapnya, lihat Logging dan monitoring in AWS CodeBuild.

Kolom laporan

- Status
- Wilayah
- Sumber Daya
- AWS Config Aturan
- Parameter Input
- Waktu Terakhir Diperbarui

AWS CodeDeploy Rollback Otomatis dan Monitor Diaktifkan

Deskripsi

Memeriksa apakah grup penyebaran dikonfigurasi dengan rollback penerapan otomatis dan pemantauan penerapan dengan alarm terpasang. Jika ada yang tidak beres selama penerapan, itu secara otomatis diputar kembali, dan aplikasi Anda tetap dalam keadaan stabil

Untuk informasi selengkapnya, lihat Menerapkan ulang dan memutar kembali penerapan dengan. CodeDeploy

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

`c18d2gz114`

Sumber

```
AWS Config Managed Rule: codedeploy-auto-rollback-monitor-enabled
```

Kriteria Peringatan

Kuning: rollback penerapan AWS CodeDeploy otomatis dan pemantauan penerapan tidak diaktifkan.

Tindakan yang Direkomendasikan

Konfigurasikan grup penerapan atau penerapan untuk memutar kembali secara otomatis saat penerapan gagal atau saat ambang batas pemantauan yang Anda tentukan terpenuhi.

Konfigurasikan alarm untuk memantau berbagai metrik, seperti penggunaan CPU, penggunaan memori, atau lalu lintas jaringan, selama proses penyebaran. Jika salah satu metrik ini melebihi ambang batas tertentu, alarm akan memicu, dan penerapan dihentikan atau diputar kembali.

Untuk informasi tentang mengatur rollback otomatis dan mengonfigurasi alarm untuk grup penerapan Anda, lihat Mengonfigurasi opsi lanjutan untuk grup penerapan.

Sumber Daya Tambahan

Apa itu CodeDeploy?

Kolom laporan

- Status
- Wilayah
- Sumber Daya
- AWS Config Aturan
- Parameter Input
- Waktu Terakhir Diperbarui

AWS CodeDeploy Lambda menggunakan konfigurasi penerapan all-at-once

Deskripsi

Memeriksa apakah grup AWS CodeDeploy penerapan untuk platform AWS Lambda komputasi menggunakan konfigurasi all-at-once penerapan.

Untuk mengurangi risiko kegagalan penerapan fungsi CodeDeploy Lambda Anda, sebaiknya gunakan konfigurasi canary atau linear deployment alih-alih opsi default di mana semua lalu lintas digeser dari fungsi Lambda asli ke fungsi yang diperbarui sekaligus.

Untuk informasi selengkapnya, lihat Versi fungsi Lambda dan konfigurasi Deployment.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

`c18d2gz115`

Sumber

`AWS Config Managed Rule: codedeploy-lambda-allatonce-traffic-shift-disabled`

Kriteria Peringatan

Kuning: Penerapan AWS CodeDeploy Lambda menggunakan konfigurasi all-at-once penerapan untuk mengalihkan semua lalu lintas ke fungsi Lambda yang diperbarui sekaligus.

Tindakan yang Direkomendasikan

Gunakan konfigurasi penyebaran Canary atau Linear dari grup CodeDeploy penerapan untuk platform komputasi Lambda.

Sumber Daya Tambahan

Konfigurasi penyebaran

Kolom laporan

- Status
- Wilayah
- Sumber Daya
- AWS Config Aturan
- Parameter Input
- Waktu Terakhir Diperbarui

AWS Elastic Beanstalk Pelaporan Kesehatan yang Ditingkatkan Tidak Dikonfigurasi

Deskripsi

Memeriksa apakah AWS Elastic Beanstalk lingkungan dikonfigurasi untuk pelaporan kesehatan yang ditingkatkan.

Pelaporan kesehatan yang disempurnakan Elastic Beanstalk memberikan metrik kinerja terperinci, seperti penggunaan CPU, penggunaan memori, lalu lintas jaringan, dan informasi kesehatan infrastruktur, seperti jumlah instans dan status penyeimbang beban.

Untuk informasi lebih lanjut, lihat Pelaporan dan pemantauan kesehatan yang ditingkatkan.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

```
c18d2gz108
```

Sumber

```
AWS Config Managed Rule: beanstalk-enhanced-health-reporting-enabled
```

Kriteria Peringatan

Kuning: Lingkungan Elastic Beanstalk tidak dikonfigurasi untuk pelaporan kesehatan yang ditingkatkan

Tindakan yang Direkomendasikan

Pastikan bahwa lingkungan Elastic Beanstalk dikonfigurasi untuk pelaporan kesehatan yang ditingkatkan.

Untuk informasi selengkapnya, lihat Mengaktifkan pelaporan kesehatan yang ditingkatkan menggunakan konsol Elastic Beanstalk.

Sumber Daya Tambahan

- Mengaktifkan Elastic Beanstalk meningkatkan pelaporan kesehatan

- Peningkatan pelaporan dan pemantauan kesehatan

Kolom laporan

- Status
- Wilayah
- Sumber Daya
- AWS Config Aturan
- Parameter Input
- Waktu Terakhir Diperbarui

AWS Elastic Beanstalk dengan Pembaruan Platform Terkelola Dinonaktifkan

Deskripsi

Memeriksa apakah pembaruan platform terkelola di lingkungan Elastic Beanstalk dan templat konfigurasi diaktifkan.

AWS Elastic Beanstalk secara teratur merilis pembaruan platform untuk memberikan perbaikan, pembaruan perangkat lunak, dan fitur baru. Dengan pembaruan platform terkelola, Elastic Beanstalk dapat secara otomatis melakukan pembaruan platform untuk patch baru dan versi platform minor.

Anda dapat menentukan tingkat pembaruan yang Anda inginkan dalam UpdateLevelparameter AWS Config aturan Anda.

Untuk informasi selengkapnya, lihat Memperbarui versi platform lingkungan Elastic Beanstalk Anda.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

```
c18d2gz177
```

Sumber

```
AWS Config Managed Rule: elastic-beanstalk-managed-updates-enabled
```

Kriteria Peringatan

Kuning: pembaruan platform AWS Elastic Beanstalk terkelola tidak dikonfigurasi sama sekali, termasuk pada tingkat minor atau patch.

Tindakan yang Direkomendasikan

Aktifkan pembaruan platform terkelola di lingkungan Elastic Beanstalk Anda, atau konfigurasikan pada tingkat minor atau pembaruan.

Untuk informasi selengkapnya, lihat Pembaruan platform terkelola.

Sumber Daya Tambahan

- Mengaktifkan Elastic Beanstalk meningkatkan pelaporan kesehatan
- Peningkatan pelaporan dan pemantauan kesehatan

Kolom laporan

- Status
- Wilayah
- Sumber Daya
- AWS Config Aturan
- Parameter Input
- Waktu Terakhir Diperbarui

AWS Fargate versi platform tidak terbaru

Deskripsi

Memeriksa apakah Amazon ECS menjalankan versi platform terbaru. AWS Fargate Versi platform Fargate mengacu pada lingkungan runtime tertentu untuk infrastruktur tugas Fargate. Ini adalah kombinasi dari kernel dan versi runtime container. Versi platform baru dirilis saat lingkungan runtime berkembang. Misalnya, jika ada pembaruan kernel atau sistem operasi, fitur baru, perbaikan bug, atau pembaruan keamanan.

Untuk informasi lebih lanjut, lihat Pemeliharaan tugas Fargate.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

`c18d2gz174`

Sumber

`AWS Config Managed Rule: ecs-fargate-latest-platform-version`

Kriteria Peringatan

Kuning: Amazon ECS tidak berjalan pada versi terbaru dari platform Fargate.

Tindakan yang Direkomendasikan

Perbarui ke versi platform Fargate terbaru.

Untuk informasi lebih lanjut, lihat Pemeliharaan tugas Fargate.

Kolom laporan

- Status
- Wilayah
- Sumber Daya
- AWS Config Aturan
- Parameter Input
- Waktu Terakhir Diperbarui

AWS Systems Manager Asosiasi Manajer Negara dalam Status Tidak Patuh

Deskripsi

Memeriksa apakah status kepatuhan AWS Systems Manager asosiasi adalah COMPLIANT atau NON_COMPLIANT setelah eksekusi asosiasi pada instance.

State Manager, kemampuan AWS Systems Manager, adalah layanan manajemen konfigurasi yang aman dan terukur yang mengotomatiskan proses menjaga node terkelola dan AWS sumber

daya lainnya dalam keadaan yang Anda tentukan. Asosiasi Manajer Negara adalah konfigurasi yang Anda tetapkan ke AWS sumber daya Anda. Konfigurasi menentukan status yang ingin Anda pertahankan pada sumber daya Anda, sehingga membantu Anda mencapai target, seperti menghindari drift konfigurasi di seluruh instans Amazon EC2 Anda.

Untuk informasi selengkapnya, lihat Manajer AWS Systems Manager Negara.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

```
c18d2gz147
```

Sumber

```
AWS Config Managed Rule: ec2-managedinstance-association-compliance-status-check
```

Kriteria Peringatan

Kuning: Status kepatuhan AWS Systems Manager asosiasi adalah NON_COMPLIANT.

Tindakan yang Direkomendasikan

Validasi status asosiasi Manajer Negara, dan kemudian mengambil tindakan yang diperlukan untuk mengembalikan status kembali ke COMPLIANT.

Untuk informasi selengkapnya, lihat Tentang Manajer Negara.

Sumber Daya Tambahan

AWS Systems Manager Manajer Negara

Kolom laporan

- Status
- Wilayah
- Sumber Daya
- AWS Config Aturan

- Parameter Input
- Waktu Terakhir Diperbarui

CloudTrail jejak tidak dikonfigurasi dengan Amazon Logs CloudWatch

Deskripsi

Memeriksa apakah AWS CloudTrail jejak dikonfigurasi untuk mengirim log ke CloudWatch Log.

Pantau file CloudTrail CloudWatch Log dengan Log untuk memicu respons otomatis saat peristiwa penting ditangkap AWS CloudTrail.

Untuk informasi selengkapnya, lihat Memantau File CloudTrail Log dengan CloudWatch Log.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

```
c18d2gz164
```

Sumber

```
AWS Config Managed Rule: cloud-trail-cloud-watch-logs-enabled
```

Kriteria Peringatan

Kuning: AWS CloudTrail tidak diatur dengan integrasi CloudWatch Log.

Tindakan yang Direkomendasikan

Konfigurasikan CloudTrail jejak untuk mengirim peristiwa log ke CloudWatch Log.

Untuk informasi selengkapnya, lihat Membuat CloudWatch alarm untuk CloudTrail acara: contoh.

Kolom laporan

- Status
- Wilayah
- Sumber Daya

- AWS Config Aturan
- Parameter Input
- Waktu Terakhir Diperbarui

Perlindungan Penghapusan Elastic Load Balancing Tidak Diaktifkan untuk Load Balancer

Deskripsi

Memeriksa apakah perlindungan penghapusan diaktifkan untuk penyeimbang beban Anda.

Elastic Load Balancing mendukung perlindungan penghapusan untuk Application Load Balancers, Network Load Balancers, dan Gateway Load Balancer Anda. Aktifkan perlindungan penghapusan untuk mencegah penyeimbang beban Anda dari penghapusan yang tidak disengaja. Perlindungan penghapusan dimatikan secara default saat Anda membuat penyeimbang beban. Jika penyeimbang beban Anda adalah bagian dari lingkungan produksi, maka pertimbangkan untuk mengaktifkan perlindungan penghapusan.

Log akses adalah fitur opsional Elastic Load Balancing yang dinonaktifkan secara default. Setelah mengaktifkan log akses untuk penyeimbang beban, Elastic Load Balancing menangkap log dan menyimpannya di bucket Amazon S3 yang Anda tentukan.

Untuk informasi selengkapnya, lihat Perlindungan Penghapusan Application Load Balancer, Perlindungan PenghapusanNetwork Load Balancers, atau Perlindungan Penghapusan Gateway Load Balancer.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

```
c18d2gz168
```

Sumber

```
AWS Config Managed Rule: elb-deletion-protection-enabled
```

Kriteria Peringatan

Kuning: Perlindungan penghapusan tidak diaktifkan untuk penyeimbang beban.

Tindakan yang Direkomendasikan

Aktifkan perlindungan penghapusan untuk Application Load Balancers, Network Load Balancers, dan Gateway Load Balancers.

Untuk informasi selengkapnya, lihat Perlindungan Penghapusan Application Load Balancer, Perlindungan PenghapusanNetwork Load Balancers, atau Perlindungan Penghapusan Gateway Load Balancer.

Kolom laporan

- Status
- Wilayah
- Sumber Daya
- AWS Config Aturan
- Parameter Input
- Waktu Terakhir Diperbarui

Pemeriksaan Perlindungan Penghapusan Cluster RDS DB

Deskripsi

Memeriksa apakah klaster Amazon RDS DB Anda mengaktifkan perlindungan penghapusan.

Ketika cluster dikonfigurasi dengan perlindungan penghapusan, database tidak dapat dihapus oleh pengguna mana pun.

Perlindungan penghapusan tersedia untuk Amazon Aurora dan RDS untuk MySQL, RDS untuk MariaDB, RDS untuk Oracle, RDS untuk PostgreSQL, dan RDS untuk instans database SQL Server di semua Wilayah. AWS

Untuk informasi selengkapnya, lihat Perlindungan penghapusan untuk klaster Aurora.

ID pemeriksaan

`c18d2gz160`

Sumber

`AWS Config Managed Rule: rds-cluster-deletion-protection-enabled`

Kriteria Peringatan

Kuning: Anda memiliki kluster Amazon RDS DB yang tidak mengaktifkan perlindungan penghapusan.

Tindakan yang Direkomendasikan

Aktifkan perlindungan penghapusan saat Anda membuat klaster Amazon RDS DB.

Anda hanya dapat menghapus klaster yang tidak mengaktifkan perlindungan penghapusan. Mengaktifkan perlindungan penghapusan menambahkan lapisan perlindungan tambahan dan menghindari kehilangan data dari penghapusan instance database yang tidak disengaja atau tidak disengaja. Perlindungan penghapusan juga membantu memenuhi persyaratan kepatuhan peraturan dan memastikan kelangsungan bisnis.

Untuk informasi selengkapnya, lihat Perlindungan penghapusan untuk klaster Aurora.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

Sumber Daya Tambahan

Perlindungan penghapusan untuk cluster Aurora

Kolom laporan

- Status
- Wilayah
- Sumber Daya
- AWS Config Aturan
- Parameter Input
- Waktu Terakhir Diperbarui

Pemeriksaan Peningkatan Versi Kecil Otomatis Instans RDS DB

Deskripsi

Memeriksa apakah instans Amazon RDS DB memiliki peningkatan versi minor otomatis yang dikonfigurasi.

Aktifkan upgrade versi minor otomatis untuk instans Amazon RDS untuk memastikan bahwa database selalu menjalankan versi aman dan stabil terbaru. Peningkatan kecil menyediakan pembaruan keamanan, perbaikan bug, peningkatan kinerja, dan menjaga kompatibilitas dengan aplikasi yang ada.

Untuk informasi selengkapnya, lihat Memutakhirkan versi mesin instans DB.

> **Note**
>
> Hasil untuk pemeriksaan ini secara otomatis disegarkan beberapa kali setiap hari, dan permintaan penyegaran tidak diizinkan. Mungkin perlu beberapa jam untuk perubahan muncul. Saat ini, Anda tidak dapat mengecualikan sumber daya dari pemeriksaan ini.

ID pemeriksaan

```
c18d2gz155
```

Sumber

```
AWS Config Managed Rule: rds-automatic-minor-version-upgrade-enabled
```

Kriteria Peringatan

Kuning: Instans RDS DB tidak mengaktifkan upgrade versi minor otomatis.

Tindakan yang Direkomendasikan

Aktifkan upgrade versi minor otomatis saat Anda membuat instans Amazon RDS DB.

Ketika Anda mengaktifkan upgrade versi minor, versi database otomatis upgrade jika menjalankan versi minor dari mesin DB yang lebih rendah dari manual upgrade versi mesin.

Kolom laporan

- Status

- Wilayah
- Sumber Daya
- AWS Config Aturan
- Parameter Input
- Waktu Terakhir Diperbarui

Ubah log untuk AWS Trusted Advisor

Lihat topik berikut untuk perubahan terbaru pada Trusted Advisor pemeriksaan.

> **Note**
>
> Jika Anda menggunakan Trusted Advisor konsol atau AWS Support API, pemeriksaan yang dihapus tidak akan muncul di hasil pemeriksaan. Jika Anda menggunakan salah satu pemeriksaan yang dihapus seperti menentukan ID cek dalam operasi AWS Support API atau kode Anda, Anda harus menghapus pemeriksaan ini untuk menghindari kesalahan panggilan API.

Untuk informasi selengkapnya tentang pemeriksaan yang tersedia, lihatAWS Trusted Advisor periksa referensi.

Menghapus 5 cek dan menambahkan 1 cek

Trusted Advisor 3 pemeriksaan Toleransi Kesalahan yang tidak digunakan lagi, 1 pemeriksaan Kinerja, dan 1 pemeriksaan Keamanan pada 15 Mei 2024:

- Penggunaan IAM
- Penyeimbangan Beban Lintas Zona ELB
- Volume Magnetik Amazon EBS yang Digunakan Secara Terlalu Banyak
- Sejumlah Besar Aturan Grup Keamanan EC2 Diterapkan pada Instance
- Sejumlah Besar Aturan dalam Grup Keamanan EC2

Trusted Advisor menambahkan 1 pemeriksaan keamanan baru pada 15 Mei 2024:

- Log Akses Server Amazon S3 Diaktifkan

Untuk informasi selengkapnya, lihat AWS Trusted Advisor periksa referensi.

Dihapus pemeriksaan toleransi kesalahan

Trusted Advisor pemeriksaan 3 Toleransi Kesalahan yang tidak digunakan lagi pada 25 April 2024:

- AWS Direct Connect Redundansi Koneksi
- AWS Direct Connect Redundansi Lokasi
- AWS Direct Connect Redundansi Antarmuka Virtual

Untuk informasi selengkapnya, lihat AWS Trusted Advisor periksa referensi.

Pemeriksaan toleransi kesalahan baru

Trusted Advisor menambahkan 1 pemeriksaan Toleransi Kesalahan pada 29 Februari 2024:

- NLB - Sumber daya yang menghadap Internet di subnet pribadi

Untuk informasi selengkapnya, lihat AWS Trusted Advisor periksa referensi.

Toleransi kesalahan dan pemeriksaan keamanan yang diperbarui

Trusted Advisor menambahkan 1 pemeriksaan Toleransi Kesalahan baru dan mengubah 1 toleransi Kesalahan yang ada dan 1 pemeriksaan Keamanan pada 28 Maret 2024:

- Pemeriksaan Komponen AWS Resilience Hub Aplikasi Ditambahkan
- Fungsi AWS Lambda berkemampuan VPC yang diperbarui tanpa Redundansi Multi-AZ
- AWS Lambda Fungsi yang Diperbarui Menggunakan Runtime yang Tidak Digunakan Lagi

Untuk informasi selengkapnya, lihat AWS Trusted Advisor periksa referensi.

Pemeriksaan toleransi kesalahan baru

Trusted Advisor menambahkan 1 pemeriksaan Toleransi Kesalahan pada 31 Januari 2024:

- AWS Direct Connect Ketahanan Lokasi

Untuk informasi selengkapnya, lihat AWS Trusted Advisor periksa referensi.

Pemeriksaan toleransi kesalahan yang diperbarui

Trusted Advisor mengubah 1 pemeriksaan Toleransi Kesalahan pada 08 Januari 2024:

- Amazon RDS innodb_flush_log_at_trx_commit parameter bukan 1

Untuk informasi selengkapnya, lihat AWS Trusted Advisor periksa referensi.

Pemeriksaan keamanan yang diperbarui

Trusted Advisor diubah 1 Pemeriksaan keamanan pada 21 Desember 2023:

- AWS Lambda Fungsi Menggunakan Runtime yang Tidak Digunakan Lagi

Untuk informasi selengkapnya, lihat AWS Trusted Advisor periksa referensi.

Pemeriksaan keamanan dan kinerja baru

Trusted Advisor menambahkan 2 pemeriksaan Keamanan baru dan 2 pemeriksaan Kinerja baru pada 20 Desember 2023:

- Klien Amazon EFS tidak menggunakan data-in-transit enkripsi
- Cluster Amazon Aurora DB kurang disediakan untuk beban kerja baca
- Instans Amazon RDS kurang disediakan untuk kapasitas sistem
- Instans Amazon EC2 dengan dukungan standar Ubuntu LTS akhir

Untuk informasi selengkapnya, lihat AWS Trusted Advisor periksa referensi.

Pemeriksaan keamanan baru

Trusted Advisor menambahkan 1 pemeriksaan Keamanan baru pada 15 Desember 2023:

- Amazon Route 53 tidak cocok dengan catatan CNAME menunjuk langsung ke ember S3

Untuk informasi selengkapnya, lihat AWS Trusted Advisor periksa referensi.

Toleransi kesalahan baru dan pemeriksaan optimasi biaya

Trusted Advisor menambahkan 2 pemeriksaan Toleransi Kesalahan baru dan 1 pemeriksaan Pengoptimalan Biaya baru pada 07 Desember 2023:

- Cluster AZ Tunggal Amazon DocumentDB
- Konfigurasi Batalkan Unggahan Multipart Amazon S3 Tidak Lengkap
- Driver Amazon ECS AWS Logs dalam mode pemblokiran

Untuk informasi selengkapnya, lihat AWS Trusted Advisor periksa referensi.

Pemeriksaan toleransi kesalahan baru

Trusted Advisor menambahkan 3 pemeriksaan toleransi kesalahan baru pada 17 November 2023:

- ALB Multi-AZ
- NLB Multi-AZ
- Antarmuka jaringan titik akhir antarmuka VPC di beberapa AZ

Untuk informasi selengkapnya, lihat AWS Trusted Advisor periksa referensi.

Cek baru untuk Amazon RDS

Trusted Advisor menambahkan 37 cek baru untuk Amazon RDS pada 15 November 2023.

Untuk informasi selengkapnya, lihat AWS Trusted Advisor periksa referensi.

AWS Trusted Advisor API baru

AWS Trusted Advisor memperkenalkan API baru untuk memungkinkan Anda mengakses pemeriksaan praktik terbaik Trusted Advisor secara terprogram, rekomendasi, dan rekomendasi yang diprioritaskan. Trusted Advisor API memungkinkan Anda untuk berintegrasi secara terprogram Trusted Advisor dengan alat operasional pilihan Anda untuk mengotomatiskan dan mengoptimalkan beban kerja Anda dalam skala besar. Tersedia untuk pelanggan Business, Enterprise On-Ramp, atau Enterprise Support, API baru menyediakan akses ke Trusted Advisor rekomendasi untuk akun Anda atau semua akun tertaut dalam akun pembayar. Pelanggan Enterprise Support dengan akses ke manajemen atau akun administrator yang didelegasikan juga dapat secara terprogram mengambil rekomendasi yang diprioritaskan di seluruh organisasi mereka.

Trusted Advisor API baru akan menggantikan 3 fungsi yang sebelumnya ditawarkan melalui AWS Support API (SAPI). SAPI akan terus menawarkan kasus dan informasi dukungan lainnya.

Trusted Advisor API umumnya tersedia di wilayah AS Timur (Ohio), AS Timur (Virginia N.), AS Barat (Oregon), Asia Pasifik (Seoul), Asia Pasifik (Sydney), dan Eropa (Irlandia).

Untuk mempelajari lebih lanjut, silakan kunjungi halaman AWS Trusted Advisor API.

Trusted Advisor periksa penghapusan

Trusted Advisor menghapus pemeriksaan berikut pada 9 November 2023.

Nama pemeriksaan	Kategori pemeriksaan	ID pemeriksaan
Volume EBS harus dilampirkan ke instans EC2	Keamanan	`Hs4Ma3G119`
Bucket S3 harus mengaktifkan enkripsi sisi server	Keamanan	`Hs4Ma3G167`
CloudFront distribusi harus mengaktifkan identitas akses asal	Keamanan	`Hs4Ma3G195`

Integrasi AWS Config cek ke Trusted Advisor

Trusted Advisor menambahkan 64 cek baru yang didukung AWS Config pada 30 Oktober 2023.

Untuk informasi selengkapnya, lihat Lihat AWS Trusted Advisor cek yang didukung oleh AWS Config.

Pemeriksaan toleransi kesalahan baru

Trusted Advisor menambahkan cek berikut pada 12 Oktober 2023.

- Amazon RDS ReplicaLag
- Amazon RDS FreeStorageSpace
- Amazon RDS DiskQueueDepth
- Amazon Route 53 Resolver Redundansi Zona Ketersediaan Titik Akhir

- Auto Scaling IP yang tersedia di Subnet
- Broker MSK Amazon menghosting terlalu banyak partisi

Untuk informasi lebih lanjut, lihat Toleransi kesalahan kategorinya.

Pemeriksaan batas layanan baru

Trusted Advisor menambahkan cek berikut pada 17 Agustus 2023.

- Penggunaan Penyimpanan Kode Lambda

Untuk informasi lebih lanjut, lihat Batas layanan kategorinya.

Pemeriksaan toleransi kesalahan baru

Trusted Advisor menambahkan cek berikut pada 3 Agustus 2023.

- AWS Lambda Tentang Destinasi Acara Kegagalan

Untuk informasi lebih lanjut, lihat Toleransi kesalahan kategorinya.

Toleransi kesalahan baru dan pemeriksaan kinerja

Trusted Advisor menambahkan cek berikut pada 1 Juni 2023.

- Amazon EFS Tidak Ada Redundansi Target Mount
- Optimasi Mode Throughput Amazon EFS
- Redundansi Zona Ketersediaan ActiveMQ
- Redundansi Zona Ketersediaan RabbitMQ

Untuk informasi lebih lanjut, lihat Toleransi kesalahan kategori dan Kinerja kategori.

Pemeriksaan toleransi kesalahan baru

Trusted Advisor menambahkan pemeriksaan berikut pada 16 Mei 2023.

- NAT Gateway AZ Kemerdekaan
- Pemeriksaan Aplikasi AZ Tunggal

Untuk informasi lebih lanjut, lihat Toleransi kesalahan kategorinya.

Pemeriksaan toleransi kesalahan baru

Trusted Advisor menambahkan pemeriksaan berikut pada 27 April 2023.

- Jumlah Wilayah AWS dalam set replikasi Manajer Insiden
- AWS Resilience Hub usia penilaian

Untuk informasi lebih lanjut, lihat Toleransi kesalahan kategorinya.

Perluasan Wilayah Pemeriksaan Toleransi Kesalahan Amazon ECS

Trusted Advisor memperluas pemeriksaan berikut ke wilayah tambahan pada 27 April 2023. Trusted Advisor cek untuk Amazon ECS sekarang tersedia di semua wilayah di mana Amazon ECS umumnya tersedia.

- Layanan Amazon ECS menggunakan satu AZ
- Strategi penempatan Multi-AZ Amazon ECS

Wilayah yang diperluas menjadi meliputi Afrika (Cape Town), Asia Pasifik (Hong Kong), Asia Pasifik (Hyderabad), Asia Pasifik (Jakarta), Asia Pasifik (Melbourne), Eropa (Milan), Eropa (Spanyol), Eropa (Zurich), Timur Tengah (Bahrain), Timur Tengah (UEA).

Pemeriksaan toleransi kesalahan baru

Trusted Advisor menambahkan pemeriksaan berikut pada 30 Maret 2023.

- Layanan Amazon ECS menggunakan satu AZ
- Strategi penempatan Multi-AZ Amazon ECS

Untuk informasi lebih lanjut, lihat Toleransi kesalahan kategorinya.

Pemeriksaan toleransi kesalahan baru

Trusted Advisor menambahkan cek berikut pada 15 Desember 2022.

- AWS CloudHSM cluster yang menjalankan instance HSM dalam satu AZ

- Cluster Amazon ElastiCache Multi-AZ
- AmazonCluster Multi-AZ MemoryDB

Untuk menerima hasil Trusted Advisor untuk cluster AWS CloudHSM, ElastiCache, dan MemoryDB Anda, Anda harus memiliki cluster di Availability Zones Anda. Untuk informasi selengkapnya, lihat dokumentasi berikut ini:

- AWS CloudHSM Panduan Pengguna
- Amazon MemoryDB untuk Panduan Pengembang Redis
- Panduan Pengguna Amazon ElastiCache untuk Redis

Trusted Advisor memperbarui informasi cek berikut pada 15 Desember 2022.

- AWS Resilience Hub kebijakan dilanggar — Nama Aplikasi telah diperbarui ke Nama Aplikasi
- AWS Resilience Hub skor ketahanan - Nama Aplikasi dan Skor Ketahanan Aplikasi diperbarui ke Nama Aplikasi dan Skor Ketahanan Aplikasi

Untuk informasi lebih lanjut, lihat Toleransi kesalahan kategorinya.

Pembaruan Trusted Advisor integrasi dengan AWS Security Hub

Trusted Advisor membuat pembaruan berikut pada 17 November 2022.

Jika Anda menonaktifkan Security Hub atau AWS Config untuk Wilayah AWS, Trusted Advisor sekarang hapus temuan kontrol Anda untuk itu Wilayah AWS dalam 7-9 hari. Sebelumnya, kerangka waktu untuk menghapus data Security Hub Anda Trusted Advisor adalah 90 hari.

Untuk informasi selengkapnya, lihat bagian berikut dalam Pemecahan Masalah topik:

- Saya mematikan Security Hub atauAWS Config di Wilayah
- Kontrol saya diarsipkan di Security Hub, tetapi saya masih melihat temuan diTrusted Advisor

Pemeriksaan toleransi kesalahan baru untuk AWS Resilience Hub

Trusted Advisor menambahkan cek berikut pada 17 November 2022.

- AWS Resilience Hub kebijakan dilanggar

- AWS Resilience Hub skor ketahanan

Anda dapat menggunakan pemeriksaan ini untuk melihat status kebijakan ketahanan terbaru dan skor ketahanan untuk aplikasi Anda. Resilience Hub memberi Anda tempat sentral untuk menentukan, melacak, dan mengelola ketahanan dan ketersediaan aplikasi Anda.

Untuk menerima hasil Trusted Advisor untuk aplikasi Resilience Hub Anda, Anda harus menerapkan AWS aplikasi dan menggunakan Resilience Hub untuk melacak postur ketahanan aplikasi. Untuk informasi selengkapnya, silakan lihat Panduan Pengguna AWS Resilience Hub.

Untuk menerima hasil Trusted Advisor untuk cluster Anda ElastiCache dan MemoryDB, Anda harus memiliki cluster di Availability Zones Anda. Untuk informasi selengkapnya, lihat dokumentasi berikut ini:

- Amazon MemoryDB untuk Panduan Pengembang Redis
- Panduan Pengguna Amazon ElastiCache untuk Redis

Untuk informasi lebih lanjut, lihat Toleransi kesalahan kategorinya.

Perbarui ke Trusted Advisor konsol

Trusted Advisor menambahkan perubahan berikut pada 16 November 2022.

Trusted Advisor Dasbor di konsol sekarang Trusted Advisor Rekomendasi. Halaman Trusted Advisor Rekomendasi masih menampilkan hasil pemeriksaan dan pemeriksaan yang tersedia untuk setiap kategori untuk Anda Akun AWS.

Perubahan nama ini hanya memperbarui Trusted Advisor konsol. Anda dapat terus menggunakan Trusted Advisor konsol dan Trusted Advisor operasi di AWS Support API seperti biasa.

Untuk informasi selengkapnya, lihat Memulai dengan Trusted Advisor Rekomendasi.

Cek baru untuk Amazon EC2

Trusted Advisor menambahkan cek berikut pada 1 September 2022.

- Instans Amazon EC2 dengan dukungan akhir Microsoft Windows Server

Untuk informasi lebih lanjut, lihat Keamanan kategorinya.

Menambahkan pemeriksaan Security Hub ke Trusted Advisor

Per 23 Juni 2022, Trusted Advisor hanya mendukung kontrol Security Hub yang tersedia hingga 7 April 2022. Rilis ini mendukung semua kontrol dalam standar keamanan Praktik Terbaik Keamanan AWS Dasar kecuali untuk kontrol dalam Kategori: Pulih> Ketahanan. Untuk informasi selengkapnya, lihat MelihatAWS Security Hub kontrol diAWS Trusted Advisor.

Untuk daftar kontrol yang didukung, lihat Kontrol Praktik Terbaik Keamanan AWS Dasar di Panduan AWS Security Hub Pengguna.

Ditambahkan cek dari AWS Compute Optimizer

Trusted Advisor menambahkan cek berikut pada 4 Mei 2022.

Nama pemeriksaan	Kategori pemeriksaan	ID pemeriksaan
Volume Amazon EBS yang disediakan secara berlebihan	Optimasi Biaya	`COr6dfpM03`
Volume Amazon EBS yang kurang disediakan	Kinerja	`COr6dfpM04`
AWS Lambda fungsi yang disediakan secara berlebihan untuk ukuran memori	Optimasi Biaya	`COr6dfpM05`
AWS Lambda fungsi yang kurang disediakan untuk ukuran memori	Kinerja	`COr6dfpM06`

Anda harus memilih Compute Optimizer agar pemeriksaan ini dapat menerima data dari sumber daya Lambda dan Amazon EBS Anda. Akun AWS Untuk informasi selengkapnya, lihat Ikut serta AWS Compute Optimizer untuk Trusted Advisor cek.

Pembaruan pada pemeriksaan Exposed Access Keys

Trusted Advisor memperbarui cek berikut pada 25 April 2022.

Nama pemeriksaan	Kategori pemeriksaan	ID pemeriksaan
Exposed Access Keys	Keamanan	`12Fnkpl8Y5`

Trusted Advisor sekarang menyegarkan cek ini untuk Anda secara otomatis. Pemeriksaan ini tidak dapat di-refresh secara manual dari Trusted Advisor konsol atau AWS Support API. Jika aplikasi atau kode Anda menyegarkan cek ini untuk Anda Akun AWS, kami sarankan Anda memperbaruinya agar tidak lagi menyegarkan cek ini. Jika tidak, Anda akan menerima `InvalidParameterValue` kesalahan.

Kunci akses apa pun yang Anda kecualikan sebelum pembaruan ini tidak akan lagi dikecualikan dan akan muncul sebagai sumber daya yang terpengaruh. Anda tidak dapat mengecualikan kunci akses dari hasil pemeriksaan Anda. Untuk informasi selengkapnya, lihat Exposed Access Keys.

> **Note**
>
> Jika Anda membuat Akun AWS setelah 25 April 2022, hasil pemeriksaan untuk Exposed Access Keys awalnya menampilkan ikon abu-abu ( ) bahkan untuk kunci akses yang tidak terekspos. Ini berarti bahwa Trusted Advisor belum mengidentifikasi perubahan apa pun pada cek.
> Jika Trusted Advisor mengidentifikasi sumber daya yang berisiko, status akan berubah menjadi ikon tindakan yang direkomendasikan ( ).
> Setelah Anda memperbaiki atau menghapus sumber daya, hasil centang menunjukkan ikon tanda centang ( ).

Pemeriksaan yang diperbarui untuk AWS Direct Connect

Trusted Advisor memperbarui pemeriksaan berikut pada 29 Maret 2022.

Nama pemeriksaan	Kategori pemeriksaan	ID pemeriksaan
AWS Direct Connect Redundansi Koneksi	Toleransi kesalahan	`0t121N1Ty3`
AWS Direct Connect Redundansi Lokasi	Toleransi kesalahan	`8M012Ph3U5`
AWS Direct Connect Redundansi Antarmuka Virtual	Toleransi kesalahan	`4g3Nt5M1Th`

- Nilai untuk kolom Region sekarang menunjukkan Wilayah AWS kode bukan nama lengkap. Misalnya, sumber daya di AS Timur (Virginia N.) sekarang akan memiliki `us-east-1` nilai.
- Nilai untuk kolom Time Stamp sekarang muncul dalam RFC 3339 format, seperti`2022-03-30T01:02:27.000Z`.
- Sumber daya yang tidak memiliki masalah yang terdeteksi sekarang akan muncul di tabel centang. Sumber daya ini akan memiliki ikon tanda centang ( ) di sebelahnya.

  Sebelumnya, hanya sumber daya yang Trusted Advisor direkomendasikan untuk Anda selidiki yang muncul di tabel. Sumber daya ini memiliki ikon peringatan ( ) di sebelahnya.

AWS Security Hub kontrol ditambahkan ke AWS Trusted Advisor konsol

AWS Trusted Advisor menambahkan 111 kontrol Security Hub ke kategori Keamanan pada 18 Januari 2022.

Anda dapat melihat temuan Anda untuk kontrol Security Hub dari standar keamanan Praktik Terbaik Keamanan AWS Dasar. Integrasi ini tidak menyertakan kontrol yang memiliki Category: Recover > Resilience.

Untuk informasi selengkapnya tentang fitur ini, lihat MelihatAWS Security Hub kontrol diAWS Trusted Advisor.

Pemeriksaan baru untuk Amazon EC2 dan Well-Architected AWS

Trusted Advisor menambahkan cek berikut pada 20 Desember 2021.

- Amazon EC2 Instans Konsolidasi untuk Microsoft SQL Server
- Instans Amazon EC2 disediakan secara berlebihan untuk Microsoft SQL Server
- Instans Amazon EC2 dengan dukungan akhir Microsoft SQL Server
- AWS Well-Architectedmasalah risiko tinggi untuk optimalisasi biaya
- AWS Well-Architectedmasalah risiko tinggi untuk kinerja
- AWS Well-Architectedmasalah risiko tinggi untuk keamanan
- AWS Well-Architectedmasalah risiko tinggi untuk keandalan

Untuk informasi lebih lanjut, lihat referensi AWS Trusted Advisor cek.

Nama cek yang diperbarui untuk OpenSearch Layanan Amazon

Trusted Advisor memperbarui nama Amazon OpenSearch Service Reserved Instance Optimization cek pada 8 September 2021.

Rekomendasi cek, kategori, dan ID adalah sama.

Nama pemeriksaan	Kategori pemeriksaan	ID pemeriksaan
Optimasi Instans Cadangan OpenSearch Layanan Amazon	Optimasi Biaya	`7ujm6yhn5t`

> **Note**
>
> Jika Anda menggunakan Trusted Advisor CloudWatch metrik Amazon, nama metrik untuk pemeriksaan ini juga diperbarui. Untuk informasi selengkapnya, lihat Membuat CloudWatch alarm Amazon untuk memantauAWS Trusted Advisor metrik.

Menambahkan pemeriksaan untuk penyimpanan volume Amazon Elastic Block Store

Trusted Advisor menambahkan cek berikut pada 8 Juni 2021.

Nama pemeriksaan	Kategori pemeriksaan	ID pemeriksaan
Penyimpanan Volume General Purpose SSD (gp3) EBS	Batas layanan	dH7RR0l6J3
Penyimpanan Volume Provisioned IOPS SSD (io2) EBS	Batas layanan	gI7MM0l7J2

Ditambahkan cek untuk AWS Lambda

Trusted Advisor menambahkan cek berikut pada 8 Maret 2021.

Nama pemeriksaan	Kategori pemeriksaan	ID pemeriksaan
AWS Lambda Fungsi dengan Timeout Berlebihan	Optimasi Biaya	L4dfs2Q3C3
AWS Lambda Fungsi dengan Tingkat Kesalahan Tinggi	Optimasi Biaya	L4dfs2Q3C2
AWS Lambda Fungsi Menggunakan Runtime yang Tidak Digunakan Lagi	Keamanan	L4dfs2Q4C5
AWS Lambda Fungsi berkemampuan VPC tanpa Redundansi Multi-AZ	Toleransi kesalahan	L4dfs2Q4C6

Untuk informasi selengkapnya tentang cara menggunakan pemeriksaan ini dengan Lambda, lihat Contoh AWS Trusted Advisor alur kerja untuk melihat rekomendasi di Panduan Pengembang AWS Lambda .

Trusted Advisor periksa penghapusan

Trusted Advisor menghapus cek berikut untuk AWS GovCloud (US) Region tanggal 8 Maret 2021.

Nama pemeriksaan	Kategori pemeriksaan	ID pemeriksaan
Alamat IP EC2 Elastic	Batas layanan	aW9HH0l8J6

Pemeriksaan diperbarui untuk Amazon Elastic Block Store

Trusted Advisor memperbarui unit volume Amazon EBS dari gibibyte (GiB) ke tebibyte (TiB) untuk pemeriksaan berikut pada 5 Maret 2021.

> **Note**
>
> Jika Anda menggunakan Trusted Advisor CloudWatch metrik Amazon, nama metrik untuk lima pemeriksaan ini juga diperbarui. Untuk informasi selengkapnya, lihat Membuat CloudWatch alarm Amazon untuk memantauAWS Trusted Advisor metrik.

Nama pemeriksaan	Kategori pemeriksaan	ID pemeriksaan	CloudWatch Metrik yang diperbarui untuk ServiceLimit
Penyimpanan Volume Cold HDD (sc1) EBS	Batas layanan	gH5CC0e3J9	Penyimpanan volume Cold-HDD (sc1) (TiB)
Penyimpanan Volume General Purpose SSD (gp2) EBS	Batas layanan	dH7RR0l6J9	Penyimpanan volume General Purpose SSD (gp2) (TiB)
Penyimpanan Volume Magnetis EBS (standar)	Batas layanan	cG7HH0l7J9	Penyimpanan volume magnetis (standar) (TiB)

Nama pemeriksaan	Kategori pemeriksaan	ID pemeriksaan	CloudWatch Metrik yang diperbarui untuk ServiceLimit
Penyimpanan Volume Provisioned IOPS SSD (io1) EBS	Batas layanan	`gI7MM0l7J9`	Penyimpanan Provisioned IOPS (SSD) (TiB)
Penyimpanan Volume Throughput Optimized HDD (st1) EBS	Batas layanan	`wH7DD0l3J9`	Penyimpanan Volume Throughput Optimized HDD (st1) (TiB)

Trusted Advisor periksa penghapusan

> **Note**
>
> Trusted Advisor menghapus pemeriksaan berikut pada 18 November 2020.

Pemeriksaan dihapus pada 18 November 2020	Kategori pemeriksaan	ID pemeriksaan
Layanan EC2Config untuk instans Windows EC2	Toleransi kesalahan	`V77iOLlBqz`
Versi Driver ENA untuk Instans Windows EC2	Toleransi kesalahan	`TyfdMXG69d`
Versi Driver NVMe untuk Instans Windows EC2	Toleransi kesalahan	`yHAGQJV9K5`
Versi Driver PV untuk instans Windows EC2	Toleransi kesalahan	`Wnwm9Il5bG`
Volume Aktif EBS	Batas layanan	`fH7LL0l7J9`

Amazon Elastic Block Store tidak lagi membatasi jumlah volume yang dapat Anda sediakan.

Anda dapat memantau instans Amazon EC2 Anda dan memverifikasi kemutakhiran mereka dengan menggunakan AWS Systems Manager, alat pihak ketiga lainnya, atau menulis skrip Anda sendiri untuk mengembalikan informasi driver untuk Windows Management Instrumentation (WMI).

Trusted Advisor periksa penghapusan

Trusted Advisor menghapus cek berikut pada 18 Februari 2020.

Nama pemeriksaan	Kategori pemeriksaan	ID pemeriksaan
Service Limits	Kinerja	eW7HH0l7J9

AWS Support Aplikasi di Slack

Anda dapat menggunakan AWS Support Aplikasi untuk mengelola kasus AWS dukungan Anda di Slack. Undang anggota tim Anda ke saluran obrolan, menanggapi pembaruan kasus, dan mengobrol langsung dengan agen dukungan. Gunakan AWS Support Aplikasi untuk mengelola kasus dukungan dengan cepat di Slack.

Gunakan AWS Support Aplikasi untuk melakukan hal berikut:

- Membuat, memperbarui, mencari, dan menyelesaikan kasus dukungan di saluran Slack
- Lampirkan file untuk mendukung kasus
- Kuota permintaan meningkat dari Service Quotas
- Bagikan detail kasus dukungan dengan tim Anda tanpa meninggalkan saluran Slack
- Mulai sesi obrolan langsung dengan agen dukungan

Saat Anda membuat, memperbarui, atau menyelesaikan kasus dukungan di AWS Support Aplikasi, kasus ini juga diperbarui di AWS Support Center Console. Anda tidak perlu masuk ke Support Center Console untuk mengelola kasus dukungan secara terpisah.

> **Catatan**
>
> - Waktu respons untuk kasus dukungan sama, baik Anda membuat case dari Slack atau dari Support Center Console.
> - Anda dapat membuat kasus dukungan untuk dukungan akun dan penagihan, peningkatan kuota layanan, dan dukungan teknis.

Topik

- Mencari kasus dukungan di Slack
- Menyelesaikan kasus dukungan dalam Slack
- Membuka kembali kasus dukungan di Slack
- Meminta kenaikan kuota layanan
- Menghapus konfigurasi saluran Slack dariAWS Support Aplikasi
- Menghapus konfigurasi ruang kerja Slack dariAWS Support Aplikasi
- AWS SupportAplikasi dalam perintah Slack
- Lihat korespondensiAWS Support Aplikasi diAWS Support Center Console
- MembuatAWS Support Aplikasi di sumber daya Slack denganAWS CloudFormation

Prasyarat

Anda harus memenuhi persyaratan berikut untuk menggunakanAWS Support Aplikasi di Slack:

- Anda memiliki paket Business, Enterprise On-Ramp, atau Enterprise Support. Anda dapat menemukan paket Support Anda dariAWS Support Center Console atau dari halaman Paket dukungan. Untuk informasi selengkapnya, lihat BandingkanAWS Support paket.
- Anda memiliki ruang kerja dan saluran Slack untuk organisasi Anda. Anda harus menjadi administrator ruang kerja Slack, atau memiliki izin untuk menambahkan aplikasi ke ruang kerja Slack tersebut. Untuk informasi selengkapnya, lihat Pusat Bantuan Slack.
- Anda masuk keAkun AWS sebagai penggunaAWS Identity and Access Management (IAM) atau peran dengan izin yang diperlukan. Untuk informasi selengkapnya, lihat Mengelola akses ke widgetAWS Support Aplikasi.
- Anda harus membuat IAM role yang memiliki izin yang Anda perlukan. AWS SupportAplikasi menggunakan peran ini untuk melakukan panggilan API ke berbagai layanan. Untuk informasi selengkapnya, lihat Mengelola akses keAWS Support Aplikasi.

Topik

- Mengelola akses ke widgetAWS Support Aplikasi
- Mengelola akses keAWS Support Aplikasi

Mengelola akses ke widgetAWS Support Aplikasi

Anda dapat melampirkan kebijakanAWS Identity and Access Management (IAM) untuk memberikan izin pengguna IAM untuk mengonfigurasi widgetAWS Support Aplikasi di widgetAWS Support Center Console.

Untuk informasi selengkapnya tentang cara menambahkan kebijakan ke IAM, lihat Menambahkan izin identitas IAM (konsol) dalam Panduan Pengguna IAM.

> **Note**
>
> Anda juga dapat masuk sebagai root userAkun AWS, tetapi kami tidak menyarankan Anda melakukan hal ini. Untuk informasi selengkapnya tentang akses pengguna root, lihat Melindungi kredensi pengguna root Anda dan jangan menggunakannya untuk tugas sehari-hari di Panduan Pengguna IAM.

Contoh kebijakan IAM

Anda dapat memberlakukan kebijakan berikut ke entitas, seperti pengguna IAM. Kebijakan ini memungkinkan pengguna untuk mengotorisasi ruang kerja Slack dan mengkonfigurasi saluran Slack di konsol pusat Support.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "supportapp:GetSlackOauthParameters",
                "supportapp:RedeemSlackOauthCode",
                "supportapp:DescribeSlackChannels",
                "supportapp:ListSlackWorkspaceConfigurations",
                "supportapp:ListSlackChannelConfigurations",
                "supportapp:CreateSlackChannelConfiguration",
                "supportapp:DeleteSlackChannelConfiguration",
                "supportapp:DeleteSlackWorkspaceConfiguration",
                "supportapp:GetAccountAlias",
                "supportapp:PutAccountAlias",
                "supportapp:DeleteAccountAlias",
                "supportapp:UpdateSlackChannelConfiguration",
```

```
                "iam:ListRoles"
            ],
            "Resource": "*"
        }
    ]
}
```

Izin yang diperlukan untuk menghubungkanAWS Support Aplikasi ke Slack

AWS SupportAplikasi ini menyertakan tindakan khusus izin yang tidak secara langsung sesuai dengan operasi API. Tindakan ini ditunjukkan dalam Referensi Otorisasi Layanan dengan [izin saja].

AWS SupportAplikasi menggunakan tindakan API berikut untuk terhubung ke Slack dan kemudian mencantumkan saluran Slack publik Anda diAWS Support Center Console:

- `supportapp:GetSlackOauthParameters`
- `supportapp:RedeemSlackOauthCode`
- `supportapp:DescribeSlackChannels`

Tindakan API ini tidak dimaksudkan untuk dipanggil oleh kode Anda. Oleh karena itu, tindakan API ini tidak termasuk dalamAWS SDKAWS CLI dan.

Mengelola akses keAWS Support Aplikasi

Setelah Anda memiliki izin ke widgetAWS Support Aplikasi, Anda juga harus membuat peranAWS Identity and Access Management (IAM). Peran ini melakukan tindakan dari orang lainLayanan AWS untuk Anda, sepertiAWS Support API dan Service Quotas.

Anda kemudian melampirkan kebijakan IAM ke peran ini sehingga peran tersebut memiliki izin yang diperlukan untuk menyelesaikan tindakan ini. Anda memilih peran ini saat membuat konfigurasi saluran Slack di Konsol Pusat Support.

Pengguna di saluran Slack Anda memiliki izin yang sama dengan yang Anda berikan pada peran IAM. Misalnya, jika Anda menentukan akses hanya-baca ke kasus dukungan Anda, pengguna di saluran Slack Anda dapat melihat kasus dukungan Anda, tetapi tidak dapat memperbaruinya.

> **Important**
>
> Saat Anda meminta obrolan langsung dengan agen dukungan dan memilih saluran pribadi baru sebagai preferensi saluran obrolan langsung Anda,AWS Support Aplikasi akan

membuat saluran Slack terpisah. Saluran Slack ini memiliki izin yang sama dengan saluran tempat Anda membuat kasus atau memulai obrolan.
Jika Anda mengubah peran IAM atau kebijakan IAM, perubahan Anda berlaku untuk saluran Slack yang Anda konfigurasikan dan ke saluran Slack obrolan langsung baru yang dibuatAWS Support Aplikasi untuk Anda.

Ikuti prosedur ini untuk membuat peran dan kebijakan IAM Anda.

Topik

- Menggunakan kebijakan yangAWS dikelola pelanggan atau buat kebijakan yang dikelola pelanggan
- Membuat IAM role
- Pemecahan Masalah

Menggunakan kebijakan yangAWS dikelola pelanggan atau buat kebijakan yang dikelola pelanggan

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

Tip

Jika Anda tidak ingin membuat kebijakan secara manual, sebaiknya gunakan kebijakanAWS terkelola dan lewati prosedur ini. Kebijakan yang dikelola secara otomatis memiliki izin yang diperlukan untukAWS Support Aplikasi. Anda tidak perlu memperbarui kebijakan secara manual. Untuk informasi selengkapnya, lihat AWS kebijakan terkelola untuk AWS Support Aplikasi di Slack.

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

Untuk membuat kebijakan yang dikelola pelanggan untukAWS Support Aplikasi

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, dan kemudian 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 *AWSSupportAppRolePolicy*, 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 memberlakukan kebijakan berikut untuk peran IAM role Anda. Kebijakan ini memungkinkan peran memiliki izin penuh untuk semua tindakan yang diperlukan untukAWS Support Aplikasi. Setelah Anda mengonfigurasi saluran Slack dengan peran tersebut, setiap pengguna di saluran Anda memiliki izin yang sama.

> **Note**
>
> Untuk daftar kebijakan yangAWS dikelola, lihatAWS kebijakan terkelola untuk AWS Support Aplikasi di Slack.

Anda dapat memperbarui kebijakan untuk menghapus izin dariAWS Support Aplikasi.

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

```
        {
            "Effect": "Allow",
            "Action": [
                "servicequotas:GetRequestedServiceQuotaChange",
                "servicequotas:GetServiceQuota",
                "servicequotas:RequestServiceQuotaIncrease",
                "support:AddAttachmentsToSet",
                "support:AddCommunicationToCase",
                "support:CreateCase",
                "support:DescribeCases",
                "support:DescribeCommunications",
                "support:DescribeSeverityLevels",
                "support:InitiateChatForCase",
                "support:ResolveCase"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringEquals": {"iam:AWSServiceName": "servicequotas.amazonaws.com"}
            }
        }
    ]
}
```

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

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

Membuat IAM role

Setelah Anda memiliki kebijakan, Anda harus membuat IAM role, dan kemudian melampirkan kebijakan untuk peran tersebut. Anda memilih peran ini saat membuat konfigurasi saluran Slack di konsol pusat Support.

Untuk membuat peran untukAWS Support Aplikasi

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 Pilih entitas tepercaya, pilih Layanan AWS.
4. Pilih AWS SupportAplikasi.
5. Pilih Next: Permissions (Selanjutnya: Izin).
6. Masukkan nama kebijakan. Anda dapat memilih kebijakan yangAWS dikelola nasabah atau memilih kebijakan yang dikelola pelanggan yang Anda buat *`AWSSupportAppRolePolicy`*. Kemudian pilih kotak centang di samping kebijakan.
7. Pilih Berikutnya: Tag.
8. (Opsional) Anda dapat menggunakan tag sebagai pasangan nilai kunci untuk menambahkan metadata ke peran.
9. Pilih Selanjutnya: Tinjau.
10. Untuk Nama peran, masukkan nama, seperti *`AWSSupportAppRole`*.
11. (Opsional) Untuk Deskripsi peran, masukkan deskripsi untuk peran tersebut.
12. Tinjau peran dan kemudian pilih Buat peran. Anda sekarang dapat memilih peran ini ketika Anda mengkonfigurasi saluran Slack di konsol pusat Support. Lihat Mengkonfigurasi saluran Slack.

Untuk informasi lebih lanjut, lihat Membuat peran terkait layanan AWS dalam Panduan Pengguna IAM.

Pemecahan Masalah

Lihat topik berikut untuk mengelola akses keAWS Support Aplikasi.

Daftar Isi

Saya ingin membatasi pengguna tertentu di saluran Slack saya dari tindakan tertentu

Secara default, pengguna di saluran Slack Anda memiliki izin yang sama yang ditentukan dalam kebijakan IAM yang Anda lampirkan ke peran IAM yang Anda buat. Ini berarti siapa pun di saluran tersebut memiliki akses baca atau tulis ke kasus dukungan Anda, baik mereka memiliki pengguna IAMAkun AWS atau tidak.

Kami merekomendasikan praktik terbaik berikut:

- Konfigurasikan saluran Slack pribadi denganAWS Support Aplikasi
- Hanya mengundang pengguna ke channel Anda yang membutuhkan akses ke kasus dukungan Anda
- Gunakan kebijakan IAM yang memiliki izin minimum yang diperlukan untukAWS Support Aplikasi. Lihat AWS kebijakan terkelola untuk AWS Support Aplikasi di Slack.

Ketika saya mengkonfigurasi saluran Slack, saya tidak melihat peran IAM yang saya buat

Jika peran IAM Anda tidak muncul dalam peran IAM untuk daftarAWS Support Aplikasi, ini berarti peran tersebut tidak memilikiAWS Support Aplikasi sebagai entitas tepercaya, atau peran tersebut telah dihapus. Anda dapat memperbarui peran yang ada, atau membuat peran lain. Lihat Membuat IAM role.

Peran IAM saya tidak memiliki izin

Peran IAM yang Anda buat untuk saluran Slack memerlukan izin untuk melakukan tindakan yang Anda inginkan. Misalnya, jika Anda ingin pengguna di Slack membuat kasus dukungan, peran tersebut harus memiliki`support:CreateCase` izin. AWS SupportAplikasi mengasumsikan peran ini untuk melakukan tindakan ini untuk Anda.

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

Lihat sebelumnyaContoh kebijakan IAM.

Kesalahan Slack mengatakan bahwa peran IAM saya tidak valid

Pastikan Anda memilih peran yang benar untuk konfigurasi channel Anda.

Untuk memverifikasi peran Anda

1. Masuk ke halamanAWS Support Center Console di https://console.aws.amazon.com/support/app#/config.
2. Pilih saluran yang Anda konfigurasikan denganAWS Support Aplikasi.
3. Dari bagian Izin, temukan nama peran IAM yang Anda pilih.
   - Untuk mengubah peran, pilih Edit, pilih peran lain, lalu pilih Simpan.
   - Untuk memperbarui peran atau kebijakan yang dilampirkan ke peran, masuk ke konsol IAM.

AWS SupportAplikasi mengatakan bahwa saya kehilangan peran IAM untuk Service Quotas

Anda harus memiliki`AWSServiceRoleForServiceQuotas` peran dalam akun Anda untuk meminta kenaikan kuota dari Service Quotas. Jika Anda menerima kesalahan tentang sumber daya yang hilang, selesaikan salah satu langkah berikut:

- Gunakan konsol Service Quotas untuk meminta peningkatan kuota. Setelah Anda berhasil membuat permintaan, Service Quotas akan membuat peran ini untuk Anda secara otomatis. Kemudian, Anda dapat menggunakanAWS Support App untuk meminta kenaikan kuota di Slack. Untuk informasi selengkapnya, lihat Permintaan peningkatan kuota.
- Perbarui kebijakan IAM yang dilampirkan pada peran Anda. Ini memberikan izin peran untuk Service Quotas. Bagian berikut dalamContoh kebijakan IAM memungkinkanAWS Support Aplikasi untuk membuat peran Service Quotas untuk Anda.

```
{
    "Effect": "Allow",
    "Action": "iam:CreateServiceLinkedRole",
    "Resource": "*",
    "Condition": {
        "StringEquals": {"iam:AWSServiceName": "servicequotas.amazonaws.com"}
     }
}
```

Jika Anda menghapus peran IAM yang Anda konfigurasikan untuk saluran, Anda harus membuat peran secara manual atau memperbarui kebijakan IAM untuk memungkinkanAWS Support Aplikasi membuatnya untuk Anda.

Otorisasi ruang kerja Slack

Setelah Anda mengotorisasi ruang kerja Anda dan memberikan izinAWS Support Aplikasi untuk mengaksesnya, Anda kemudian memerlukan peranAWS Identity and Access Management (IAM) untuk AndaAkun AWS. AWS SupportAplikasi menggunakan peran ini untuk memanggil operasi API dari AWS Supportdan Service Quotas untuk Anda. Misalnya,AWS Support Aplikasi menggunakan peran untuk memanggil`CreateCase` operasi untuk membuat kasus dukungan untuk Anda di Slack.

> **Catatan**
>
> - Saluran Slack mewarisi izin dari peran IAM. Ini berarti bahwa setiap pengguna di saluran Slack memiliki izin yang sama yang ditentukan dalam kebijakan IAM yang dilampirkan ke peran.
>
> Misalnya, jika kebijakan IAM Anda memungkinkan peran tersebut memiliki izin membaca dan menulis lengkap untuk kasus dukungan Anda, siapa pun di saluran Slack Anda dapat membuat, memperbarui, dan menyelesaikan kasus dukungan Anda. Jika kebijakan IAM Anda mengizinkan izin hanya-baca peran, maka pengguna di saluran Slack Anda hanya memiliki izin membaca untuk kasus dukungan Anda.
> - Kami menyarankan Anda menambahkan ruang kerja dan saluran Slack yang Anda perlukan untuk mengelola operasi dukungan Anda. Sebaiknya Anda membuat konfigurasi pada saluran pribadi dan hanya mengundang pengguna diperlukan.

Anda harus mengotorisasi setiap ruang kerja Slack yang ingin Anda gunakan untuk AndaAkun AWS. Jika Anda memiliki beberapaAkun AWS, Anda harus masuk ke setiap akun dan ulangi prosedur berikut untuk mengotorisasi ruang kerja. Jika akun Anda milik organisasiAWS Organizations dan Anda ingin mengotorisasi beberapa akun, lewati ke Otorisasi beberapa akun.

Untuk mengotorisasi ruang kerja Slack untukAkun AWS

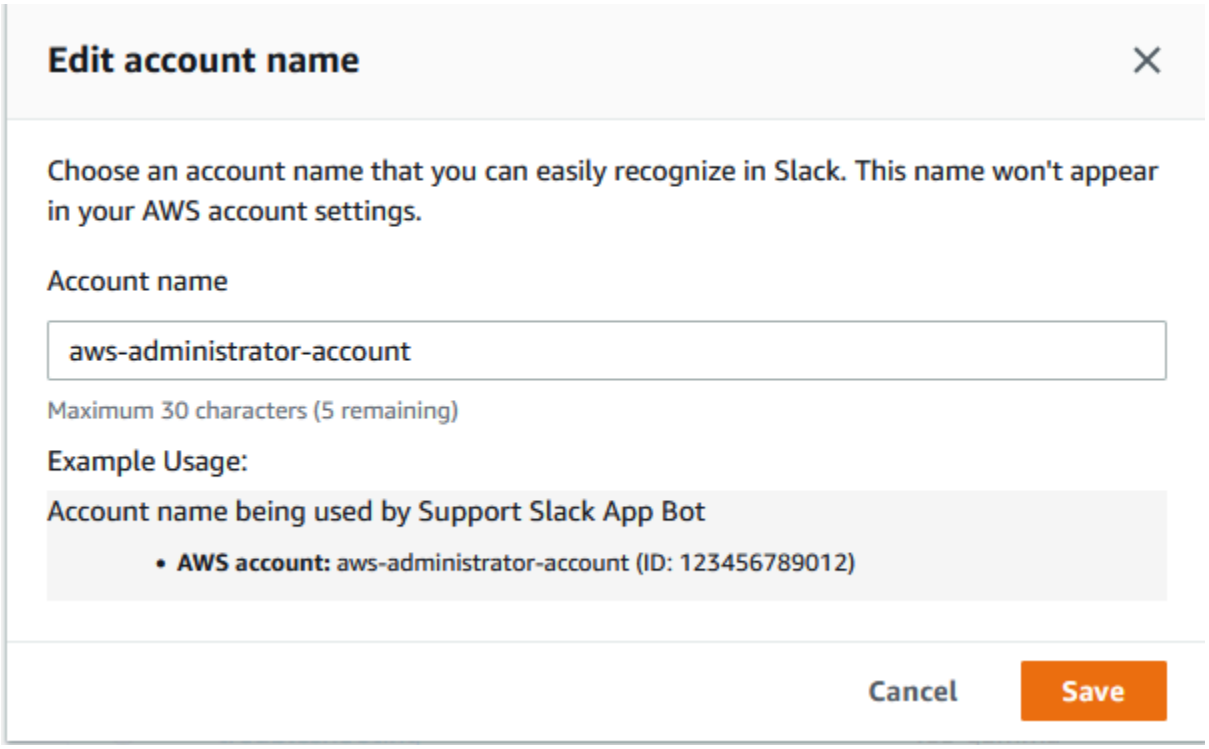
1. Masuk ke AWS Support Center Consoledan pilih konfigurasi Slack.
2. Pada halaman Memulai, pilih Otorisasi ruang kerja.
3. Jika Anda belum masuk ke Slack, di halaman Login ke ruang kerja Anda, masukkan nama ruang kerja Anda, lalu pilih Lanjutkan.
4. Pada AWS Supportmeminta izin untuk mengakses halaman your-workspace-name Slack, pilih Izinkan.

> **Note**
>
> Jika Anda tidak dapat mengizinkan Slack mengakses ruang kerja Anda, pastikan Anda memiliki izin dari administrator Slack untuk menambahkanAWS Support Aplikasi ke ruang kerja. Lihat Prasyarat.

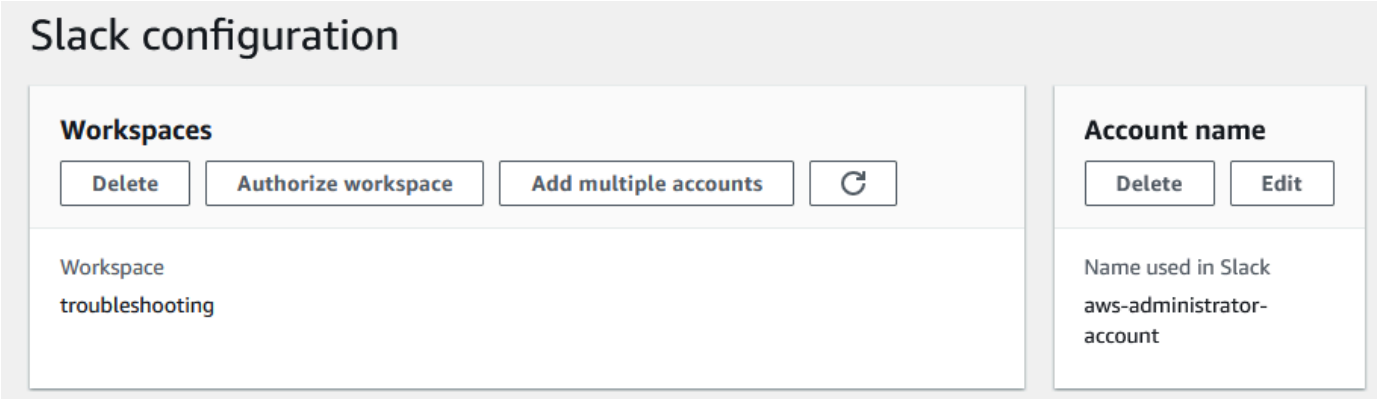
Pada halaman konfigurasi Slack, nama ruang kerja Anda muncul di bawah Workspaces.

5. (Opsional) Untuk menambahkan lebih banyak ruang kerja, pilih Otorisasi ruang kerja dan ulangi langkah 3-4. Anda dapat menambahkan hingga lima ruang kerja ke akun Anda.
6. (Opsional) Secara default, nomorAkun AWS ID Anda muncul sebagai nama akun di saluran Slack Anda. Untuk mengubah nilai ini, di bawah Nama akun, pilih Edit, masukkan nama akun Anda, lalu pilih Simpan.

> **Tip**
>
> Gunakan nama yang dapat Anda dan tim Anda kenali dengan mudah. AWS SupportAplikasi menggunakan nama ini untuk mengidentifikasi akun Anda di saluran Slack. Anda dapat memperbarui nama ini kapan saja.



Ruang kerja dan nama akun Anda muncul di halaman konfigurasi Slack.



Mengelola beberapa akun

Untuk mengotorisasi beberapaAkun AWS untuk menggunakan ruang kerja Slack, Anda dapat menggunakan AWS CloudFormationatau Terraform untuk membuat resourceAWS Support Aplikasi.

Mengkonfigurasi saluran Slack

Setelah mengotorisasi ruang kerja Slack, Anda dapat mengonfigurasi saluran Slack untuk menggunakanAWS Support Aplikasi.

Saluran tempat Anda mengundang dan menambahkanAWS Support Aplikasi adalah tempat Anda dapat membuat dan mencari kasus, dan menerima pemberitahuan kasus. Saluran ini menampilkan pembaruan kasus, seperti kasus yang baru dibuat atau diselesaikan, korespondensi tambahan, dan detail kasus bersama.

Saluran Slack mewarisi izin dari peran IAM. Ini berarti bahwa setiap pengguna di saluran Slack memiliki izin yang sama yang ditentukan dalam kebijakan IAM yang dilampirkan ke peran.

Misalnya, jika kebijakan IAM Anda memungkinkan peran tersebut memiliki izin membaca dan menulis lengkap untuk kasus dukungan Anda, siapa pun di saluran Slack Anda dapat membuat, memperbarui, dan menyelesaikan kasus dukungan Anda. Jika kebijakan IAM Anda mengizinkan izin hanya-baca peran, maka pengguna di saluran Slack Anda hanya memiliki izin membaca untuk kasus dukungan Anda.

Anda dapat menambahkan hingga 20 saluran untuk akun. Saluran Slack dapat memiliki hingga 100Akun AWS. Ini berarti bahwa hanya 100 akun yang dapat menambahkan saluran Slack yang sama keAWS Support Aplikasi. Kami menyarankan Anda hanya menambahkan akun yang diperlukan untuk mengelola kasus dukungan untuk organisasi Anda. Ini dapat mengurangi jumlah notifikasi yang Anda terima di saluran sehingga Anda dan tim Anda memiliki lebih sedikit gangguan.

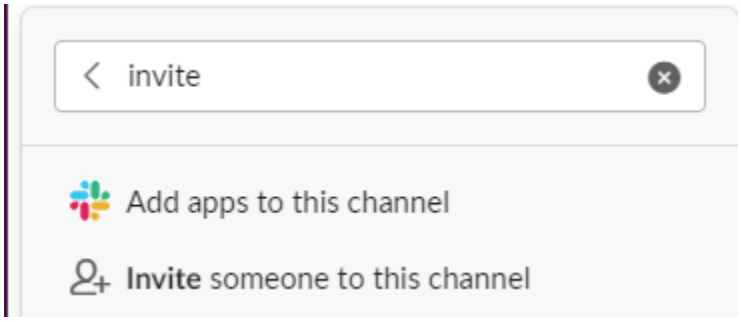
Masing-masingAkun AWS harus mengonfigurasi saluran Slack secara terpisah diAWS Support Aplikasi. Dengan cara ini,AWS Support Aplikasi dapat mengakses kasus dukungan dalam hal ituAkun AWS. Jika yang lainAkun AWS di organisasi Anda sudah mengundangAWS Support Aplikasi ke saluran Slack itu, lanjutkan ke langkah 3.

> **Note**
>
> Anda dapat mengonfigurasi saluran yang merupakan bagian dari Slack Connect dan saluran yang dibagikan dengan beberapa ruang kerja. Namun, hanya ruang kerja pertama yang mengonfigurasi saluran bersama untukAkun AWS dapat menggunakanAWS Support Aplikasi. AWS SupportAplikasi mengembalikan pesan kesalahan jika Anda mencoba mengonfigurasi saluran Slack yang sama untuk ruang kerja lain.

Cara mengonfigurasi saluran Slack

1. Dari aplikasi Slack, pilih saluran Slack yang ingin Anda gunakan denganAWS Support Aplikasi.
2. Selesaikan langkah-langkah berikut untuk mengundangAWS Support Aplikasi ke saluran Anda:

   a. Pilih ikon + dan masukkan`invite`, lalu, saat diminta, pilih Tambahkan aplikasi ke saluran ini.

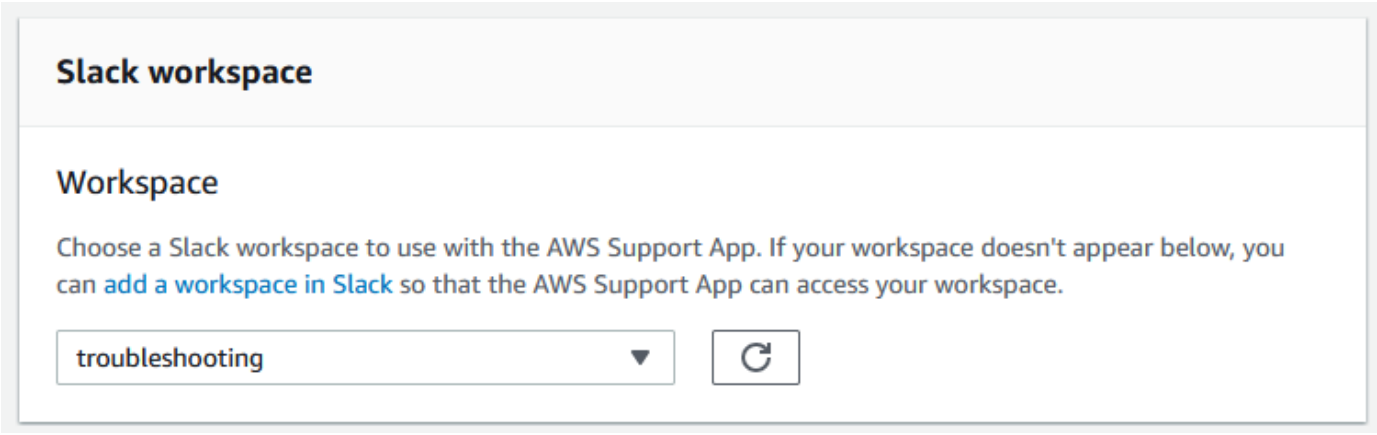
   

   b. Untuk mencari aplikasi, di bagian Tambahkan aplikasi ke channelName, masukkan AWS SupportAplikasi.

   c. Pilih Tambah di samping AWS SupportAplikasi.

3. Masuk ke Konsol Pusat Support dan pilih konfigurasi Slack.
4. Pilih Tambahkan saluran.
5. Pada halaman Tambahkan saluran, di bawah Workspace, pilih nama ruang kerja yang sebelumnya Anda otorisasi. Anda dapat memilih ikon refresh jika nama ruang kerja tidak muncul dalam daftar.

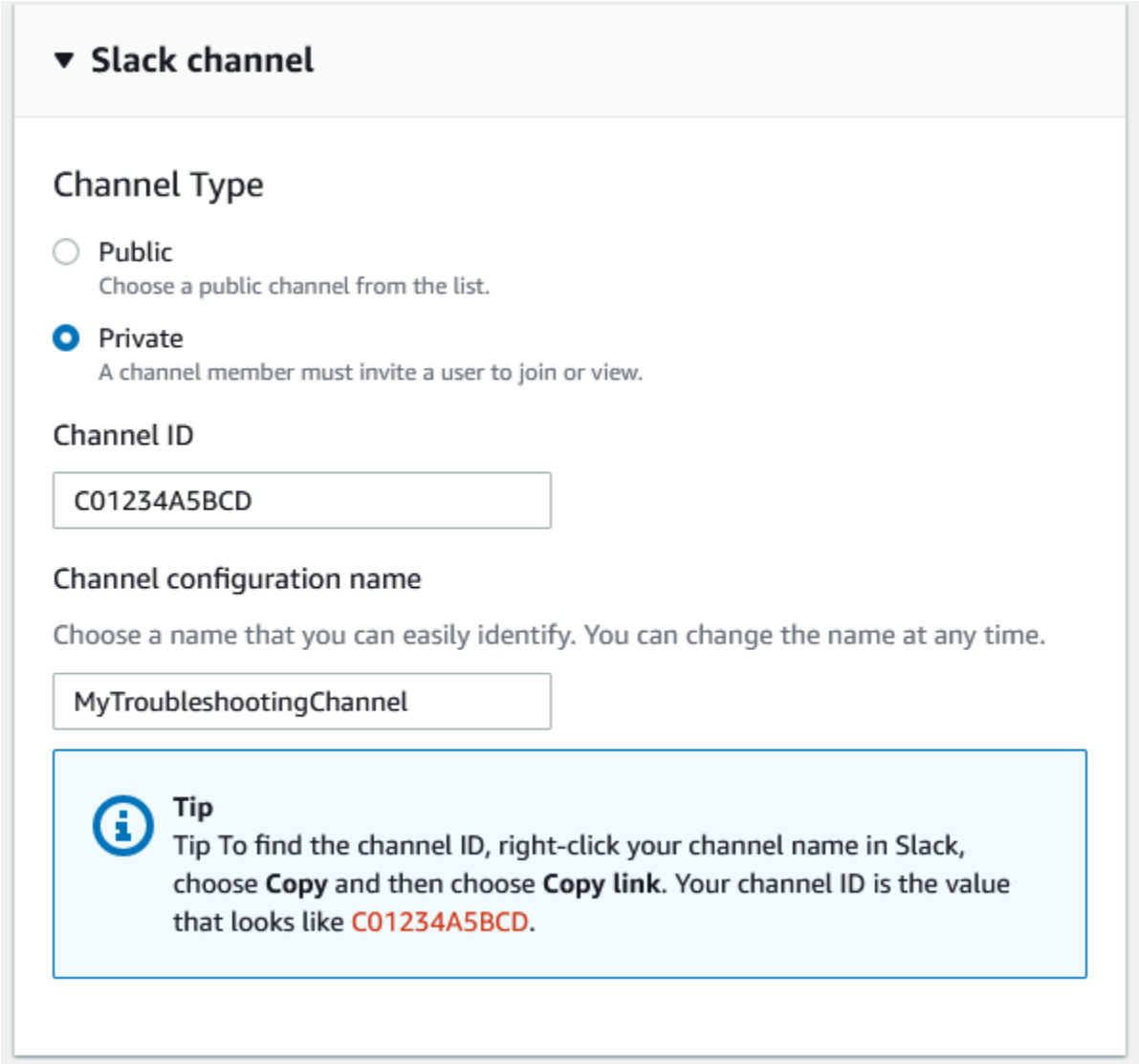


6. Di bawah saluran Slack, untuk jenis Channel, pilih salah satu dari berikut ini:
   - Publik — Di bawah Saluran publik, pilih saluran Slack tempat Anda mengundangAWS Support Aplikasi (langkah 2). Jika saluran Anda tidak muncul dalam daftar, pilih ikon refresh lalu coba lagi.
   - Pribadi — Di bawah ID Saluran, masukkan ID atau URL saluran Slack tempat Anda mengundangAWS Support Aplikasi.

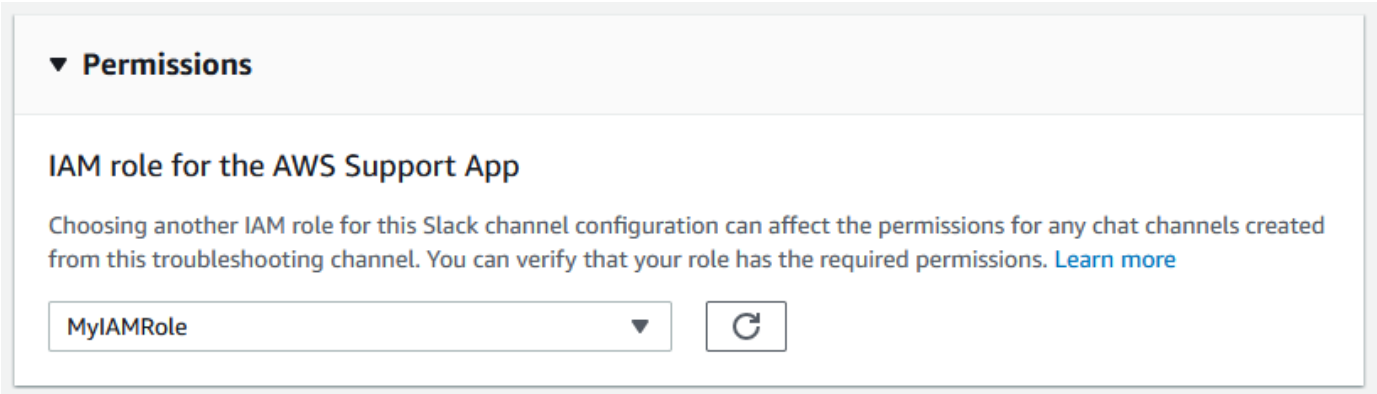
   > **Tip**
   >
   > Untuk menemukan ID saluran, buka menu konteks (klik kanan) untuk nama saluran di Slack, dan kemudian pilih Salin, dan kemudian pilih Salin tautan. ID saluran Anda adalah nilai yang terlihat seperti *C01234A5BCD*.

7. Di bawah Nama konfigurasi saluran, masukkan nama yang dengan mudah mengidentifikasi konfigurasi saluran Slack Anda untukAWS Support Aplikasi. Nama ini hanya muncul di AndaAkun AWS dan tidak muncul di Slack. Anda dapat mengganti nama konfigurasi saluran Anda nanti.

   Jenis saluran Slack Anda mungkin akan terlihat seperti contoh berikut ini.



8. Di bawah Izin, untuk peran IAM untukAWS Support Aplikasi di Slack, pilih peran yang Anda buat untukAWS Support Aplikasi. Hanya peran yang memilikiAWS Support Aplikasi sebagai entitas tepercaya yang muncul dalam daftar.



> **Note**
>
> Jika Anda belum membuat peran atau tidak melihat peran Anda dalam daftar, lihatMengelola akses keAWS Support Aplikasi.

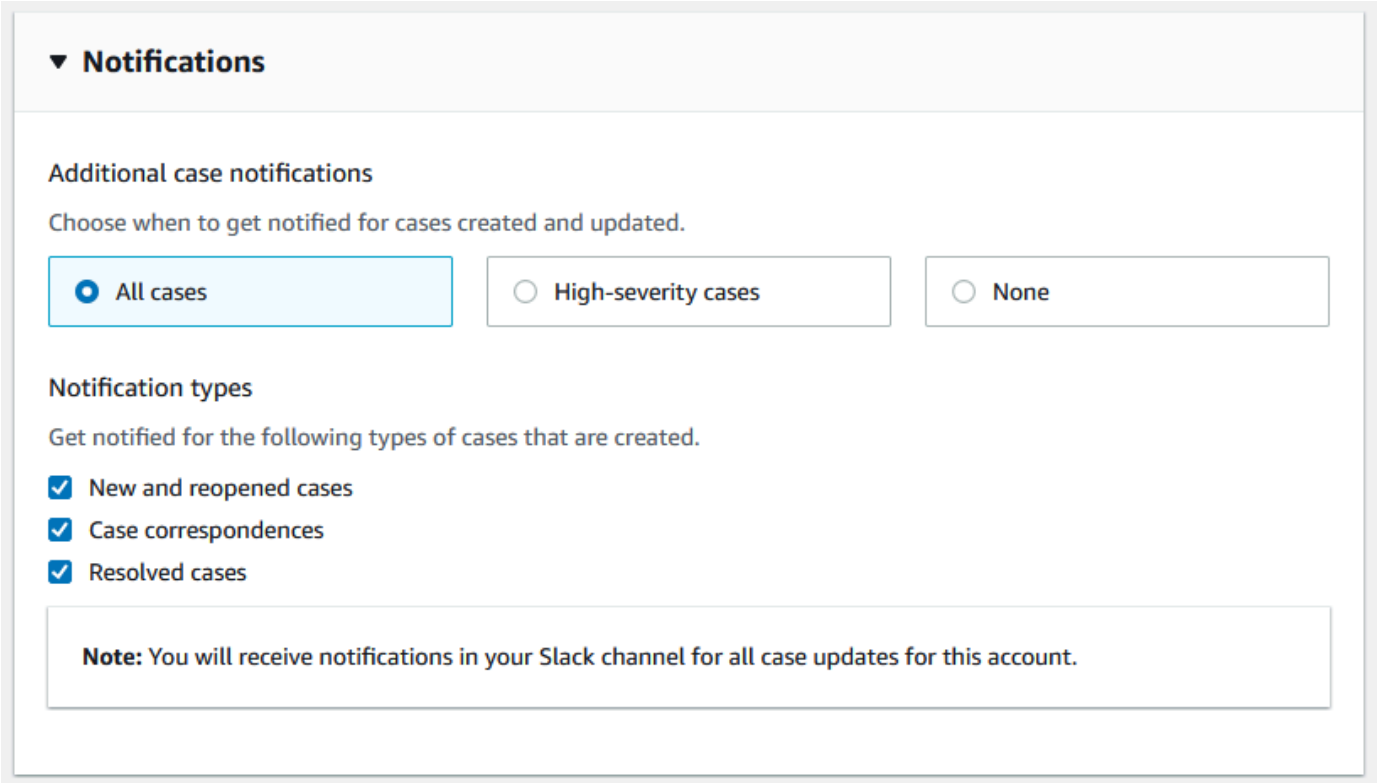
9. Di bawah Notifikasi, tentukan cara mendapatkan pemberitahuan untuk kasus.

   - Semua kasus - Dapatkan pemberitahuan untuk semua pembaruan kasus.
   - Kasus tingkat keparahan tinggi - Dapatkan pemberitahuan hanya untuk kasus yang memengaruhi sistem produksi atau lebih tinggi. Untuk informasi selengkapnya, lihat Memilih kepelikan.
   - Tidak ada - Jangan mendapatkan pemberitahuan untuk pembaruan kasus.

10. (Opsional) Jika Anda memilih Semua kasus atau Kasus tingkat keparahan tinggi, Anda harus memilih setidaknya satu dari opsi berikut:

    - Kasus baru dan dibuka kembali
    - Korespondensi kasus
    - Kasus terselesaikan

    Saluran berikut menerima pemberitahuan kasus untuk semua pembaruan kasus di Slack.



11. Tinjau konfigurasi Anda dan pilih Tambahkan saluran. Saluran Anda muncul di halaman konfigurasi Slack.

Memperbarui konfigurasi saluran Slack

Setelah mengonfigurasi saluran Slack, Anda dapat memperbaruinya nanti untuk mengubah peran IAM atau pemberitahuan kasus.

Untuk memperbarui konfigurasi saluran Slack

1. Masuk ke Konsol Pusat Support dan pilih konfigurasi Slack.
2. Di bawah Saluran, pilih konfigurasi saluran yang Anda inginkan.
3. Pada halaman ***channelName***, Anda dapat melakukan tugas-tugas berikut:
   - Pilih Ubah nama untuk memperbarui nama konfigurasi saluran Anda. Nama ini hanya muncul di AndaAkun AWS dan tidak akan muncul di Slack.
   - Pilih Hapus untuk menghapus konfigurasi saluran dariAWS Support Aplikasi. Lihat Menghapus konfigurasi saluran Slack dariAWS Support Aplikasi.
   - Pilih Buka di Slack untuk membuka saluran Slack di browser Anda.
   - Pilih Edit untuk mengubah peran atau notifikasi IAM.

Membuat kasus dukungan di saluran Slack

Setelah Anda mengotorisasi ruang kerja Slack Anda dan menambahkan saluran Slack Anda, Anda dapat membuat kasus dukungan di saluran Slack Anda.

Untuk membuat kasus dukungan di Slack

1. Di saluran Slack Anda, masukkan perintah berikut:

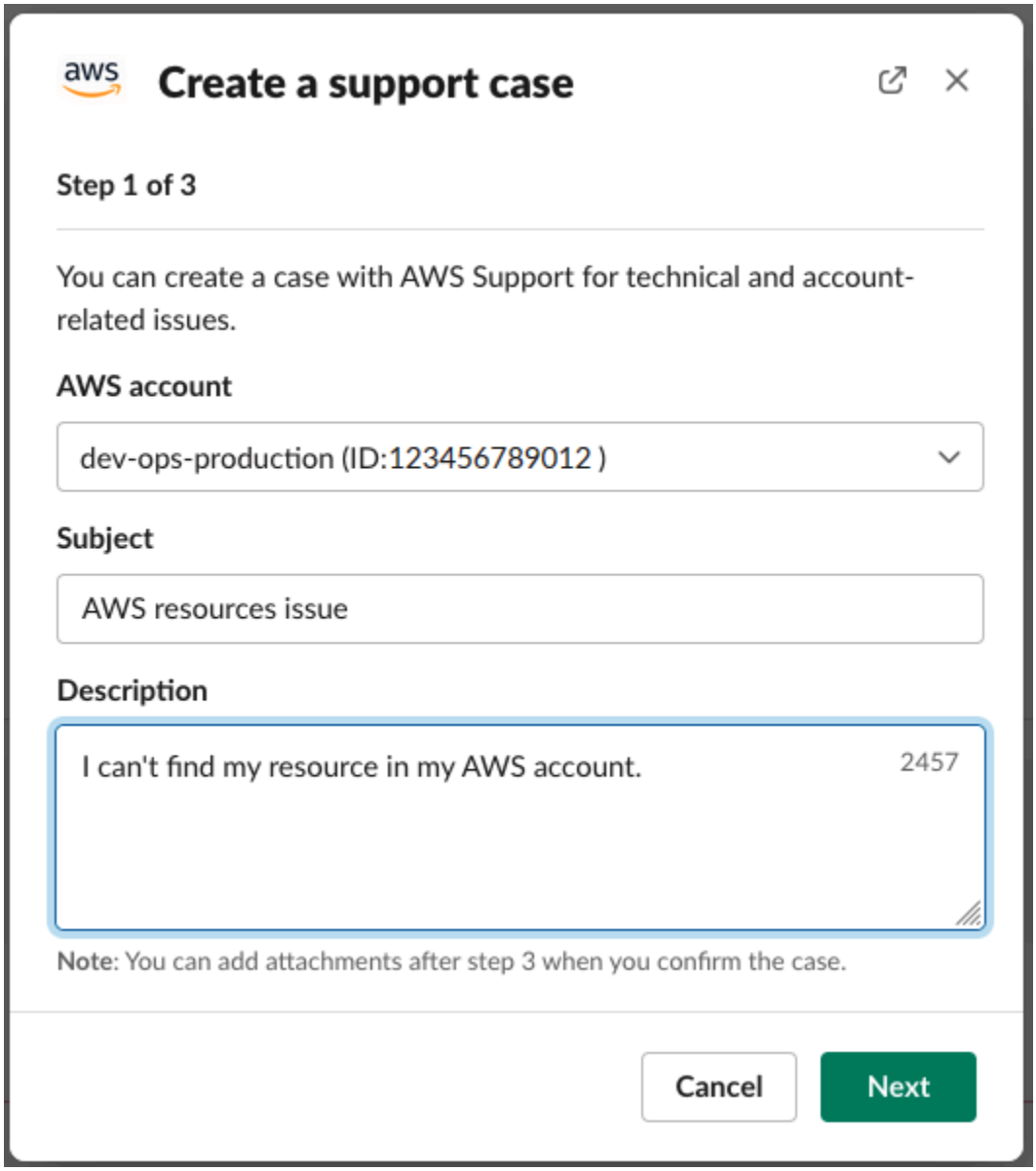
   ```
   /awssupport create
   ```

2. Di kotak dialog Buat kasus dukungan, lakukan hal berikut:

   a. Jika Anda mengonfigurasi lebih dari satu akun untuk saluran Slack ini Akun AWS, pilih ID akun. Jika Anda membuat nama akun, nilai ini muncul di samping ID akun. Untuk informasi selengkapnya, lihat Otorisasi ruang kerja Slack.

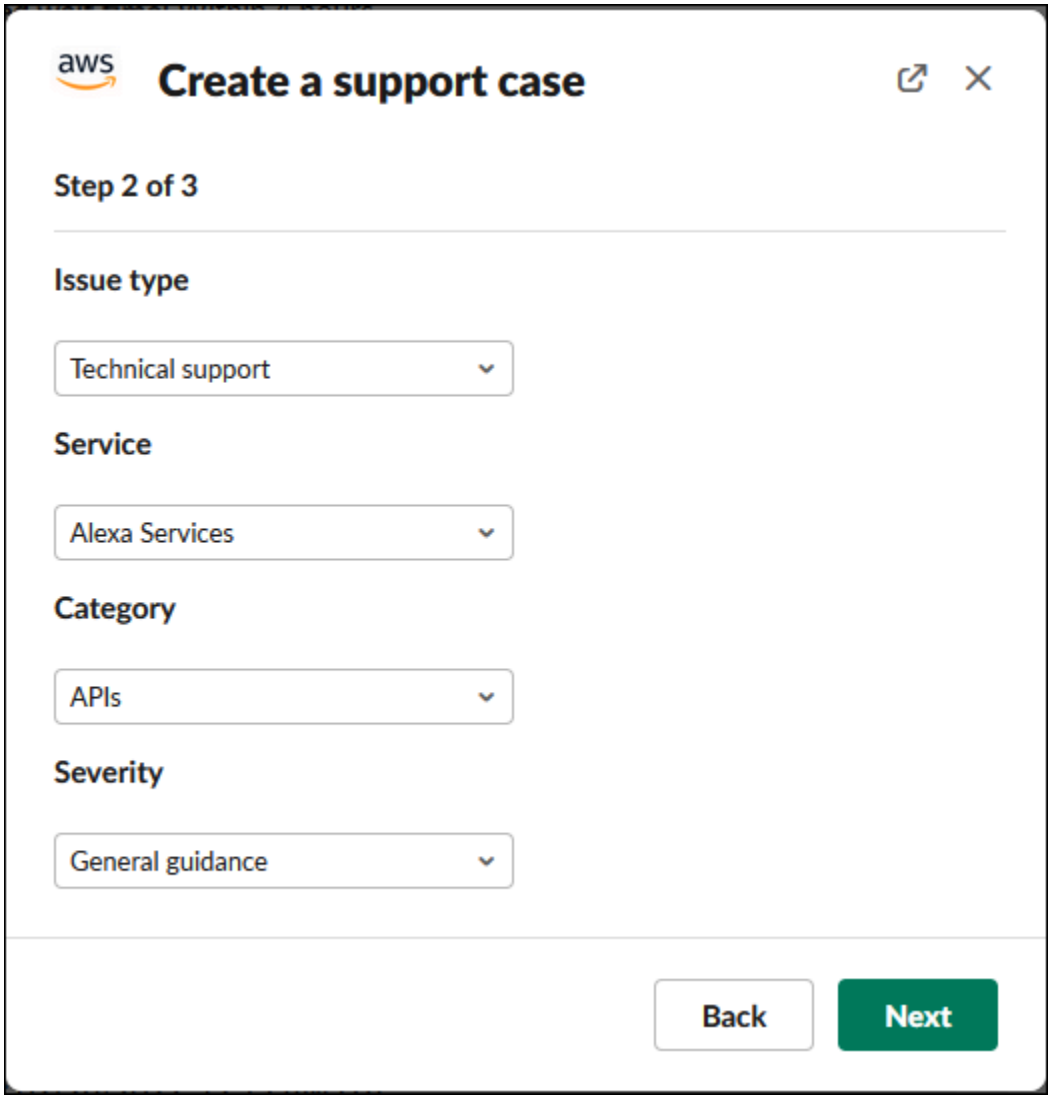
   b. Untuk Subject, masukkan judul untuk kasus dukungan.

   c. Untuk Deskripsi, jelaskan kasus dukungan. Berikan detail, seperti cara Anda menggunakanLayanan AWS dan langkah-langkah pemecahan masalah apa yang Anda coba.



3. Pilih Selanjutnya.
4. Pada Buat kasus dukungan kotak dialog, tentukan pilihan berikut:
   a. Pilih jenis Masalah.
   b. Pilih Layanan.
   c. Pilih Kategori.
   d. Pilih Keparahan.
   e. Tinjau detail kasus Anda dan pilih Berikutnya.

   Contoh berikut menunjukkan kasus dukungan teknis untukAlexa Layanan.

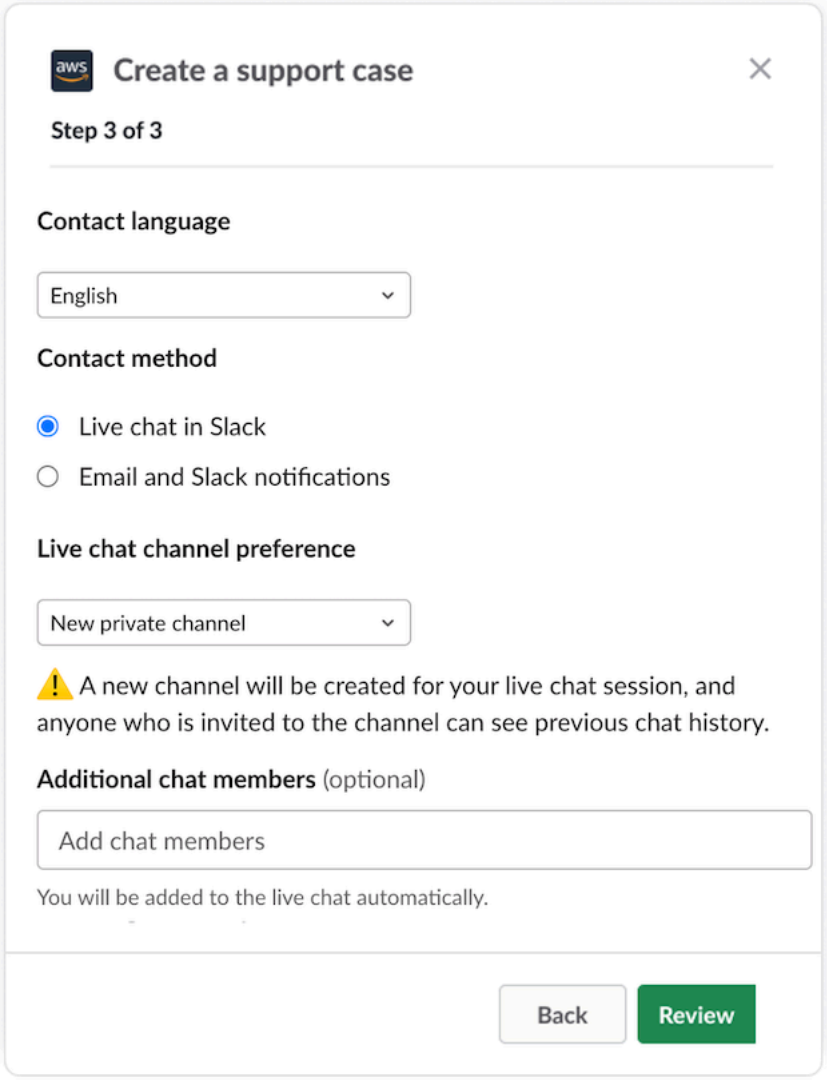


5. Untuk bahasa Kontak, pilih bahasa pilihan Anda untuk kasus dukungan Anda.

> **Note**
>
> Dukungan bahasa Jepang tidak tersedia untuk obrolan langsung di Slack untuk kasus akun dan penagihan.

6. Untuk metode Kontak, pilih notifikasi Email dan Slack atau Obrolan langsung di Slack.

   Contoh berikut menunjukkan cara memilih obrolan langsung di Slack.



a. Jika Anda memilih Obrolan langsung di Slack, pilih Saluran pribadi baru atau Saluran saat ini sebagai preferensi saluran obrolan langsung Anda. Saluran pribadi baru akan membuat saluran pribadi terpisah bagi Anda untuk mengobrol denganAWS Support agen, dan saluran saat ini akan menggunakan utas di saluran saat ini bagi Anda untuk mengobrol denganAWS Support agen.

b. (Opsional) Jika Anda memilih Obrolan langsung di Slack, Anda dapat memasukkan nama anggota Slack lainnya. Untuk saluran pribadi baru,AWS Support Aplikasi akan secara otomatis menambahkan Anda dan anggota yang dipilih ke saluran baru. Untuk Saluran saat ini,AWS Support Aplikasi akan secara otomatis menandai Anda dan anggota yang dipilih di utas obrolan saatAWS Support agen bergabung.

> **Important**
>
> - Kami menyarankan Anda untuk memperoleh akses ke rincian kasus dukungan dan riwayat obrolan.
> - Jika Anda memulai sesi obrolan langsung baru untuk kasus dukungan yang ada,AWS Support Aplikasi menggunakan saluran obrolan atau thread yang sama yang digunakan untuk obrolan langsung sebelumnya. AWS SupportAplikasi ini juga menggunakan preferensi saluran obrolan langsung yang sama yang digunakan sebelumnya.
> - Opsi saluran saat ini hanya tersedia jika obrolan diminta dari saluran pribadi. Kami menyarankan Anda hanya menggunakan opsi ini jika Anda ingin semua anggota saluran memiliki akses ke obrolan Anda.

7. (Opsional) Untuk kontak tambahan untuk memberi tahu, masukkan alamat email untuk juga menerima pembaruan tentang kasus dukungan ini. Anda dapat menambahkan hingga 10 alamat email.
8. Pilih Tinjau.
9. Di saluran Slack, tinjau detail kasus. Anda dapat melakukan hal berikut:
   - Pilih Edit untuk mengubah detail kasus.
   - Tambahkan file ke kasus Anda. Untuk melakukannya, ikuti langkah-langkah berikut:
     a. Pilih Lampirkan file, pilih ikon + di Slack, dan pilih Komputer Anda.
     b. Arahkan ke dan pilih file Anda.
     c. Di kotak dialog Upload file, masukkan`@awssupport`, dan tekan
        
        ikon kirim pesan.

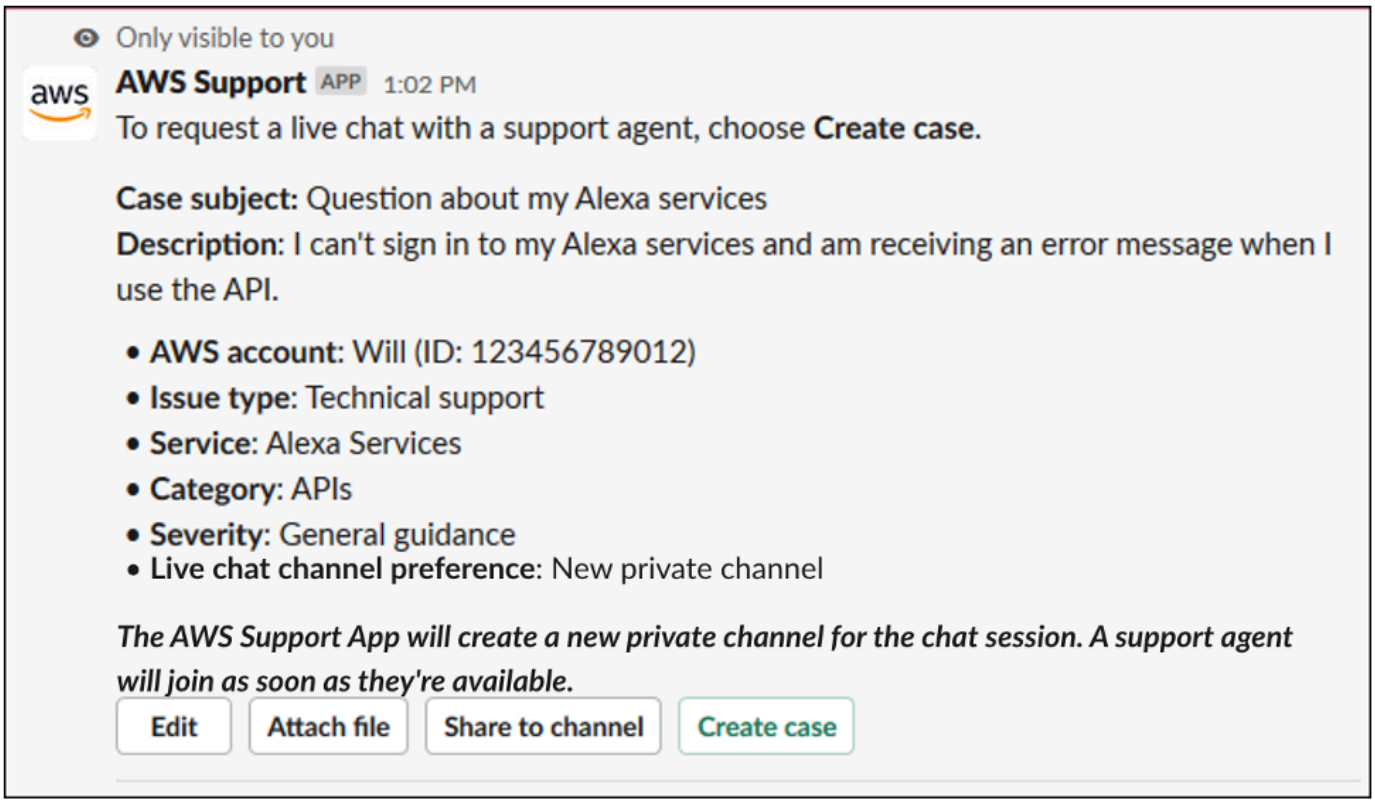
> **Catatan**
>
> - Anda dapat melampirkan hingga tiga file. Setiap file bisa mencapai 5 MB.

- Jika Anda melampirkan file ke kasus dukungan Anda, Anda harus mengirimkan kasus Anda dalam waktu 1 jam. Jika tidak, Anda harus menambahkan file lagi.

- Pilih Bagikan ke saluran untuk membagikan detail kasus dengan orang lain di saluran Slack. Anda dapat menggunakan opsi ini untuk membagikan detail kasus dengan tim Anda sebelum membuat kasus ini.

10. Tinjau rincian kasus Anda, lalu pilih kasus Buat.

    Contoh berikut menunjukkan kasus dukungan teknis untukAlexa Layanan.



    Setelah Anda membuat kasus dukungan, mungkin perlu beberapa menit agar detail kasus Anda muncul.

11. Ketika kasus dukungan Anda diperbarui, Anda dapat memilih Lihat detail untuk melihat informasi kasus Anda. Kemudian, Anda dapat melakukan hal berikut:

    - Pilih Bagikan ke saluran untuk membagikan detail kasus dengan orang lain di saluran Slack.
    - Pilih Balas untuk menambahkan korespondensi.
    - Pilih Resolve case (Selesaikan kasus).

> **Note**
>
> Jika Anda tidak memilih untuk menerima pembaruan kasus otomatis di Slack, Anda dapat mencari kasus dukungan untuk menemukan opsi Lihat detail.

Membalas kasus pendukung di Slack

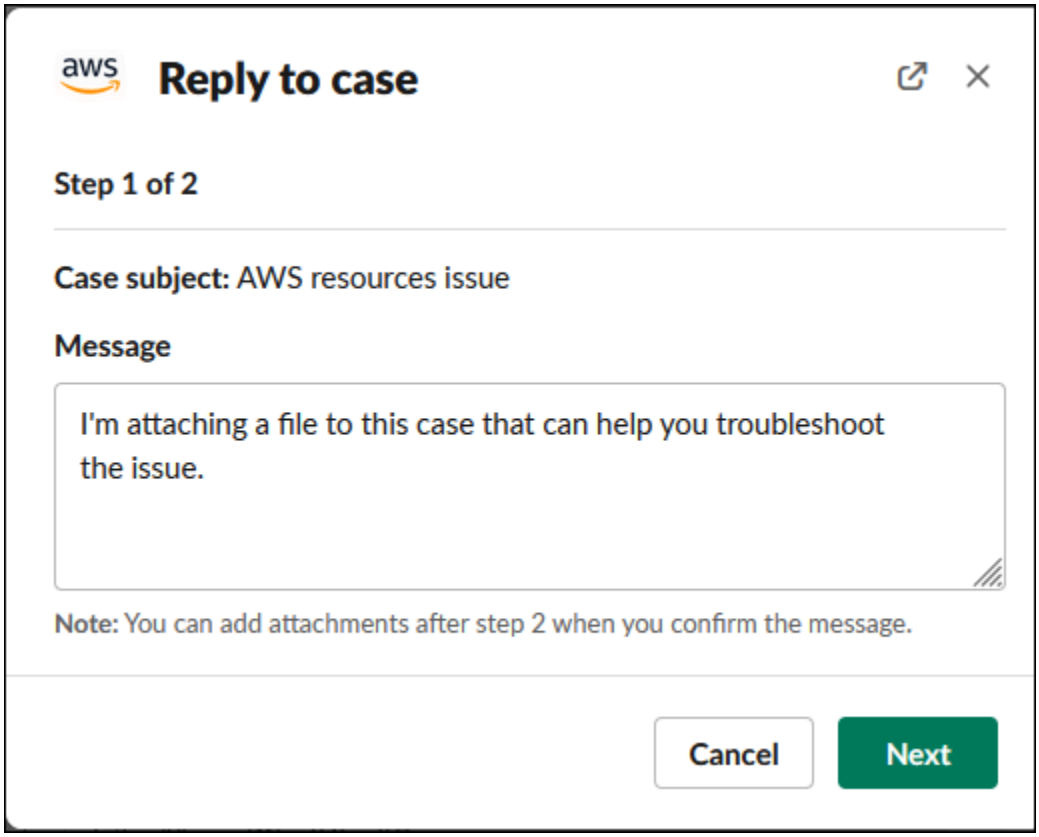
Anda dapat menambahkan pembaruan pada kasus Anda seperti detail kasus dan lampiran, dan membalas tanggapan dari agen dukungan.

> **Note**
>
> - Anda juga dapat menggunakanAWS Support Center Console untuk membalas agen pendukung. Untuk informasi selengkapnya, lihat Memperbarui, menyelesaikan, dan membuka kembali kasus Anda.
> - Anda tidak dapat menambahkan korespondensi ke kasus dari saluran obrolan yang dibuat olehAWS Support Aplikasi. Saluran obrolan langsung hanya mengirim pesan ke agen selama obrolan langsung.

Untuk membalas kasus dukungan di Slack

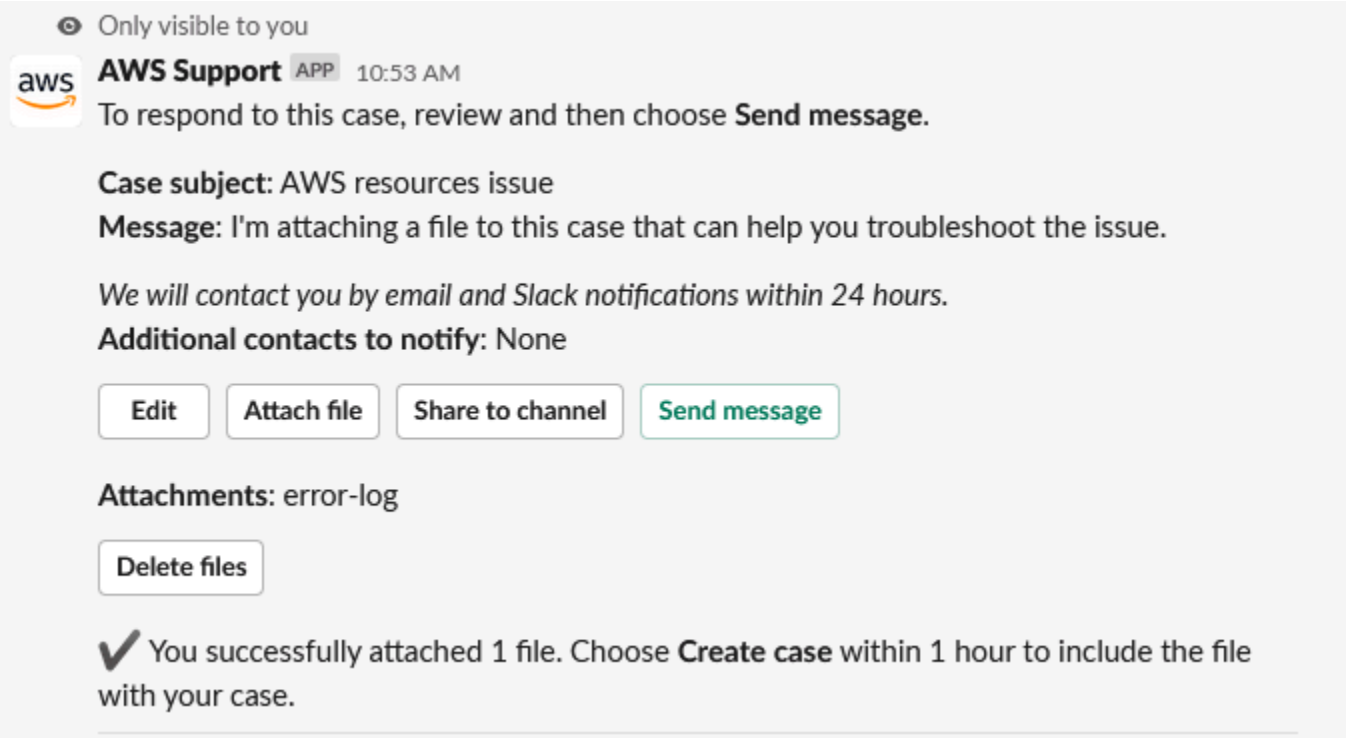
1. Di saluran Slack, pilih kasus yang ingin Anda membalas saluran Slack. Anda dapat masuk`/awssupport search` untuk menemukan kasus dukungan Anda.
2. Pilih Lihat detail di samping kasus yang Anda inginkan.
3. Di bagian bawah detail kasus, pilih membalas.

4. Di kotak dialog Balas kasus, masukkan deskripsi singkat tentang masalah di bidang Pesan. Kemudian pilih Selanjutnya.



5. Pilih metode kontak Anda. Metode kontak yang tersedia bergantung pada jenis kasus dan rencana dukungan Anda.
6. (Opsional) Agar kontak tambahan dapat diberitahukan, masukkan alamat email tambahan yang ingin Anda terima pembaruan tentang kasus dukungan ini. Anda dapat menambahkan hingga 10 alamat email.
7. Pilih Tinjau. Anda kemudian dapat memilih apakah Anda ingin mengedit balasan, melampirkan file, atau berbagi ke saluran.
8. Saat Anda siap membalas membalas email.
9. (Opsional) Untuk melihat korespondensi sebelumnya untuk kasus Anda, pilih Korespondensi sebelumnya. Untuk melihat pesan singkat, pilih Tampilkan pesan lengkap.

Example : Membalas kasus di Slack



Bergabunglah dengan sesi obrolan langsung AWS Support

Saat Anda meminta obrolan langsung untuk kasus Anda, Anda memilih untuk menggunakan saluran obrolan baru atau utas di saluran saat ini untuk Anda dan AWS Support agen. Gunakan saluran obrolan atau utas ini untuk berkomunikasi dengan agen dukungan dan orang lain yang Anda undang ke obrolan langsung.

Important

Siapa pun yang bergabung dengan saluran dengan obrolan langsung dapat melihat detail tentang kasus dukungan spesifik dan riwayat obrolan. Ini adalah praktik terbaik untuk menambahkan hanya pengguna yang memerlukan akses ke kasus dukungan Anda. Setiap anggota saluran obrolan atau utas juga dapat berpartisipasi dalam obrolan aktif.

Note

Saluran dan utas obrolan langsung juga menerima pemberitahuan saat korespondensi ditambahkan ke kasing di luar sesi obrolan langsung. Ini terjadi sebelum, selama, dan setelah

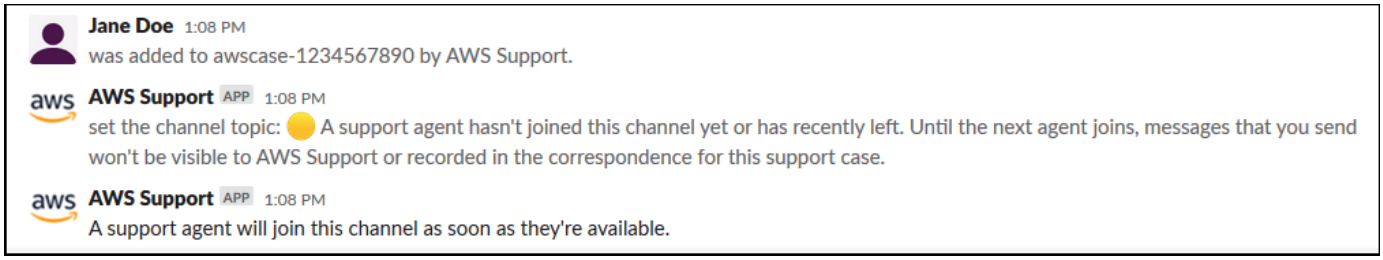
sesi obrolan, sehingga Anda dapat menggunakan saluran obrolan atau utas untuk memantau semua pembaruan kasus. Jika Anda memilih untuk menggunakan saluran obrolan baru, gunakan saluran konfigurasi yang Anda undang AWS Support Aplikasi untuk membalas korespondensi ini.

Untuk bergabung dengan sesi obrolan langsung dengan AWS Support di saluran baru

1. Di aplikasi Slack, navigasikan ke saluran yang dibuat AWS Support Aplikasi untuk Anda. Nama saluran menyertakan ID kasus dukungan Anda, seperti *awscase-1234567890*.

   > **Note**
   >
   > AWS Support Aplikasi menambahkan pesan yang disematkan ke saluran obrolan langsung yang berisi detail tentang kasus dukungan Anda. Dari pesan yang disematkan, Anda dapat mengakhiri obrolan atau menyelesaikan kasus. Anda dapat menemukan semua pesan yang disematkan di saluran ini dengan nama saluran.

2. Ketika agen dukungan bergabung dengan saluran, Anda dapat mengobrol tentang kasus dukungan Anda. Sampai agen dukungan bergabung dengan saluran, agen tidak akan melihat pesan dalam obrolan itu dan pesan tidak muncul dalam korespondensi kasus Anda.

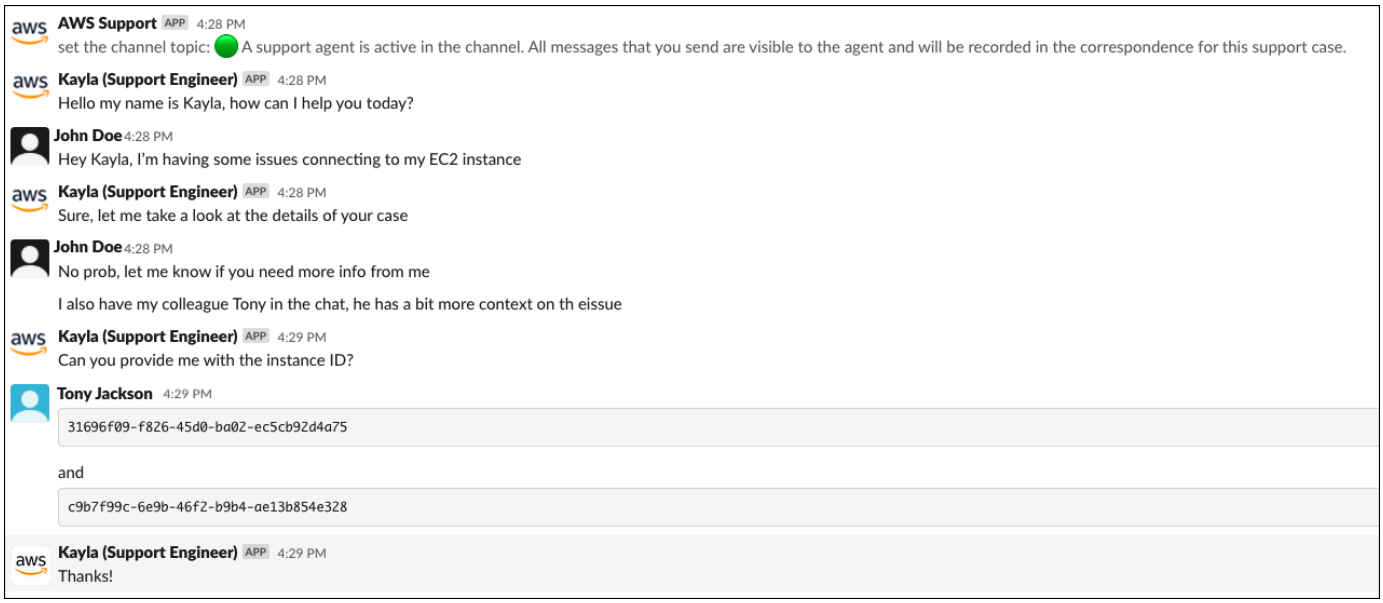
3. (Opsional) Tambahkan anggota lain ke saluran obrolan. Secara default, saluran obrolan bersifat pribadi.
4. Setelah agen dukungan bergabung dengan obrolan, saluran obrolan aktif dan AWS Support Aplikasi merekam obrolan.

   Anda dapat mengobrol dengan agen tentang kasus dukungan Anda dan mengunggah lampiran file apa pun ke saluran. AWS Support Aplikasi secara otomatis menyimpan file dan log obrolan Anda ke korespondensi kasus Anda.

> **Note**
>
> Saat Anda mengobrol dengan agen dukungan, perhatikan perbedaan berikut dalam Slack untuk AWS Support Aplikasi:
>
> - Agen Dukungan tidak dapat melihat pesan atau utas bersama. Untuk berbagi teks dari pesan atau utas, masukkan teks sebagai pesan baru.
> - Jika Anda mengedit atau menghapus pesan, agen masih melihat pesan asli. Anda harus memasukkan pesan baru Anda lagi untuk menampilkan revisi.

Example : Sesi obrolan langsung

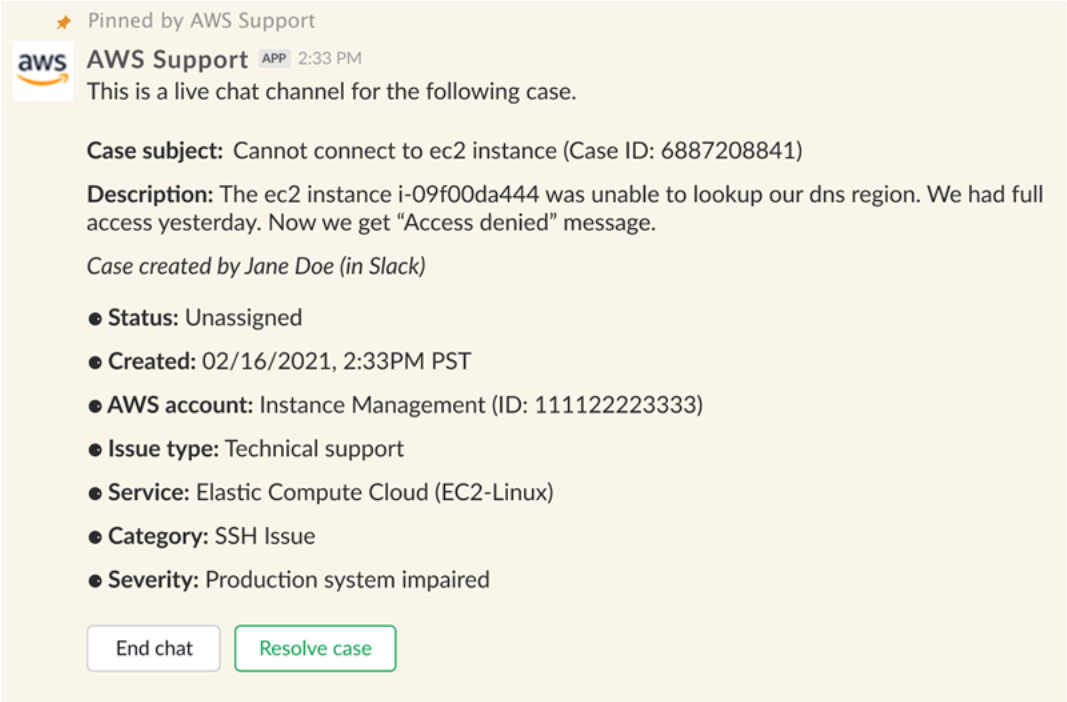
Berikut ini adalah contoh sesi obrolan langsung dengan agen dukungan untuk memperbaiki masalah konektivitas untuk dua instans Amazon Elastic Compute Cloud (Amazon EC2).



5. (Opsional) Untuk menghentikan obrolan langsung, pilih Akhiri obrolan. Agen dukungan meninggalkan saluran dan AWS Support Aplikasi berhenti merekam obrolan langsung. Anda dapat menemukan riwayat obrolan yang dilampirkan pada korespondensi kasus untuk kasus dukungan ini.
6. Jika masalah teratasi, Anda dapat memilih Selesaikan kasus dari pesan yang disematkan atau masukkan `/awssupport resolve`.

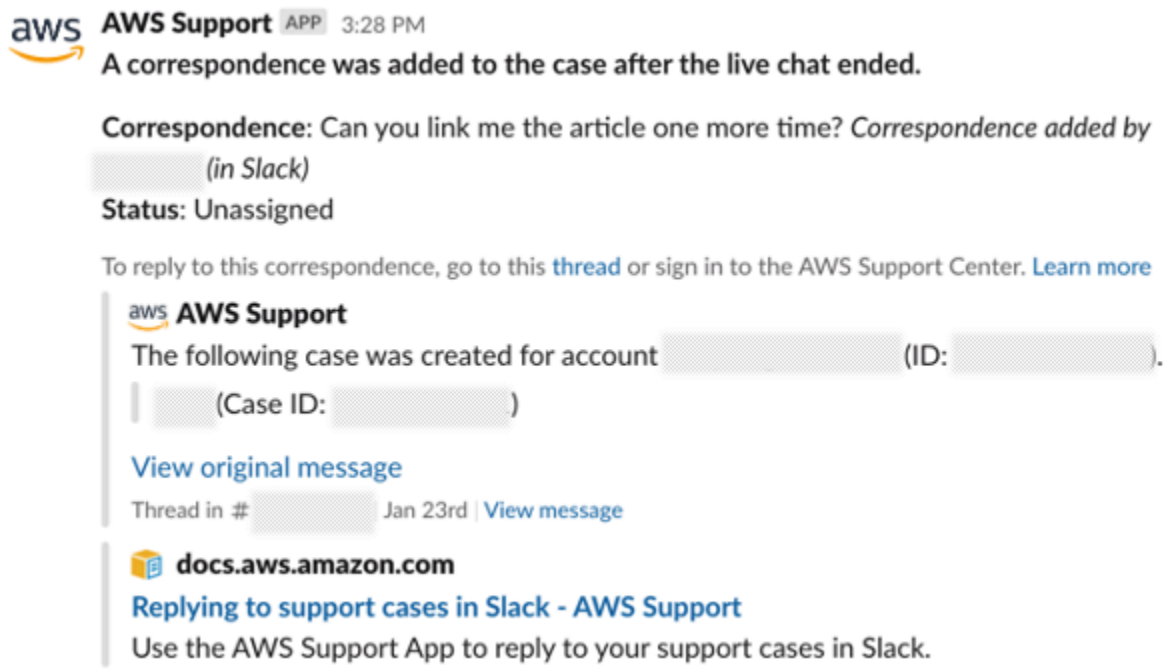
Example : Akhiri obrolan langsung

Pesan yang disematkan berikut menunjukkan detail kasus tentang instans Amazon EC2. Anda dapat menemukan pesan yang disematkan di bawah nama saluran Slack.



Example : Pemberitahuan korespondensi di saluran obrolan

Berikut ini adalah contoh saluran obrolan langsung yang menerima pemberitahuan saat kolaborator lain menambahkan pembaruan setelah obrolan berakhir.

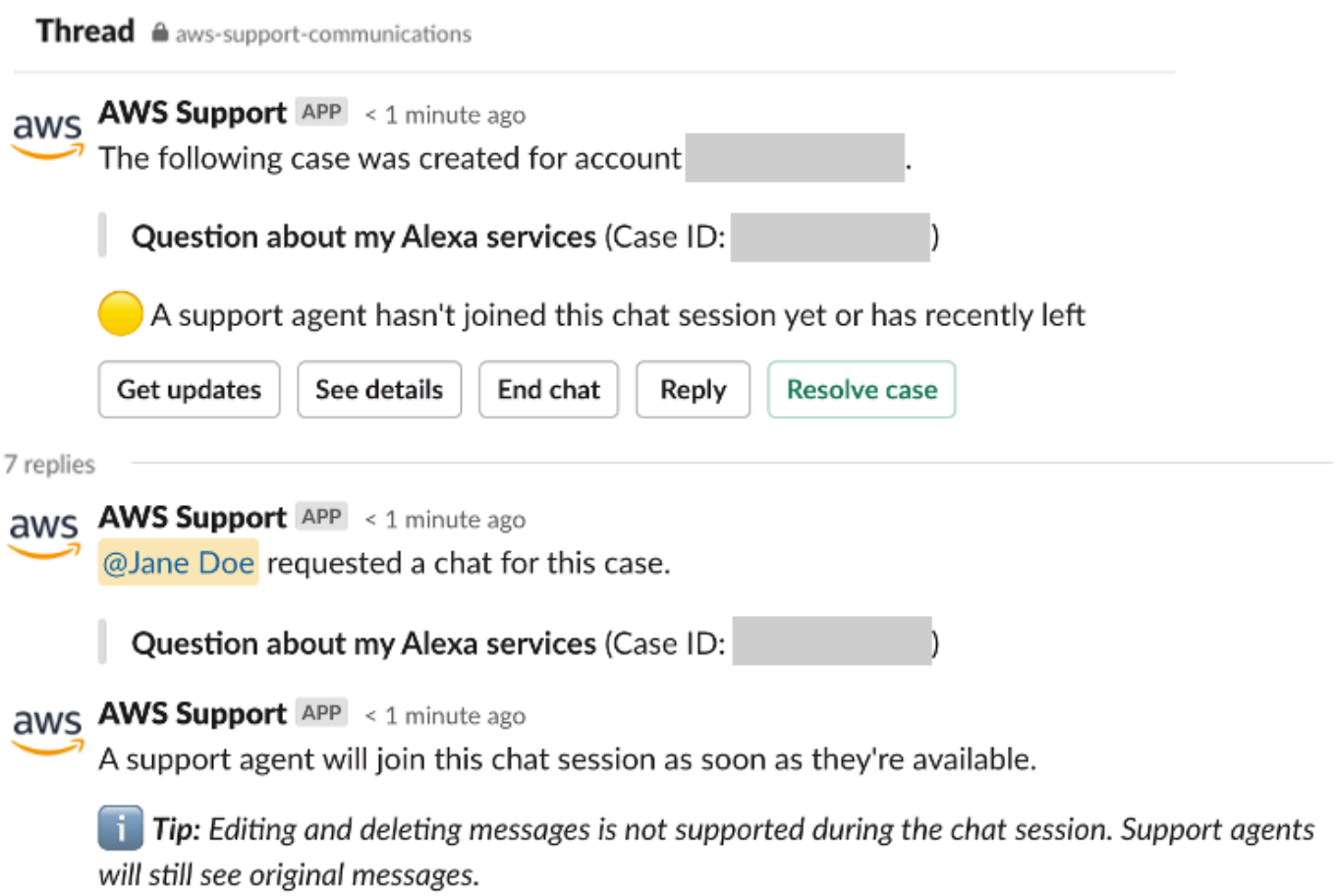


Pemberitahuan akan menunjukkan status obrolan (diminta, sedang berlangsung, atau berakhir) dan apakah korespondensi ditambahkan oleh agen atau oleh kolaborator lain. Aplikasi Support juga akan mencoba menautkan kembali ke thread atau saluran Slack asli tempat obrolan ini diminta. Anda dapat membalas kasus ini dari saluran itu, atau saluran lain dengan akses ke kasus ini.

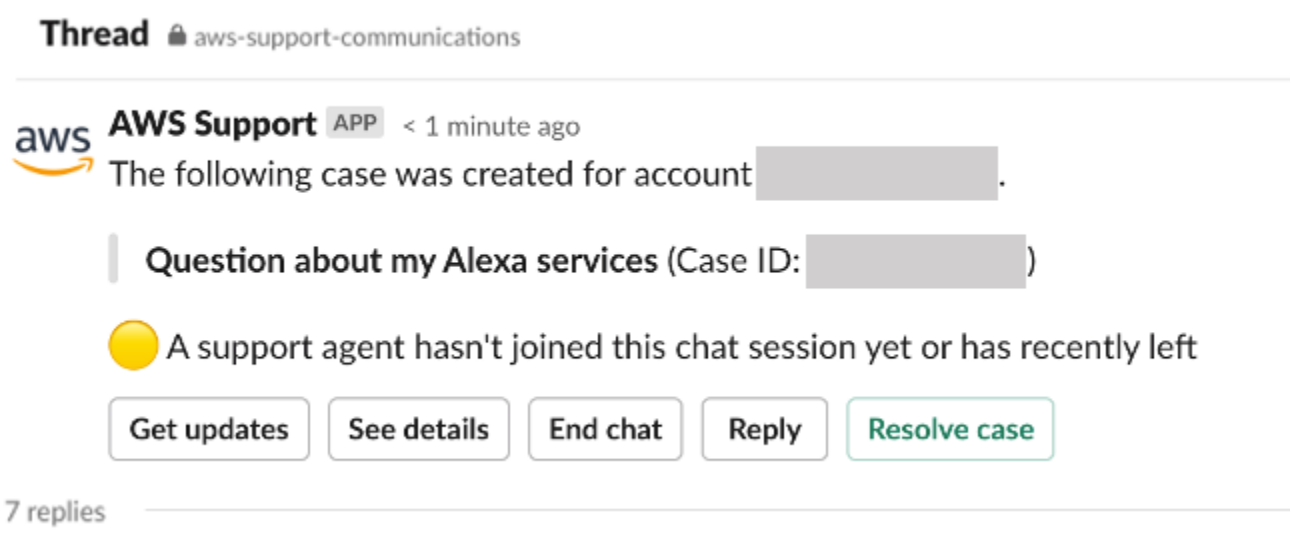
Untuk bergabung dengan sesi obrolan langsung dengan AWS Support di saluran saat ini

1. Di aplikasi Slack, navigasikan ke utas di saluran saat ini yang digunakan AWS Support Aplikasi untuk obrolan. Dalam kebanyakan kasus, ini akan menjadi utas yang dimulai saat kasus pertama kali dibuat.
2. Ketika agen dukungan bergabung dengan utas, Anda dapat mengobrol tentang kasus dukungan Anda. Sampai agen dukungan bergabung dengan thread, agen tidak akan melihat pesan di thread itu, dan pesan tidak akan muncul dalam korespondensi kasus Anda ketika obrolan berakhir.

> **Note**
>
> Pesan yang dikirim ke saluran ini di luar utas obrolan tidak pernah dilihat oleh AWS Support, bahkan saat obrolan aktif.



3. (Opsional) Tandai anggota saluran lain untuk memberi tahu mereka di utas obrolan.
4. Setelah agen dukungan bergabung dengan obrolan, utas obrolan aktif dan AWS Support Aplikasi merekam obrolan. Mirip dengan opsi saluran obrolan baru, Anda dapat mengobrol dengan agen tentang kasus dukungan Anda dan mengunggah lampiran file apa pun ke utas. AWS Support Aplikasi secara otomatis menyimpan file dan log obrolan Anda ke korespondensi kasus Anda.
5. (Opsional) Untuk menghentikan obrolan langsung, pilih Akhiri obrolan dari pesan awal untuk utas ini. Agen dukungan meninggalkan utas dan AWS Support Aplikasi berhenti merekam obrolan langsung. Anda dapat menemukan riwayat obrolan yang dilampirkan pada korespondensi kasus untuk kasus dukungan ini.
6. Jika masalah teratasi, Anda dapat memilih Selesaikan kasus dari pesan awal untuk utas ini.



Mencari kasus dukungan di Slack

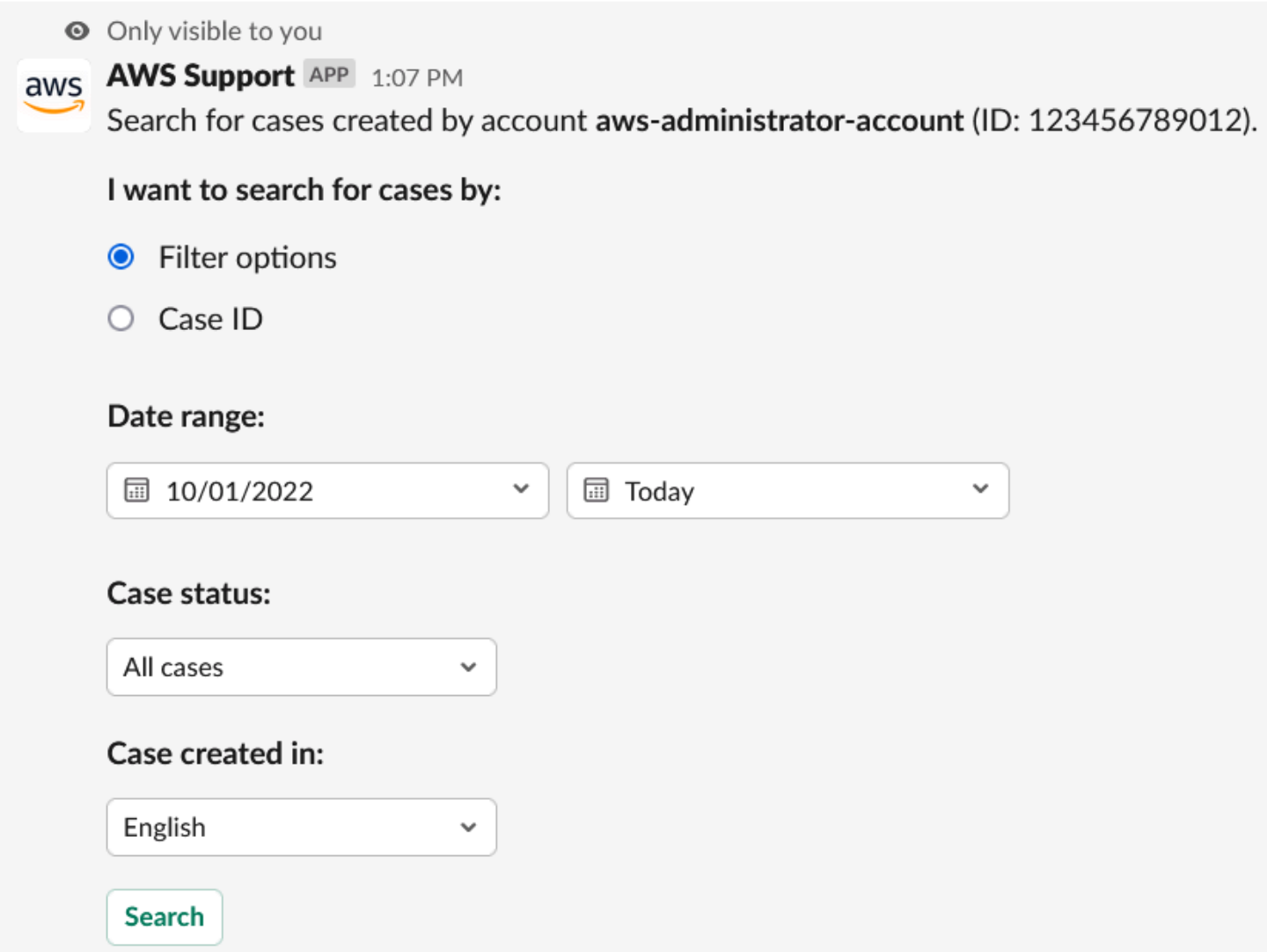
Dari saluran Slack, Anda dapat mencari kasus dukungan dariAkun AWS dan dari akun lain yang mengonfigurasi saluran dan ruang kerja yang sama. Misalnya, jika akun Anda (123456789012) dan akun rekan kerja Anda (111122223333) telah mengonfigurasi ruang kerja dan saluran yang sama diAWS Support Center Console, Anda dapat menggunakanAWS Support Aplikasi untuk mencari kasus dukungan satu sama lain.

Untuk memfilter hasil pencarian, Anda dapat menggunakan opsi berikut:

- ID Akun
- ID Kasus
- Status kasus
- Bahasa kontak bahasa kontak bahasa kontak bahasa
- Rentang tanggal

Example : Cari kasus di Slack

Contoh berikut menunjukkan cara mencari berdasarkan opsi Filter untuk satu akun dengan menentukan rentang tanggal, status kasus, dan bahasa kontak.



Untuk mencari kasus dukungan di Slack

1. Di saluran Slack, masukkan perintah berikut:

   ```
   /awssupport search
   ```

2. Untuk saya ingin mencari kasus dengan: pilihan, pilih salah satu dari berikut ini:

   A. Opsi filter - Anda dapat memfilter kasus dengan opsi berikut:

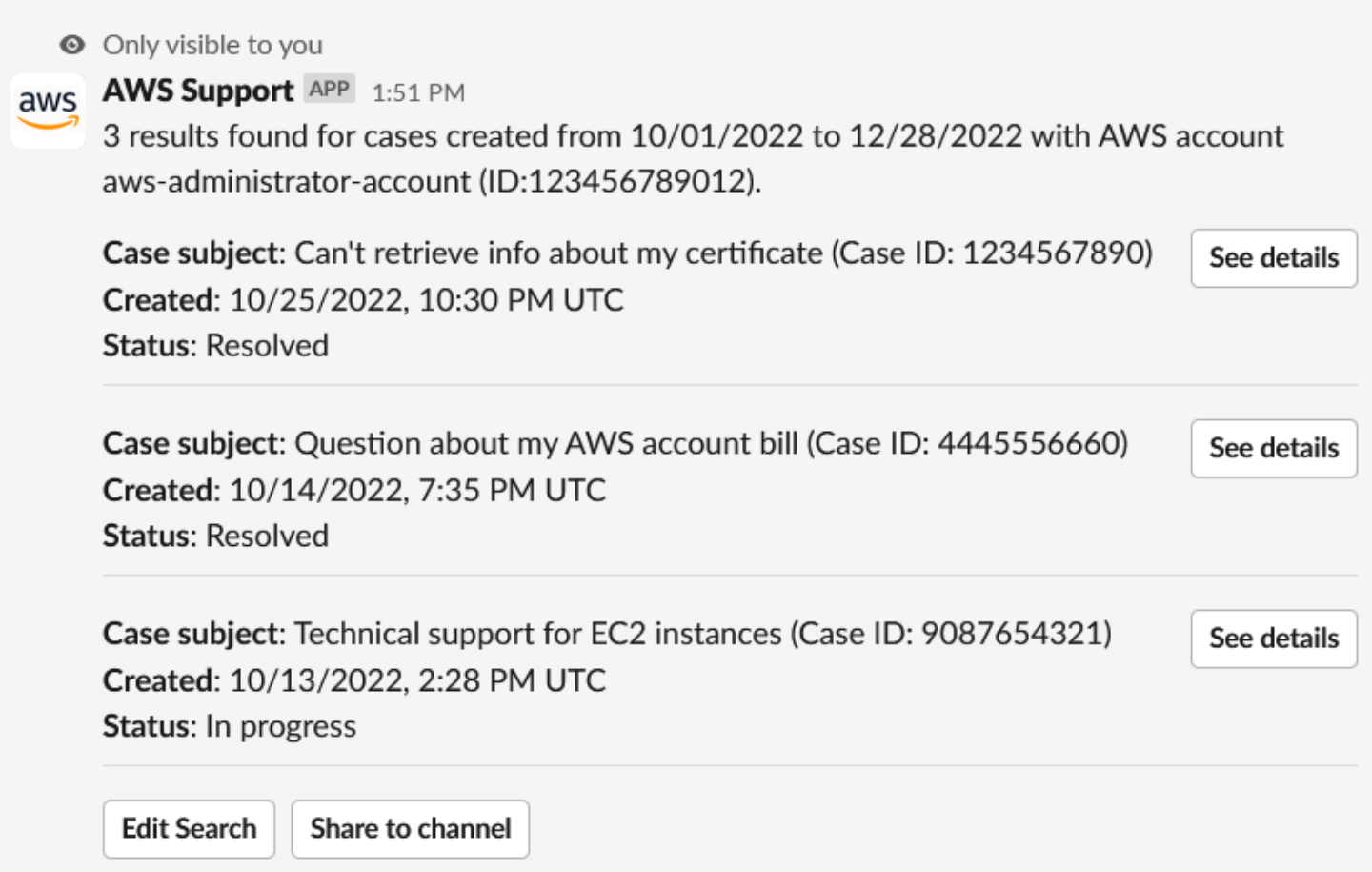
   - Akun AWS- Daftar ini hanya muncul jika Anda memiliki beberapa akun di saluran.
   - Rentang tanggal - Tanggal kasus dibuat.
   - Status kasus - Status kasus saat ini, seperti Semua kasus terbuka atau Terselesaikan.
   - Kasus dibuat di - Bahasa kontak untuk kasus ini.

B. ID Kasus - Masukkan ID kasus. Anda hanya dapat memasukkan satu ID kasus kasus pada satu waktu. Jika Anda memiliki beberapa akun di saluran, pilihAkun AWS untuk mencari kasus ini.

3. Pilih Cari. Hasil pencarian akan muncul di Slack.

Menggunakan hasil hasil pencarian Anda. Gunakan hasil pencarian Anda.

Contoh berikut mengembalikan tiga kasus dukungan dari satuAkun AWS.



Setelah menerima hasil pencarian, Anda dapat melakukan hal berikut:

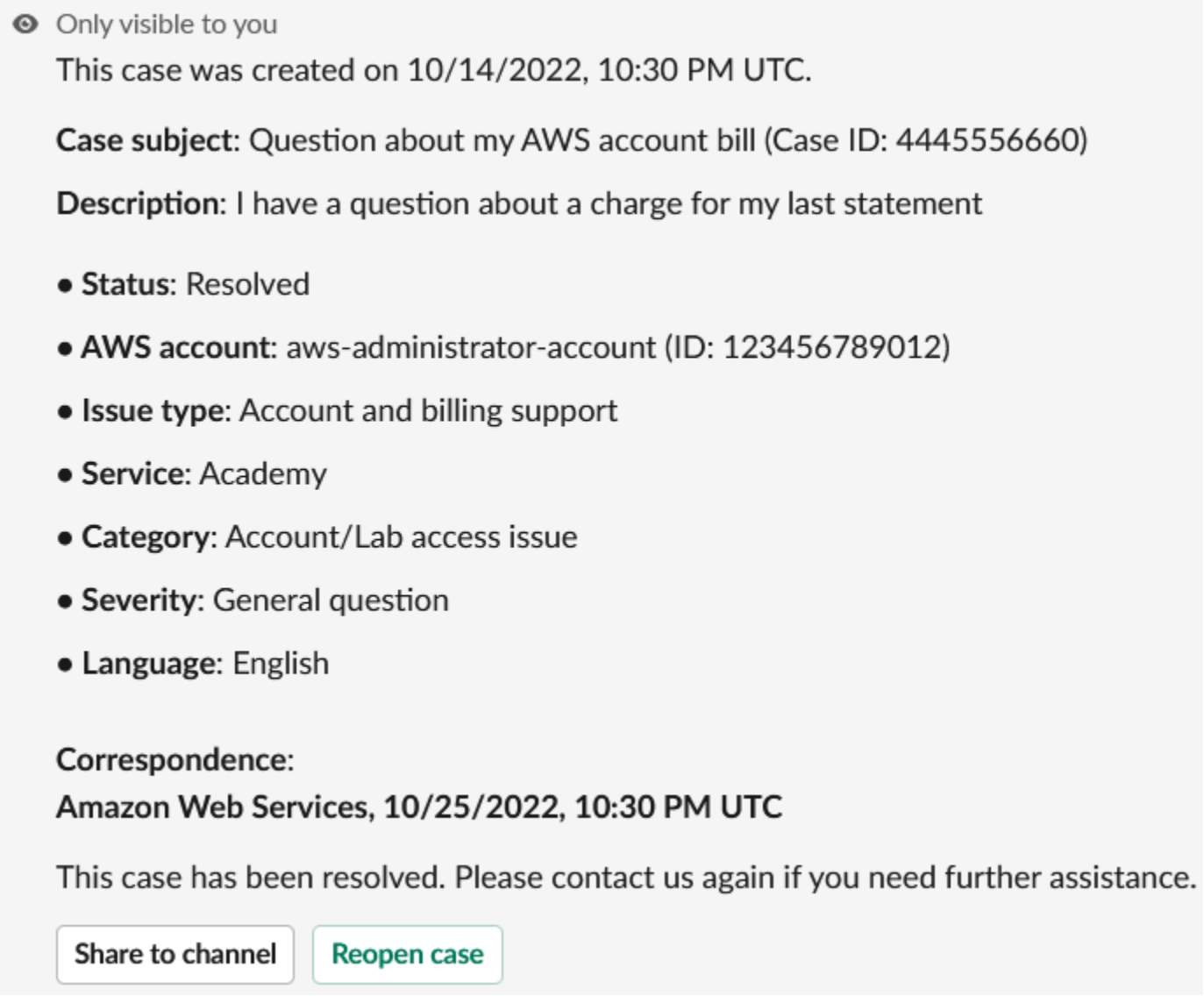
Untuk menggunakan hasil pencarian

1. Pilih Edit Pencarian untuk mengubah opsi filter atau ID kasus sebelumnya.
2. Pilih Bagikan ke saluran untuk membagikan hasil pencarian dengan saluran.
3. Pilih Lihat detail untuk informasi selengkapnya tentang suatu kasus. Anda dapat memilih Tampilkan pesan lengkap untuk melihat sisa korespondensi terbaru.

4. Jika Anda mencari berdasarkan opsi Filter, hasil pencarian dapat mengembalikan beberapa kasus. Pilih 5 hasil Berikutnya atau 5 hasil Sebelumnya untuk melihat 5 kasus berikutnya atau sebelumnya.

Example : kasus dukungan terselesaikan kasus dukungan terselesaikan kasus dukungan

Contoh berikut menunjukkan kasus dukungan yang diselesaikan untuk masalah akun dan penagihan setelah memilih Lihat detail.



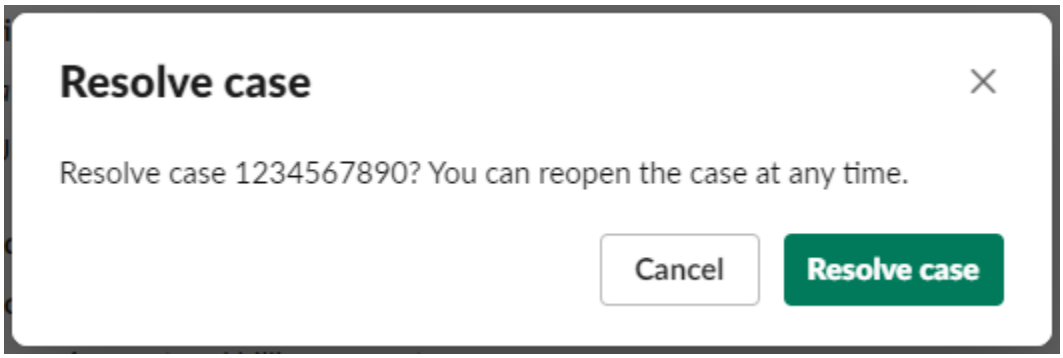
Menyelesaikan kasus dukungan dalam Slack

Jika Anda tidak memerlukan kasus dukungan Anda lagi, atau Anda memperbaiki masalah, Anda dapat menyelesaikan kasus dukungan langsung di Slack. Hal ini juga menyelesaikan kasus diAWS

Support Center Console. Setelah Anda menyelesaikan kasus, Anda dapat membuka kembali kasus ini nanti.

Untuk menyelesaikan kasus dukungan dalam Slack

1. Dalam saluran Slack, membuka kasus dukungan. Lihat Mencari kasus dukungan di Slack.
2. Pilih Lihat detail untuk kasus ini.
3. Pilih Resolve case (Selesaikan kasus).
4. Dalam Selesaikan kasus kotak dialog, pilih Selesaikan kasus. Anda dapat membuka kembali kasus di saluran Slack atau dari Konsol Pusat Support.

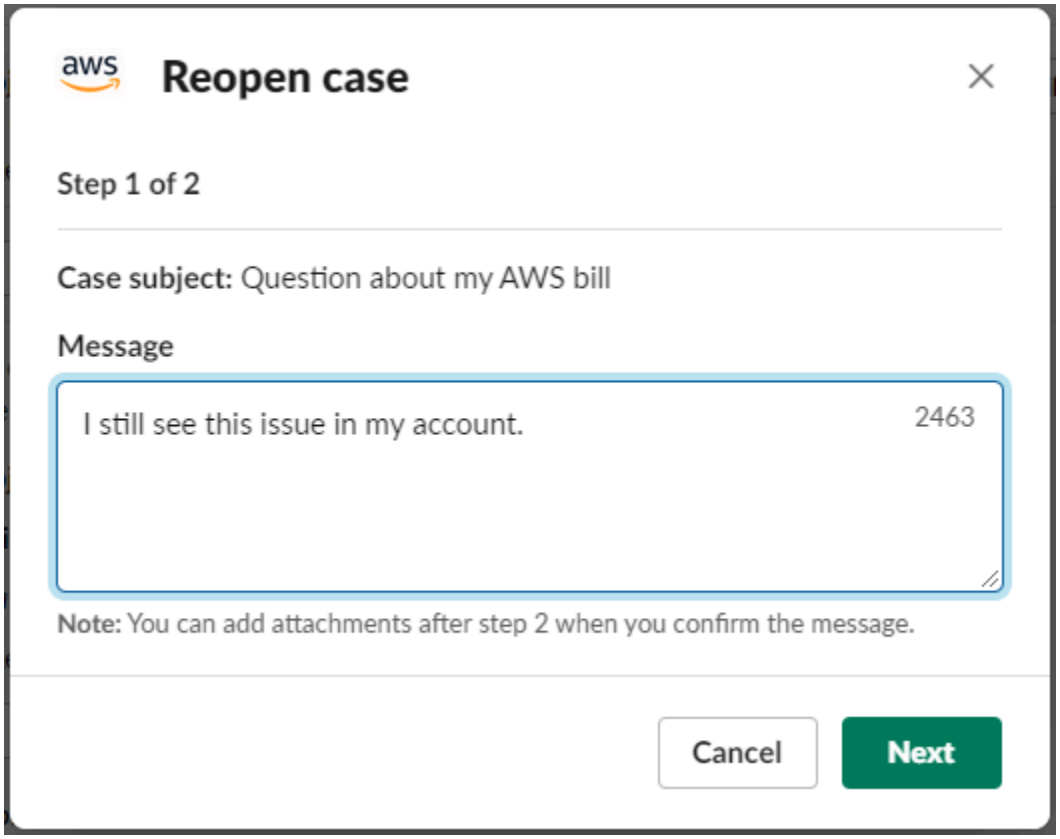


Membuka kembali kasus dukungan di Slack

Setelah Anda menyelesaikan kasus dukungan, Anda dapat membuka kembali kasus dari Slack.

Untuk membuka kembali kasus dukungan di Slack

1. Temukan kasus dukungan untuk dibuka kembali di Slack. Lihat Mencari kasus dukungan di Slack.
2. Pilih Lihat detail.
3. Pilih Reopen case (Buka lagi kasus).
4. Di kotak dialog kasus Buka kembali, masukkan deskripsi singkat tentang masalah di bidang Pesan.
5. Pilih Selanjutnya.



6. (Opsional) Masukkan kontak tambahan.
7. Pilih Tinjau.
8. Tinjau detail detail penggunaan Anda, lalu pilih Kirim. Kasus Anda dibuka kembali. Jika Anda meminta obrolan langsung baru dengan agen dukungan, Slack menggunakan saluran atau thread obrolan yang sama dengan yang digunakan untuk obrolan langsung sebelumnya. Jika Anda meminta obrolan langsung di saluran baru dan sejauh ini belum memilikinya, saluran obrolan baru akan terbuka. Jika Anda meminta obrolan langsung di saluran saat ini dan sejauh ini belum memilikinya, utas di saluran saat ini digunakan.

Meminta kenaikan kuota layanan

Anda dapat meminta kenaikan kuota layanan untuk akun Anda dari saluran Slack Anda.

Untuk permintaan kuota layanan meningkat

1. Di saluran Slack, masukkan perintah berikut:

```
/awssupport quota
```

2. Di kotak dialog Tambah (beberapa) ARN, masukkan informasi berikut:

    a. Pilih Akun AWS.

    b. Pilih Wilayah AWS.

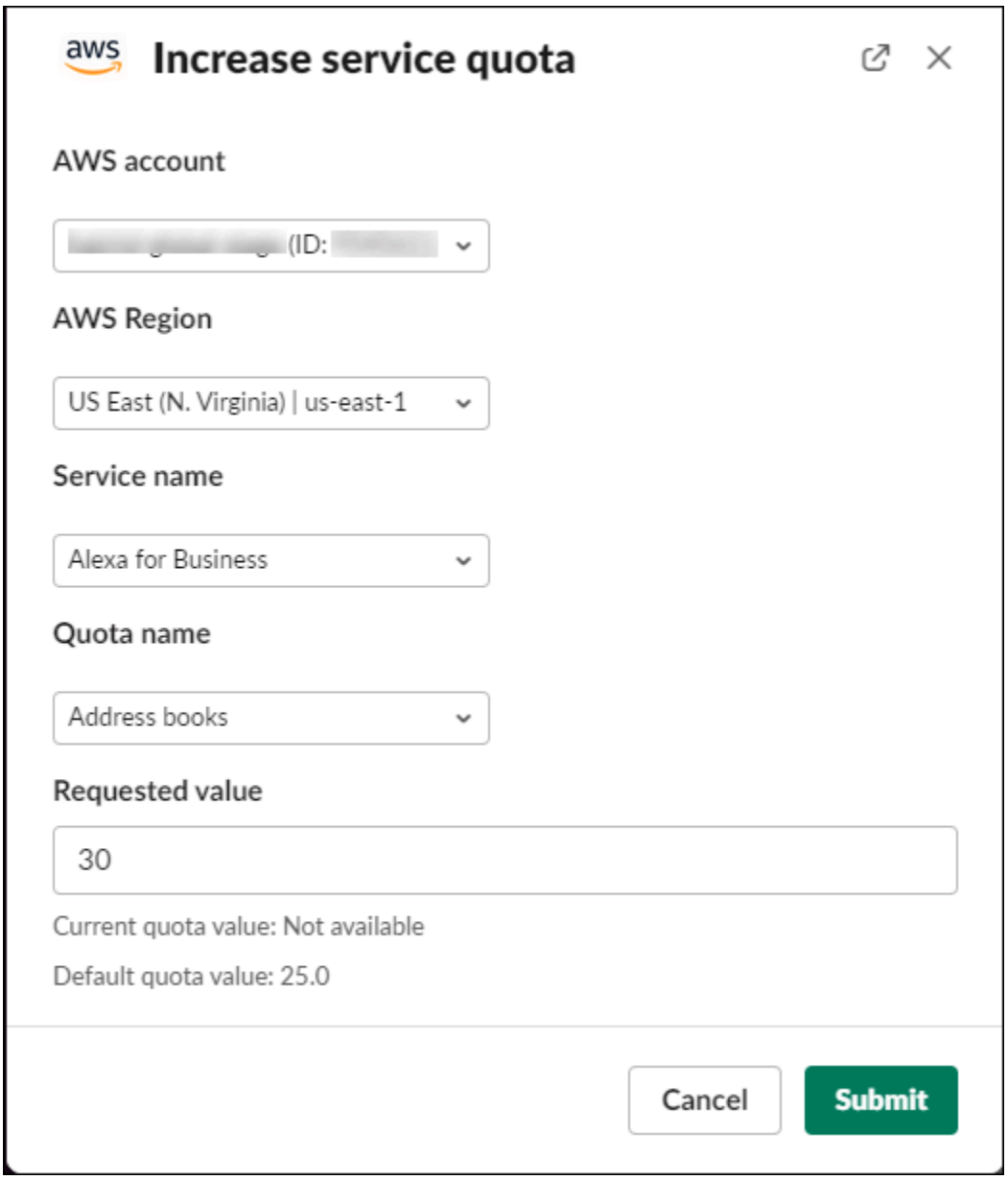
    c. Pilih nama Layanan.

    d. Pilih nama Kuota.

    e. Masukkan nilai yang Diminta untuk kenaikan kuota. Anda harus memasukkan nilai yang lebih besar dari kuota default.

3. Pilih Submit (Kirim).

Example : Kenaikan kuota untuk Alexa for Business



Anda juga dapat melihat permintaan dari konsol Service Quotas. Untuk informasi lebih lanjut, lihat Meminta peningkatan kuota di Panduan Pengguna Service Quotas.

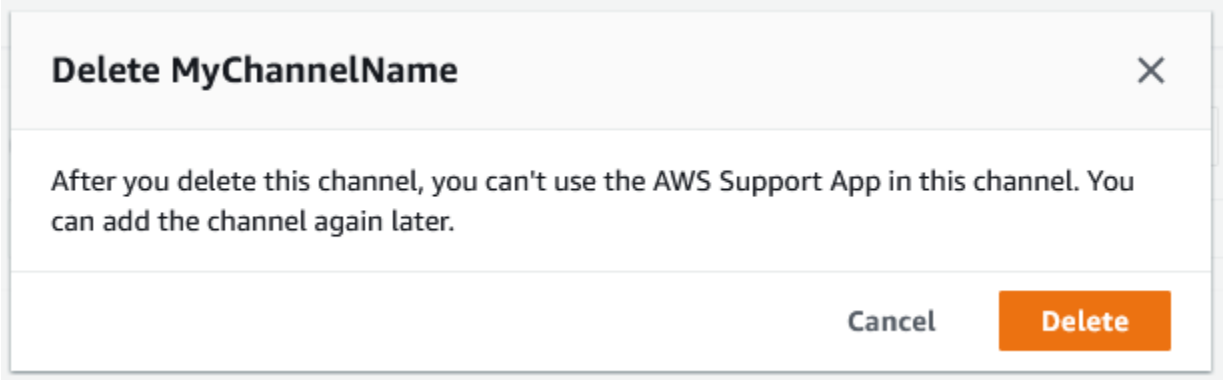
Menghapus konfigurasi saluran Slack dariAWS Support Aplikasi

Anda dapat menghapus konfigurasi saluran dariAWS Support Aplikasi jika Anda tidak membutuhkannya. Tindakan ini hanya menghapus saluran dariAWS Support Aplikasi danAWS Support Center Console. Channel Anda tidak dihapus dari Slack.

Anda dapat menambahkan hingga 20 saluran untukAkun AWS aplikasi Jika Anda sudah mencapai kuota ini, Anda harus menghapus saluran sebelum dapat menambahkan yang lain.

Untuk menghapus konfigurasi saluran Slack

1. Masuk ke Konsol Pusat Support dan pilih konfigurasi Slack.
2. Pada halaman konfigurasi Slack, di bawah Saluran, pilih nama saluran, lalu pilih Hapus.
3. Dalam Hapus nama saluran kotak dialog, pilih Menghapus. Anda dapat menambahkan saluran ini keAWS Support Aplikasi lagi nanti.



Menghapus konfigurasi ruang kerja Slack dariAWS Support Aplikasi

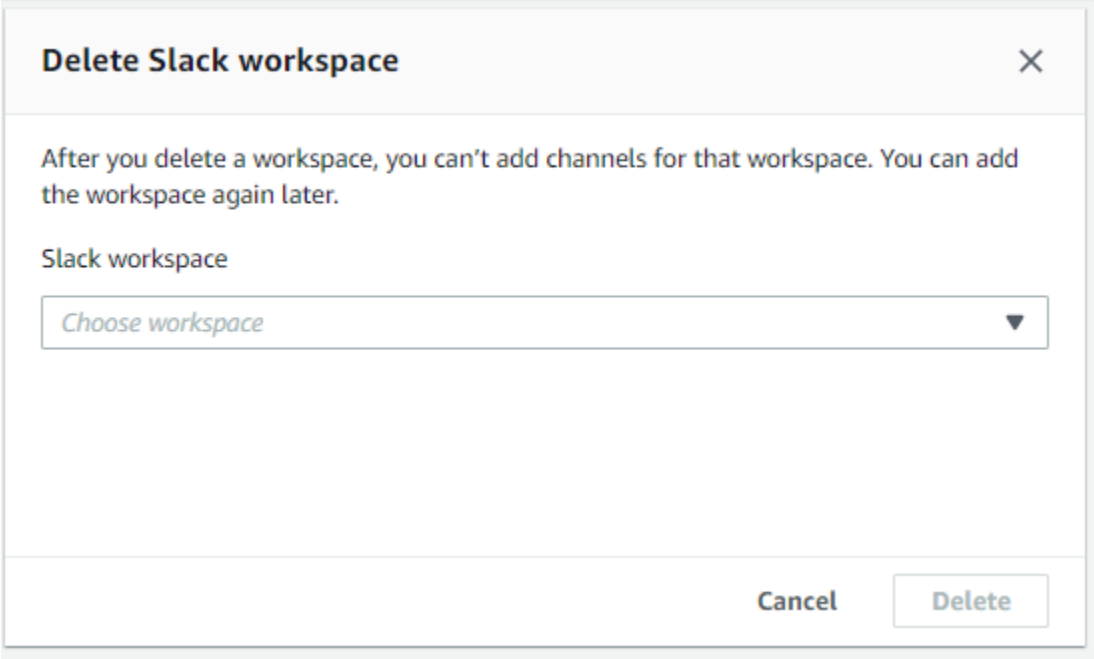
Anda dapat menghapus konfigurasi ruang kerja dariAWS Support Aplikasi jika Anda tidak membutuhkannya. Tindakan ini hanya menghapus ruang kerja dariAWS Support Aplikasi danAWS Support Center Console. Ruang kerja Anda tidak dihapus dari Slack.

Anda dapat menambahkan hingga 5 WorkspaceAkun AWS. Jika Anda sudah mencapai kuota ini, Anda harus menghapus ruang kerja Slack sebelum dapat menambahkan yang lain.

> **Note**
>
> Jika Anda menambahkan saluran dari ruang kerja ini keAWS Support Aplikasi, Anda harus menghapus saluran ini terlebih dahulu sebelum dapat menghapus ruang kerja. Lihat Menghapus konfigurasi saluran Slack dariAWS Support Aplikasi.

Untuk Untuk Untuk Untuk menghapus Workspace

1. Masuk ke AWS Support Center Consoledan pilih konfigurasi Slack.
2. Pada halaman konfigurasi Slack, di bawah ruang kerja Slack, pilih Hapus ruang kerja.
3. Di kotak dialog Delete Slack workspace, pilih nama workspace Slack, lalu pilih Delete. Anda dapat menambahkan ruang kerja keAkun AWS lagi nanti.



AWS SupportAplikasi dalam perintah Slack

Perintah saluran kendur

Anda dapat memasukkan perintah berikut di saluran Slack tempat Anda mengundangAWS Support Aplikasi. Nama saluran Slack ini juga muncul sebagai saluran yang dikonfigurasi diAWS Support Center Console.

`/awssupport create` atau `/awssupport create-case`

Membuat kasus dukungan.

`/awssupport search` atau `/awssupport search-case`

Mencari kasus. Anda dapat mencari kasus dukungan untukAkun AWS yang mengonfigurasiAWS Support Aplikasi untuk saluran Slack yang sama.

`/awssupport quota` atau `/awssupport service-quota-increase`

Minta peningkatan kuota layanan.

Perintah saluran obrolan langsung

Anda dapat memasukkan perintah berikut di saluran obrolan langsung. Ini adalah saluran yang dibuatAWS Support Aplikasi untuk Anda jika Anda memilih saluran baru untuk obrolan AndaAWS Support. Saluran obrolan menyertakan ID kasus dukungan Anda, seperti *awscase-1234567890*.

> **Note**
>
> Perintah berikut tidak tersedia saat menggunakan utas di saluran saat ini untuk obrolan langsung. Sebagai gantinya, gunakan tombol yang dilampirkan ke pesan thread awal untuk mengakhiri obrolan, mengundang agen baru, atau menyelesaikan kasus tersebut.

`/awssupport endchat`

Hapus agen dukungan dan akhiri sesi obrolan langsung.

`/awssupport invite`

Undang agen dukungan baru ke saluran ini.

`/awssupport resolve`

Selesaikan kasus dukungan ini.

Lihat korespondensiAWS Support Aplikasi diAWS Support Center Console

Saat membuat, memperbarui, atau menyelesaikan kasus Support untuk akun Anda di saluran Slack, Anda juga dapat masuk ke Konsol Pusat Dukungan untuk melihat kasus Anda. Anda dapat melihat korespondensi kasus untuk menentukan apakah kasus telah diperbarui di saluran Slack, melihat riwayat obrolan dengan agen dukungan, dan menemukan lampiran yang Anda unggah dari Slack.

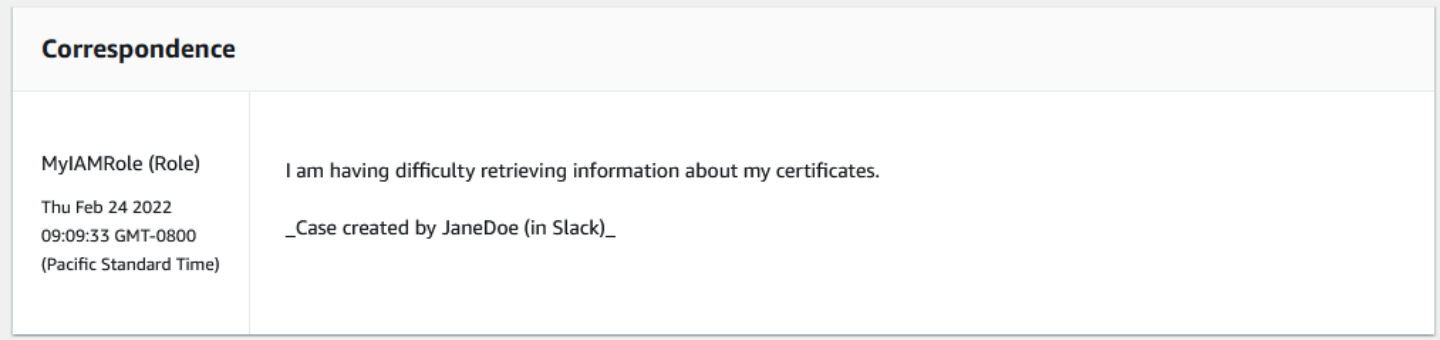
Untuk melihat korespondensi kasus dari Slack

1. Masuk ke akun AWS Support Center Consoleuntuk Anda.

2. Pilih kasus dukungan Anda.
3. Dalam Korespondensi, Anda dapat melihat apakah kasus itu dibuat dan diperbarui dari saluran Slack.

Example Kasus Support

Pada screenshot berikut, Jane Doe membuka kembali kasus dukungan di Slack. Tampaknya korespondensi ini muncul untuk kasus Support di Pusat Dukungan.



MembuatAWS Support Aplikasi di sumber daya Slack denganAWS CloudFormation

AWS SupportAplikasi di Slack terintegrasi denganAWS CloudFormation, layanan yang membantu Anda membuat model dan mengaturAWS sumber daya agar Anda dapat menghabiskan lebih sedikit waktu untuk membuat dan mengelola sumber daya dan infrastruktur Anda. Anda membuat templat yang menggambarkanAWS sumber daya yang Anda inginkan (seperti AndaAccountAlias danSlackChannelConfiguration), dan memasokAWS CloudFormation persediaan dan mengonfigurasi sumber daya tersebut untuk Anda.

Saat menggunakanAWS CloudFormation, Anda dapat menggunakan kembali templat Anda untuk menyiapkan sumber dayaAWS Support aplikasi secara konsisten dan berulang kali. Jelaskan sumber daya Anda satu kali, lalu sediakan sumber daya yang sama berulang kali dalam beberapa Akun AWS dan Wilayah.

AWS SupportAplikasi danAWS CloudFormation template

Untuk menyediakan dan mengonfigurasi sumber daya untukAWS Support Aplikasi dan layanan terkait, Anda harus memahami AWS CloudFormationtemplat. Templat adalah file teks dengan

format JSON atau YAML. Templat ini menjelaskan sumber daya yang ingin Anda sediakan di tumpukan AWS CloudFormation Anda. Jika Anda tidak terbiasa dengan JSON atau YAML, Anda dapat menggunakan AWS CloudFormation Designer untuk membantu Anda memulai dengan templat AWS CloudFormation. Untuk informasi selengkapnya, lihat Apa yang dimaksud dengan AWS CloudFormation Designer? dalam Panduan Pengguna AWS CloudFormation.

AWS SupportApp mendukung menciptakan AndaAccountAlias danSlackChannelConfiguration diAWS CloudFormation. Untuk informasi selengkapnya, termasuk contoh templat JSON dan YAKL untukSlackChannelConfiguration sumber dayaAccountAlias dan sumber daya daya aplikasi, lihat referensi tipe sumber dayaAWS Support app dalam PanduanAWS CloudFormation Pengguna Panduan Pengguna.

Membuat sumber daya konfigurasi Slack untuk organisasi Anda

Anda dapat menggunakanCloudFormation template untuk membuat sumber daya yang Anda butuhkan untukAWS Support Aplikasi. Jika Anda adalah akun manajemen untuk organisasi Anda, Anda dapat menggunakan template untuk membuat sumber daya ini untuk akun anggota AndaAWS Organizations.

Misalnya, Anda dapat menggunakan template untuk membuat konfigurasi ruang kerja Slack yang sama untuk semua akun di organisasi, tetapi kemudian menggunakan template terpisah untuk membuat konfigurasi saluran Slack yang berbeda untuk unit tertentuAkun AWS atau organisasi (oU). Anda juga dapat menggunakan template untuk membuat konfigurasi ruang kerja Slack sehingga akun anggota kemudian dapat mengkonfigurasi saluran Slack yang mereka inginkan untuk merekaAkun AWS.

Anda dapat memilih apakah akan menggunakanCloudFormation template atau tidak. Jika Anda tidak menggunakanCloudFormation template, Anda dapat menyelesaikan langkah-langkah manual berikut sebagai gantinya:

- Buat sumber dayaAWS Support App diAWS Support Center Console.
- Buat kasus dukunganAWS Support untuk mengotorisasi beberapa akun untuk menggunakanAWS Support Aplikasi.
- Panggil operasi RegisterSlackWorkspaceForOrganizationAPI untuk mendaftarkan ruang kerja Slack untuk akun Anda. CloudFormationTumpukan memanggil operasi API ini untuk Anda.

Ikuti prosedur ini untuk mengunggahCloudFormation template ke organisasi Anda. Anda dapat menggunakan contoh template dari halaman referensi jenis sumber dayaAWS Support App.

Template memberitahuCloudFormation untuk membuat sumber daya berikut:

- Konfigurasi saluran Slack.
- Konfigurasi ruang kerja Slack.
- Peran IAM dengan`AWSSupportSlackAppCFNRole` nama. Kebijakan yangAWSSupportAppFullAccessAWS dikelola dilampirkan.

Daftar Isi

PerbaruiCloudFormation template Anda untuk Slack

Untuk memulai, gunakan templat berikut untuk membuat tumpukan. Anda harus mengganti template dengan nilai yang valid untuk ruang kerja dan saluran Slack Anda.

> **Note**
>
> Kami tidak merekomendasikan penggunaan templat untuk membuatAccountAlias sumber daya untuk organisasi Anda. AccountAliasSumber daya mengidentifikasi secara unikAkun AWS diAWS Support Aplikasi. Akun anggota Anda dapat memasukkan nama akun di Konsol Pusat Support. Untuk informasi selengkapnya, lihat Otorisasi ruang kerja Slack.

Untuk memperbaruiCloudFormation template Anda untuk Slack

1. Jika Anda adalah akun manajemen untuk organisasi, Anda harus secara manual mengotorisasi ruang kerja Slack untuk akun Anda sebelum akun anggota dapat digunakanCloudFormation untuk membuat sumber daya. Jika Anda belum melakukannya, lihatOtorisasi ruang kerja Slack.
2. Dari halaman referensi jenis sumber dayaAWS Support App, salin template JSON atau YAKL untuk sumber daya yang Anda inginkan.
3. Di editor teks, tempel templat ke file baru.
4. Dalam template, tentukan parameter yang Anda inginkan. Minimal, ganti nilai untuk bidang berikut:

- `TeamId`dengan ID ruang kerja Slack Anda
- `ChannelId`dengan ID saluran Slack
- `ChannelName`dengan nama untuk mengidentifikasi konfigurasi saluran Slack

> **Tip**
>
> Untuk menemukan ruang kerja dan ID saluran, buka saluran Slack Anda di browser. Di URL, ID ruang kerja Anda adalah pengidentifikasi pertama dan ID saluran adalah yang kedua. Misalnya, dihttps://app.slack.com/client/T012ABCDEFG/C01234A5BCD, T012ABCDEFG adalah ID ruang kerja dan C01234A5BCD adalah ID saluran.

5. Simpan file sebagai file JSON atau YAKL.

Buat tumpukan untuk akun manajemen

Selanjutnya, Anda harus membuat tumpukan untuk akun manajemen di organisasi. Langkah ini memanggil operasi RegisterSlackWorkspaceForOrganizationAPI untuk Anda dan mengotorisasi ruang kerja dengan Slack.

> **Note**
>
> Kami menyarankan Anda mengunggah template konfigurasi ruang kerja Slack yang Anda perbarui di prosedur sebelumnya untuk akun manajemen. Anda tidak perlu mengupload template konfigurasi saluran Slack kecuali Anda juga mengonfigurasi akun manajemen untuk menggunakanAWS Support Aplikasi.

Untuk membuat tumpukan untuk akun manajemen

1. Masuk ke akunAWS Management Console sebagai manajemen untuk organisasi Anda.
2. Buka AWS CloudFormation konsol di https://console.aws.amazon.com/cloudformation.
3. Jika belum, di Region selector (Pemilih wilayah), pilih salah satu dari yang berikutWilayah AWS:

   - Europe (Frankfurt)
   - Europe (Ireland)
   - Europe (London)

- AS Timur (N. Virginia)
- US East (Ohio)
- US West (Oregon)
- Asia Pacific (Singapore)
- Asia Pacific (Tokyo)
- (Canada (Central)

4. Ikuti prosedur untuk membuat tumpukan. Untuk informasi selengkapnya, lihat Membuat tumpukan diAWS CloudFormation konsol.

   SetelahCloudFormation berhasil membuat tumpukan, Anda dapat menggunakan template yang sama untuk membuat kumpulan tumpukan untuk organisasi Anda.

Buat set set set set set set set set set set set set set untuk organisasi Anda

Selanjutnya, gunakan template yang sama untuk konfigurasi ruang kerja Slack untuk membuat set tumpukan dengan`service-managed` izin. Anda dapat menggunakan set tumpukan untuk membuat tumpukan untuk seluruh organisasi Anda atau menentukan OU yang Anda inginkan. Untuk informasi selengkapnya, lihat Buat set set set set set set set set set set set.

Prosedur ini juga memanggil operasi RegisterSlackWorkspaceForOrganizationAPI untuk Anda. Operasi API ini mengotorisasi ruang kerja dengan Slack untuk akun anggota.

Membuat kumpulan tumpukan untuk organisasi Anda

1. Masuk ke akunAWS Management Console sebagai manajemen untuk organisasi Anda.
2. Buka AWS CloudFormation konsol di https://console.aws.amazon.com/cloudformation.
3. Jika belum, di Region selector (Pemilih wilayah), pilih yang sama denganWilayah AWS yang telah Anda gunakan di prosedur sebelumnya.
4. Di panel navigasi, pilih panel navigasi panel navigasi panel navigasi, pilih StackSets.
5. Pilih BuatStackSet.
6. Pada halaman Pilih template, simpan opsi default untuk opsi berikut:

   - Untuk Izin, simpan izin yang dikelola Layanan.
   - Untuk Prasyarat - Siapkan template, simpan Template sudah siap.

7. Di bawah Tentukan template, pilih Unggah file template, lalu pilih Pilih file.

8. Pilih file dan kemudian pilih Berikutnya.
9. Pada halaman TentukanStackSet detail, masukkan nama tumpukan seperti**`support-app-slack-workspace`**, masukkan deskripsi, lalu pilih Berikutnya.
10. Pada halaman KonfigurasiStackSet opsi, simpan opsi default dan kemudian pilih Berikutnya.
11. Pada halaman Atur opsi penyebaran, untuk Tambahkan tumpukan ke set tumpukan, simpan opsi Deploy tumpukan baru default.
12. Untuk target Deployment, pilih apakah Anda ingin membuat tumpukan untuk seluruh organisasi atau OU tertentu. Jika Anda memilih OU, masukkan ID OU.
13. Untuk Tentukan wilayah, masukkan hanya satu dari yang berikut iniWilayah AWS:

    - Europe (Frankfurt)
    - Europe (Ireland)
    - Europe (London)
    - AS Timur (N. Virginia)
    - US East (Ohio)
    - US West (Oregon)
    - Asia Pacific (Singapore)
    - Asia Pacific (Tokyo)
    - (Canada (Central)

    > Catatan:
    >
    > - Untuk menyederhanakan alur kerja Anda, sebaiknya gunakan yang samaWilayah AWS dengan yang telah Anda pilih di langkah 3.
    > - Memilih lebih dari satuWilayah AWS dapat menyebabkan konflik dengan membuat tumpukan Anda.

14. Untuk opsi Deployment, untuk Toleransi kegagalan - opsional, masukkan jumlah akun di mana tumpukan dapat gagal sebelumCloudFormation menghentikan operasi. Kami menyarankan Anda memasukkan jumlah akun yang ingin Anda tambahkan, minus satu. Misalnya, jika OU yang Anda tentukan memiliki 10 akun anggota, masukkan 9. Ini berarti bahwa bahkan jikaCloudFormation gagal operasi 9 kali, setidaknya satu akun akan berhasil.
15. Pilih Selanjutnya.

16. Pada halaman Tinjau, tinjau opsi Anda, lalu pilih Kirim. Anda dapat memeriksa status tumpukan Anda pada tab Stack instances.
17. (Opsional) Ulangi prosedur ini untuk mengupload template untuk konfigurasi saluran Slack. Contoh template juga membuat peran IAM dan melampirkan kebijakanAWS terkelola. Peran ini memiliki izin yang diperlukan untuk mengakses layanan lain untuk Anda. Untuk informasi selengkapnya, lihat Mengelola akses keAWS Support Aplikasi.

    Jika Anda tidak membuat set tumpukan untuk membuat konfigurasi saluran Slack, akun anggota Anda dapat mengonfigurasi saluran Slack secara manual. Untuk informasi selengkapnya, lihat Mengkonfigurasi saluran Slack.

SetelahCloudFormation membuat tumpukan, setiap akun anggota dapat masuk ke Konsol Pusat Support dan menemukan ruang kerja dan saluran Slack yang dikonfigurasi. Mereka kemudian dapat menggunakanAWS Support Aplikasi untuk merekaAkun AWS. Lihat Membuat kasus dukungan di saluran Slack.

> **Tip**
>
> Jika Anda perlu mengunggah templat baru, sebaiknya gunakan templat yang baru, sebaiknya gunakan templatWilayah AWS yang telah Anda tentukan sebelumnya.

Pelajari selengkapnya tentang CloudFormation

Untuk mempelajari selengkapnya tentang CloudFormation, lihat sumber daya berikut:

- AWS CloudFormation
- AWS CloudFormationPanduan Pengguna
- AWS CloudFormationReferensi API
- AWS CloudFormationPanduan Pengguna Baris Baris Perintah Baris Perintah Bar

Buat sumber dayaAWS Support Aplikasi dengan menggunakan Terraform

Anda juga dapat menggunakan Terraform untuk membuat sumber dayaAWS Support App untuk AndaAkun AWS. Terraform adalahinfrastructure-as-code alat yang dapat Anda gunakan untuk aplikasi cloud Anda. Anda dapat menggunakan Terraform untuk membuat sumber dayaAWS Support Aplikasi alih-alih menerapkanCloudFormation tumpukan ke akun.

Setelah Anda menginstal Terraform, Anda dapat menentukan sumber dayaAWS Support App yang Anda inginkan. Terraform memanggil operasi RegisterSlackWorkspaceForOrganizationAPI untuk mendaftarkan ruang kerja Slack untuk Anda dan membuat sumber daya Anda. Anda kemudian dapat masuk ke Konsol Pusat Support dan menemukan ruang kerja dan saluran Slack yang dikonfigurasi.

> **Catatan**
>
> - Jika Anda adalah akun manajemen untuk organisasi, Anda harus secara manual mengotorisasi ruang kerja Slack untuk akun Anda sebelum akun anggota Anda dapat menggunakan Terraform untuk membuat sumber daya. Jika Anda belum melakukannya, lihatOtorisasi ruang kerja Slack.
> - Tidak seperti kumpulanCloudFormation tumpukan, Anda tidak dapat menggunakan Terraform untuk membuat resourceAWS Support Aplikasi untuk OU di organisasi Anda.
> - Anda juga dapat menemukan riwayat acara untuk pembaruan ini dari Terraform diAWS CloudTrail. `eventSource`Untuk acara ini akan`cloudcontrolapi.amazonaws.com` dan`supportapp.amazonaws.com`. Untuk informasi selengkapnya, lihat LoggingAWS Support App di Slack API panggilan menggunakanAWS CloudTrail.

Pelajari selengkapnya

Untuk mempelajari selengkapnya tentang Terraform, lihat topik berikut:

- Instalasi Terraform
- Terraform tutorial: Membangun infrastruktur untukAWS
- `awscc_support_app_account_alias`
- `awscc_supportapp_slack_workspace_configuration`
- `awscc_supportapp_slack_channel_configuration`

Keamanan di AWS Support

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 . Untuk mempelajari tentang program kepatuhan yang berlaku AWS Support, lihat AWS layanan dalam cakupan berdasarkan program kepatuhan .
- Keamanan di cloud — Tanggung jawab Anda ditentukan oleh AWS layanan 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 membantu Anda memahami cara menerapkan model tanggung jawab bersama saat menggunakan AWS Support. Topik berikut menunjukkan cara mengonfigurasi AWS Support untuk memenuhi tujuan keamanan dan kepatuhan Anda. Anda juga mempelajari cara menggunakan Amazon Web Services lain yang membantu Anda memantau dan mengamankan AWS Support sumber daya Anda.

Topik

Perlindungan data di AWS Support

Model tanggung jawab AWS bersama model berlaku untuk perlindungan data di AWS Support. 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 Layanan AWS 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 logging aktivitas pengguna dengan AWS CloudTrail.
- Gunakan solusi AWS enkripsi, bersama dengan semua kontrol keamanan default di dalamnya Layanan AWS.
- 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 AWS Support atau lainnya Layanan AWS 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.

Keamanan untuk AWS Support kasus Anda

Ketika Anda membuat kasus dukungan, Anda memiliki informasi yang Anda sertakan dalam kasus dukungan Anda. AWS tidak mengakses Akun AWS data Anda tanpa izin Anda. AWS tidak membagikan informasi Anda dengan pihak ketiga.

Saat Anda membuat kasus dukungan, perhatikan hal berikut:

- AWS Support menggunakan izin yang ditentukan dalam peran `AWSServiceRoleForSupport` terkait layanan untuk memanggil orang lain Layanan AWS yang memecahkan masalah pelanggan untuk Anda. Untuk informasi selengkapnya, lihat Menggunakan peran terkait layanan untuk AWS Support dan kebijakan AWS terkelola:. AWSSupportServiceRolePolicy
- Anda dapat melihat panggilan API ke panggilan AWS Support yang terjadi di Anda Akun AWS. Misalnya, Anda dapat melihat informasi log ketika seseorang di akun Anda membuat atau menyelesaikan kasus dukungan. Untuk informasi selengkapnya, lihat Logging panggilan AWS Support API dengan AWS CloudTrail.
- Anda dapat menggunakan AWS Support API untuk memanggil `DescribeCases` API. API ini mengembalikan informasi kasus dukungan, seperti ID kasus, tanggal pembuatan dan penyelesaian, dan korespondensi dengan agen dukungan. Anda dapat melihat detail kasus hingga 12 bulan setelah kasus dibuat. Untuk informasi selengkapnya, lihat DescribeCasesdi Referensi AWS Support API.
- Kasus dukungan Anda mengikuti validasi Kepatuhan untuk AWS Support.
- Saat Anda membuat kasus dukungan, AWS tidak mendapatkan akses akun Anda. Jika perlu, agen pendukung menggunakan alat berbagi layar untuk melihat layar Anda dari jarak jauh dan mengidentifikasi serta memecahkan masalah. Alat ini hanya lihat. AWS Support tidak dapat bertindak untuk Anda selama sesi berbagi layar. Anda harus memberikan persetujuan untuk berbagi layar dengan agen dukungan. Untuk informasi lebih lanjut, lihat AWS Support FAQ.
- Anda dapat mengubah AWS Support paket Anda untuk mendapatkan bantuan yang Anda butuhkan untuk akun Anda. Untuk informasi selengkapnya, lihat Membandingkan AWS Support Paket dan Mengubah AWS Support paket Anda.

Manajemen identitas dan akses untuk AWS Support

AWS Identity and Access Management (IAM) adalah Layanan AWS yang membantu administrator mengontrol akses ke AWS sumber daya dengan aman. Administrator IAM mengontrol siapa yang dapat diautentikasi (masuk) dan diberi wewenang (memiliki izin) untuk menggunakan sumber daya. AWS Support IAM adalah Layanan AWS yang dapat Anda gunakan tanpa biaya tambahan.

Topik

Audiens

Cara Anda menggunakan AWS Identity and Access Management (IAM) berbeda, tergantung pada pekerjaan yang Anda lakukan. AWS Support

Pengguna layanan — Jika Anda menggunakan AWS Support layanan untuk melakukan pekerjaan Anda, maka administrator Anda memberi Anda kredensi dan izin yang Anda butuhkan. Saat Anda menggunakan lebih banyak AWS Support fitur untuk melakukan pekerjaan Anda, Anda mungkin memerlukan izin tambahan. Memahami cara mengelola akses dapat membantu Anda meminta izin yang tepat dari administrator Anda. Jika Anda tidak dapat mengakses fitur di AWS Support, lihat Memecahkan masalah AWS Support identitas dan akses.

Administrator layanan — Jika Anda bertanggung jawab atas AWS Support sumber daya di perusahaan Anda, Anda mungkin memiliki akses penuh ke AWS Support. Tugas Anda adalah

menentukan AWS Support fitur dan sumber daya mana yang harus diakses pengguna layanan Anda. Kemudian, Anda harus mengirimkan permintaan kepada administrator IAM untuk mengubah izin pengguna layanan Anda. Tinjau informasi di halaman ini untuk memahami konsep Basic IAM. Untuk mempelajari lebih lanjut tentang bagaimana perusahaan Anda dapat menggunakan IAM AWS Support, lihatBagaimana AWS Support bekerja dengan IAM.

Administrator IAM – Jika Anda adalah administrator IAM, Anda mungkin ingin belajar dengan lebih detail tentang cara Anda menulis kebijakan untuk mengelola akses ke AWS Support. Untuk melihat contoh kebijakan AWS Support berbasis identitas yang dapat Anda gunakan di IAM, lihat. AWS Support contoh kebijakan berbasis identitas

Mengautentikasi dengan identitas

Otentikasi adalah cara Anda masuk AWS menggunakan kredensi identitas Anda. Anda harus diautentikasi (masuk ke AWS) sebagai Pengguna root akun AWS, sebagai pengguna IAM, atau dengan mengasumsikan peran IAM.

Anda dapat masuk AWS sebagai identitas federasi dengan menggunakan kredensyal yang disediakan melalui sumber identitas. AWS IAM Identity Center Pengguna (IAM Identity Center), autentikasi masuk tunggal perusahaan Anda, dan kredensi Google atau Facebook Anda adalah contoh identitas federasi. Saat Anda masuk sebagai identitas terfederasi, administrator Anda sebelumnya menyiapkan federasi identitas menggunakan peran IAM. 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 masuk ke Panduan AWS Sign-In Pengguna Anda Akun AWS.

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

Apa pun metode autentikasi yang digunakan, Anda mungkin diminta untuk menyediakan informasi keamanan tambahan. Misalnya, AWS merekomendasikan agar Anda menggunakan otentikasi multi-faktor (MFA) untuk meningkatkan keamanan akun Anda. Untuk mempelajari selengkapnya, lihat

Autentikasi multi-faktor dalam Panduan Pengguna AWS IAM Identity Center dan Menggunakan autentikasi multi-faktor (MFA) dalam AWS dalam Panduan Pengguna IAM.

AWS pengguna root akun

Saat Anda membuat Akun AWS, Anda mulai dengan satu identitas masuk yang memiliki akses lengkap ke semua Layanan AWS dan sumber daya di akun. Identitas ini disebut pengguna Akun AWS root dan diakses dengan masuk dengan 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 kredensial pengguna root Anda dan gunakan kredensial tersebut untuk melakukan tugas yang hanya dapat dilakukan pengguna root. Untuk daftar lengkap tugas yang mengharuskan Anda masuk sebagai pengguna root, lihat Tugas yang memerlukan kredensial pengguna root dalam Panduan Pengguna IAM.

Pengguna dan grup IAM

Pengguna IAM adalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus untuk satu orang atau aplikasi. Jika memungkinkan, kami merekomendasikan untuk mengandalkan kredensial sementara, bukan membuat pengguna IAM yang memiliki kredensial jangka panjang seperti kata sandi dan kunci akses. Namun, jika Anda memiliki kasus penggunaan tertentu yang memerlukan kredensial jangka panjang dengan pengguna IAM, kami merekomendasikan Anda merotasi kunci akses. Untuk informasi selengkapnya, lihat Merotasi kunci akses secara teratur untuk kasus penggunaan yang memerlukan kredensial jangka panjang dalam Panduan Pengguna IAM.

Grup IAM adalah identitas yang menentukan sekumpulan 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 bernama IAMAdmins dan memberikan izin ke 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 selengkapnya, lihat Kapan harus membuat pengguna IAM (bukan peran) dalam Panduan Pengguna IAM.

Peran IAM

Peran IAM 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 mengambil peran IAM

untuk sementara AWS Management Console dengan beralih peran. Anda dapat mengambil peran dengan memanggil operasi AWS CLI atau AWS API atau dengan menggunakan URL kustom. Untuk informasi selengkapnya tentang cara menggunakan peran, lihat Menggunakan peran IAM dalam Panduan Pengguna IAM.

Peran IAM dengan kredensial sementara berguna dalam situasi berikut:

- Akses pengguna terfederasi – Untuk menetapkan izin ke identitas terfederasi, 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 identitas tersebut diautentikasi, Pusat Identitas IAM akan mengorelasikan set izin ke peran dalam IAM. Untuk informasi tentang set izin, lihat Set izin dalam Panduan Pengguna AWS IAM Identity Center .
- Izin pengguna IAM sementara – Pengguna atau peran IAM dapat mengambil peran IAM guna mendapatkan berbagai izin secara sementara untuk tugas tertentu.
- Akses lintas akun – Anda dapat menggunakan peran IAM untuk mengizinkan seseorang (prinsipal tepercaya) di akun lain untuk mengakses sumber daya di akun Anda. Peran adalah cara utama untuk memberikan akses lintas akun. Namun, dengan beberapa Layanan AWS, Anda dapat melampirkan kebijakan secara langsung ke sumber daya (alih-alih menggunakan peran sebagai proxy). Untuk mempelajari perbedaan antara peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Bagaimana peran IAM berbeda dari kebijakan berbasis sumber daya dalam Panduan Pengguna IAM.
- Akses lintas layanan — Beberapa Layanan AWS menggunakan fitur lain Layanan AWS. Sebagai contoh, ketika Anda memanggil suatu layanan, biasanya layanan tersebut menjalankan aplikasi di Amazon EC2 atau menyimpan objek di Amazon S3. Sebuah layanan mungkin melakukannya menggunakan izin prinsipal yang memanggil, menggunakan peran layanan, atau peran terkait layanan.
  - Sesi akses teruskan (FAS) — Saat Anda menggunakan pengguna atau peran IAM untuk melakukan tindakan 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 peran IAM yang dijalankan oleh layanan untuk melakukan tindakan atas nama Anda. Administrator IAM dapat membuat, mengubah, 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 terkait layanan — Peran terkait layanan adalah jenis peran layanan yang ditautkan ke peran layanan. Layanan AWS Layanan tersebut dapat menjalankan peran untuk melakukan tindakan atas nama Anda. Peran terkait layanan muncul di Anda Akun AWS dan dimiliki oleh layanan. Administrator IAM dapat melihat, tetapi tidak dapat mengedit izin untuk peran terkait layanan.

- Aplikasi yang berjalan di Amazon EC2 — Anda dapat menggunakan peran IAM untuk mengelola kredensi sementara untuk aplikasi yang berjalan pada instans EC2 dan membuat atau permintaan API. AWS CLI AWS Cara ini lebih dianjurkan daripada menyimpan kunci akses dalam instans EC2. Untuk menetapkan AWS peran ke instans EC2 dan membuatnya tersedia untuk semua aplikasinya, Anda membuat profil instance yang dilampirkan ke instance. Profil instans berisi peran dan memungkinkan program yang berjalan di instans EC2 mendapatkan kredensial sementara. Untuk informasi selengkapnya, lihat Menggunakan peran IAM untuk memberikan izin ke aplikasi yang berjalan dalam instans Amazon EC2 dalam Panduan Pengguna IAM.

Untuk mempelajari apakah kita harus menggunakan peran IAM atau pengguna IAM, lihat Kapan harus membuat peran IAM (bukan pengguna) dalam Panduan Pengguna IAM.

Mengelola akses menggunakan kebijakan

Anda mengontrol akses AWS dengan membuat kebijakan dan melampirkannya ke AWS identitas atau sumber daya. Kebijakan adalah objek AWS yang, ketika dikaitkan dengan identitas atau sumber daya, menentukan izinnya. AWS mengevaluasi kebijakan ini ketika prinsipal (pengguna, pengguna root, atau sesi peran) membuat permintaan. Izin dalam kebijakan menentukan apakah permintaan diizinkan atau ditolak. Sebagian besar kebijakan disimpan AWS sebagai 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 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 memberikan izin kepada pengguna untuk melakukan tindakan di sumber daya yang mereka perlukan, administrator IAM dapat membuat kebijakan IAM. Administrator kemudian dapat menambahkan kebijakan IAM ke peran, dan pengguna dapat mengambil peran.

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

Kebijakan berbasis identitas

Kebijakan berbasis identitas adalah dokumen kebijakan izin JSON yang dapat Anda lampirkan ke sebuah identitas, seperti pengguna IAM, grup pengguna IAM, atau peran IAM. 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 kebijakan IAM dalam 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 Anda lampirkan ke beberapa pengguna, grup, dan peran dalam. Akun AWS Kebijakan AWS terkelola mencakup kebijakan terkelola dan kebijakan yang dikelola pelanggan. Untuk mempelajari cara memilih antara kebijakan terkelola atau kebijakan inline, lihat memilih antara kebijakan terkelola dan kebijakan inline di Panduan Pengguna IAM.

Jenis-jenis kebijakan lain

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

- Batasan izin – Batasan izin adalah fitur lanjutan tempat Anda mengatur izin maksimum yang dapat diberikan oleh kebijakan berbasis identitas ke entitas IAM (pengguna IAM atau peran IAM). Anda dapat menetapkan batasan izin untuk suatu entitas. Izin yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas milik entitas 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 batasan izin, lihat Batasan izin untuk entitas IAM dalam Panduan Pengguna IAM.

- Kebijakan kontrol layanan (SCP) — SCP adalah kebijakan JSON yang menentukan izin maksimum untuk organisasi atau unit organisasi (OU) di. AWS Organizations AWS Organizations adalah layanan untuk mengelompokkan dan mengelola secara terpusat beberapa Akun AWS yang dimiliki bisnis Anda. Jika Anda mengaktifkan semua fitur di organisasi, Anda dapat menerapkan kebijakan kontrol layanan (SCP) ke salah satu atau semua akun Anda. SCP membatasi izin untuk entitas di akun anggota, termasuk masing-masing. Pengguna root akun AWS Untuk informasi selengkapnya tentang Organisasi dan SCP, lihat Cara kerja SCP dalam Panduan Pengguna AWS Organizations .
- Kebijakan sesi – Kebijakan sesi adalah kebijakan lanjutan yang Anda berikan sebagai parameter ketika Anda membuat sesi sementara secara programatis untuk peran atau pengguna terfederasi. Izin sesi yang dihasilkan adalah perpotongan 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 saat beberapa jenis kebijakan terlibat, lihat Logika evaluasi kebijakan di Panduan Pengguna IAM.

Bagaimana AWS Support bekerja dengan IAM

Sebelum Anda menggunakan IAM untuk mengelola akses AWS Support, Anda harus memahami fitur IAM apa yang tersedia untuk digunakan. AWS Support Untuk mendapatkan pandangan tingkat tinggi tentang bagaimana AWS Support dan AWS layanan lain bekerja dengan IAM, lihat AWS layanan yang bekerja dengan IAM di Panduan Pengguna IAM.

Untuk informasi tentang cara mengelola akses untuk AWS Support menggunakan IAM, lihat Mengelola akses untuk AWS Support.

Topik

- Kebijakan berbasis identitas AWS Support
- AWS Support Peran IAM

Kebijakan berbasis identitas AWS Support

Dengan kebijakan berbasis identitas IAM, Anda dapat menentukan tindakan dan sumber daya yang diizinkan atau ditolak, serta syarat diperbolehkan atau ditolaknya tindakan tersebut. AWS Support 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 AWS Support menggunakan awalan berikut sebelum tindakan:`support:`. Misalnya, untuk memberikan izin kepada seseorang untuk menjalankan instans Amazon EC2 dengan operasi API `RunInstances` Amazon EC2, Anda menyertakan tindakan `ec2:RunInstances` dalam kebijakan mereka. Pernyataan kebijakan harus mencakup elemen `Action` atau `NotAction`. AWS Support menentukan serangkaian tindakan sendiri yang menjelaskan tugas yang dapat Anda lakukan dengan layanan ini.

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

```
"Action": [
      "ec2:action1",
      "ec2:action2"
```

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

```
"Action": "ec2:Describe*"
```

Untuk melihat daftar tindakan, lihat AWS Support Tindakan yang Ditentukan oleh AWS Support dalam Panduan Pengguna IAM.

Contoh

Untuk melihat contoh kebijakan AWS Support berbasis identitas, lihat. AWS Support contoh kebijakan berbasis identitas

AWS Support Peran IAM

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

Menggunakan kredensi sementara dengan AWS Support

Anda dapat menggunakan kredensial sementara untuk masuk dengan gabungan, menjalankan IAM role, atau menjalankan peran lintas akun. Anda memperoleh kredensil keamanan sementara dengan memanggil operasi AWS STS API seperti AssumeRoleatau GetFederation Token.

AWS Support mendukung menggunakan kredensyal sementara.

Peran terkait layanan

Peran terkait AWS layanan memungkinkan layanan mengakses sumber daya di layanan lain untuk menyelesaikan tindakan atas nama 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.

AWS Support mendukung peran terkait layanan. Untuk detail tentang membuat atau mengelola peran AWS Support terkait layanan, lihat. Menggunakan peran terkait layanan untuk AWS Support

Peran layanan

Fitur ini memungkinkan layanan untuk menerima peran layanan atas nama Anda. Peran ini mengizinkan layanan untuk mengakses sumber daya di layanan lain untuk menyelesaikan tindakan atas nama Anda. 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.

AWS Support mendukung peran layanan.

AWS Support contoh kebijakan berbasis identitas

Secara default, pengguna dan IAM role tidak memiliki izin untuk membuat atau memodifikasi AWS Support sumber daya. 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 di tab JSON dalam Panduan Pengguna IAM.

Topik

Praktik terbaik kebijakan

Kebijakan berbasis identitas adalah pilihan yang sangat tepat. Mereka menentukan apakah seseorang dapat membuat, mengakses, atau menghapus AWS Support sumber daya di akun Anda. Ketika Anda membuat atau mengedit kebijakan berbasis identitas, ikuti panduan dan rekomendasi ini:

- Memulai Menggunakan Kebijakan AWS Terkelola — Untuk mulai menggunakan AWS Support dengan cepat, gunakan kebijakan AWS terkelola untuk memberi karyawan Anda izin yang mereka butuhkan. Kebijakan ini sudah tersedia di akun Anda dan dikelola, serta diperbarui oleh AWS. Untuk informasi selengkapnya, lihat Memulai menggunakan izin dengan kebijakan AWS terkelola di Panduan Pengguna IAM.
- Berikan hak akses terkecil – Saat Anda membuat kebijakan khusus, berikan izin yang diperlukan untuk melaksanakan tugas saja. Mulai dengan satu set izin minimum dan berikan izin tambahan sesuai kebutuhan. Melakukan hal tersebut lebih aman daripada memulai dengan izin yang terlalu fleksibel, lalu mencoba memperketatnya nanti. Untuk informasi selengkapnya, lihat Pemberian hak istimewa terendah dalam Panduan Pengguna IAM.
- Aktifkan MFA untuk operasi sensitif Untuk keamanan ekstra, mintalah pengguna IAM untuk menggunakan multi-factor authentication (MFA) untuk mengakses sumber daya sensitif atau operasi API. Untuk informasi selengkapnya, lihat Menggunakan autentikasi multifaktor (MFA) dalam AWS dalam Panduan Pengguna IAM.

- Gunakan Kondisi Kebijakan untuk Keamanan Tambahan – Selama praktis, tentukan ketentuan di mana kebijakan berbasis identitas Anda memungkinkan akses ke sumber daya. Misalnya, Anda dapat menulis persyaratan untuk menentukan jangkauan alamat IP yang diizinkan untuk mengajukan permintaan. Anda juga dapat menulis persyaratan untuk mengizinkan permintaan hanya dalam rentang tanggal atau waktu tertentu, atau untuk mewajibkan penggunaan SSL atau autentikasi multifaktor (MFA). Untuk informasi lebih lanjut, lihat elemen kebijakan JSON IAM: Syarat dalam Panduan Pengguna IAM.

Menggunakan konsol AWS Support tersebut

Untuk mengakses AWS Support konsol, Anda harus memiliki set izin minimum. Izin ini harus memungkinkan Anda untuk membuat daftar dan melihat detail tentang AWS Support sumber daya di AWS akun Anda. Jika Anda membuat kebijakan berbasis identitas yang lebih ketat daripada izin minimum yang diperlukan, konsol tersebut tidak akan berfungsi sebagaimana mestinya untuk entitas (pengguna IAM atau peran) dengan kebijakan tersebut.

Untuk memastikan bahwa entitas tersebut masih dapat menggunakan AWS Support konsol, lampirkan juga kebijakan AWS terkelola berikut ke entitas. Untuk informasi selengkapnya, lihat Menambahkan izin ke pengguna dalam Panduan Pengguna IAM:

Anda tidak perlu mengizinkan izin konsol minimum untuk pengguna yang melakukan panggilan hanya ke AWS CLI atau AWS API. Sebagai alternatif, hanya izinkan akses ke tindakan yang cocok dengan operasi API yang sedang Anda coba lakukan.

Izinkan para pengguna untuk 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": "*"
        }
    ]
}
```

Menggunakan peran terkait layanan

AWS Support dan AWS Trusted Advisor menggunakan peran AWS Identity and Access Management terkait layanan (IAM). Peran terkait layanan adalah peran IAM unik yang ditautkan langsung ke dan. AWS Support Trusted Advisor Dalam setiap kasus, peran terkait layanan adalah peran yang telah ditentukan sebelumnya. Peran ini mencakup semua izin yang AWS Support atau Trusted Advisor diperlukan untuk memanggil AWS layanan lain atas nama Anda. Topik-topik berikut menjelaskan peran terkait layanan apa yang dilakukan dan bagaimana bekerja dengannya di dalam AWS Support dan. Trusted Advisor

Topik

- Menggunakan peran terkait layanan untuk AWS Support
- Menggunakan peran terkait layanan untuk Trusted Advisor

Menggunakan peran terkait layanan untuk AWS Support

AWS Support alat mengumpulkan informasi tentang AWS sumber daya Anda melalui panggilan API untuk menyediakan layanan pelanggan dan dukungan teknis. Untuk meningkatkan transparansi dan auditabilitas kegiatan pendukung, AWS Support gunakan peran terkait layanan AWS Identity and Access Management (IAM).

Peran `AWSServiceRoleForSupport` terkait layanan adalah peran IAM unik yang ditautkan langsung ke. AWS Support Peran terkait layanan ini telah ditentukan sebelumnya, dan ini termasuk izin yang AWS Support diperlukan untuk memanggil AWS layanan lain atas nama Anda.

Peran terkait layanan `AWSServiceRoleForSupport` memercayai layanan `support.amazonaws.com` untuk menjalankan peran.

Untuk menyediakan layanan ini, izin peran yang telah ditentukan sebelumnya memberikan AWS Support akses ke metadata sumber daya, bukan data pelanggan. Hanya AWS Support alat yang dapat mengambil peran ini, yang ada di dalam AWS akun Anda.

Kami menutup bidang yang dapat berisi data pelanggan. Misalnya, `Output` bidang `Input` dan GetExecutionHistory untuk panggilan AWS Step Functions API tidak terlihat AWS Support. Kami gunakan AWS KMS keys untuk mengenkripsi bidang sensitif. Bidang ini disunting dalam respons API dan tidak terlihat oleh AWS Support agen.

> **Note**
>
> AWS Trusted Advisor menggunakan peran terkait layanan IAM terpisah untuk mengakses AWS sumber daya akun Anda guna memberikan rekomendasi dan pemeriksaan praktik terbaik. Untuk informasi selengkapnya, lihat Menggunakan peran terkait layanan untuk Trusted Advisor.

Peran `AWSServiceRoleForSupport` terkait layanan memungkinkan semua panggilan AWS Support API dapat dilihat oleh pelanggan melalui. AWS CloudTrail Ini membantu dengan persyaratan pemantauan dan audit, karena menyediakan cara transparan untuk memahami tindakan yang AWS Support dilakukan atas nama Anda. Untuk selengkapnya CloudTrail, lihat Panduan AWS CloudTrail Pengguna.

Izin peran terkait layanan untuk AWS Support

Peran ini menggunakan kebijakan `AWSSupportServiceRolePolicy` AWS terkelola. Kebijakan terkelola ini dilampirkan pada peran dan memungkinkan izin peran menyelesaikan tindakan atas nama Anda.

Tindakan ini dapat mencakup hal-hal berikut:

- Penagihan, administrasi, dukungan, dan layanan pelanggan lainnya — layanan AWS pelanggan menggunakan izin yang diberikan oleh kebijakan terkelola untuk melakukan sejumlah layanan sebagai bagian dari paket dukungan Anda. Ini termasuk menyelidiki dan menjawab pertanyaan akun dan penagihan, memberikan dukungan administratif untuk akun Anda, meningkatkan service quotas, dan menawarkan dukungan pelanggan tambahan.
- Pemrosesan atribut layanan dan data penggunaan untuk AWS akun Anda — AWS Support mungkin menggunakan izin yang diberikan oleh kebijakan terkelola untuk mengakses atribut layanan dan data penggunaan untuk AWS akun Anda. Kebijakan ini memungkinkan AWS Support untuk memberikan dukungan penagihan, administratif, dan teknis untuk akun Anda. Atribut layanan mencakup pengidentifikasi sumber daya akun, tanda metadata, peran, dan izin. Data penggunaan mencakup kebijakan penggunaan, statistik penggunaan, dan analitik.
- Menjaga kesehatan operasional akun Anda dan sumber dayanya — AWS Support menggunakan alat otomatis untuk melakukan tindakan yang terkait dengan dukungan operasional dan teknis.

Untuk informasi selengkapnya tentang layanan dan tindakan yang diizinkan, lihat AWSSupportServiceRolePolicykebijakan di konsol IAM.

> **Note**
>
> AWS Support memperbarui `AWSSupportServiceRolePolicy` kebijakan secara otomatis sebulan sekali untuk menambahkan izin untuk AWS layanan dan tindakan baru.

Untuk informasi selengkapnya, lihat AWS kebijakan terkelola untuk AWS Support.

Membuat peran terkait layanan untuk AWS Support

Anda tidak perlu membuat peran `AWSServiceRoleForSupport` secara manual. Saat Anda membuat AWS akun, peran ini secara otomatis dibuat dan dikonfigurasi untuk Anda.

> **Important**
>
> Jika Anda menggunakannya AWS Support sebelum mulai mendukung peran terkait layanan, maka AWS buat `AWSServiceRoleForSupport` peran tersebut di akun Anda. Untuk informasi lebih lanjut, lihat Peran baru yang muncul di akun IAM saya.

Mengedit dan menghapus peran terkait layanan untuk AWS Support

Anda dapat menggunakan IAM untuk mengedit penjelasan peran terkait layanan `AWSServiceRoleForSupport`. Untuk informasi selengkapnya, lihat Mengedit peran tertaut layanan dalam Panduan Pengguna IAM.

`AWSServiceRoleForSupport`Peran ini diperlukan AWS Support untuk memberikan dukungan administratif, operasional, dan teknis untuk akun Anda. Akibatnya, peran ini tidak dapat dihapus melalui konsol IAM, API, atau AWS Command Line Interface (AWS CLI). Ini melindungi akun AWS karena Anda tidak dapat secara tidak sengaja menghapus izin yang diperlukan untuk mengelola layanan dukungan.

Untuk informasi lebih lanjut tentang peran `AWSServiceRoleForSupport` atau penggunaannya, hubungi AWS Support.

Menggunakan peran terkait layanan untuk Trusted Advisor

AWS Trusted Advisor menggunakan peran AWS Identity and Access Management terkait layanan (IAM). Peran terkait layanan adalah peran IAM unik yang ditautkan langsung ke. AWS Trusted Advisor Peran terkait layanan telah ditentukan sebelumnya oleh Trusted Advisor, dan peran tersebut mencakup semua izin yang diperlukan layanan untuk memanggil AWS layanan lain atas nama Anda. Trusted Advisor menggunakan peran ini untuk memeriksa penggunaan Anda di seluruh AWS dan untuk memberikan rekomendasi untuk meningkatkan AWS lingkungan Anda. Misalnya, Trusted Advisor menganalisis penggunaan instans Amazon Elastic Compute Cloud (Amazon EC2) untuk membantu mengurangi biaya, meningkatkan kinerja, mentolerir kegagalan, dan meningkatkan keamanan.

> **Note**
>
> AWS Support menggunakan peran terkait layanan IAM terpisah untuk mengakses sumber daya akun Anda guna menyediakan layanan penagihan, administrasi, dan dukungan. Untuk informasi selengkapnya, lihat Menggunakan peran terkait layanan untuk AWS Support.

Untuk informasi tentang layanan lain yang mendukung peran terkait layanan, lihat Layanan AWS yang bekerja dengan IAM. Cari layanan yang memiliki Ya di kolom Peran terkait layanan. Pilih Ya dengan tautan untuk melihat dokumentasi peran tertaut layanan untuk layanan tersebut.

Topik

Izin peran terkait layanan untuk Trusted Advisor

Trusted Advisor menggunakan dua peran terkait layanan:

- AWSServiceRoleForTrustedAdvisorPeran ini mempercayai Trusted Advisor layanan untuk mengambil peran untuk mengakses AWS layanan atas nama Anda. Kebijakan izin peran memungkinkan akses Trusted Advisor hanya-baca untuk semua sumber daya. AWS Peran ini menyederhanakan memulai dengan AWS akun Anda, karena Anda tidak perlu menambahkan izin yang diperlukan untuk. Trusted Advisor Saat Anda membuka AWS akun, Trusted Advisor buat peran ini untuk Anda. Izin yang ditentukan mencakup kebijakan kepercayaan dan kebijakan izin. Kebijakan izin tidak dapat dilampirkan ke entitas IAM lainnya.

  Untuk informasi selengkapnya tentang kebijakan terlampir, lihat AWSTrustedAdvisorServiceRolePolicy.
- AWSServiceRoleForTrustedAdvisorReporting— Peran ini mempercayai Trusted Advisor layanan untuk mengambil peran untuk fitur tampilan organisasi. Peran ini memungkinkan Trusted Advisor sebagai layanan tepercaya di AWS Organizations organisasi Anda. Trusted Advisor membuat peran ini untuk Anda saat Anda mengaktifkan tampilan organisasi.

  Untuk informasi selengkapnya tentang kebijakan terlampir, lihat AWSTrustedAdvisorReportingServiceRolePolicy.

  Anda dapat menggunakan tampilan organisasi untuk membuat laporan untuk Trusted Advisor memeriksa hasil untuk semua akun di organisasi Anda. Untuk informasi selengkapnya tentang fitur ini, lihat Tampilan organisasi untuk AWS Trusted Advisor.

Mengelola izin untuk peran terkait layanan

Anda harus mengonfigurasikan izin untuk mengizinkan entitas IAM (seperti pengguna, grup, atau peran) untuk membuat, menyunting, atau menghapus peran terkait layanan. Contoh berikut menggunakan peran terkait layanan `AWSServiceRoleForTrustedAdvisor`.

Example : Mengizinkan entitas IAM membuat peran terkait layanan **`AWSServiceRoleForTrustedAdvisor`**.

Langkah ini diperlukan hanya jika Trusted Advisor akun dinonaktifkan, peran terkait layanan dihapus, dan pengguna harus membuat ulang peran untuk mengaktifkan kembali. Trusted Advisor

Anda dapat menambahkan pernyataan berikut ke kebijakan izin untuk entitas IAM untuk membuat peran terkait layanan.

```
{
    "Effect": "Allow",
    "Action": [
        "iam:CreateServiceLinkedRole",
        "iam:PutRolePolicy"
    ],
    "Resource": "arn:aws:iam::*:role/aws-service-role/trustedadvisor.amazonaws.com/
AWSServiceRoleForTrustedAdvisor*",
    "Condition": {"StringLike": {"iam:AWSServiceName": "trustedadvisor.amazonaws.com"}}
}
```

Example : Mengizinkan entitas IAM mengedit deskripsi peran terkait layanan **`AWSServiceRoleForTrustedAdvisor`**

Anda hanya dapat mengedit deskripsi untuk peran `AWSServiceRoleForTrustedAdvisor`. Anda dapat menambahkan pernyataan berikut ke kebijakan izin untuk entitas IAM untuk mengedit deskripsi peran terkait layanan.

```
{
    "Effect": "Allow",
    "Action": [
        "iam:UpdateRoleDescription"
    ],
    "Resource": "arn:aws:iam::*:role/aws-service-role/trustedadvisor.amazonaws.com/
AWSServiceRoleForTrustedAdvisor*",
    "Condition": {"StringLike": {"iam:AWSServiceName": "trustedadvisor.amazonaws.com"}}
}
```

Example : Mengizinkan entitas IAM menghapus peran terkait layanan **AWSServiceRoleForTrustedAdvisor**

Anda dapat menambahkan pernyataan berikut ke kebijakan izin untuk entitas IAM untuk menghapus peran terkait layanan.

```
{
    "Effect": "Allow",
    "Action": [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
    ],
    "Resource": "arn:aws:iam::*:role/aws-service-role/trustedadvisor.amazonaws.com/
AWSServiceRoleForTrustedAdvisor*",
    "Condition": {"StringLike": {"iam:AWSServiceName": "trustedadvisor.amazonaws.com"}}
}
```

Anda juga dapat menggunakan kebijakan AWS terkelola, seperti AdministratorAccess, untuk menyediakan akses penuh Trusted Advisor.

Membuat peran terkait layanan untuk Trusted Advisor

Anda tidak perlu membuat peran terkait layanan `AWSServiceRoleForTrustedAdvisor` secara manual. Saat Anda membuka AWS akun, Trusted Advisor buat peran terkait layanan untuk Anda.

> **Important**
>
> Jika Anda menggunakan Trusted Advisor layanan sebelum mulai mendukung peran terkait layanan, maka Trusted Advisor sudah membuat `AWSServiceRoleForTrustedAdvisor` peran di akun Anda. Untuk informasi lebih lanjut, lihat Peran baru yang muncul di akun IAM saya di Panduan Pengguna IAM.

Jika akun Anda tidak memiliki peran terkait layanan `AWSServiceRoleForTrustedAdvisor`, Trusted Advisor tidak akan bekerja sesuai dengan yang diharapkan. Hal ini dapat terjadi jika seseorang di akun Anda menonaktifkan Trusted Advisor dan kemudian menghapus peran terkait layanan. Dalam hal ini, Anda dapat menggunakan IAM untuk membuat peran terkait layanan `AWSServiceRoleForTrustedAdvisor` dan kemudian mengaktifkan kembali Trusted Advisor.

Untuk mengaktifkan Trusted Advisor (konsol)

1. Gunakan konsol IAM AWS CLI, atau IAM API untuk membuat peran terkait layanan. Trusted Advisor Untuk informasi selengkapnya, lihat Membuat peran terkait layanan.
2. Masuk ke AWS Management Console, lalu navigasikan ke Trusted Advisor konsol dihttps://console.aws.amazon.com/trustedadvisor.

   Banner status Disabled Trusted Advisor (Trusted Advisor Nonaktif) muncul di konsol.
3. Pilih Aktifkan Trusted Advisor Peran dari spanduk status. Jika `AWSServiceRoleForTrustedAdvisor` yang diperlukan tidak terdeteksi, banner status nonaktif tetap ada.

Mengedit peran terkait layanan untuk Trusted Advisor

Anda tidak dapat mengubah nama peran terkait layanan karena berbagai entitas mungkin mereferensikan peran tersebut. Namun, Anda dapat menggunakan konsol IAM, AWS CLI, atau API IAM untuk mengedit deskripsi peran. Untuk informasi lebih lanjut, lihat Mengedit peran terkait layanan dalam Panduan Pengguna IAM.

Menghapus peran terkait layanan untuk Trusted Advisor

Jika Anda tidak perlu menggunakan fitur atau layanan Trusted Advisor, Anda dapat menghapus `AWSServiceRoleForTrustedAdvisor` peran tersebut. Anda harus menonaktifkan Trusted Advisor sebelum dapat menghapus peran terkait layanan ini. Hal ini mencegah Anda menghapus izin yang diperlukan oleh operasi Trusted Advisor . Ketika Anda menonaktifkan Trusted Advisor, Anda menonaktifkan semua fitur layanan, termasuk pemrosesan offline dan pemberitahuan. Selain itu, jika Anda Trusted Advisor menonaktifkan akun anggota, maka akun pembayar terpisah juga terpengaruh, yang berarti Anda tidak akan menerima Trusted Advisor cek yang mengidentifikasi cara untuk menghemat biaya. Anda tidak dapat mengakses konsol Trusted Advisor . Panggilan API untuk Trusted Advisor mengembalikan kesalahan akses ditolak.

Anda harus membuat ulang peran terkait layanan `AWSServiceRoleForTrustedAdvisor` di akun sebelum Anda dapat mengaktifkan kembali Trusted Advisor.

Anda harus menonaktifkan Trusted Advisor terlebih dahulu di konsol sebelum Anda dapat menghapus peran `AWSServiceRoleForTrustedAdvisor` terkait layanan.

Untuk menonaktifkan Trusted Advisor

1. Masuk ke AWS Management Console dan arahkan ke Trusted Advisor konsol dihttps://console.aws.amazon.com/trustedadvisor.
2. Di panel navigasi, pilih Preferensi.
3. Di bagian Service Linked Role Permission (Izin Peran Terkait Layanan), pilih Disable Trusted Advisor(Nonaktifkan Trusted Advisor).
4. Di kotak dialog konfirmasi, pilih OK (OKE) untuk mengonfirmasi bahwa Anda ingin menonaktifkan Trusted Advisor.

Setelah Anda menonaktifkan Trusted Advisor, semua Trusted Advisor fungsionalitas dinonaktifkan, dan Trusted Advisor konsol hanya menampilkan spanduk status yang dinonaktifkan.

Anda kemudian dapat menggunakan konsol IAM, API IAM AWS CLI, atau IAM untuk menghapus nama peran Trusted Advisor terkait layanan. `AWSServiceRoleForTrustedAdvisor` Untuk informasi selengkapnya, lihat Menghapus peran tertaut layanan dalam Panduan Pengguna IAM.

AWS kebijakan terkelola untuk AWS Support

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 kepada 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, pemutakhiran akan memengaruhi semua identitas utama (pengguna, grup, dan peran) yang dilampirkan kebijakan tersebut. AWS kemungkinan besar akan memperbarui kebijakan AWS terkelola saat baru Layanan AWS diluncurkan atau operasi API baru tersedia untuk layanan yang ada.

Untuk informasi selengkapnya, lihat AWS kebijakan yang dikelola dalam Panduan Pengguna IAM.

Topik

- AWS kebijakan terkelola untuk AWS Support
- AWS kebijakan terkelola untuk AWS Support Aplikasi di Slack
- AWS kebijakan terkelola untuk AWS Trusted Advisor
- AWS kebijakan terkelola untuk AWS Support Rencana

AWS kebijakan terkelola untuk AWS Support

AWS Support memiliki kebijakan terkelola berikut.

Daftar Isi

AWS kebijakan terkelola: AWSSupportServiceRolePolicy

AWS Support menggunakan kebijakan AWSSupportServiceRolePolicy AWS terkelola. Kebijakan terkelola ini dilampirkan pada peran terkait layanan `AWSServiceRoleForSupport`. Kebijakan tersebut mengizinkan peran terkait layanan untuk menyelesaikan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke entitas IAM Anda. Untuk informasi selengkapnya, lihat Izin peran terkait layanan untuk AWS Support.

Untuk daftar perubahan kebijakan, lihat AWS Support pembaruan kebijakan AWS terkelola dan Perubahan izin untuk AWSSupportServiceRolePolicy.

AWS Support pembaruan kebijakan AWS terkelola

Lihat detail tentang pembaruan kebijakan AWS terkelola AWS Support 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 AWS Support terkelola sejak 17 Februari 2022.

AWS Support

Perubahan	Deskripsi	Tanggal
AWSSupportServiceRolePolicy — Permbaruan ke kebijakan yang sudah ada	Menambahkan 17 izin baru ke layanan berikut untuk melakukan tindakan yang membantu memecahkan masalah pelanggan yang terkait dengan penagihan, administrasi, dan dukungan teknis: • Monitor CloudWatch Jaringan Amazon — Untuk memecahkan masalah yang terkait dengan layanan Monitor Jaringan. • CloudWatch Log Amazon — Untuk men-debug masalah yang terkait dengan Amazon CloudWatch Logs. • Amazon Managed Streaming for Apache Kafka - Untuk men-debug masalah yang terkait dengan Amazon Managed Streaming for Apache Kafka. • Layanan Terkelola Amazon untuk Prometheus — Untuk memecahkan masalah yang terkait dengan Layanan Terkelola Amazon untuk Prometheus.	Mar 22, 2024

Perubahan	Deskripsi	Tanggal
AWSSupportServiceRolePolicy – Pembaruan ke kebijakan yang ada	Menambahkan 63 izin baru ke layanan berikut untuk melakukan tindakan yang membantu memecahkan masalah pelanggan yang terkait dengan penagihan, administrasi, dan dukungan teknis: • AWS Kamar Bersih — Untuk memecahkan masalah yang terkait dengan Kamar AWS Bersih. • CodeConnections — Untuk memecahkan masalah yang terkait dengan. CodeConnections • Amazon EKS — Untuk men-debug masalah yang terkait dengan Amazon EKS. • Image Builder - Untuk men-debug masalah yang terkait dengan Image Builder. • Amazon Inspector2 - Untuk memecahkan masalah yang terkait dengan Amazon Inspector2. • Amazon Inspector Scan — Untuk men-debug masalah yang terkait dengan Amazon Inspector Scan. • Amazon CloudWatch Logs — Untuk memecahka	Jan 17, 2024

Perubahan	Deskripsi	Tanggal
	n masalah yang terkait dengan Amazon CloudWatch Logs. • AWS Outposts — Untuk memecahkan masalah yang terkait dengan. AWS Outposts • Amazon RDS - Untuk men-debug masalah yang terkait dengan Amazon RDS. • AWS IAM Identity Center — Untuk memecahkan masalah yang terkait dengan. AWS IAM Identity Center • Amazon S3 Express — Untuk men-debug masalah yang terkait dengan Amazon S3 Express. • AWS Trusted Advisor — Untuk memecahkan masalah yang terkait dengan. AWS Trusted Advisor	

Perubahan	Deskripsi	Tanggal
AWSSupportServiceRolePolicy – Pembaruan ke kebijakan yang ada	Menambahkan 126 izin baru ke layanan berikut untuk melakukan tindakan yang membantu memecahkan masalah pelanggan yang terkait dengan penagihan, administrasi, dan dukungan teknis: • AWS Direct Connect — Untuk memecahkan masalah yang terkait dengan layanan. AWS Direct Connect • Amazon SageMaker — Untuk memecahkan masalah yang terkait dengan layanan Amazon SageMaker . • Amazon AppStream — Untuk men-debug masalah yang terkait dengan Amazon AppStream. • Penjelajah Sumber Daya AWS — Untuk men-debug masalah yang terkait dengan. Penjelajah Sumber Daya AWS • Amazon Redshift tanpa server — Untuk memecahkan masalah yang terkait dengan Amazon Redshift tanpa server.	6 Des 2023

Perubahan	Deskripsi	Tanggal
	• Amazon ElastiCache — Untuk men-debug masalah yang terkait dengan Amazon ElastiCache. • Amazon Comprehend — Untuk memecahkan masalah yang terkait dengan Amazon Comprehend. • Amazon EC2 — Untuk memecahkan masalah yang terkait dengan Amazon EC2. • Amazon Elastic Kubernetes Service — Untuk men-debug masalah yang terkait dengan Amazon Elastic Kubernetes Service. • AWS Elastic Disaster Recovery — Untuk memecahkan masalah yang terkait dengan. AWS Elastic Disaster Recovery • AWS AppSync — Untuk men-debug masalah yang terkait AWS AppSync dengan. • Amazon CloudWatch Logs — Untuk memecahkan masalah yang terkait dengan Amazon CloudWatch Logs.	

Perubahan	Deskripsi	Tanggal
	• AWS Health Untuk men-debug masalah yang terkait dengan AWS Health La yanan. • Amazon Connect — Untuk men-debug masalah yang terkait dengan Amazon Connect. • AWS Snowball — Untuk memecahkan masalah yang terkait dengan. AWS Snowball • AWS Health Pencitraa n — Untuk memecahka n masalah yang terkait dengan Pencitraan. AWS Health	

Perubahan	Deskripsi	Tanggal
AWSSupportServiceRolePolicy – Pembaruan ke kebijakan yang ada	Menambahkan 163 izin baru ke layanan berikut untuk melakukan tindakan yang membantu memecahkan masalah pelanggan yang terkait dengan penagihan, administrasi, dan dukungan teknis: • Amazon CloudFront — Untuk memecahkan masalah yang terkait dengan layanan. CloudFront • Amazon EC2 — Untuk memecahkan masalah yang terkait dengan layanan Amazon EC2. • Amazon AppStream — Untuk men-debug masalah yang terkait dengan Amazon AppStream. • AWS WAF — Untuk men-debug masalah yang terkait dengan Firewall Aplikasi AWS Web. • Amazon Connect — Untuk memecahkan masalah yang terkait dengan Amazon Connect. • AWS IoT — Untuk men-debug masalah yang terkait dengan. AWS IoT • Amazon Route 53 — Untuk memecahkan masalah yang	Okt 27, 2023

Perubahan	Deskripsi	Tanggal
	terkait dengan Amazon Route 53. • AWS Akses Terverifikasi — Untuk memecahkan masalah yang terkait dengan layanan Akses AWS Terverifikasi. • Amazon Simple Email Service - Untuk men-debug masalah yang terkait dengan Amazon Simple Email Service. • AWS Elastic Beanstalk — Untuk memecahkan masalah yang terkait dengan. AWS Elastic Beanstalk • Amazon DynamoDB — Untuk men-debug masalah yang terkait dengan Amazon DynamoDB. • AWS EC2 Image Builder — Untuk memecahkan masalah yang terkait dengan EC2 AWS Image Builder. • AWS Outposts Untuk men-debug masalah yang terkait dengan AWS Outposts Layanan. • AWS Glue — Untuk men-debug masalah yang terkait dengan. AWS Glue	

Perubahan	Deskripsi	Tanggal
	• AWS Directory Service — Untuk memecahkan masalah yang terkait dengan. AWS Directory Service • AWS Elastic Disaster Recovery — Untuk memecahkan masalah yang terkait dengan. AWS Elastic Disaster Recovery • AWS Step Functions — Untuk men-debug masalah yang terkait AWS Step Functions dengan. • Amazon EMR - Untuk memecahkan masalah yang terkait dengan Amazon EMR. • Amazon Relational Database Service — Untuk memecahkan masalah yang terkait dengan Amazon Relational Database Service. • Amazon EC2 Systems Manager — Untuk men-debug masalah yang terkait dengan Amazon EC2 Systems Manager.	

Perubahan	Deskripsi	Tanggal
AWSSupportServiceRolePolicy – Pembaruan ke kebijakan yang ada	Menambahkan 176 izin baru ke layanan berikut untuk melakukan tindakan yang membantu memecahkan masalah pelanggan yang terkait dengan penagihan, administrasi, dan dukungan teknis: • AWS Glue — Untuk memecahkan masalah yang terkait dengan layanan AWS Glue • Amazon EMR - Untuk memecahkan masalah yang terkait dengan layanan Amazon EMR. • Amazon Security Lake — Untuk men-debug masalah yang terkait dengan Amazon Security Lake. • AWS Systems Manager — Untuk men-debug masalah yang terkait dengan layanan Systems Manager. • Izin Terverifikasi Amazon — Untuk memecahkan masalah yang terkait dengan Izin Terverifikasi Amazon. • AWS IAM Access Analyzer — Untuk men-debug masalah yang terkait	Agustus 28, 2023

Perubahan	Deskripsi	Tanggal
	dengan layanan IAM Access Analyzer. • AWS Backup — Untuk memecahkan masalah yang terkait dengan. AWS Backup • AWS Database Migration Service — Untuk memecahkan masalah yang terkait dengan layanan DMS. • Amazon DynamoDB — Untuk men-debug masalah yang terkait dengan Dynamo DB. • Amazon Elastic Container Registry (Amazon ECR) - Untuk memecahkan masalah yang terkait dengan Amazon Elastic Container Registry (Amazon ECR). • Amazon Elastic Container Service — Untuk men-debug masalah yang terkait dengan Amazon Elastic Container Service. • Amazon Elastic Kubernetes Service — Untuk memecahkan masalah yang terkait dengan Amazon Elastic Kubernetes Service.	

Perubahan	Deskripsi	Tanggal
	• Amazon EMR Tanpa Server - Untuk men-debug masalah yang terkait dengan Layanan Tanpa Server Amazon EMR. • AWS Identity and Access Management — Untuk memecahkan masalah yang terkait dengan. AWS Identity and Access Management • AWS Network Firewall — Untuk memecahka n masalah yang terkait dengan AWS Network Firewall. • AWS HealthOmics — Untuk men-debug masalah yang terkait AWS HealthOmics dengan. • Amazon QuickSight — Untuk men-debug masalah yang terkait dengan Amazon QuickSight. • Amazon Relational Database Service — Untuk memecahkan masalah yang terkait dengan Amazon Relational Database Service. • Amazon Redshift — Untuk memecahkan masalah yang terkait dengan Amazon Redshift.	

Perubahan	Deskripsi	Tanggal
	• Amazon Redshift Tanpa Server — Untuk men-debug masalah yang terkait dengan Amazon Redshift Tanpa Server. • Amazon SageMaker — Untuk men-debug masalah yang terkait dengan Amazon SageMaker.	

Perubahan	Deskripsi	Tanggal
AWSSupportServiceRolePolicy – Pembaruan ke kebijakan yang ada	Menambahkan 141 izin baru ke layanan berikut untuk melakukan tindakan yang membantu memecahkan masalah pelanggan yang terkait dengan penagihan, administrasi, dan dukungan teknis: • Lambda — Untuk memecahkan masalah yang terkait dengan layanan Lambda. • Amazon Lex — Untuk memecahkan masalah yang terkait dengan layanan Amazon Lex. • AWS Transfer — Untuk men-debug masalah yang terkait dengan layanan Transfer. • AWS Amplify — Untuk men-debug masalah yang terkait dengan layanan Amplify. • Amazon EventBridge Pipes — Untuk memecahkan masalah izin dan penagihan yang terkait dengan Pipa. • Amazon EventBridge - Untuk men-debug masalah yang terkait dengan Amazon EventBridge • Amazon CloudWatch Logs — Untuk memecahka	26 Juni 2023

Perubahan	Deskripsi	Tanggal
	n masalah yang terkait dengan Amazon CloudWatch Logs. • AWS Systems Manager — Untuk memecahkan masalah yang terkait dengan Systems Manager. • Amazon CloudWatch — Untuk men-debug masalah yang terkait CloudWatch dengan. • Amazon ElastiCache — Untuk memecahkan masalah yang terkait dengan Amazon. ElastiCache • Amazon Athena — Untuk men-debug masalah yang terkait dengan Athena. • AWS Elastic Disaster Recovery — Untuk memecahkan masalah yang terkait dengan Elastic Disaster Recovery. • Amazon CloudWatch — Untuk memecahkan masalah konfigurasi Amazon. CloudWatch • Amazon EC2 — Untuk men-debug masalah yang terkait dengan layanan EC2. • AWS Certificate Manager — Untuk memecahka	

Perubahan	Deskripsi	Tanggal
	n masalah yang terkait dengan Certificate Manager. • Amazon EventBridge Scheduler — Untuk memecahkan masalah yang terkait dengan Scheduler. EventBridge • OpenSearch Layanan Amazon — Untuk memecahkan masalah yang terkait dengan. OpenSearch • EventBridge Skema Amazon — Untuk men-debug masalah yang terkait dengan Skema. EventBrid ge • AWS Pemberitahuan Pengguna — Untuk memecahkan masalah yang terkait dengan Pemberita huan Pengguna. • Amazon CloudWatc h Application Insights — Untuk memecahka n masalah yang terkait dengan Application Insights. CloudWatch • Amazon DynamoDB — Untuk memecahka n masalah yang terkait dengan DynamoDB. • Amazon DocumentDB Elastic Clusters — Untuk	

Perubahan	Deskripsi	Tanggal
	memecahkan masalah yang terkait dengan DocumentDB Elastic Clusters.	

Perubahan	Deskripsi	Tanggal
AWSSupportServiceRolePolicy – Pembaruan ke kebijakan yang ada	Menambahkan 53 izin baru ke layanan berikut untuk melakukan tindakan yang membantu memecahkan masalah pelanggan yang terkait dengan penagihan, administrasi, dan dukungan teknis: • Auto Scaling — Untuk memecahkan masalah yang terkait dengan layanan Auto Scaling. • Amazon CloudWatch — Untuk memecahkan masalah yang terkait dengan Amazon. CloudWatch • AWS Compute Optimizer — Untuk memecahkan masalah yang terkait dengan Compute Optimizer. • Amazon CloudWatch Terbukti — Untuk memecahkan masalah yang terkait dengan Evidently. • EC2 Image Builder — Untuk memecahkan masalah yang terkait dengan layanan Image Builder. • AWS IoT TwinMaker — Untuk memecahkan masalah yang terkait	02 Mei 2023

Perubahan	Deskripsi	Tanggal
	dengan. AWS IoT TwinMaker • Amazon CloudWatch Logs — Untuk memecahkan masalah yang terkait dengan Amazon CloudWatch Logs. • Amazon Pinpoint — Untuk memecahkan masalah yang terkait dengan Amazon Pinpoint. • AWS OAM Link - Untuk men-debug masalah yang terkait dengan sumber daya OAM. • AWS Outposts — Untuk memecahkan masalah yang terkait dengan. AWS Outposts • Amazon RDS - Untuk men-debug masalah yang terkait dengan Amazon RDS. • Penjelajah Sumber Daya AWS — Untuk memecahkan masalah yang terkait dengan Resource Explorer. • Amazon CloudWatch RUM — Untuk memecahkan masalah konfigurasi sumber daya layanan RUM. • Amazon SNS - Untuk memecahkan masalah yang	

Perubahan	Deskripsi	Tanggal
	terkait dengan Amazon SNS. • Amazon CloudWatch Synthetics — Untuk memecahkan masalah yang terkait dengan Synthetics. CloudWatch	

Perubahan	Deskripsi	Tanggal
AWSSupportServiceRolePolicy – Pembaruan ke kebijakan yang ada	Menambahkan 52 izin baru ke layanan berikut untuk melakukan tindakan yang membantu memecahkan masalah pelanggan yang terkait dengan penagihan, administrasi, dan dukungan teknis: • AWS Backup gateway — Untuk memecahkan masalah yang terkait dengan gateway Backup. • Amazon S3 - Untuk men-debug masalah yang terkait dengan Amazon S3. • AWS Application Migration Service — Untuk memecahkan masalah yang terkait dengan Layanan Migrasi Aplikasi. • AWS Kamar Bersih — Untuk men-debug masalah yang terkait dengan Kamar AWS Bersih; • AWS Systems Manager untuk SAP - Untuk memecahkan masalah yang terkait dengan SAP. AWS Systems Manager • Amazon VPC Lattice — Untuk men-debug masalah	16 Maret 2023

Perubahan	Deskripsi	Tanggal
	yang terkait dengan Amazon VPC Lattice.	

Perubahan	Deskripsi	Tanggal
AWSSupportServiceRolePolicy – Pembaruan ke kebijakan yang ada	Menambahkan 220 izin baru ke layanan berikut untuk melakukan tindakan yang membantu memecahkan masalah pelanggan yang terkait dengan penagihan, administrasi, dan dukungan teknis: • Amazon Athena — Untuk memungkinkan AWS Support untuk mengembangkan alat yang dapat digunakan untuk membantu pelanggan dengan pertanyaan mereka terkait dengan Athena. • Amazon Chime — Untuk memecahkan masalah yang terkait dengan Amazon Chime. • Amazon CloudWatch Internet Monitor — Untuk men-debug masalah yang terkait dengan Internet Monitor. • Amazon Comprehend — Untuk memecahkan masalah yang terkait dengan Amazon Comprehend. • Amazon Elastic Compute Cloud — Untuk men-debug masalah yang terkait	10 Januari 2023

Perubahan	Deskripsi	Tanggal
	dengan Transit Gateway Connect dan fitur multicast. • Amazon EventBridge Pipes — Untuk memecahkan masalah yang terkait dengan Pipa. EventBridge • Layanan Video Interaktif Amazon — AWS Support Untuk mengaktifkan kueri sumber daya Amazon IVS untuk memecahkan masalah pelanggan. • Amazon FSx - Untuk memungkinkan mengembangkan alat AWS Support untuk mendukung pengimporan dan ekspor untuk repositori data Amazon FSx. • Amazon GameLift — Untuk memecahkan masalah yang terkait dengan Amazon. GameLift • AWS Glue— Untuk memecahkan masalah yang terkait dengan Kualitas AWS Glue Data. • Amazon Kinesis Video Streams— Untuk memecahkan masalah yang terkait dengan Kinesis Video Streams.	

Perubahan	Deskripsi	Tanggal
	• Layanan Terkelola Amazon untuk Prometheus — Untuk memecahkan masalah yang terkait dengan Layanan Terkelola Amazon untuk Prometheus. • Amazon Managed Streaming for Apache Kafka - Untuk memecahkan masalah yang terkait dengan Amazon MSK Connect. • AWS Network Manager — Untuk memecahkan masalah yang terkait dengan Network Manager. • Amazon Nimble Studio — Untuk men-debug masalah yang terkait dengan Nimble Studio. • Amazon Personalize — Untuk men-debug masalah yang terkait dengan Amazon Personalize. • Amazon Pinpoint — Untuk memecahkan masalah yang terkait dengan Amazon Pinpoint. • AWS HealthOmics — Untuk memecahkan masalah yang terkait dengan. HealthOmics • Amazon Transcribe — Untuk men-debug masalah	

Perubahan	Deskripsi	Tanggal
	yang terkait dengan Amazon Transcribe.	

Perubahan	Deskripsi	Tanggal
AWSSupportServiceRolePolicy – Pembaruan ke kebijakan yang ada	Menambahkan 47 izin baru ke layanan berikut untuk melakukan tindakan yang membantu memecahkan masalah pelanggan yang terkait dengan penagihan, administrasi, dan dukungan teknis: • AWS Application Migration Service — Untuk memecahkan masalah replikasi dan peluncuran. • AWS CloudFormation kait — Untuk memungkinkan AWS Support untuk mengembangkan alat otomatisasi yang dapat membantu menyelesaikan masalah. • Amazon Elastic Kubernetes Service — Untuk memecahkan masalah yang terkait dengan Amazon EKS. • AWS IoT FleetWise— Untuk memecahkan masalah yang terkait dengan. AWS IoT FleetWise • AWS Mainframe Modernization — Untuk men-debug masalah yang terkait dengan Modernisasi Mainframe.	4 Oktober 2022

Perubahan	Deskripsi	Tanggal
	• AWS Outposts — Untuk membantu AWS Support mendapatkan daftar host dan aset khusus. • AWS Private 5G— Untuk memecahkan masalah yang terkait dengan. Private 5G • AWS Tiros— Untuk men-debug masalah yang terkait Tiros dengan.	

Perubahan	Deskripsi	Tanggal
AWSSupportServiceRolePolicy – Pembaruan ke kebijakan yang ada	Menambahkan 46 izin baru ke layanan berikut untuk melakukan tindakan yang membantu memecahkan masalah pelanggan yang terkait dengan penagihan, administrasi, dan dukungan teknis: • Amazon Managed Streaming for Apache Kafka - Untuk memecahkan masalah yang terkait dengan Amazon MSK. • AWS DataSync — Untuk memecahkan masalah yang terkait dengan. DataSync • AWS Elastic Disaster Recovery — Untuk memecahkan masalah replikasi dan peluncuran. • Amazon GameSparks — Untuk memecahkan masalah yang terkait dengan. GameSparks • AWS IoT TwinMaker — Untuk men-debug masalah yang terkait AWS IoT TwinMaker dengan. • AWS Lambda — Untuk melihat konfigurasi URL fungsi untuk memecahkan masalah.	17 Agustus 2022

Perubahan	Deskripsi	Tanggal
	• Amazon Lookout for Equipment — Untuk memecahkan masalah yang terkait dengan Lookout for Equipment. • Amazon Route 53 dan Amazon Route 53 Resolver — Untuk mendapatk an konfigurasi resolver sehingga AWS Support dapat memeriksa perilaku resolusi DNS VPC.	

Perubahan	Deskripsi	Tanggal
AWSSupportServiceRolePolicy – Pembaruan ke kebijakan yang ada	Menambahkan izin baru ke layanan berikut untuk melakukan tindakan yang membantu memecahkan masalah pelanggan yang terkait dengan penagihan, administrasi, dan dukungan teknis: • Amazon CloudWatch Logs — Untuk membantu memecahkan masalah terkait CloudWatch Log. • Layanan Video Interaktif Amazon — Untuk membantu AWS Support memeriksa sumber daya Amazon IVS yang ada untuk kasus dukungan terkait penipuan atau akun yang disusupi. • Amazon Inspector - Untuk memecahkan masalah terkait Amazon Inspector. Izin yang dihapus untuk layanan, seperti Amazon WorkLink. Amazon WorkLink tidak digunakan lagi pada 19 April 2022.	Juni 23, 2022

Perubahan	Deskripsi	Tanggal
AWSSupportServiceRolePolicy – Pembaruan ke kebijakan yang ada	Menambahkan 25 izin baru ke layanan berikut untuk melakukan tindakan yang membantu memecahkan masalah pelanggan yang terkait dengan penagihan, administrasi, dan dukungan teknis: • AWS Amplify UI Builder - Untuk memecahkan masalah yang terkait dengan komponen dan pembuatan tema. • Amazon AppStream — Untuk memecahkan masalah dengan mengambil sumber daya untuk fitur yang diluncurkan baru-baru ini. • AWS Backup — Untuk memecahkan masalah yang terkait dengan pekerjaan cadangan. • AWS CloudFormation — Untuk melakukan diagnosa pada isu-isu yang berkaitan dengan IAM, ekstensi, dan versioning. • Amazon Kinesis — Untuk memecahkan masalah yang terkait dengan Kinesis. • AWS Transfer Family — Untuk memecahka	27 April 2022

Perubahan	Deskripsi	Tanggal
	n masalah yang terkait dengan Transfer Family.	

Perubahan	Deskripsi	Tanggal

AWSSupportServiceRolePolicy – Pembaruan ke kebijakan yang ada	Menambahkan 54 izin baru ke layanan berikut untuk melakukan tindakan yang membantu memecahkan masalah pelanggan yang terkait dengan penagihan, administrasi, dan dukungan teknis:
	• Amazon Elastic Compute Cloud
	  • Untuk memecahkan masalah yang terkait dengan daftar awalan pelanggan dan AWS-managed.
	  • Untuk memecahkan masalah yang terkait dengan Amazon VPC IP Address Manager (IPAM).
	• AWS Network Manager — Untuk memecahkan masalah yang terkait dengan Network Manager.
	• Savings Plans — Untuk mendapatkan metadata tentang komitmen Savings Plan yang luar biasa.
	• AWS Serverless Application Repository — Untuk meningkatkan dan mendukung tindakan respons sebagai bagian dari
		Maret 14, 2022

Perubahan	Deskripsi	Tanggal
	penelitian dan penyelesaian kasus pendukung. • Amazon WorkSpaces Web — Untuk men-debug dan memecahkan masalah dengan WorkSpaces layanan Web.	

Perubahan	Deskripsi	Tanggal
AWSSupportServiceRolePolicy – Pembaruan ke kebijakan yang ada	Menambahkan 74 izin baru ke layanan berikut untuk melakukan tindakan yang membantu memecahkan masalah pelanggan yang terkait dengan penagihan, administrasi, dan dukungan teknis: • AWS Application Migration Service — Untuk mendukung replikasi tanpa agen di Layanan Migrasi Aplikasi. • AWS CloudFormation — Untuk melakukan diagnosa pada IAM, ekstensi, dan masalah terkait versi. • CloudWatch Log Amazon — Untuk memvalidasi kebijakan sumber daya. • Amazon EC2 Recycle Bin — Untuk mendapatkan metadata tentang aturan retensi Recycle Bin. • AWS Elastic Disaster Recovery — Untuk memecahkan masalah replikasi dan peluncuran di akun pelanggan. • Amazon FSx - Untuk melihat deskripsi snapshot Amazon FSx.	Februari 17, 2022

Perubahan	Deskripsi	Tanggal
	• Amazon Lightsail — Untuk melihat detail metadata dan konfigurasi untuk bucket Lightsail. • Amazon Macie — Untuk melihat konfigurasi Macie, seperti pekerjaan klasifikasi, pengidentifikasi data kustom, ekspresi reguler, dan temuan. • Amazon S3 — Untuk mengumpulkan metadata dan konfigurasi untuk bucket Amazon S3. • AWS Storage Gateway — Untuk melihat metadata tentang kebijakan pembuatan kaset otomatis pelanggan. • Elastic Load Balancing — Untuk melihat deskripsi batas sumber daya saat menggunakan konsol Service Quotas. Untuk informasi selengkapnya, lihat Perubahan izin untuk AWSSupportServiceRolePolicy.	
Ubah log diterbitkan	Ubah log untuk kebijakan AWS Support terkelola.	Februari 17, 2022

Perubahan izin untuk AWSSupportServiceRolePolicy

Sebagian besar izin ditambahkan untuk `AWSSupportServiceRolePolicy` memungkinkan AWS Support untuk memanggil operasi API dengan nama yang sama. Namun, beberapa operasi API memerlukan izin yang memiliki nama berbeda.

Tabel berikut hanya mencantumkan operasi API yang memerlukan izin dengan nama berbeda. Tabel ini menjelaskan perbedaan-perbedaan ini dimulai pada 17 Februari 2022.

Tanggal	Nama operasi API	Izin kebijakan yang diperlukan
Menambahkan izin pada 17 Februari 2022	`s3.GetBucketAnalyticsConfiguration`	`s3:GetAnalyticsConfiguration`
	`s3.ListBucketAnalyticsConfiguration`	
	`s3.GetBucketNotificationConfiguration`	`s3:GetBucketNotification`
	`s3.GetBucketEncryption`	`s3:GetEncryptionConfiguration`
	`s3.GetBucketIntelligentTieringConfiguration`	`s3:GetIntelligentTieringConfiguration`
	`s3.ListBucketIntelligentTieringConfiguration`	
	`s3.GetBucketInventoryConfiguration`	`s3:GetInventoryConfiguration`
	`s3.ListBucketInventoryConfiguration`	
	`s3.GetBucketLifecycleConfiguration`	`s3:GetLifecycleConfiguration`

Tanggal	Nama operasi API	Izin kebijakan yang diperlukan
	s3.GetBucketMetricsConfiguration s3.ListBucketMetricsConfiguration	s3:GetMetricsConfiguration
	s3.GetBucketReplication	s3:GetReplicationConfiguration
	s3.HeadBucket s3.ListObjects	s3:ListBucket
	s3.ListBuckets	s3:ListAllMyBuckets
	s3.ListMultipartUploads	s3:ListBucketMultipartUploads
	s3.ListObjectVersions	s3:ListBucketVersions
	s3.ListParts	s3:ListMultipartUploadParts

AWS kebijakan terkelola untuk AWS Support Aplikasi di Slack

> **Note**
>
> Untuk mengakses dan melihat kasus dukungan di AWS Support Center Console, lihatMengelola akses ke AWS Support Pusat.

AWS Support Aplikasi memiliki kebijakan terkelola berikut.

Daftar Isi

- AWS kebijakan terkelola: AWSSupportAppReadOnlyAccess
- AWS Support Pembaruan aplikasi ke kebijakan AWS terkelola

AWS kebijakan terkelola: AWSSupportAppFullAccess

Anda dapat menggunakan kebijakan AWSSupportAppFullAccessterkelola untuk memberikan izin kepada peran IAM ke konfigurasi saluran Slack. Anda juga dapat melampirkan AWSSupportAppFullAccess kebijakan ke entitas IAM Anda.

Untuk informasi selengkapnya, lihat AWS Support Aplikasi di Slack.

Kebijakan ini memberikan izin yang memungkinkan entitas melakukan AWS Support, Service Quotas, dan tindakan IAM untuk Aplikasi. AWS Support

Detail izin

Kebijakan ini mencakup izin berikut:

- `servicequotas`— Menjelaskan kuota dan permintaan layanan yang ada, dan membuat peningkatan kuota layanan untuk akun Anda.
- `support`— Membuat, memperbarui, dan menyelesaikan kasus dukungan Anda. Memperbarui dan menjelaskan informasi tentang kasus Anda, seperti lampiran file, korespondensi, dan tingkat keparahan. Memulai sesi obrolan langsung dengan agen dukungan.
- `iam`— Membuat peran terkait layanan untuk Service Quotas.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "servicequotas:GetRequestedServiceQuotaChange",
                "servicequotas:GetServiceQuota",
                "servicequotas:RequestServiceQuotaIncrease",
                "support:AddAttachmentsToSet",
                "support:AddCommunicationToCase",
```

```
                "support:CreateCase",
                "support:DescribeCases",
                "support:DescribeCommunications",
                "support:DescribeSeverityLevels",
                "support:InitiateChatForCase",
                "support:ResolveCase"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringEquals": {"iam:AWSServiceName": "servicequotas.amazonaws.com"}
            }
        }
    ]
}
```

Untuk informasi selengkapnya, lihat Mengelola akses keAWS Support Aplikasi.

AWS kebijakan terkelola: AWSSupportAppReadOnlyAccess

AWSSupportAppReadOnlyAccessKebijakan ini memberikan izin yang memungkinkan entitas melakukan tindakan Aplikasi hanya-baca AWS Support . Untuk informasi selengkapnya, lihat AWS Support Aplikasi di Slack.

Detail izin

Kebijakan ini mencakup izin berikut:

- `support`— Menjelaskan detail kasus dukungan dan komunikasi yang ditambahkan ke kasus dukungan.

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

```
            "Action": [
                "support:DescribeCases",
                "support:DescribeCommunications"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS Support Pembaruan aplikasi ke kebijakan AWS terkelola

Lihat detail tentang pembaruan kebijakan AWS terkelola untuk AWS Support Aplikasi 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 AWS Support Aplikasi sejak 17 Agustus 2022.

AWS Support Aplikasi

Perubahan	Deskripsi	Tanggal
AWSSupportAppFullAccessdan AWSSupportAppReadOnlyAccess Kebijakan AWS terkelola baru untuk AWS Support Aplikasi	Anda dapat menggunakan kebijakan ini untuk peran IAM yang dikonfigurasi untuk konfigurasi saluran Slack. Untuk informasi selengkapnya, lihat Mengelola akses keAWS Support Aplikasi.	Agustus 19, 2022
Ubah log diterbitkan	Ubah log untuk kebijakan terkelola AWS Support Aplikasi.	Agustus 19, 2022

AWS kebijakan terkelola untuk AWS Trusted Advisor

Trusted Advisor memiliki kebijakan AWS terkelola berikut.

Daftar Isi

AWS kebijakan terkelola: AWSTrustedAdvisorPriorityFullAccess

AWSTrustedAdvisorPriorityFullAccessKebijakan ini memberikan akses penuh ke Trusted Advisor Prioritas. Kebijakan ini juga memungkinkan pengguna untuk menambahkan Trusted Advisor sebagai layanan tepercaya dengan AWS Organizations dan menentukan akun administrator yang didelegasikan untuk Trusted Advisor Prioritas.

Detail izin

Dalam pernyataan pertama, kebijakan mencakup izin berikut untuk`trustedadvisor`:

- Menjelaskan akun dan organisasi Anda.
- Menjelaskan risiko yang diidentifikasi dari Trusted Advisor Prioritas. Izin memungkinkan Anda mengunduh dan memperbarui status risiko.
- Menjelaskan konfigurasi Anda untuk pemberitahuan email Trusted Advisor Prioritas. Izin memungkinkan Anda mengonfigurasi notifikasi email dan menonaktifkannya untuk administrator yang didelegasikan.
- Mengatur Trusted Advisor agar akun Anda dapat diaktifkan AWS Organizations.

Dalam pernyataan kedua, kebijakan mencakup izin berikut untuk`organizations`:

- Menjelaskan Trusted Advisor akun dan organisasi Anda.
- Daftar Layanan AWS yang Anda aktifkan untuk menggunakan Organizations.

Dalam pernyataan ketiga, kebijakan mencakup izin berikut untuk`organizations`:

- Daftar administrator yang didelegasikan untuk Trusted Advisor Prioritas.
- Mengaktifkan dan menonaktifkan akses tepercaya dengan Organizations.

Dalam pernyataan keempat, kebijakan mencakup izin berikut untuk`iam`:

- Menciptakan peran `AWSServiceRoleForTrustedAdvisorReporting` terkait layanan.

Dalam pernyataan kelima, kebijakan mencakup izin berikut untuk`organizations`:

- Memungkinkan Anda untuk mendaftar dan membatalkan pendaftaran administrator yang didelegasikan untuk Prioritas. Trusted Advisor

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "AWSTrustedAdvisorPriorityFullAccess",
   "Effect": "Allow",
   "Action": [
    "trustedadvisor:DescribeAccount*",
    "trustedadvisor:DescribeOrganization",
    "trustedadvisor:DescribeRisk*",
    "trustedadvisor:DownloadRisk",
    "trustedadvisor:UpdateRiskStatus",
    "trustedadvisor:DescribeNotificationConfigurations",
    "trustedadvisor:UpdateNotificationConfigurations",
    "trustedadvisor:DeleteNotificationConfigurationForDelegatedAdmin",
    "trustedadvisor:SetOrganizationAccess"
   ],
   "Resource": "*"
  },
  {
   "Sid": "AllowAccessForOrganization",
   "Effect": "Allow",
   "Action": [
    "organizations:DescribeAccount",
    "organizations:DescribeOrganization",
    "organizations:ListAWSServiceAccessForOrganization"
   ],
   "Resource": "*"
  },
  {
   "Sid": "AllowListDelegatedAdministrators",
   "Effect": "Allow",
```

```
    "Action": [
     "organizations:ListDelegatedAdministrators",
     "organizations:EnableAWSServiceAccess",
     "organizations:DisableAWSServiceAccess"
    ],
    "Resource": "*",
    "Condition": {
     "StringEquals": {
      "organizations:ServicePrincipal": [
       "reporting.trustedadvisor.amazonaws.com"
      ]
     }
    }
   },
   {
    "Sid": "AllowCreateServiceLinkedRole",
    "Effect": "Allow",
    "Action": "iam:CreateServiceLinkedRole",
    "Resource": "arn:aws:iam::*:role/aws-service-role/
reporting.trustedadvisor.amazonaws.com/AWSServiceRoleForTrustedAdvisorReporting",
    "Condition": {
     "StringLike": {
      "iam:AWSServiceName": "reporting.trustedadvisor.amazonaws.com"
     }
    }
   },
   {
    "Sid": "AllowRegisterDelegatedAdministrators",
    "Effect": "Allow",
    "Action": [
     "organizations:RegisterDelegatedAdministrator",
     "organizations:DeregisterDelegatedAdministrator"
    ],
    "Resource": "arn:aws:organizations::*:*",
    "Condition": {
     "StringEquals": {
      "organizations:ServicePrincipal": [
       "reporting.trustedadvisor.amazonaws.com"
      ]
     }
    }
   }
  ]
```

```
}
```

AWS kebijakan terkelola: AWSTrustedAdvisorPriorityReadOnlyAccess

AWSTrustedAdvisorPriorityReadOnlyAccessKebijakan ini memberikan izin hanya-baca ke Trusted Advisor Prioritas, termasuk izin untuk melihat akun administrator yang didelegasikan.

Detail izin

Dalam pernyataan pertama, kebijakan mencakup izin berikut untuk`trustedadvisor`:

- Menjelaskan Trusted Advisor akun dan organisasi Anda.
- Menjelaskan risiko yang diidentifikasi dari Trusted Advisor Prioritas dan memungkinkan Anda untuk mengunduhnya.
- Menjelaskan konfigurasi untuk pemberitahuan email Trusted Advisor Prioritas.

Dalam pernyataan kedua dan ketiga, kebijakan mencakup izin berikut untuk`organizations`:

- Menjelaskan organisasi Anda dengan Organizations.
- Daftar Layanan AWS yang Anda aktifkan untuk menggunakan Organizations.
- Daftar administrator yang didelegasikan untuk Prioritas Trusted Advisor

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "AWSTrustedAdvisorPriorityReadOnlyAccess",
   "Effect": "Allow",
   "Action": [
    "trustedadvisor:DescribeAccount*",
    "trustedadvisor:DescribeOrganization",
    "trustedadvisor:DescribeRisk*",
    "trustedadvisor:DownloadRisk",
    "trustedadvisor:DescribeNotificationConfigurations"
   ],
   "Resource": "*"
  },
  {
   "Sid": "AllowAccessForOrganization",
   "Effect": "Allow",
```

```
    "Action": [
     "organizations:DescribeOrganization",
     "organizations:ListAWSServiceAccessForOrganization"
    ],
    "Resource": "*"
   },
   {
    "Sid": "AllowListDelegatedAdministrators",
    "Effect": "Allow",
    "Action": [
     "organizations:ListDelegatedAdministrators"
    ],
    "Resource": "*",
    "Condition": {
     "StringEquals": {
      "organizations:ServicePrincipal": [
       "reporting.trustedadvisor.amazonaws.com"
      ]
     }
    }
   }
  ]
}
```

Kebijakan terkelola AWS : AWSTrustedAdvisorServiceRolePolicy

Kebijakan ini dilampirkan pada peran `AWSServiceRoleForTrustedAdvisor` terkait layanan. Ini memungkinkan peran terkait layanan untuk melakukan tindakan untuk Anda. Anda tidak dapat melampirkan AWSTrustedAdvisorServiceRolePolicyke entitas AWS Identity and Access Management (IAM) Anda. Untuk informasi selengkapnya, lihat Menggunakan peran terkait layanan untuk Trusted Advisor.

Kebijakan ini memberikan izin administratif yang memungkinkan akses peran terkait layanan. Layanan AWS Izin ini memungkinkan pemeriksaan Trusted Advisor untuk mengevaluasi akun Anda.

Detail izin

Kebijakan ini mencakup izin berikut.

- `accessanalyzer`— Menjelaskan AWS Identity and Access Management Access Analyzer sumber daya
- `Auto Scaling`— Menjelaskan kuota dan sumber daya akun Amazon EC2 Auto Scaling
- `cloudformation`— Menjelaskan AWS CloudFormation (CloudFormation) kuota dan tumpukan akun
- `cloudfront`— Menjelaskan CloudFront distribusi Amazon
- `cloudtrail`— Menjelaskan AWS CloudTrail (CloudTrail) jalur
- `dynamodb`— Menjelaskan kuota dan sumber daya akun Amazon DynamoDB
- `dynamodbaccelerator`— Menjelaskan sumber daya DynamoDB Accelerator
- `ec2`— Menjelaskan kuota dan sumber daya akun Amazon Elastic Compute Cloud (Amazon EC2)
- `elasticloadbalancing`— Menjelaskan kuota dan sumber daya akun Elastic Load Balancing (ELB)
- `iam`— Mendapat sumber daya IAM, seperti kredensi, kebijakan kata sandi, dan sertifikat
- `networkfirewall`— Menjelaskan AWS Network Firewall sumber daya
- `kinesis`— Menjelaskan kuota akun Amazon Kinesis (Kinesis)
- `rds`— Menjelaskan sumber daya Amazon Relational Database Service (Amazon RDS)
- `redshift`— Menjelaskan sumber daya Amazon Redshift
- `route53`— Menjelaskan kuota dan sumber daya akun Amazon Route 53
- `s3`— Menjelaskan sumber daya Amazon Simple Storage Service (Amazon S3)
- `ses`— Mendapat Layanan Email Sederhana Amazon (Amazon SES) kirim kuota
- `sqs`— Daftar antrian Layanan Antrian Sederhana Amazon (Amazon SQS)
- `cloudwatch`— Mendapat statistik metrik CloudWatch CloudWatch Acara Amazon (Acara)
- `ce`— Mendapat rekomendasi Layanan Cost Explorer (Cost Explorer)
- `route53resolver`— Mendapat Titik Akhir Amazon Route 53 Resolver Resolver dan sumber daya
- `kafka`— Mendapat Amazon Managed Streaming untuk sumber daya Apache Kafka
- `ecs`— Mendapatkan sumber daya Amazon ECS
- `outposts`— Mendapat AWS Outposts sumber daya

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

```
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "access-analyzer:ListAnalyzers"
                "autoscaling:DescribeAccountLimits",
                "autoscaling:DescribeAutoScalingGroups",
                "autoscaling:DescribeLaunchConfigurations",
                "ce:GetReservationPurchaseRecommendation",
                "ce:GetSavingsPlansPurchaseRecommendation",
                "cloudformation:DescribeAccountLimits",
                "cloudformation:DescribeStacks",
                "cloudformation:ListStacks",
                "cloudfront:ListDistributions",
                "cloudtrail:DescribeTrails",
                "cloudtrail:GetTrailStatus",
                "cloudtrail:GetTrail",
                "cloudtrail:ListTrails",
                "cloudtrail:GetEventSelectors",
                "cloudwatch:GetMetricStatistics",
                "cloudwatch:ListMetrics",
                "dax:DescribeClusters",
                "dynamodb:DescribeLimits",
                "dynamodb:DescribeTable",
                "dynamodb:ListTables",
                "ec2:DescribeAddresses",
                "ec2:DescribeReservedInstances",
                "ec2:DescribeInstances",
                "ec2:DescribeVpcs",
                "ec2:DescribeInternetGateways",
                "ec2:DescribeImages",
                "ec2:DescribeNatGateways",
                "ec2:DescribeVolumes",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeRegions",
                "ec2:DescribeReservedInstancesOfferings",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSnapshots",
                "ec2:DescribeVpcEndpoints",
                "ec2:DescribeVpnConnections",
                "ec2:DescribeVpnGateways",
                "ec2:DescribeLaunchTemplateVersions",
                "ec2:GetManagedPrefixListEntries",
```

```
                "ecs:DescribeTaskDefinition",
                "ecs:ListTaskDefinitions"
                "elasticloadbalancing:DescribeAccountLimits",
                "elasticloadbalancing:DescribeInstanceHealth",
                "elasticloadbalancing:DescribeLoadBalancerAttributes",
                "elasticloadbalancing:DescribeLoadBalancerPolicies",
                "elasticloadbalancing:DescribeLoadBalancerPolicyTypes",
                "elasticloadbalancing:DescribeLoadBalancers",
                "elasticloadbalancing:DescribeTargetGroups",
                "elasticloadbalancing:DescribeTargetHealth",
                "iam:GenerateCredentialReport",
                "iam:GetAccountPasswordPolicy",
                "iam:GetAccountSummary",
                "iam:GetCredentialReport",
                "iam:GetServerCertificate",
                "iam:ListServerCertificates",
                "iam:ListSAMLProviders",
                "kinesis:DescribeLimits",
                "kafka:DescribeClusterV2",
                "kafka:ListClustersV2",
                "kafka:ListNodes",
                "network-firewall:ListFirewalls",
                "network-firewall:DescribeFirewall",
                "outposts:GetOutpost",
                "outposts:ListAssets",
                "outposts:ListOutposts",
                "rds:DescribeAccountAttributes",
                "rds:DescribeDBClusters",
                "rds:DescribeDBEngineVersions",
                "rds:DescribeDBInstances",
                "rds:DescribeDBParameterGroups",
                "rds:DescribeDBParameters",
                "rds:DescribeDBSecurityGroups",
                "rds:DescribeDBSnapshots",
                "rds:DescribeDBSubnetGroups",
                "rds:DescribeEngineDefaultParameters",
                "rds:DescribeEvents",
                "rds:DescribeOptionGroupOptions",
                "rds:DescribeOptionGroups",
                "rds:DescribeOrderableDBInstanceOptions",
                "rds:DescribeReservedDBInstances",
                "rds:DescribeReservedDBInstancesOfferings",
                "rds:ListTagsForResource",
                "redshift:DescribeClusters",
```

```
                "redshift:DescribeReservedNodeOfferings",
                "redshift:DescribeReservedNodes",
                "route53:GetAccountLimit",
                "route53:GetHealthCheck",
                "route53:GetHostedZone",
                "route53:ListHealthChecks",
                "route53:ListHostedZones",
                "route53:ListHostedZonesByName",
                "route53:ListResourceRecordSets",
                "route53resolver:ListResolverEndpoints",
                "route53resolver:ListResolverEndpointIpAddresses",
                "s3:GetAccountPublicAccessBlock",
                "s3:GetBucketAcl",
                "s3:GetBucketPolicy",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketLocation",
                "s3:GetBucketLogging",
                "s3:GetBucketVersioning",
                "s3:GetBucketPublicAccessBlock",
                "s3:GetLifecycleConfiguration",
                "s3:ListBucket",
                "s3:ListAllMyBuckets",
                "ses:GetSendQuota",
                "sqs:GetQueueAttributes",
                "sqs:ListQueues"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS kebijakan terkelola: AWSTrustedAdvisorReportingServiceRolePolicy

Kebijakan ini dilampirkan pada peran `AWSServiceRoleForTrustedAdvisorReporting` terkait layanan yang memungkinkan Trusted Advisor untuk melakukan tindakan untuk fitur tampilan organisasi. Anda tidak dapat melampirkan AWSTrustedAdvisorReportingServiceRolePolicyke entitas IAM Anda. Untuk informasi selengkapnya, lihat Menggunakan peran terkait layanan untuk Trusted Advisor.

Kebijakan ini memberikan izin administratif yang memungkinkan peran terkait layanan untuk melakukan tindakan. AWS Organizations

Detail izin

Kebijakan ini mencakup izin berikut.

- `organizations`— Menjelaskan organisasi Anda dan mencantumkan akses layanan, akun, orang tua, anak-anak, dan unit organisasi

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "organizations:DescribeOrganization",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:ListAccounts",
                "organizations:ListAccountsForParent",
                "organizations:ListDelegatedAdministrators",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListChildren",
                "organizations:ListParents",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribeAccount"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

Trusted Advisor pembaruan kebijakan AWS terkelola

Lihat detail tentang pembaruan kebijakan AWS terkelola untuk AWS Support dan Trusted Advisor 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 Trusted Advisor terkelola sejak 10 Agustus 2021.

Trusted Advisor

Perubahan	Deskripsi	Tanggal
AWSTrustedAdvisorServiceRolePolicy Perbarui ke kebijakan yang ada.	Trusted Advisor menambahkan tindakan baru untuk memberikan `access-analyzer:ListAnalyzers` ,, `cloudwatch:ListMetrics` `dax:DescribeClusters` ,`ec2:DescribeNatGateways` ,`ec2:DescribeRouteTables` ,`ec2:DescribeVpcEndpoints` ,`ec2:GetManagedPrefixListEntries` ,`elasticloadbalancing:DescribeTargetHealth` ,`iam:ListSAMLProviders` , `kafka:DescribeClusterV2` `network-firewall:ListFirewalls` `network-firewall:DescribeFirewall` dan `sqs:GetQueueAttributes` izin.	Juni 11, 2024
AWSTrustedAdvisorServiceRolePolicy Perbarui ke kebijakan yang ada.	Trusted Advisor menambahkan tindakan baru untuk memberikan `cloudtrail:GetTrail` `cloudtrail:ListTrails`	Januari 18, 2024

Perubahan	Deskripsi	Tanggal
	`cloudtrail:GetEventSelectors` `outposts:GetOutpost` , `outposts:ListAssets` dan `outposts:ListOutposts` izin.	
AWSTrustedAdvisorPriorityFullAccess Perbarui ke kebijakan yang ada.	Trusted Advisor memperbarui kebijakan `AWSTrustedAdvisorPriorityFullAccess` AWS terkelola untuk menyertakan ID pernyataan.	6 Desember 2023
AWSTrustedAdvisorPriorityReadOnlyAccess Perbarui ke kebijakan yang ada.	Trusted Advisor memperbarui kebijakan `AWSTrustedAdvisorPriorityReadOnlyAccess` AWS terkelola untuk menyertakan ID pernyataan.	6 Desember 2023
AWSTrustedAdvisorServiceRolePolicy – Pembaruan ke kebijakan yang ada	Trusted Advisor menambahkan tindakan baru untuk memberikan `ec2:DescribeRegions` `s3:GetLifecycleConfiguration` `ecs:DescribeTaskDefinition` dan `ecs:ListTaskDefinitions` izin.	9 November 2023

Perubahan	Deskripsi	Tanggal
AWSTrustedAdvisorServiceRolePolicy – Pembaruan ke kebijakan yang ada	Trusted Advisor menambahkan tindakan IAM baru `route53resolver:ListResolverEndpoints`, `route53resolver:ListResolverEndpointIpAddresses`, `ec2:DescribeSubnets`, `kafka:ListClustersV2` dan `kafka:ListNodes` untuk melakukan pemeriksaan ketahanan baru.	14 September 2023
AWSTrustedAdvisorReportingServiceRolePolicy V2 kebijakan terkelola yang dilampirkan pada Trusted Advisor `AWSServiceRoleForTrustedAdvisorReporting` peran terkait layanan	Upgrade kebijakan AWS terkelola ke V2 untuk Trusted Advisor `AWSServiceRoleForTrustedAdvisorReporting` peran terkait layanan. V2 akan menambahkan satu aksi IAM lagi `organizations:ListDelegatedAdministrators`	Februari 28, 2023
AWSTrustedAdvisorPriorityFullAccess dan AWSTrustedAdvisorPriorityReadOnlyAccess Kebijakan AWS terkelola baru untuk Trusted Advisor	Trusted Advisor menambahkan dua kebijakan terkelola baru yang dapat Anda gunakan untuk mengontrol akses ke Trusted Advisor Prioritas.	17 Agustus 2022

Perubahan	Deskripsi	Tanggal
AWSTrustedAdvisorServiceRolePolicy – Pembaruan ke kebijakan yang ada	Trusted Advisor menambahkan tindakan baru untuk memberikan `DescribeTargetGroups` dan `GetAccountPublicAccessBlock` izin. `DescribeTargetGroup` Izin diperlukan untuk Pemeriksaan Kesehatan Grup Auto Scaling untuk mengambil Load Balancer non-klasik yang dilampirkan ke grup Auto Scaling. `GetAccountPublicAccessBlock` Izin diperlukan untuk pemeriksaan Izin Bucket Amazon S3 untuk mengambil setelan blokir akses publik untuk file. Akun AWS	Agustus 10, 2021
Ubah log diterbitkan	Trusted Advisor mulai melacak perubahan untuk kebijakan yang AWS dikelola.	Agustus 10, 2021

AWS kebijakan terkelola untuk AWS Support Rencana

AWS Support Rencana memiliki kebijakan terkelola berikut.

Daftar Isi

AWS kebijakan terkelola: AWSSupportPlansFullAccess

AWS Support Paket menggunakan kebijakan AWSSupportPlansFullAccess AWS terkelola. Entitas IAM menggunakan kebijakan ini untuk menyelesaikan tindakan Support Plans berikut untuk Anda:

- Lihat paket dukungan Anda untuk Akun AWS
- Melihat detail tentang status permintaan untuk mengubah paket dukungan Anda
- Ubah rencana dukungan untuk Anda Akun AWS
- Buat jadwal rencana dukungan untuk Anda Akun AWS

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "supportplans:GetSupportPlan",
                "supportplans:GetSupportPlanUpdateStatus",
                "supportplans:StartSupportPlanUpdate",
                "supportplans:CreateSupportPlanSchedule"
            ],
            "Resource": "*"
        }
    ]
}
```

Untuk daftar perubahan kebijakan, lihatAWS Support Memperbarui rencana kebijakan AWS terkelola.

AWS kebijakan terkelola: AWSSupportPlansReadOnlyAccess

AWS Support Paket menggunakan kebijakan AWSSupportPlansReadOnlyAccess AWS terkelola. Entitas IAM menggunakan kebijakan ini untuk menyelesaikan tindakan Support Plans hanya-baca berikut untuk Anda:

- Lihat paket dukungan Anda untuk Akun AWS
- Melihat detail tentang status permintaan untuk mengubah paket dukungan Anda

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

```
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "supportplans:GetSupportPlan",
                "supportplans:GetSupportPlanUpdateStatus"
            ],
            "Resource": "*"
        }
    ]
}
```

Untuk daftar perubahan kebijakan, lihatAWS Support Memperbarui rencana kebijakan AWS terkelola.

AWS Support Memperbarui rencana kebijakan AWS terkelola

Lihat detail tentang pembaruan kebijakan AWS terkelola untuk Paket Dukungan 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 Support Plans sejak 29 September 2022.

AWS Support

Perubahan	Deskripsi	Tanggal
AWSSupportPlansFullAccess - Pembaruan ke kebijakan yang tersedia	Tambahkan `CreateSupportPlanSchedule` tindakan ke kebijakan `AWSSupportPlansFullAccess` terkelola.	8 Mei 2023
Ubah log diterbitkan	Ubah log untuk kebijakan terkelola Support Plans.	29 September 2022

Mengelola akses ke AWS Support Pusat

Anda harus memiliki izin untuk mengakses Pusat Dukungan dan membuat kasus dukungan.

Anda dapat menggunakan salah satu opsi berikut untuk mengakses Pusat Dukungan:

- Gunakan alamat email dan kata sandi yang terkait dengan AWS akun Anda. Identitas ini disebut pengguna root AWS akun.
- Gunakan AWS Identity and Access Management (IAM).

Jika Anda memiliki paket Business, Enterprise On-Ramp, atau Enterprise Support, Anda juga dapat menggunakan AWS Support API untuk mengakses AWS Support dan Trusted Advisor mengoperasikannya secara terprogram. Untuk informasi lebih lanjut, lihat Referensi API AWS Support.

> **Note**
>
> Jika Anda tidak dapat masuk ke Pusat Dukungan, Anda dapat menggunakan halaman Hubungi Kami sebagai gantinya. Anda dapat menggunakan halaman ini untuk mendapatkan bantuan terkait masalah penagihan dan akun.

AWS akun

Anda dapat masuk ke AWS Management Console dan mengakses Pusat Dukungan dengan menggunakan alamat email dan kata sandi AWS akun Anda. Identitas ini disebut pengguna root AWS akun. Kami sangat menyarankan agar Anda tidak menggunakan pengguna root untuk tugas sehari-hari, bahkan tugas administratif. Sebagai gantinya, sebaiknya gunakan IAM yang mengizinkan Anda mengontrol siapa yang dapat melakukan tugas tertentu di akun Anda.

AWS tindakan dukungan

Anda dapat melakukan AWS Support tindakan berikut di konsol. Anda juga dapat menentukan AWS Support tindakan ini dalam kebijakan IAM untuk mengizinkan atau menolak tindakan tertentu.

> **Note**
>
> Jika Anda menolak salah satu tindakan di bawah ini dalam kebijakan IAM Anda, hal itu dapat mengakibatkan perilaku yang tidak diinginkan di Pusat Dukungan saat membuat atau berinteraksi dengan kasus dukungan.

Tindakan	Deskripsi
`DescribeSupportLevel`	Memberikan izin untuk mengembalikan level dukungan untuk pengenal AWS akun. Ini digunakan secara internal oleh AWS Support Center untuk mengidentifikasi tingkat dukungan Anda.
`InitiateCallForCase`	Memberikan izin untuk memulai panggilan di AWS Support Center. Ini digunakan secara internal oleh AWS Support Center untuk memulai panggilan atas nama Anda.
`InitiateChatForCase`	Memberikan izin untuk memulai obrolan di AWS Support Center. Ini digunakan secara internal oleh AWS Support Center untuk memulai obrolan atas nama Anda.
`RateCaseCommunication`	Memberikan izin untuk menilai komunikasi AWS Support kasus.
`DescribeCaseAttributes`	Memberikan izin untuk mengizinkan layanan sekunder membaca atribut AWS Support kasus. Ini digunakan secara internal oleh AWS Support Center untuk mendapatkan atribut yang ditandai pada kasus Anda.
`DescribeIssueTypes`	Memberikan izin untuk mengembalikan jenis masalah untuk AWS Support kasus. Ini digunakan secara internal oleh AWS Support Center untuk mendapatkan jenis masalah yang tersedia untuk akun Anda.
`SearchForCases`	Memberikan izin untuk mengembalikan daftar AWS Support kasus yang cocok dengan input yang diberikan. Ini digunakan secara internal oleh AWS Support Center untuk menemukan kasus yang dicari.

Tindakan	Deskripsi
`PutCaseAttributes`	Memberikan izin untuk mengizinkan layanan sekunder melampirkan atribut ke AWS Support kasus. Ini digunakan secara internal oleh AWS Support Center untuk menambahkan tag operasional ke AWS Support kasus Anda.

IAM

Secara default, pengguna IAM tidak dapat mengakses Pusat Dukungan. Anda dapat menggunakan IAM untuk membuat pengguna individu atau grup. Kemudian, Anda melampirkan kebijakan IAM ke entitas ini, sehingga mereka memiliki izin untuk melakukan tindakan dan mengakses sumber daya, seperti membuka kasus Support Center dan menggunakan AWS Support API.

Setelah Anda membuat pengguna IAM, Anda dapat memberikan pengguna tersebut sandi individu dan halaman masuk khusus akun. Mereka kemudian dapat masuk ke AWS akun Anda dan bekerja di Pusat Dukungan. Pengguna IAM yang memiliki AWS Support akses dapat melihat semua kasus yang dibuat untuk akun tersebut.

Untuk informasi selengkapnya, lihat Masuk ke pengguna IAM AWS Management Console sebagai pengguna IAM di Panduan Pengguna IAM.

Cara termudah untuk memberikan izin adalah dengan melampirkan kebijakan AWS terkelola AWSSupportAccesske pengguna, grup, atau peran. AWS Support memungkinkan izin tingkat tindakan untuk mengontrol akses ke operasi tertentu. AWS Support AWS Support tidak menyediakan akses tingkat sumber daya, jadi `Resource` elemen selalu disetel ke. * Anda tidak dapat mengizinkan atau menolak akses ke kasus dukungan tertentu.

Example : Izinkan akses ke semua AWS Support tindakan

Kebijakan AWS terkelola AWSSupportAccessmemberikan akses kepada pengguna IAM. AWS Support Pengguna IAM dengan kebijakan ini dapat mengakses semua AWS Support operasi dan sumber daya.

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

```
        {
            "Effect": "Allow",
            "Action": ["support:*"],
            "Resource": "*"
        }
    ]
}
```

Untuk informasi lebih lanjut tentang cara melampirkan kebijakan `AWSSupportAccess` ke entitas Anda, lihat Menambahkan izin identitas IAM (konsol) dalam Panduan Pengguna IAM.

Example : Izinkan akses ke semua tindakan kecuali ResolveCase tindakan

Anda juga dapat membuat kebijakan yang dikelola pelanggan di IAM untuk menentukan tindakan apa yang diizinkan atau ditolak. Pernyataan kebijakan berikut memungkinkan pengguna IAM untuk melakukan semua tindakan AWS Support kecuali menyelesaikan kasus.

```
{
   "Version": "2012-10-17",
   "Statement": [
   {
      "Effect": "Allow",
      "Action": "support:*",
      "Resource": "*"
   },
   {
       "Effect": "Deny",
       "Action": "support:ResolveCase",
       "Resource": "*"
    }]
}
```

Untuk informasi selengkapnya tentang pembuatan kebijakan IAM yang dikelola pelanggan, lihat Membuat kebijakan yang dikelola pelanggan di Panduan Pengguna IAM.

Jika pengguna atau grup sudah memiliki kebijakan, Anda dapat menambahkan pernyataan kebijakan AWS Support-specific ke kebijakan tersebut.

> **Important**
>
> - Jika Anda tidak dapat melihat kasus di Pusat Dukungan, pastikan bahwa Anda memiliki izin yang diperlukan. Anda mungkin harus menghubungi administrator IAM. Untuk informasi selengkapnya, lihat Manajemen identitas dan akses untuk AWS Support.

Akses ke AWS Trusted Advisor

Dalam AWS Management Console, namespace `trustedadvisor` IAM terpisah mengontrol akses ke. Trusted Advisor Di AWS Support API, namespace `support` IAM mengontrol akses ke. Trusted Advisor Untuk informasi selengkapnya, lihat Kelola akses ke AWS Trusted Advisor.

Mengelola akses ke AWS Support Paket

Topik

- Izin untuk konsol Support Plans
- Tindakan Support Plans
- Contoh kebijakan IAM untuk Support Plans
- Pemecahan Masalah

Izin untuk konsol Support Plans

Untuk mengakses konsol Support Plans, pengguna harus memiliki set izin minimum. Izin ini harus memungkinkan pengguna untuk membuat daftar dan melihat detail tentang sumber daya Rencana Dukungan di Anda Akun AWS.

Anda dapat membuat kebijakan AWS Identity and Access Management (IAM) dengan `supportplans` namespace. Anda dapat menggunakan kebijakan ini untuk menentukan izin untuk tindakan dan sumber daya.

Ketika Anda membuat kebijakan, Anda dapat menentukan namespace layanan untuk mengizinkan atau menolak tindakan. Namespace untuk Support Plans adalah. `supportplans`

Anda dapat menggunakan kebijakan AWS terkelola dan melampirkannya ke entitas IAM Anda. Untuk informasi selengkapnya, lihat AWS kebijakan terkelola untuk AWS Support Rencana.

Tindakan Support Plans

Anda dapat melakukan tindakan Support Plans berikut di konsol. Anda juga dapat menentukan tindakan Support Plans ini dalam kebijakan IAM untuk mengizinkan atau menolak tindakan tertentu.

Tindakan	Deskripsi
`GetSupportPlan`	Memberikan izin untuk melihat detail tentang rencana dukungan saat ini untuk ini Akun AWS.
`GetSupportPlanUpdateStatus`	Memberikan izin untuk melihat detail tentang status permintaan untuk memperbarui paket dukungan.
`StartSupportPlanUpdate`	Memberikan izin untuk memulai permintaan untuk memperbarui rencana dukungan untuk ini Akun AWS.
`CreateSupportPlanSchedule`	Memberikan izin untuk membuat jadwal rencana dukungan untuk ini. Akun AWS

Contoh kebijakan IAM untuk Support Plans

Anda dapat menggunakan contoh kebijakan berikut untuk mengelola akses ke Support Plans.

Akses penuh ke Support Plans

Kebijakan berikut memungkinkan pengguna akses penuh ke Support Plans.

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

Akses read-only ke Support Plans

Kebijakan berikut memungkinkan akses read-only ke Support Plans.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "supportplans:Get*",
            "Resource": "*"
        }
    ]
}
```

Tolak akses ke Support Plans

Kebijakan berikut tidak mengizinkan pengguna mengakses Support Plans.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "supportplans:*",
            "Resource": "*"
        }
    ]
}
```

Pemecahan Masalah

Lihat topik berikut untuk mengelola akses ke Support Plans.

Ketika saya mencoba melihat atau mengubah paket dukungan saya, konsol Support Plans mengatakan bahwa saya kehilangan **`GetSupportPlan`** izin

Pengguna IAM harus memiliki izin yang diperlukan untuk mengakses konsol Support Plans. Anda dapat memperbarui kebijakan IAM Anda untuk menyertakan izin yang hilang atau menggunakan kebijakan AWS terkelola, seperti AWSSupportPlansFullAccess atauAWSSupportPlansReadOnlyAccess. Untuk informasi selengkapnya, lihat AWS kebijakan terkelola untuk AWS Support Rencana.

Jika Anda tidak memiliki akses untuk memperbarui kebijakan IAM Anda, hubungi Akun AWS administrator Anda.

Informasi terkait

Untuk informasi selengkapnya, lihat topik berikut di Panduan Pengguna IAM:

- Menguji kebijakan IAM dengan simulator kebijakan IAM
- Memecahkan masalah akses ditolak pesan kesalahan

Saya memiliki izin Support Plans yang benar, tetapi saya masih mendapatkan kesalahan yang sama

Jika Anda Akun AWS adalah akun anggota yang merupakan bagian dari AWS Organizations, kebijakan kontrol layanan (SCP) mungkin perlu diperbarui. SCP adalah jenis kebijakan yang mengelola izin dalam suatu organisasi.

Karena Support Plans adalah layanan global, kebijakan yang membatasi Wilayah AWS dapat mencegah akun anggota melihat atau mengubah paket dukungan mereka. Untuk mengizinkan layanan global bagi organisasi Anda, seperti IAM dan Support Plans, Anda harus menambahkan layanan ke daftar pengecualian di SCP yang berlaku. Ini berarti bahwa akun dalam organisasi dapat mengakses layanan ini, bahkan jika SCP menyangkal yang ditentukan. Wilayah AWS

Untuk menambahkan Support Plans sebagai pengecualian, masukkan `"supportplans:*"` ke `"NotAction"` daftar di SCP.

```
"supportplans:*",
```

SCP Anda mungkin muncul sebagai cuplikan kebijakan berikut.

Example : SCP yang memungkinkan akses Support Plans dalam suatu organisasi

```
{ "Version":  "2012-10-17",
   "Statement": [
     { "Sid":  "GRREGIONDENY",
       "Effect":  "Deny",
       "NotAction": [
         "aws-portal:*",
         "budgets:*",
         "chime:*"
         "iam:*",
         "supportplans:*",
```

```
        ....
```

Jika Anda memiliki akun anggota dan tidak dapat memperbarui SCP, hubungi Akun AWS administrator Anda. Akun manajemen mungkin perlu memperbarui SCP sehingga semua akun anggota dapat mengakses Support Plans.

> **Catatan untuk AWS Control Tower**
>
> - Jika organisasi Anda menggunakan SCP AWS Control Tower, Anda dapat memperbarui akses Tolak AWS berdasarkan Wilayah AWS kontrol yang diminta (biasanya disebut sebagai kontrol penolakan Wilayah).
> - Jika Anda memperbarui SCP AWS Control Tower untuk mengizinkan`supportplans`, memperbaiki drift akan menghapus pembaruan Anda ke SCP. Untuk informasi selengkapnya, lihat Mendeteksi dan menyelesaikan penyimpangan masuk AWS Control Tower.

Informasi terkait

Untuk informasi selengkapnya, lihat topik berikut.

- Kebijakan kontrol layanan (SCP) dalam Panduan AWS Organizations Pengguna.
- Konfigurasikan wilayah tolak kontrol di Panduan AWS Control Tower Pengguna
- Tolak akses AWS berdasarkan permintaan Wilayah AWS dalam Panduan AWS Control Tower Pengguna

Kelola akses ke AWS Trusted Advisor

Anda dapat mengakses AWS Trusted Advisor dari AWS Management Console. Semua Akun AWS memiliki akses ke Trusted Advisor pemeriksaan inti tertentu. Jika Anda memiliki paket Business, Enterprise On-Ramp, atau Enterprise Support, Anda dapat mengakses semua cek. untuk informasi selengkapnya, lihat. AWS Trusted Advisor periksa referensi

Anda dapat menggunakan AWS Identity and Access Management (IAM) untuk mengontrol akses ke Trusted Advisor.

Topik

Izin untuk konsol Trusted Advisor

Untuk mengakses Trusted Advisor konsol, pengguna harus memiliki set izin minimum. Izin ini harus memungkinkan pengguna untuk membuat daftar dan melihat detail tentang Trusted Advisor sumber daya di Anda Akun AWS.

Anda dapat menggunakan opsi berikut untuk mengontrol akses ke Trusted Advisor:

- Gunakan fitur filter tag Trusted Advisor konsol. Pengguna atau peran harus memiliki izin yang terkait dengan tanda.

  Anda dapat menggunakan kebijakan AWS terkelola atau kebijakan khusus untuk menetapkan izin berdasarkan tag. Untuk informasi selengkapnya, lihat Mengontrol akses ke dan untuk pengguna dan peran IAM menggunakan tag.
- Buat kebijakan IAM dengan `trustedadvisor` namespace. Anda dapat menggunakan kebijakan ini untuk menentukan izin untuk tindakan dan sumber daya.

Ketika Anda membuat kebijakan, Anda dapat menentukan namespace layanan untuk mengizinkan atau menolak tindakan. Namespace untuk Trusted Advisor adalah. `trustedadvisor` Namun, Anda tidak dapat menggunakan `trustedadvisor` namespace untuk mengizinkan atau menolak operasi Trusted Advisor API di AWS Support API. Anda harus menggunakan `support` namespace untuk AWS Support sebagai gantinya.

> **Note**
>
> Jika Anda memiliki izin ke AWS SupportAPI, Trusted Advisor widget di AWS Management Console menampilkan tampilan ringkasan Trusted Advisor hasil Anda. Untuk melihat hasil Anda di Trusted Advisor konsol, Anda harus memiliki izin ke `trustedadvisor` namespace.

Trusted Advisor tindakan

Anda dapat melakukan Trusted Advisor tindakan berikut di konsol. Anda juga dapat menentukan Trusted Advisor tindakan ini dalam kebijakan IAM untuk mengizinkan atau menolak tindakan tertentu.

Tindakan	Deskripsi
`DescribeAccount`	Memberikan izin untuk melihat AWS Support rencana dan berbagai Trusted Advisor p referensi.
`DescribeAccountAccess`	Memberikan izin untuk melihat apakah Akun AWS telah diaktifkan atau dinonaktifkan Trusted Advisor.
`DescribeCheckItems`	Memberikan izin untuk melihat detail untuk item pemeriksaan.
`DescribeCheckRefreshStatuses`	Memberikan izin untuk melihat status penyegaran untuk pemeriksaan Trusted Advisor .
`DescribeCheckSummaries`	Memberikan izin untuk melihat ringkasan Trusted Advisor cek.
`DescribeChecks`	Memberikan izin untuk melihat detail untuk Trusted Advisor pemeriksaan.
`DescribeNotificationPreferences`	Memberikan izin untuk melihat preferensi notifikasi untuk akun AWS .
`ExcludeCheckItems`	Memberikan izin untuk mengecualikan rekomendasi untuk pemeriksaan Trusted Advisor .
`IncludeCheckItems`	Memberikan izin untuk memasukkan rekomendasi untuk pemeriksaan Trusted Advisor .

Tindakan	Deskripsi
`RefreshCheck`	Memberikan izin untuk menyegarkan Trusted Advisor cek.
`SetAccountAccess`	Memberikan izin untuk mengaktifkan atau menonaktifkan Trusted Advisor akun.
`UpdateNotificationPreferences`	Memberikan izin untuk memperbarui preferensi notifikasi untuk Trusted Advisor.
`DescribeCheckStatusHistoryChanges`	Memberikan izin untuk melihat hasil dan mengubah status pemeriksaan dalam 30 hari terakhir.

Trusted Advisor tindakan untuk tampilan organisasi

Trusted Advisor Tindakan berikut adalah untuk fitur tampilan organisasi. Untuk informasi selengkapnya, lihat Tampilan organisasi untuk AWS Trusted Advisor.

Tindakan	Deskripsi
`DescribeOrganization`	Memberikan izin untuk melihat apakah Akun AWS memenuhi persyaratan untuk mengaktifkan fitur tampilan organisasi.
`DescribeOrganizationAccounts`	Memberikan izin untuk melihat AWS akun tertaut yang ada di organisasi.
`DescribeReports`	Memberikan izin untuk melihat detail laporan tampilan organisasi, seperti nama laporan, waktu aktif, tanggal dibuat, status, dan format.
`DescribeServiceMetadata`	Memberikan izin untuk melihat informasi tentang laporan tampilan organisasi, seperti, memeriksa kategori Wilayah AWS, memeriksa nama, dan status sumber daya.

Tindakan	Deskripsi
`GenerateReport`	Memberikan izin untuk membuat laporan untuk Trusted Advisor pemeriksaan di organisasi Anda.
`ListAccountsForParent`	Memberikan izin untuk melihat, di Trusted Advisor konsol, semua akun dalam AWS organisasi yang terkandung oleh root atau unit organisasi (OU).
`ListOrganizationalUnitsForParent`	Memberikan izin untuk melihat, di Trusted Advisor konsol, semua unit organisasi (OU) di unit organisasi induk atau root.
`ListRoots`	Memberikan izin untuk melihat, di Trusted Advisor konsol, semua akar yang ditentukan dalam suatu AWS organisasi.
`SetOrganizationAccess`	Memberikan izin untuk mengaktifkan fitur tampilan organisasi untuk Trusted Advisor.

Trusted Advisor Tindakan prioritas

Jika Trusted Advisor Prioritas diaktifkan untuk akun, Anda dapat melakukan Trusted Advisor tindakan berikut di konsol. Anda juga dapat menambahkan Trusted Advisor tindakan ini dalam kebijakan IAM untuk mengizinkan atau menolak tindakan tertentu. Untuk informasi selengkapnya, lihat Contoh kebijakan IAM untuk Prioritas Trusted Advisor.

> **Note**
>
> Risiko yang muncul di Trusted Advisor Priority adalah rekomendasi yang telah diidentifikasi oleh manajer akun teknis (TAM) Anda untuk akun Anda. Rekomendasi dari layanan, seperti Trusted Advisor cek, dibuat untuk Anda secara otomatis. Rekomendasi dari TAM Anda dibuat untuk Anda secara manual. Selanjutnya, TAM Anda mengirimkan rekomendasi ini sehingga muncul di Trusted Advisor Prioritas untuk akun Anda.

Untuk informasi selengkapnya, lihat Memulai dengan AWS Trusted Advisor Prioritas.

Tindakan	Deskripsi
`DescribeRisks`	Memberikan izin untuk melihat risiko dalam Trusted Advisor Prioritas.
`DescribeRisk`	Memberikan izin untuk melihat detail risiko di Trusted Advisor Prioritas.
`DescribeRiskResources`	Memberikan izin untuk melihat sumber daya yang terpengaruh untuk risiko dalam Trusted Advisor Prioritas.
`DownloadRisk`	Memberikan izin untuk mengunduh file yang berisi rincian tentang risiko dalam Trusted Advisor Prioritas.
`UpdateRiskStatus`	Memberikan izin untuk memperbarui status risiko di Trusted Advisor Prioritas.
`DescribeNotificationConfigurations`	Memberikan izin untuk mendapatkan preferensi notifikasi email Anda untuk Trusted Advisor Prioritas.
`UpdateNotificationConfigurations`	Memberikan izin untuk membuat atau memperbarui preferensi pemberitahuan email Anda untuk Trusted Advisor Prioritas.
`DeleteNotificationConfigurationForDelegatedAdmin`	Memberikan izin ke akun manajemen organisasi untuk menghapus preferensi pemberitahuan email dari akun administrator yang didelegasikan untuk Trusted Advisor Prioritas.

Trusted Advisor Libatkan tindakan

Jika Trusted Advisor Engage diaktifkan untuk akun Anda, Anda dapat melakukan Trusted Advisor tindakan berikut di konsol. Anda juga dapat menambahkan Trusted Advisor tindakan ini dalam

kebijakan IAM untuk mengizinkan atau menolak tindakan tertentu. Untuk informasi selengkapnya, lihat Contoh kebijakan IAM untuk Engage Trusted Advisor.

Untuk informasi selengkapnya, lihat Memulai dengan AWS Trusted Advisor Engage (Pratinjau).

Tindakan	Deskripsi
`CreateEngagement`	Memberikan izin untuk membuat keterlibatan di Trusted Advisor Engage.
`CreateEngagementAttachment`	Memberikan izin untuk membuat lampiran keterlibatan di Trusted Advisor Engage.
`CreateEngagementCommunication`	Memberikan izin untuk membuat komunikasi keterlibatan di Trusted Advisor Engage.
`GetEngagement`	Memberikan izin untuk melihat keterlibatan dalam Engage. Trusted Advisor
`GetEngagementAttachment`	Memberikan izin untuk melihat lampiran keterlibatan di Engage. Trusted Advisor
`GetEngagementType`	Memberikan izin untuk melihat jenis keterliba tan tertentu di Trusted Advisor Engage.
`ListEngagementCommunications`	Memberikan izin untuk melihat semua komunikasi untuk keterlibatan dalam Trusted Advisor Engage.
`ListEngagements`	Memberikan izin untuk melihat semua keterliba tan di Engage. Trusted Advisor
`ListEngagementTypes`	Memberikan izin untuk melihat semua jenis keterlibatan di Trusted Advisor Engage.
`UpdateEngagement`	Memberikan izin untuk memperbarui detail keterlibatan di Trusted Advisor Engage.
`UpdateEngagementStatus`	Memberikan izin untuk memperbarui status keterlibatan di Trusted Advisor Engage.

Contoh kebijakan IAM

Kebijakan berikut menunjukkan cara mengizinkan dan menolak akses ke Trusted Advisor. Anda dapat menggunakan salah satu kebijakan berikut untuk membuat kebijakan terkelola pelanggan di konsol IAM. Misalnya, Anda dapat menyalin kebijakan contoh, lalu menempelkan ke tab JSON konsol IAM. Kemudian, lampirkan kebijakan tersebut pada pengguna, grup, atau IAM role Anda.

Untuk informasi selengkapnya tentang cara membuat kebijakan IAM, lihat Membuat kebijakan IAM (konsol) di Panduan Pengguna IAM.

Contoh

- Akses penuh ke Trusted Advisor
- Akses hanya-baca ke Trusted Advisor
- Tolak akses ke Trusted Advisor
- Mengizinkan dan menolak tindakan tertentu
- Kontrol akses ke operasi AWS Support API untuk Trusted Advisor
- Contoh kebijakan IAM untuk Prioritas Trusted Advisor
- Contoh kebijakan IAM untuk Engage Trusted Advisor

Akses penuh ke Trusted Advisor

Kebijakan berikut memungkinkan pengguna untuk melihat dan mengambil semua tindakan pada semua Trusted Advisor pemeriksaan di Trusted Advisor konsol.

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

Akses hanya-baca ke Trusted Advisor

Kebijakan berikut memungkinkan pengguna akses hanya-baca ke konsol. Trusted Advisor Pengguna tidak dapat membuat perubahan, seperti menyegarkan pemeriksaan atau mengubah preferensi notifikasi.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "trustedadvisor:Describe*",
                "trustedadvisor:Get*",
                "trustedadvisor:List*"
            ],
            "Resource": "*"
        }
    ]
}
```

Tolak akses ke Trusted Advisor

Kebijakan berikut tidak mengizinkan pengguna untuk melihat atau mengambil tindakan untuk Trusted Advisor pemeriksaan di Trusted Advisor konsol.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "trustedadvisor:*",
            "Resource": "*"
        }
    ]
}
```

Mengizinkan dan menolak tindakan tertentu

Kebijakan berikut memungkinkan pengguna untuk melihat semua Trusted Advisor pemeriksaan di Trusted Advisor konsol, tetapi tidak memungkinkan mereka untuk menyegarkan pemeriksaan apa pun.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "trustedadvisor:*",
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": "trustedadvisor:RefreshCheck",
            "Resource": "*"
        }
    ]
}
```

Kontrol akses ke operasi AWS Support API untuk Trusted Advisor

Dalam AWS Management Console, namespace `trustedadvisor` IAM terpisah mengontrol akses ke. Trusted Advisor Anda tidak dapat menggunakan `trustedadvisor` namespace untuk mengizinkan atau menolak operasi Trusted Advisor API di AWS Support API. Sebagai gantinya, Anda menggunakan `support` namespace. Anda harus memiliki izin ke AWS Support API untuk memanggil secara Trusted Advisor terprogram.

Misalnya, jika Anda ingin memanggil RefreshTrustedAdvisorCheckoperasi, Anda harus memiliki izin untuk tindakan ini dalam kebijakan.

Example : Izinkan operasi Trusted Advisor API saja

Kebijakan berikut memungkinkan pengguna mengakses operasi AWS Support API untuk Trusted Advisor, tetapi tidak untuk operasi AWS Support API lainnya. Misalnya, pengguna dapat menggunakan API untuk melihat dan menyegarkan pemeriksaan. Mereka tidak dapat membuat, melihat, memperbarui, atau menyelesaikan AWS Support kasus.

Anda dapat menggunakan kebijakan ini untuk memanggil operasi Trusted Advisor API secara terprogram, tetapi Anda tidak dapat menggunakan kebijakan ini untuk melihat atau menyegarkan pemeriksaan di Trusted Advisor konsol.

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

```
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "support:DescribeTrustedAdvisorCheckRefreshStatuses",
                "support:DescribeTrustedAdvisorCheckResult",
                "support:DescribeTrustedAdvisorChecks",
                "support:DescribeTrustedAdvisorCheckSummaries",
                "support:RefreshTrustedAdvisorCheck",
                "trustedadvisor:Describe*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": [
                "support:AddAttachmentsToSet",
                "support:AddCommunicationToCase",
                "support:CreateCase",
                "support:DescribeAttachment",
                "support:DescribeCases",
                "support:DescribeCommunications",
                "support:DescribeServices",
                "support:DescribeSeverityLevels",
                "support:ResolveCase"
            ],
            "Resource": "*"
        }
    ]
}
```

Untuk informasi lebih lanjut tentang bagaimana IAM bekerja dengan AWS Support dan Trusted Advisor, lihatTindakan.

Contoh kebijakan IAM untuk Prioritas Trusted Advisor

Anda dapat menggunakan kebijakan AWS terkelola berikut untuk mengontrol akses ke Trusted Advisor Prioritas. Untuk informasi selengkapnya, lihat AWS kebijakan terkelola untuk AWS Trusted Advisor dan Memulai dengan AWS Trusted Advisor Prioritas.

Contoh kebijakan IAM untuk Engage Trusted Advisor

> **Note**
>
> Trusted Advisor Engage sedang dalam rilis pratinjau dan saat ini tidak memiliki kebijakan AWS terkelola apa pun. Anda dapat menggunakan salah satu kebijakan berikut untuk membuat kebijakan terkelola pelanggan di konsol IAM.

Contoh kebijakan yang memberikan akses baca dan tulis di Trusted Advisor Engage:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "trustedadvisor:CreateEngagement*",
                "trustedadvisor:DescribeAccount*",
                "trustedadvisor:GetEngagement*",
                "trustedadvisor:ListEngagement*",
                "trustedadvisor:UpdateEngagement*"
            ],
            "Resource": "*"
        }
    ]
}
```

Contoh kebijakan yang memberikan akses hanya-baca di Engage: Trusted Advisor

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "trustedadvisor:DescribeAccount*",
                "trustedadvisor:GetEngagement*",
                "trustedadvisor:ListEngagement*"
            ],
            "Resource": "*"
        }
```

```
    ]
}
```

Contoh kebijakan yang memberikan akses baca dan tulis di Trusted Advisor Engage dan kemampuan untuk mengaktifkan akses tepercaya ke Trusted Advisor:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "organizations:DescribeOrganization",
                "organizations:ListAWSServiceAccessForOrganization",
                "trustedadvisor:CreateEngagement*",
                "trustedadvisor:DescribeAccount*",
                "trustedadvisor:DescribeOrganization",
                "trustedadvisor:GetEngagement*",
                "trustedadvisor:ListEngagement*",
                "trustedadvisor:SetOrganizationAccess",
                "trustedadvisor:UpdateEngagement*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "organizations:EnableAWSServiceAccess",
                "organizations:DisableAWSServiceAccess"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "organizations:ServicePrincipal": [
                        "reporting.trustedadvisor.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
```

```
            "Resource": "arn:aws:iam::*:role/aws-service-role/
reporting.trustedadvisor.amazonaws.com/AWSServiceRoleForTrustedAdvisorReporting",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "reporting.trustedadvisor.amazonaws.com"
                }
            }
        }
    ]
}
```

Lihat juga

Untuk informasi selengkapnya tentang Trusted Advisor izin, lihat sumber daya berikut:

- Tindakan yang ditentukan oleh AWS Trusted Advisor dalam Panduan Pengguna IAM.
- Mengontrol Akses ke Trusted Advisor Konsol

Contoh Kebijakan Kontrol Layanan untuk AWS Trusted Advisor

AWS Trusted Advisor mendukung kebijakan kontrol layanan (SCP). SCP adalah kebijakan yang Anda lampirkan ke elemen dalam organisasi untuk mengelola izin dalam organisasi tersebut. SCP berlaku untuk semua AWS akun di bawah elemen tempat Anda melampirkan SCP. SCP menawarkan kontrol pusat atas izin maksimum yang tersedia untuk semua akun di organisasi Anda. Mereka dapat membantu Anda memastikan AWS akun Anda tetap berada dalam pedoman kontrol akses organisasi Anda. Untuk informasi selengkapnya, lihat Kebijakan kontrol layanan di Panduan Pengguna AWS Organizations .

Topik

- Prasyarat
- Contoh Kebijakan Kontrol Layanan

Prasyarat

Untuk menggunakan SCP, Anda harus terlebih dahulu melakukan hal berikut:

- Aktifkan semua fitur di organisasi Anda. Untuk informasi selengkapnya, lihat Mengaktifkan semua fitur di organisasi Anda dalam Panduan Pengguna AWS Organizations .

- Aktifkan SCP untuk digunakan dalam organisasi Anda. Untuk informasi selengkapnya, lihat Mengaktifkan dan menonaktifkan jenis kebijakan di Panduan Pengguna.AWS Organizations
- Buat SCP yang Anda butuhkan. Untuk informasi selengkapnya tentang membuat SCP, lihat Membuat, memperbarui, dan menghapus kebijakan kontrol layanan di AWS Organizations Panduan Pengguna.

Contoh Kebijakan Kontrol Layanan

Contoh berikut menunjukkan bagaimana Anda dapat mengontrol berbagai aspek berbagi sumber daya dalam suatu organisasi.

Example : Mencegah pengguna membuat atau mengedit keterlibatan di Engage Trusted Advisor

SCP berikut mencegah pengguna membuat keterlibatan baru atau mengedit keterlibatan yang ada.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "trustedadvisor:CreateEngagement",
        "trustedadvisor:UpdateEngagement*"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

Example : Tolak Trusted Advisor Keterlibatan dan Akses Trusted Advisor Prioritas

SCP berikut mencegah pengguna mengakses atau melakukan tindakan apa pun dalam Trusted Advisor Engage and Trusted Advisor Priority.

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

```
      "Action": [
        "trustedadvisor:ListEngagement*",
        "trustedadvisor:GetEngagement*",
        "trustedadvisor:CreateEngagement*",
        "trustedadvisor:UpdateEngagement*",
        "trustedadvisor:DescribeRisk*",
        "trustedadvisor:UpdateRisk*",
        "trustedadvisor:DownloadRisk"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

Memecahkan masalah AWS Support identitas dan akses

Gunakan informasi berikut untuk membantu Anda mendiagnosis dan memperbaiki masalah umum yang mungkin Anda temui saat bekerja dengan AWS Support dan IAM.

Topik

- Saya tidak berwenang untuk melakukan iam: PassRole
- Saya ingin melihat access key saya
- Saya seorang administrator dan ingin mengizinkan orang lain mengakses AWS Support
- Saya ingin mengizinkan orang di luar AWS akun saya untuk mengakses AWS Support sumber daya saya

Saya tidak berwenang untuk melakukan iam: PassRole

Jika Anda menerima kesalahan yang tidak diizinkan untuk melakukan `iam:PassRole` tindakan, kebijakan Anda harus diperbarui agar Anda dapat meneruskan peran AWS Support.

Beberapa Layanan AWS 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 tersebut untuk melakukan tindakan di AWS Support. 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 melihat access key saya

Setelah membuat access key pengguna IAM, Anda dapat melihat access key ID Anda setiap saat. Namun, Anda tidak dapat melihat secret access key Anda lagi. Jika Anda kehilangan secret key, Anda harus membuat pasangan access key baru.

Access key terdiri dari dua bagian: access key ID (misalnya, `AKIAIOSFODNN7EXAMPLE`) dan secret access key (misalnya, `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`). Seperti nama pengguna dan kata sandi, Anda harus menggunakan access key ID dan secret access key sekaligus untuk mengautentikasi permintaan Anda. Kelola access key Anda seaman nama pengguna dan kata sandi Anda.

> **Important**
>
> Jangan memberikan access key Anda kepada pihak ke tiga, bahkan untuk membantu menemukan ID pengguna kanonis Anda. Dengan melakukan ini, Anda mungkin memberi seseorang akses permanen ke Anda Akun AWS.

Saat Anda membuat pasangan access key, Anda diminta menyimpan access key ID dan secret access key di lokasi yang aman. secret access key hanya tersedia saat Anda membuatnya. Jika Anda kehilangan secret access key Anda, Anda harus menambahkan access key baru ke pengguna IAM Anda. Anda dapat memiliki maksimum dua access key. Jika Anda sudah memiliki dua, Anda harus menghapus satu pasangan kunci sebelum membuat pasangan baru. Untuk melihat instruksi, lihat Mengelola access keys di Panduan Pengguna IAM.

Saya seorang administrator dan ingin mengizinkan orang lain mengakses AWS Support

Untuk memungkinkan orang lain mengakses AWS Support, Anda harus membuat entitas IAM (pengguna atau peran) untuk orang atau aplikasi yang membutuhkan akses. Mereka akan menggunakan kredensial untuk entitas tersebut untuk mengakses AWS. Anda kemudian harus melampirkan kebijakan yang memberi mereka izin yang tepat di AWS Support.

Untuk segera memulai, lihat Membuat pengguna dan grup IAM pertama Anda yang didelegasikan di Panduan Pengguna IAM.

Saya ingin mengizinkan orang di luar AWS akun saya untuk mengakses AWS Support sumber daya 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 mempelajari apakah AWS Support mendukung fitur ini, lihatBagaimana AWS Support 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 penggunaan kebijakan peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Bagaimana peran IAM berbeda dari kebijakan berbasis sumber daya dalam Panduan Pengguna IAM.

Respons insiden

Respon insiden AWS Support adalah AWS tanggung jawab. AWS memiliki kebijakan dan program formal yang terdokumentasi yang mengatur respons insiden. Untuk informasi selengkapnya, lihat Whitepaper Memperkenalkan AWS Security Incident Response.

Gunakan opsi berikut untuk menginformasikan diri Anda tentang masalah operasional:

- Lihat masalah AWS operasional dengan dampak luas pada Dashboard AWS Service Health. Misalnya, peristiwa yang memengaruhi layanan atau Wilayah yang tidak spesifik untuk akun Anda.
- Lihat masalah operasional untuk akun individu di AWS Health Dashboard. Misalnya, peristiwa yang memengaruhi layanan atau sumber daya di akun Anda. Untuk informasi selengkapnya, lihat Memulai AWS Health Dashboard dalam Panduan Pengguna AWS Health .

Pencatatan dan pemantauan di AWS Support dan AWS Trusted Advisor

Pemantauan adalah bagian penting dari menjaga keandalan, ketersediaan, dan kinerja AWS Support dan AWS Trusted Advisor dan AWS solusi Anda yang lain. AWS menyediakan alat pemantauan berikut untuk menonton AWS Support dan AWS Trusted Advisor, melaporkan ketika ada sesuatu yang salah, dan mengambil tindakan 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 Elastic Compute Cloud (Amazon EC2) dan secara otomatis meluncurkan instans baru bila diperlukan. Untuk informasi selengkapnya, lihat Panduan CloudWatch Pengguna Amazon.
- Amazon EventBridge memberikan aliran peristiwa sistem yang mendekati real-time yang menggambarkan perubahan AWS sumber daya. EventBridge mengaktifkan komputasi berbasis peristiwa otomatis, karena Anda dapat menulis aturan yang mengawasi peristiwa tertentu dan memicu tindakan otomatis di AWS layanan lain saat peristiwa ini terjadi. Untuk informasi selengkapnya, lihat Panduan EventBridge Pengguna Amazon.
- AWS CloudTrailmenangkap panggilan API dan peristiwa terkait yang dibuat oleh atau atas nama AWS akun Anda dan mengirimkan file log ke bucket Amazon Simple Storage Service (Amazon S3)

yang Anda tentukan. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. Untuk informasi selengkapnya, silakan lihat Panduan Pengguna AWS CloudTrail.

Untuk informasi selengkapnya, lihat Pemantauan dan loggingAWS Support dan Pemantauan dan loggingAWS Trusted Advisor.

Validasi kepatuhan untuk AWS Support

Untuk mempelajari apakah an Layanan AWS berada dalam lingkup program kepatuhan tertentu, lihat Layanan AWS di Lingkup oleh Program Kepatuhan Layanan AWS 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 Layanan AWS 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 Layanan AWS 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 Layanan AWS 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 Layanan AWS 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 Layanan AWS 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 Layanan AWS membantu Anda terus mengaudit AWS penggunaan Anda untuk menyederhanakan cara Anda mengelola risiko dan kepatuhan terhadap peraturan dan standar industri.

Ketahanan di AWS Support

Infrastruktur AWS global dibangun di sekitar AWS Wilayah dan Zona Ketersediaan. AWS Wilayah menyediakan beberapa Availability Zone yang terpisah secara fisik dan terisolasi, yang terhubung dengan latensi rendah, throughput tinggi, dan jaringan yang sangat redundan. Dengan Availability Zone, Anda dapat mendesain dan mengoperasikan aplikasi dan basis data yang secara otomatis mengalami kegagalan 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 AWS Wilayah dan Availability Zone, lihat infrastruktur AWS global.

Keamanan infrastruktur di AWS Support

Sebagai layanan terkelola, AWS Support dilindungi oleh prosedur keamanan jaringan AWS global yang dijelaskan dalam Amazon Web Services: Ringkasan proses keamanan whitepaper.

Anda menggunakan panggilan API yang AWS dipublikasikan untuk mengakses AWS Support 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 sistem yang lebih baru mendukung 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.

Analisis konfigurasi dan kerentanan di AWS Support

Untuk AWS Trusted Advisor, AWS menangani tugas-tugas keamanan dasar seperti sistem operasi tamu (OS) dan patch database, konfigurasi firewall, dan pemulihan bencana.

Konfigurasi dan kontrol TI adalah tanggung jawab bersama antara AWS dan Anda, pelanggan kami. Untuk informasi selengkapnya, lihat model tanggung jawab AWS bersama.

Contoh kode untuk AWS Support menggunakan AWS SDK

Contoh kode berikut menunjukkan cara menggunakan AWS Support kit pengembangan AWS perangkat lunak (SDK).

Tindakan adalah kutipan kode dari program yang lebih besar dan harus dijalankan dalam konteks. Meskipun tindakan menunjukkan cara memanggil fungsi layanan individual, Anda dapat melihat tindakan dalam konteks pada skenario terkait dan contoh lintas layanan.

Skenario adalah contoh kode yang menunjukkan cara menyelesaikan tugas tertentu dengan memanggil beberapa fungsi dalam layanan yang sama.

Untuk daftar lengkap panduan pengembang AWS SDK dan contoh kode, lihatMenggunakan AWS Support dengan AWS SDK. Topik ini juga mencakup informasi tentang memulai dan detail tentang versi SDK sebelumnya.

Memulai

Halo AWS Support

Contoh kode berikut menunjukkan cara untuk mulai menggunakan AWS Support.

.NET

AWS SDK for .NET

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di AWS Repositori Contoh Kode.

```
using Amazon.AWSSupport;
using Microsoft.Extensions.DependencyInjection;
using Microsoft.Extensions.Hosting;

public static class HelloSupport
{
    static async Task Main(string[] args)
    {
```

```
        // Use the AWS .NET Core Setup package to set up dependency injection for
 the AWS Support service.
        // Use your AWS profile name, or leave it blank to use the default
 profile.
        // You must have one of the following AWS Support plans: Business,
 Enterprise On-Ramp, or Enterprise. Otherwise, an exception will be thrown.
        using var host = Host.CreateDefaultBuilder(args)
            .ConfigureServices((_, services) =>
                services.AddAWSService<IAmazonAWSSupport>()
            ).Build();

        // Now the client is available for injection.
        var supportClient =
 host.Services.GetRequiredService<IAmazonAWSSupport>();

        // You can use await and any of the async methods to get a response.
        var response = await supportClient.DescribeServicesAsync();
        Console.WriteLine($"\tHello AWS Support! There are
 {response.Services.Count} services available.");
    }
}
```

- Untuk detail API, lihat DescribeServicesdi Referensi AWS SDK for .NET API.

Java

SDK untuk Java 2.x

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di AWS Repositori Contoh Kode.

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.support.SupportClient;
import software.amazon.awssdk.services.support.model.Category;
import software.amazon.awssdk.services.support.model.DescribeServicesRequest;
import software.amazon.awssdk.services.support.model.DescribeServicesResponse;
import software.amazon.awssdk.services.support.model.Service;
import software.amazon.awssdk.services.support.model.SupportException;
```

```
import java.util.ArrayList;
import java.util.List;

/**
 * Before running this Java (v2) code example, set up your development
 * environment, including your credentials.
 *
 * For more information, see the following documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
 *
 * In addition, you must have the AWS Business Support Plan to use the AWS
 * Support Java API. For more information, see:
 *
 * https://aws.amazon.com/premiumsupport/plans/
 *
 * This Java example performs the following task:
 *
 * 1. Gets and displays available services.
 *
 *
 * NOTE: To see multiple operations, see SupportScenario.
 */

public class HelloSupport {
    public static void main(String[] args) {
        Region region = Region.US_WEST_2;
        SupportClient supportClient = SupportClient.builder()
                .region(region)
                .build();

        System.out.println("***** Step 1. Get and display available services.");
        displayServices(supportClient);
    }

    // Return a List that contains a Service name and Category name.
    public static void displayServices(SupportClient supportClient) {
        try {
            DescribeServicesRequest servicesRequest =
 DescribeServicesRequest.builder()
                    .language("en")
                    .build();
```

```
            DescribeServicesResponse response =
 supportClient.describeServices(servicesRequest);
            List<Service> services = response.services();

            System.out.println("Get the first 10 services");
            int index = 1;
            for (Service service : services) {
                if (index == 11)
                    break;

                System.out.println("The Service name is: " + service.name());

                // Display the Categories for this service.
                List<Category> categories = service.categories();
                for (Category cat : categories) {
                    System.out.println("The category name is: " + cat.name());
                }
                index++;
            }

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }
}
```

- Untuk detail API, lihat DescribeServicesdi Referensi AWS SDK for Java 2.x API.

JavaScript

SDK untuk JavaScript (v3)

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di AWS Repositori Contoh Kode.

Panggil `main () `untuk menjalankan contoh.

```
import {
  DescribeServicesCommand,
  SupportClient,
} from "@aws-sdk/client-support";

// Change the value of 'region' to your preferred AWS Region.
const client = new SupportClient({ region: "us-east-1" });

const getServiceCount = async () => {
  try {
    const { services } = await client.send(new DescribeServicesCommand({}));
    return services.length;
  } catch (err) {
    if (err.name === "SubscriptionRequiredException") {
      throw new Error(
        "You must be subscribed to the AWS Support plan to use this feature.",
      );
    } else {
      throw err;
    }
  }
};

export const main = async () => {
  try {
    const count = await getServiceCount();
    console.log(`Hello, AWS Support! There are ${count} services available.`);
  } catch (err) {
    console.error("Failed to get service count: ", err.message);
  }
};
```

- Untuk detail API, lihat DescribeServicesdi Referensi AWS SDK for JavaScript API.

Kotlin

SDK untuk Kotlin

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di AWS Repositori Contoh Kode.

```
/**
Before running this Kotlin code example, set up your development environment,
including your credentials.

For more information, see the following documentation topic:
https://docs.aws.amazon.com/sdk-for-kotlin/latest/developer-guide/setup.html

In addition, you must have the AWS Business Support Plan to use the AWS Support
 Java API. For more information, see:

https://aws.amazon.com/premiumsupport/plans/

This Kotlin example performs the following task:

1. Gets and displays available services.
 */

suspend fun main() {
    displaySomeServices()
}

// Return a List that contains a Service name and Category name.
suspend fun displaySomeServices() {
    val servicesRequest =
        DescribeServicesRequest {
            language = "en"
        }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.describeServices(servicesRequest)
        println("Get the first 10 services")
```

```
        var index = 1

        response.services?.forEach { service ->
            if (index == 11) {
                return@forEach
            }

            println("The Service name is: " + service.name)

            // Get the categories for this service.
            service.categories?.forEach { cat ->
                println("The category name is ${cat.name}")
                index++
            }
        }
    }
}
```

- Untuk detail API, lihat DescribeServicesdi AWS SDK untuk referensi API Kotlin.

Python

SDK untuk Python (Boto3)

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di AWS Repositori Contoh Kode.

```
import logging
import boto3
from botocore.exceptions import ClientError

logger = logging.getLogger(__name__)


def hello_support(support_client):
    """
    Use the AWS SDK for Python (Boto3) to create an AWS Support client and count
```

```
    the available services in your account.
    This example uses the default settings specified in your shared credentials
    and config files.

    :param support_client: A Boto3 Support Client object.
    """
    try:
        print("Hello, AWS Support! Let's count the available Support services:")
        response = support_client.describe_services()
        print(f"There are {len(response['services'])} services available.")
    except ClientError as err:
        if err.response["Error"]["Code"] == "SubscriptionRequiredException":
            logger.info(
                "You must have a Business, Enterprise On-Ramp, or Enterprise
 Support "
                "plan to use the AWS Support API. \n\tPlease upgrade your
 subscription to run these "
                "examples."
            )
        else:
            logger.error(
                "Couldn't count services. Here's why: %s: %s",
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise


if __name__ == "__main__":
    hello_support(boto3.client("support"))
```

- Untuk detail API, lihat DescribeServicesdi AWS SDK for Python (Boto3) Referensi API.

Contoh kode

- Tindakan untuk AWS Support menggunakan AWS SDK
  - Gunakan AddAttachmentsToSet dengan AWS SDK atau CLI
  - Gunakan AddCommunicationToCase dengan AWS SDK atau CLI
  - Gunakan CreateCase dengan AWS SDK atau CLI
  - Gunakan DescribeAttachment dengan AWS SDK atau CLI

- Gunakan DescribeCases dengan AWS SDK atau CLI
- Gunakan DescribeCommunications dengan AWS SDK atau CLI
- Gunakan DescribeServices dengan AWS SDK atau CLI
- Gunakan DescribeSeverityLevels dengan AWS SDK atau CLI
- Gunakan DescribeTrustedAdvisorCheckRefreshStatuses dengan AWS SDK atau CLI
- Gunakan DescribeTrustedAdvisorCheckResult dengan AWS SDK atau CLI
- Gunakan DescribeTrustedAdvisorCheckSummaries dengan AWS SDK atau CLI
- Gunakan DescribeTrustedAdvisorChecks dengan AWS SDK atau CLI
- Gunakan RefreshTrustedAdvisorCheck dengan AWS SDK atau CLI
- Gunakan ResolveCase dengan AWS SDK atau CLI

- Skenario untuk AWS Support menggunakan AWS SDK
  - Memulai AWS Support kasus menggunakan AWS SDK

Tindakan untuk AWS Support menggunakan AWS SDK

Contoh kode berikut menunjukkan cara melakukan AWS Support tindakan individual dengan AWS SDK. Kutipan ini memanggil AWS Support API dan merupakan kutipan kode dari program yang lebih besar yang harus dijalankan dalam konteks. Setiap contoh menyertakan tautan ke GitHub, di mana Anda dapat menemukan instruksi untuk mengatur dan menjalankan kode.

Contoh berikut hanya mencakup tindakan yang paling umum digunakan. Untuk daftar lengkapnya, lihat Referensi AWS Support API.

Contoh

- Gunakan AddAttachmentsToSet dengan AWS SDK atau CLI
- Gunakan AddCommunicationToCase dengan AWS SDK atau CLI
- Gunakan CreateCase dengan AWS SDK atau CLI
- Gunakan DescribeAttachment dengan AWS SDK atau CLI
- Gunakan DescribeCases dengan AWS SDK atau CLI
- Gunakan DescribeCommunications dengan AWS SDK atau CLI
- Gunakan DescribeServices dengan AWS SDK atau CLI
- Gunakan DescribeSeverityLevels dengan AWS SDK atau CLI
- Gunakan DescribeTrustedAdvisorCheckRefreshStatuses dengan AWS SDK atau CLI

- Gunakan DescribeTrustedAdvisorCheckResult dengan AWS SDK atau CLI
- Gunakan DescribeTrustedAdvisorCheckSummaries dengan AWS SDK atau CLI
- Gunakan DescribeTrustedAdvisorChecks dengan AWS SDK atau CLI
- Gunakan RefreshTrustedAdvisorCheck dengan AWS SDK atau CLI
- Gunakan ResolveCase dengan AWS SDK atau CLI

Gunakan **AddAttachmentsToSet** dengan AWS SDK atau CLI

Contoh kode berikut menunjukkan cara menggunakan`AddAttachmentsToSet`.

Contoh tindakan adalah kutipan kode dari program yang lebih besar dan harus dijalankan dalam konteks. Anda dapat melihat tindakan ini dalam konteks dalam contoh kode berikut:

- Memulai kasus

.NET

AWS SDK for .NET

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di AWS Repositori Contoh Kode.

```
   /// <summary>
   /// Add an attachment to a set, or create a new attachment set if one does
not exist.
   /// </summary>
   /// <param name="data">The data for the attachment.</param>
   /// <param name="fileName">The file name for the attachment.</param>
   /// <param name="attachmentSetId">Optional setId for the attachment. Creates
a new attachment set if empty.</param>
   /// <returns>The setId of the attachment.</returns>
   public async Task<string> AddAttachmentToSet(MemoryStream data, string
fileName, string? attachmentSetId = null)
   {
```

```
        var response = await _amazonSupport.AddAttachmentsToSetAsync(
            new AddAttachmentsToSetRequest
            {
                AttachmentSetId = attachmentSetId,
                Attachments = new List<Attachment>
                {
                    new Attachment
                    {
                        Data = data,
                        FileName = fileName
                    }
                }
            });
        return response.AttachmentSetId;
    }
```

- Untuk detail API, lihat AddAttachmentsToSetdi Referensi AWS SDK for .NET API.

CLI

AWS CLI

Untuk menambahkan lampiran ke set

`add-attachments-to-set`Contoh berikut menambahkan gambar ke set yang kemudian dapat Anda tentukan untuk kasus dukungan di AWS akun Anda.

```
aws support add-attachments-to-set \
    --attachment-set-id "as-2f5a6faa2a4a1e600-mu-nk5xQlBr70-
G1cUos5LZkd38KOAHZa9BMDVzNEXAMPLE" \
    --attachments fileName=troubleshoot-screenshot.png,data=base64-encoded-string
```

Output:

```
{
    "attachmentSetId": "as-2f5a6faa2a4a1e600-mu-nk5xQlBr70-
G1cUos5LZkd38KOAHZa9BMDVzNEXAMPLE",
    "expiryTime": "2020-05-14T17:04:40.790+0000"
}
```

Untuk informasi selengkapnya, lihat Manajemen kasus di AWS Support User Guide.

- Untuk detail API, lihat AddAttachmentsToSetdi Referensi AWS CLI Perintah.

Java

SDK untuk Java 2.x

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di AWS Repositori Contoh Kode.

```
   public static String addAttachment(SupportClient supportClient, String
fileAttachment) {
       try {
           File myFile = new File(fileAttachment);
           InputStream sourceStream = new FileInputStream(myFile);
           SdkBytes sourceBytes = SdkBytes.fromInputStream(sourceStream);

           Attachment attachment = Attachment.builder()
                   .fileName(myFile.getName())
                   .data(sourceBytes)
                   .build();

           AddAttachmentsToSetRequest setRequest =
AddAttachmentsToSetRequest.builder()
                   .attachments(attachment)
                   .build();

           AddAttachmentsToSetResponse response =
supportClient.addAttachmentsToSet(setRequest);
           return response.attachmentSetId();

       } catch (SupportException | FileNotFoundException e) {
           System.out.println(e.getLocalizedMessage());
           System.exit(1);
       }
       return "";
   }
```

- Untuk detail API, lihat AddAttachmentsToSetdi Referensi AWS SDK for Java 2.x API.

JavaScript

SDK untuk JavaScript (v3)

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di AWS Repositori Contoh Kode.

```
import { AddAttachmentsToSetCommand } from "@aws-sdk/client-support";

import { client } from "../libs/client.js";

export const main = async () => {
  try {
    // Create a new attachment set or add attachments to an existing set.
    // Provide an 'attachmentSetId' value to add attachments to an existing set.
    // Use AddCommunicationToCase or CreateCase to associate an attachment set
 with a support case.
    const response = await client.send(
      new AddAttachmentsToSetCommand({
        // You can add up to three attachments per set. The size limit is 5 MB
 per attachment.
        attachments: [
          {
            fileName: "example.txt",
            data: new TextEncoder().encode("some example text"),
          },
        ],
      }),
    );
    // Use this ID in AddCommunicationToCase or CreateCase.
    console.log(response.attachmentSetId);
    return response;
  } catch (err) {
    console.error(err);
  }
};
```

- Untuk detail API, lihat AddAttachmentsToSetdi Referensi AWS SDK for JavaScript API.

Kotlin

SDK untuk Kotlin

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di AWS Repositori Contoh Kode.

```
suspend fun addAttachment(fileAttachment: String): String? {
    val myFile = File(fileAttachment)
    val sourceBytes = (File(fileAttachment).readBytes())
    val attachmentVal =
        Attachment {
            fileName = myFile.name
            data = sourceBytes
        }

    val setRequest =
        AddAttachmentsToSetRequest {
            attachments = listOf(attachmentVal)
        }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.addAttachmentsToSet(setRequest)
        return response.attachmentSetId
    }
}
```

- Untuk detail API, lihat AddAttachmentsToSetdi AWS SDK untuk referensi API Kotlin.

Python

SDK untuk Python (Boto3)

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di AWS Repositori Contoh Kode.

```
class SupportWrapper:
    """Encapsulates Support actions."""

    def __init__(self, support_client):
        """
        :param support_client: A Boto3 Support client.
        """
        self.support_client = support_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        support_client = boto3.client("support")
        return cls(support_client)


    def add_attachment_to_set(self):
        """
        Add an attachment to a set, or create a new attachment set if one does
 not exist.

        :return: The attachment set ID.
        """
        try:
            response = self.support_client.add_attachments_to_set(
                attachments=[
                    {
                        "fileName": "attachment_file.txt",
                        "data": b"This is a sample file for attachment to a
 support case.",
```

```
                    }
                ]
            )
            new_set_id = response["attachmentSetId"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't add attachment. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return new_set_id
```

- Untuk detail API, lihat AddAttachmentsToSetdi AWS SDK for Python (Boto3) Referensi API.

Untuk daftar lengkap panduan pengembang AWS SDK dan contoh kode, lihatMenggunakan AWS Support dengan AWS SDK. Topik ini juga mencakup informasi tentang memulai dan detail tentang versi SDK sebelumnya.

Gunakan **`AddCommunicationToCase`** dengan AWS SDK atau CLI

Contoh kode berikut menunjukkan cara menggunakan`AddCommunicationToCase`.

Contoh tindakan adalah kutipan kode dari program yang lebih besar dan harus dijalankan dalam konteks. Anda dapat melihat tindakan ini dalam konteks dalam contoh kode berikut:

- Memulai kasus

.NET

AWS SDK for .NET

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di AWS Repositori Contoh Kode.

```
    /// <summary>
    /// Add communication to a case, including optional attachment set ID and CC
 email addresses.
    /// </summary>
    /// <param name="caseId">Id for the support case.</param>
    /// <param name="body">Body text of the communication.</param>
    /// <param name="attachmentSetId">Optional Id for an attachment set.</param>
    /// <param name="ccEmailAddresses">Optional list of CC email addresses.</
param>
    /// <returns>True if successful.</returns>
    public async Task<bool> AddCommunicationToCase(string caseId, string body,
        string? attachmentSetId = null, List<string>? ccEmailAddresses = null)
    {
        var response = await _amazonSupport.AddCommunicationToCaseAsync(
            new AddCommunicationToCaseRequest()
            {
                CaseId = caseId,
                CommunicationBody = body,
                AttachmentSetId = attachmentSetId,
                CcEmailAddresses = ccEmailAddresses
            });
        return response.Result;
    }
```

- Untuk detail API, lihat AddCommunicationToCasedi Referensi AWS SDK for .NET API.

CLI

AWS CLI

Untuk menambahkan komunikasi ke sebuah kasus

`add-communication-to-case`Contoh berikut menambahkan komunikasi ke kasus dukungan di AWS akun Anda.

```
aws support add-communication-to-case \
    --case-id "case-12345678910-2013-c4c1d2bf33c5cf47" \
    --communication-body "I'm attaching a set of images to this case." \
    --cc-email-addresses "myemail@example.com" \
    --attachment-set-id "as-2f5a6faa2a4a1e600-mu-nk5xQlBr70-
G1cUos5LZkd38KOAHZa9BMDVzNEXAMPLE"
```

Output:

```
{
    "result": true
}
```

Untuk informasi selengkapnya, lihat Manajemen kasus di AWS Support User Guide.

- Untuk detail API, lihat AddCommunicationToCasedi Referensi AWS CLI Perintah.

Java

SDK untuk Java 2.x

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di AWS Repositori Contoh Kode.

```
   public static void addAttachSupportCase(SupportClient supportClient, String
 caseId, String attachmentSetId) {
       try {
           AddCommunicationToCaseRequest caseRequest =
AddCommunicationToCaseRequest.builder()
```

```
                    .caseId(caseId)
                    .attachmentSetId(attachmentSetId)
                    .communicationBody("Please refer to attachment for details.")
                    .build();

            AddCommunicationToCaseResponse response =
 supportClient.addCommunicationToCase(caseRequest);
            if (response.result())
                System.out.println("You have successfully added a communication
 to an AWS Support case");
            else
                System.out.println("There was an error adding the communication
 to an AWS Support case");

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }
```

- Untuk detail API, lihat AddCommunicationToCasedi Referensi AWS SDK for Java 2.x API.

JavaScript

SDK untuk JavaScript (v3)

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di AWS Repositori Contoh Kode.

```
import { AddCommunicationToCaseCommand } from "@aws-sdk/client-support";

import { client } from "../libs/client.js";

export const main = async () => {
  let attachmentSetId;

  try {
    // Add a communication to a case.
```

```
    const response = await client.send(
      new AddCommunicationToCaseCommand({
        communicationBody: "Adding an attachment.",
        // Set value to an existing support case id.
        caseId: "CASE_ID",
        // Optional. Set value to an existing attachment set id to add
 attachments to the case.
        attachmentSetId,
      }),
    );
    console.log(response);
    return response;
  } catch (err) {
    console.error(err);
  }
};
```

- Untuk detail API, lihat AddCommunicationToCasedi Referensi AWS SDK for JavaScript API.

Kotlin

SDK untuk Kotlin

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di AWS Repositori Contoh Kode.

```
suspend fun addAttachSupportCase(
    caseIdVal: String?,
    attachmentSetIdVal: String?
) {
    val caseRequest =
        AddCommunicationToCaseRequest {
            caseId = caseIdVal
            attachmentSetId = attachmentSetIdVal
            communicationBody = "Please refer to attachment for details."
        }

    SupportClient { region = "us-west-2" }.use { supportClient ->
```

```
        val response = supportClient.addCommunicationToCase(caseRequest)
        if (response.result) {
            println("You have successfully added a communication to an AWS
 Support case")
        } else {
            println("There was an error adding the communication to an AWS
 Support case")
        }
    }
}
```

- Untuk detail API, lihat AddCommunicationToCasedi AWS SDK untuk referensi API Kotlin.

PowerShell

Alat untuk PowerShell

Contoh 1: Menambahkan badan komunikasi email ke kasus yang ditentukan.

```
Add-ASACommunicationToCase -CaseId "case-12345678910-2013-c4c1d2bf33c5cf47" -
CommunicationBody "Some text about the case"
```

Contoh 2: Menambahkan badan komunikasi email ke kasus yang ditentukan ditambah satu atau lebih alamat email yang terkandung dalam baris CC email.

```
Add-ASACommunicationToCase -CaseId "case-12345678910-2013-c4c1d2bf33c5cf47" -
CcEmailAddress @("email1@address.com", "email2@address.com") -CommunicationBody
 "Some text about the case"
```

- Untuk detail API, lihat AddCommunicationToCasedi Referensi AWS Tools for PowerShell Cmdlet.

Python

SDK untuk Python (Boto3)

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di AWS Repositori Contoh Kode.

```
class SupportWrapper:
    """Encapsulates Support actions."""

    def __init__(self, support_client):
        """
        :param support_client: A Boto3 Support client.
        """
        self.support_client = support_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        support_client = boto3.client("support")
        return cls(support_client)


    def add_communication_to_case(self, attachment_set_id, case_id):
        """
        Add a communication and an attachment set to a case.

        :param attachment_set_id: The ID of an existing attachment set.
        :param case_id: The ID of the case.
        """
        try:
            self.support_client.add_communication_to_case(
                caseId=case_id,
                communicationBody="This is an example communication added to a
 support case.",
                attachmentSetId=attachment_set_id,
            )
```

```
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't add communication. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
```

- Untuk detail API, lihat AddCommunicationToCasedi AWS SDK for Python (Boto3) Referensi API.

Untuk daftar lengkap panduan pengembang AWS SDK dan contoh kode, lihatMenggunakan AWS Support dengan AWS SDK. Topik ini juga mencakup informasi tentang memulai dan detail tentang versi SDK sebelumnya.

Gunakan **`CreateCase`** dengan AWS SDK atau CLI

Contoh kode berikut menunjukkan cara menggunakan`CreateCase`.

Contoh tindakan adalah kutipan kode dari program yang lebih besar dan harus dijalankan dalam konteks. Anda dapat melihat tindakan ini dalam konteks dalam contoh kode berikut:

- Memulai kasus

.NET

AWS SDK for .NET

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di AWS Repositori Contoh Kode.

```
   /// <summary>
   /// Create a new support case.
   /// </summary>
   /// <param name="serviceCode">Service code for the new case.</param>
   /// <param name="categoryCode">Category for the new case.</param>
   /// <param name="severityCode">Severity code for the new case.</param>
   /// <param name="subject">Subject of the new case.</param>
   /// <param name="body">Body text of the new case.</param>
   /// <param name="language">Optional language support for your case.
   /// Currently Chinese (“zh”), English ("en"), Japanese ("ja") and Korean
(“ko”) are supported.</param>
   /// <param name="attachmentSetId">Optional Id for an attachment set for the
new case.</param>
   /// <param name="issueType">Optional issue type for the new case. Options are
"customer-service" or "technical".</param>
   /// <returns>The caseId of the new support case.</returns>
   public async Task<string> CreateCase(string serviceCode, string categoryCode,
string severityCode, string subject,
       string body, string language = "en", string? attachmentSetId = null,
string issueType = "customer-service")
   {
       var response = await _amazonSupport.CreateCaseAsync(
           new CreateCaseRequest()
           {
               ServiceCode = serviceCode,
               CategoryCode = categoryCode,
               SeverityCode = severityCode,
               Subject = subject,
               Language = language,
               AttachmentSetId = attachmentSetId,
               IssueType = issueType,
```

```
                CommunicationBody = body
            });
        return response.CaseId;
    }
```

- Untuk detail API, lihat CreateCasedi Referensi AWS SDK for .NET API.

CLI

AWS CLI

Untuk membuat kasus

`create-case`Contoh berikut membuat kasus dukungan untuk AWS akun Anda.

```
aws support create-case \
    --category-code "using-aws" \
    --cc-email-addresses "myemail@example.com" \
    --communication-body "I want to learn more about an AWS service." \
    --issue-type "technical" \
    --language "en" \
    --service-code "general-info" \
    --severity-code "low" \
    --subject "Question about my account"
```

Output:

```
{
    "caseId": "case-12345678910-2013-c4c1d2bf33c5cf47"
}
```

Untuk informasi selengkapnya, lihat Manajemen kasus di AWS Support User Guide.

- Untuk detail API, lihat CreateCasedi Referensi AWS CLI Perintah.

Java

SDK untuk Java 2.x

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di AWS Repositori Contoh Kode.

```
   public static String createSupportCase(SupportClient supportClient,
List<String> sevCatList, String sevLevel) {
       try {
           String serviceCode = sevCatList.get(0);
           String caseCat = sevCatList.get(1);
           CreateCaseRequest caseRequest = CreateCaseRequest.builder()
                   .categoryCode(caseCat.toLowerCase())
                   .serviceCode(serviceCode.toLowerCase())
                   .severityCode(sevLevel.toLowerCase())
                   .communicationBody("Test issue with " +
serviceCode.toLowerCase())
                   .subject("Test case, please ignore")
                   .language("en")
                   .issueType("technical")
                   .build();

           CreateCaseResponse response = supportClient.createCase(caseRequest);
           return response.caseId();

       } catch (SupportException e) {
           System.out.println(e.getLocalizedMessage());
           System.exit(1);
       }
       return "";
   }
```

- Untuk detail API, lihat CreateCasedi Referensi AWS SDK for Java 2.x API.

JavaScript

SDK untuk JavaScript (v3)

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di AWS Repositori Contoh Kode.

```
import { CreateCaseCommand } from "@aws-sdk/client-support";

import { client } from "../libs/client.js";

export const main = async () => {
  try {
    // Create a new case and log the case id.
    // Important: This creates a real support case in your account.
    const response = await client.send(
      new CreateCaseCommand({
        // The subject line of the case.
        subject: "IGNORE: Test case",
        // Use DescribeServices to find available service codes for each service.
        serviceCode: "service-quicksight-end-user",
        // Use DescribeSecurityLevels to find available severity codes for your
 support plan.
        severityCode: "low",
        // Use DescribeServices to find available category codes for each
 service.
        categoryCode: "end-user-support",
        // The main description of the support case.
        communicationBody: "This is a test. Please ignore.",
      }),
    );
    console.log(response.caseId);
    return response;
  } catch (err) {
    console.error(err);
  }
};
```

- Untuk detail API, lihat CreateCasedi Referensi AWS SDK for JavaScript API.

Kotlin

SDK untuk Kotlin

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di AWS Repositori Contoh Kode.

```
suspend fun createSupportCase(
    sevCatListVal: List<String>,
    sevLevelVal: String
): String? {
    val serCode = sevCatListVal[0]
    val caseCategory = sevCatListVal[1]
    val caseRequest =
        CreateCaseRequest {
            categoryCode = caseCategory.lowercase(Locale.getDefault())
            serviceCode = serCode.lowercase(Locale.getDefault())
            severityCode = sevLevelVal.lowercase(Locale.getDefault())
            communicationBody = "Test issue with
 ${serCode.lowercase(Locale.getDefault())}"
            subject = "Test case, please ignore"
            language = "en"
            issueType = "technical"
        }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.createCase(caseRequest)
        return response.caseId
    }
}
```

- Untuk detail API, lihat CreateCasedi AWS SDK untuk referensi API Kotlin.

PowerShell

Alat untuk PowerShell

Contoh 1: Membuat kasus baru di AWS Support Center. Nilai untuk CategoryCode parameter - ServiceCode dan - dapat diperoleh dengan menggunakan cmdlet Get-AsaService. Nilai untuk SeverityCode parameter - dapat diperoleh dengan menggunakan cmdlet SeverityLevel Get-Asa. Nilai - IssueType parameter dapat berupa “layanan pelanggan” atau “teknis”. Jika berhasil, nomor kasus AWS Support adalah output. Secara default kasus akan ditangani dalam bahasa Inggris, untuk menggunakan bahasa Jepang tambahkan parameter -Language “ja”. CommunicationBody Parameter -ServiceCode, -CategoryCode, -Subjek dan - adalah wajib.

```
New-ASACase -ServiceCode "amazon-cloudfront" -CategoryCode "APIs" -SeverityCode
 "low" -Subject "subject text" -CommunicationBody "description of the case" -
CcEmailAddress @("email1@domain.com", "email2@domain.com") -IssueType "technical"
```

- Untuk detail API, lihat CreateCasedi Referensi AWS Tools for PowerShell Cmdlet.

Python

SDK untuk Python (Boto3)

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di AWS Repositori Contoh Kode.

```
class SupportWrapper:
    """Encapsulates Support actions."""

    def __init__(self, support_client):
        """
        :param support_client: A Boto3 Support client.
        """
        self.support_client = support_client

    @classmethod
    def from_client(cls):
```

```
        """
        Instantiates this class from a Boto3 client.
        """
        support_client = boto3.client("support")
        return cls(support_client)


    def create_case(self, service, category, severity):
        """
        Create a new support case.

        :param service: The service to use for the new case.
        :param category: The category to use for the new case.
        :param severity: The severity to use for the new case.
        :return: The caseId of the new case.
        """
        try:
            response = self.support_client.create_case(
                subject="Example case for testing, ignore.",
                serviceCode=service["code"],
                severityCode=severity["code"],
                categoryCode=category["code"],
                communicationBody="Example support case body.",
                language="en",
                issueType="customer-service",
            )
            case_id = response["caseId"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't create case. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
```

```
            return case_id
```

- Untuk detail API, lihat CreateCasedi AWS SDK for Python (Boto3) Referensi API.

Untuk daftar lengkap panduan pengembang AWS SDK dan contoh kode, lihatMenggunakan AWS Support dengan AWS SDK. Topik ini juga mencakup informasi tentang memulai dan detail tentang versi SDK sebelumnya.

Gunakan **`DescribeAttachment`** dengan AWS SDK atau CLI

Contoh kode berikut menunjukkan cara menggunakan`DescribeAttachment`.

Contoh tindakan adalah kutipan kode dari program yang lebih besar dan harus dijalankan dalam konteks. Anda dapat melihat tindakan ini dalam konteks dalam contoh kode berikut:

- Memulai kasus

.NET

AWS SDK for .NET

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di AWS Repositori Contoh Kode.

```
    /// <summary>
    /// Get description of a specific attachment.
    /// </summary>
    /// <param name="attachmentId">Id of the attachment, usually fetched by
describing the communications of a case.</param>
    /// <returns>The attachment object.</returns>
    public async Task<Attachment> DescribeAttachment(string attachmentId)
    {
        var response = await _amazonSupport.DescribeAttachmentAsync(
```

```
            new DescribeAttachmentRequest()
            {
                AttachmentId = attachmentId
            });
        return response.Attachment;
    }
```

- Untuk detail API, lihat DescribeAttachmentdi Referensi AWS SDK for .NET API.

CLI

AWS CLI

Untuk menggambarkan lampiran

`describe-attachment`Contoh berikut mengembalikan informasi tentang lampiran dengan ID yang ditentukan.

```
aws support describe-attachment \
    --attachment-id "attachment-KBnjRNrePd9D6Jx0-Mm00xZuDEaL2JAj_0-
gJv9qqDooTipsz3V1Nb19rCfkZneeQeDPgp8X1iVJyHH7UuhZDdNeqGoduZsPrAhyMakqlc60-
iJjL5HqyYGiT1FG8EXAMPLE"
```

Output:

```
{
    "attachment": {
        "fileName": "troubleshoot-screenshot.png",
        "data": "base64-blob"
    }
}
```

Untuk informasi selengkapnya, lihat Manajemen kasus di AWS Support User Guide.

- Untuk detail API, lihat DescribeAttachmentdi Referensi AWS CLI Perintah.

Java

SDK untuk Java 2.x

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di AWS Repositori Contoh Kode.

```
   public static void describeAttachment(SupportClient supportClient, String
attachId) {
       try {
           DescribeAttachmentRequest attachmentRequest =
DescribeAttachmentRequest.builder()
                   .attachmentId(attachId)
                   .build();

           DescribeAttachmentResponse response =
supportClient.describeAttachment(attachmentRequest);
           System.out.println("The name of the file is " +
response.attachment().fileName());

       } catch (SupportException e) {
           System.out.println(e.getLocalizedMessage());
           System.exit(1);
       }
   }
```

- Untuk detail API, lihat DescribeAttachmentdi Referensi AWS SDK for Java 2.x API.

JavaScript

SDK untuk JavaScript (v3)

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di AWS Repositori Contoh Kode.

```
import { DescribeAttachmentCommand } from "@aws-sdk/client-support";

import { client } from "../libs/client.js";

export const main = async () => {
  try {
    // Get the metadata and content of an attachment.
    const response = await client.send(
      new DescribeAttachmentCommand({
        // Set value to an existing attachment id.
        // Use DescribeCommunications or DescribeCases to find an attachment id.
        attachmentId: "ATTACHMENT_ID",
      }),
    );
    console.log(response.attachment?.fileName);
    return response;
  } catch (err) {
    console.error(err);
  }
};
```

- Untuk detail API, lihat DescribeAttachmentdi Referensi AWS SDK for JavaScript API.

Kotlin

SDK untuk Kotlin

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di AWS Repositori Contoh Kode.

```
suspend fun describeAttachment(attachId: String?) {
    val attachmentRequest =
        DescribeAttachmentRequest {
            attachmentId = attachId
        }

    SupportClient { region = "us-west-2" }.use { supportClient ->
```

```
        val response = supportClient.describeAttachment(attachmentRequest)
        println("The name of the file is ${response.attachment?.fileName}")
    }
}
```

- Untuk detail API, lihat DescribeAttachmentdi AWS SDK untuk referensi API Kotlin.

Python

SDK untuk Python (Boto3)

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di AWS Repositori Contoh Kode.

```
class SupportWrapper:
    """Encapsulates Support actions."""

    def __init__(self, support_client):
        """
        :param support_client: A Boto3 Support client.
        """
        self.support_client = support_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        support_client = boto3.client("support")
        return cls(support_client)


    def describe_attachment(self, attachment_id):
        """
        Get information about an attachment by its attachmentID.

        :param attachment_id: The ID of the attachment.
        :return: The name of the attached file.
```

```
        """
        try:
            response = self.support_client.describe_attachment(
                attachmentId=attachment_id
            )
            attached_file = response["attachment"]["fileName"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't get attachment description. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return attached_file
```

- Untuk detail API, lihat DescribeAttachmentdi AWS SDK for Python (Boto3) Referensi API.

Untuk daftar lengkap panduan pengembang AWS SDK dan contoh kode, lihatMenggunakan AWS Support dengan AWS SDK. Topik ini juga mencakup informasi tentang memulai dan detail tentang versi SDK sebelumnya.

Gunakan **`DescribeCases`** dengan AWS SDK atau CLI

Contoh kode berikut menunjukkan cara menggunakan`DescribeCases`.

Contoh tindakan adalah kutipan kode dari program yang lebih besar dan harus dijalankan dalam konteks. Anda dapat melihat tindakan ini dalam konteks dalam contoh kode berikut:

- Memulai kasus

.NET

AWS SDK for .NET

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di AWS Repositori Contoh Kode.

```
    /// <summary>
    /// Get case details for a list of case ids, optionally with date filters.
    /// </summary>
    /// <param name="caseIds">The list of case IDs.</param>
    /// <param name="displayId">Optional display ID.</param>
    /// <param name="includeCommunication">True to include communication.
 Defaults to true.</param>
    /// <param name="includeResolvedCases">True to include resolved cases.
 Defaults to false.</param>
    /// <param name="afterTime">The optional start date for a filtered search.</
param>
    /// <param name="beforeTime">The optional end date for a filtered search.</
param>
    /// <param name="language">Optional language support for your case.
    /// Currently Chinese (“zh”), English ("en"), Japanese ("ja") and Korean
 (“ko”) are supported.</param>
    /// <returns>A list of CaseDetails.</returns>
    public async Task<List<CaseDetails>> DescribeCases(List<string> caseIds,
 string? displayId = null, bool includeCommunication = true,
        bool includeResolvedCases = false, DateTime? afterTime = null, DateTime?
 beforeTime = null,
        string language = "en")
    {
        var results = new List<CaseDetails>();
        var paginateCases = _amazonSupport.Paginators.DescribeCases(
            new DescribeCasesRequest()
            {
                CaseIdList = caseIds,
                DisplayId = displayId,
                IncludeCommunications = includeCommunication,
                IncludeResolvedCases = includeResolvedCases,
```

```
                AfterTime = afterTime?.ToString("s"),
                BeforeTime = beforeTime?.ToString("s"),
                Language = language
            });
        // Get the entire list using the paginator.
        await foreach (var cases in paginateCases.Cases)
        {
            results.Add(cases);
        }
        return results;
    }
```

- Untuk detail API, lihat DescribeCasesdi Referensi AWS SDK for .NET API.

CLI

AWS CLI

Untuk menggambarkan sebuah kasus

`describe-cases`Contoh berikut mengembalikan informasi tentang kasus dukungan yang ditentukan di AWS akun Anda.

```
aws support describe-cases \
    --display-id "1234567890" \
    --after-time "2020-03-23T21:31:47.774Z" \
    --include-resolved-cases \
    --language "en" \
    --no-include-communications \
    --max-item 1
```

Output:

```
{
    "cases": [
        {
            "status": "resolved",
            "ccEmailAddresses": [],
            "timeCreated": "2020-03-23T21:31:47.774Z",
            "caseId": "case-12345678910-2013-c4c1d2bf33c5cf47",
```

```
            "severityCode": "low",
            "language": "en",
            "categoryCode": "using-aws",
            "serviceCode": "general-info",
            "submittedBy": "myemail@example.com",
            "displayId": "1234567890",
            "subject": "Question about my account"
        }
    ]
}
```

Untuk informasi selengkapnya, lihat Manajemen kasus di AWS Support User Guide.

- Untuk detail API, lihat DescribeCasesdi Referensi AWS CLI Perintah.

Java

SDK untuk Java 2.x

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di AWS Repositori Contoh Kode.

```
    public static void getOpenCase(SupportClient supportClient) {
        try {
            // Specify the start and end time.
            Instant now = Instant.now();
            java.time.LocalDate.now();
            Instant yesterday = now.minus(1, ChronoUnit.DAYS);

            DescribeCasesRequest describeCasesRequest =
DescribeCasesRequest.builder()
                    .maxResults(20)
                    .afterTime(yesterday.toString())
                    .beforeTime(now.toString())
                    .build();

            DescribeCasesResponse response =
supportClient.describeCases(describeCasesRequest);
            List<CaseDetails> cases = response.cases();
```

```
            for (CaseDetails sinCase : cases) {
                System.out.println("The case status is " + sinCase.status());
                System.out.println("The case Id is " + sinCase.caseId());
                System.out.println("The case subject is " + sinCase.subject());
            }

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }
```

- Untuk detail API, lihat DescribeCasesdi Referensi AWS SDK for Java 2.x API.

JavaScript

SDK untuk JavaScript (v3)

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di AWS Repositori Contoh Kode.

```
import { DescribeCasesCommand } from "@aws-sdk/client-support";

import { client } from "../libs/client.js";

export const main = async () => {
  try {
    // Get all of the unresolved cases in your account.
    // Filter or expand results by providing parameters to the
 DescribeCasesCommand. Refer
    // to the TypeScript definition and the API doc for more information on
 possible parameters.
    // https://docs.aws.amazon.com/AWSJavaScriptSDK/v3/latest/clients/client-
support/interfaces/describecasescommandinput.html
    const response = await client.send(new DescribeCasesCommand({}));
    const caseIds = response.cases.map((supportCase) => supportCase.caseId);
    console.log(caseIds);
    return response;
```

```
  } catch (err) {
    console.error(err);
  }
};
```

- Untuk detail API, lihat DescribeCasesdi Referensi AWS SDK for JavaScript API.

Kotlin

SDK untuk Kotlin

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di AWS Repositori Contoh Kode.

```
suspend fun getOpenCase() {
    // Specify the start and end time.
    val now = Instant.now()
    LocalDate.now()
    val yesterday = now.minus(1, ChronoUnit.DAYS)
    val describeCasesRequest =
        DescribeCasesRequest {
            maxResults = 20
            afterTime = yesterday.toString()
            beforeTime = now.toString()
        }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.describeCases(describeCasesRequest)
        response.cases?.forEach { sinCase ->
            println("The case status is ${sinCase.status}")
            println("The case Id is ${sinCase.caseId}")
            println("The case subject is ${sinCase.subject}")
        }
    }
}
```

- Untuk detail API, lihat DescribeCasesdi AWS SDK untuk referensi API Kotlin.

PowerShell

Alat untuk PowerShell

Contoh 1: Mengembalikan rincian semua kasus dukungan.

```
Get-ASACase
```

Contoh 2: Mengembalikan rincian semua kasus dukungan sejak tanggal dan waktu yang ditentukan.

```
Get-ASACase -AfterTime "2013-09-10T03:06Z"
```

Contoh 3: Mengembalikan rincian 10 kasus dukungan pertama, termasuk yang telah diselesaikan.

```
Get-ASACase -MaxResult 10 -IncludeResolvedCases $true
```

Contoh 4: Mengembalikan rincian kasus dukungan tunggal yang ditentukan.

```
Get-ASACase -CaseIdList "case-12345678910-2013-c4c1d2bf33c5cf47"
```

Contoh 5: Mengembalikan rincian kasus dukungan tertentu.

```
Get-ASACase -CaseIdList @("case-12345678910-2013-c4c1d2bf33c5cf47",
 "case-18929034710-2011-c4fdeabf33c5cf47")
```

Contoh 6: Mengembalikan semua kasus dukungan menggunakan paging manual. Kasus diambil dalam batch 20.

```
$nextToken = $null
do {
  Get-ASACase -NextToken $nextToken -MaxResult 20
  $nextToken = $AWSHistory.LastServiceResponse.NextToken
} while ($nextToken -ne $null)
```

- Untuk detail API, lihat DescribeCasesdi Referensi AWS Tools for PowerShell Cmdlet.

Python

SDK untuk Python (Boto3)

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di AWS Repositori Contoh Kode.

```
class SupportWrapper:
    """Encapsulates Support actions."""

    def __init__(self, support_client):
        """
        :param support_client: A Boto3 Support client.
        """
        self.support_client = support_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        support_client = boto3.client("support")
        return cls(support_client)


    def describe_cases(self, after_time, before_time, resolved):
        """
        Describe support cases over a period of time, optionally filtering
        by status.

        :param after_time: The start time to include for cases.
        :param before_time: The end time to include for cases.
        :param resolved: True to include resolved cases in the results,
            otherwise results are open cases.
        :return: The final status of the case.
        """
        try:
            cases = []
            paginator = self.support_client.get_paginator("describe_cases")
```

```
            for page in paginator.paginate(
                afterTime=after_time,
                beforeTime=before_time,
                includeResolvedCases=resolved,
                language="en",
            ):
                cases += page["cases"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't describe cases. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            if resolved:
                cases = filter(lambda case: case["status"] == "resolved", cases)
            return cases
```

- Untuk detail API, lihat DescribeCasesdi AWS SDK for Python (Boto3) Referensi API.

Untuk daftar lengkap panduan pengembang AWS SDK dan contoh kode, lihatMenggunakan AWS Support dengan AWS SDK. Topik ini juga mencakup informasi tentang memulai dan detail tentang versi SDK sebelumnya.

Gunakan **`DescribeCommunications`** dengan AWS SDK atau CLI

Contoh kode berikut menunjukkan cara menggunakan`DescribeCommunications`.

Contoh tindakan adalah kutipan kode dari program yang lebih besar dan harus dijalankan dalam konteks. Anda dapat melihat tindakan ini dalam konteks dalam contoh kode berikut:

- Memulai kasus

.NET

AWS SDK for .NET

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di AWS Repositori Contoh Kode.

```
    /// <summary>
    /// Describe the communications for a case, optionally with a date filter.
    /// </summary>
    /// <param name="caseId">The ID of the support case.</param>
    /// <param name="afterTime">The optional start date for a filtered search.</
param>
    /// <param name="beforeTime">The optional end date for a filtered search.</
param>
    /// <returns>The list of communications for the case.</returns>
    public async Task<List<Communication>> DescribeCommunications(string caseId,
 DateTime? afterTime = null, DateTime? beforeTime = null)
    {
        var results = new List<Communication>();
        var paginateCommunications =
 _amazonSupport.Paginators.DescribeCommunications(
            new DescribeCommunicationsRequest()
            {
                CaseId = caseId,
                AfterTime = afterTime?.ToString("s"),
                BeforeTime = beforeTime?.ToString("s")
            });
        // Get the entire list using the paginator.
        await foreach (var communications in
 paginateCommunications.Communications)
        {
            results.Add(communications);
        }
        return results;
    }
```

- Untuk detail API, lihat DescribeCommunicationsdi Referensi AWS SDK for .NET API.

CLI

AWS CLI

Untuk menggambarkan komunikasi terbaru untuk suatu kasus

`describe-communications`Contoh berikut mengembalikan komunikasi terbaru untuk kasus dukungan yang ditentukan di AWS akun Anda.

```
aws support describe-communications \
    --case-id "case-12345678910-2013-c4c1d2bf33c5cf47" \
    --after-time "2020-03-23T21:31:47.774Z" \
    --max-item 1
```

Output:

```
{
    "communications": [
        {
            "body": "I want to learn more about an AWS service.",
            "attachmentSet": [],
            "caseId": "case-12345678910-2013-c4c1d2bf33c5cf47",
            "timeCreated": "2020-05-12T23:12:35.000Z",
            "submittedBy": "Amazon Web Services"
        }
    ],
    "NextToken":
 "eyJuZXh0VG9rZW4iOiBudWxsLCAiYm90b190cnVuY2F0ZV9hbW91bnQEXAMPLE=="
}
```

Untuk informasi selengkapnya, lihat Manajemen kasus di AWS Support User Guide.

- Untuk detail API, lihat DescribeCommunicationsdi Referensi AWS CLI Perintah.

Java

SDK untuk Java 2.x

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di AWS Repositori Contoh Kode.

```
   public static String listCommunications(SupportClient supportClient, String
caseId) {
       try {
           String attachId = null;
           DescribeCommunicationsRequest communicationsRequest =
DescribeCommunicationsRequest.builder()
                   .caseId(caseId)
                   .maxResults(10)
                   .build();

           DescribeCommunicationsResponse response =
supportClient.describeCommunications(communicationsRequest);
           List<Communication> communications = response.communications();
           for (Communication comm : communications) {
               System.out.println("the body is: " + comm.body());

               // Get the attachment id value.
               List<AttachmentDetails> attachments = comm.attachmentSet();
               for (AttachmentDetails detail : attachments) {
                   attachId = detail.attachmentId();
               }
           }
           return attachId;

       } catch (SupportException e) {
           System.out.println(e.getLocalizedMessage());
           System.exit(1);
       }
       return "";
   }
```

- Untuk detail API, lihat DescribeCommunicationsdi Referensi AWS SDK for Java 2.x API.

JavaScript

SDK untuk JavaScript (v3)

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di AWS Repositori Contoh Kode.

```
import { DescribeCommunicationsCommand } from "@aws-sdk/client-support";

import { client } from "../libs/client.js";

export const main = async () => {
  try {
    // Get all communications for the support case.
    // Filter results by providing parameters to the
 DescribeCommunicationsCommand. Refer
    // to the TypeScript definition and the API doc for more information on
 possible parameters.
    // https://docs.aws.amazon.com/AWSJavaScriptSDK/v3/latest/clients/client-
support/interfaces/describecommunicationscommandinput.html
    const response = await client.send(
      new DescribeCommunicationsCommand({
        // Set value to an existing case id.
        caseId: "CASE_ID",
      }),
    );
    const text = response.communications.map((item) => item.body).join("\n");
    console.log(text);
    return response;
  } catch (err) {
    console.error(err);
  }
};
```

- Untuk detail API, lihat DescribeCommunicationsdi Referensi AWS SDK for JavaScript API.

Kotlin

SDK untuk Kotlin

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di AWS Repositori Contoh Kode.

```
suspend fun listCommunications(caseIdVal: String?): String? {
    val communicationsRequest =
        DescribeCommunicationsRequest {
            caseId = caseIdVal
            maxResults = 10
        }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response =
 supportClient.describeCommunications(communicationsRequest)
        response.communications?.forEach { comm ->
            println("the body is: " + comm.body)
            comm.attachmentSet?.forEach { detail ->
                return detail.attachmentId
            }
        }
    }
    return ""
}
```

- Untuk detail API, lihat DescribeCommunicationsdi AWS SDK untuk referensi API Kotlin.

PowerShell

Alat untuk PowerShell

Contoh 1: Mengembalikan semua komunikasi untuk kasus tertentu.

```
Get-ASACommunication -CaseId "case-12345678910-2013-c4c1d2bf33c5cf47"
```

Contoh 2: Mengembalikan semua komunikasi sejak tengah malam UTC pada 1 Januari 2012 untuk kasus yang ditentukan.

```
Get-ASACommunication -CaseId "case-12345678910-2013-c4c1d2bf33c5cf47" -AfterTime
 "2012-01-10T00:00Z"
```

Contoh 3: Mengembalikan semua komunikasi sejak tengah malam UTC pada 1 Januari 2012 untuk kasus yang ditentukan, menggunakan paging manual. Komunikasi diambil dalam batch 20.

```
$nextToken = $null
do {
  Get-ASACommunication -CaseId "case-12345678910-2013-c4c1d2bf33c5cf47" -
NextToken $nextToken -MaxResult 20
  $nextToken = $AWSHistory.LastServiceResponse.NextToken
} while ($nextToken -ne $null)
```

- Untuk detail API, lihat DescribeCommunicationsdi Referensi AWS Tools for PowerShell Cmdlet.

Python

SDK untuk Python (Boto3)

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di AWS Repositori Contoh Kode.

```
class SupportWrapper:
    """Encapsulates Support actions."""

    def __init__(self, support_client):
        """
        :param support_client: A Boto3 Support client.
        """
        self.support_client = support_client

    @classmethod
```

```
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        support_client = boto3.client("support")
        return cls(support_client)


    def describe_all_case_communications(self, case_id):
        """
        Describe all the communications for a case using a paginator.

        :param case_id: The ID of the case.
        :return: The communications for the case.
        """
        try:
            communications = []
            paginator =
self.support_client.get_paginator("describe_communications")
            for page in paginator.paginate(caseId=case_id):
                communications += page["communications"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't describe communications. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return communications
```

- Untuk detail API, lihat DescribeCommunicationsdi AWS SDK for Python (Boto3) Referensi API.

Untuk daftar lengkap panduan pengembang AWS SDK dan contoh kode, lihatMenggunakan AWS Support dengan AWS SDK. Topik ini juga mencakup informasi tentang memulai dan detail tentang versi SDK sebelumnya.

Gunakan `DescribeServices` dengan AWS SDK atau CLI

Contoh kode berikut menunjukkan cara menggunakan`DescribeServices`.

Contoh tindakan adalah kutipan kode dari program yang lebih besar dan harus dijalankan dalam konteks. Anda dapat melihat tindakan ini dalam konteks dalam contoh kode berikut:

- Memulai kasus

.NET

AWS SDK for .NET

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di AWS Repositori Contoh Kode.

```
    /// <summary>
    /// Get the descriptions of AWS services.
    /// </summary>
    /// <param name="name">Optional language for services.
    /// Currently Chinese (“zh”), English ("en"), Japanese ("ja") and Korean
(“ko”) are supported.</param>
    /// <returns>The list of AWS service descriptions.</returns>
    public async Task<List<Service>> DescribeServices(string language = "en")
    {
        var response = await _amazonSupport.DescribeServicesAsync(
            new DescribeServicesRequest()
            {
                Language = language
```

```
            });
        return response.Services;
    }
```

- Untuk detail API, lihat DescribeServicesdi Referensi AWS SDK for .NET API.

CLI

AWS CLI

Untuk daftar AWS layanan dan kategori layanan

`describe-services`Contoh berikut mencantumkan kategori layanan yang tersedia untuk meminta informasi umum.

```
aws support describe-services \
    --service-code-list "general-info"
```

Output:

```
{
    "services": [
        {
            "code": "general-info",
            "name": "General Info and Getting Started",
            "categories": [
                {
                    "code": "charges",
                    "name": "How Will I Be Charged?"
                },
                {
                    "code": "gdpr-queries",
                    "name": "Data Privacy Query"
                },
                {
                    "code": "reserved-instances",
                    "name": "Reserved Instances"
                },
                {
                    "code": "resource",
```

```
                    "name": "Where is my Resource?"
                },
                {
                    "code": "using-aws",
                    "name": "Using AWS & Services"
                },
                {
                    "code": "free-tier",
                    "name": "Free Tier"
                },
                {
                    "code": "security-and-compliance",
                    "name": "Security & Compliance"
                },
                {
                    "code": "account-structure",
                    "name": "Account Structure"
                }
            ]
        }
    ]
}
```

Untuk informasi selengkapnya, lihat Manajemen kasus di AWS Support User Guide.

- Untuk detail API, lihat DescribeServicesdi Referensi AWS CLI Perintah.

Java

SDK untuk Java 2.x

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di AWS Repositori Contoh Kode.

```
    // Return a List that contains a Service name and Category name.
    public static List<String> displayServices(SupportClient supportClient) {
        try {
            DescribeServicesRequest servicesRequest =
DescribeServicesRequest.builder()
```

```
                    .language("en")
                    .build();

            DescribeServicesResponse response =
supportClient.describeServices(servicesRequest);
            String serviceCode = null;
            String catName = null;
            List<String> sevCatList = new ArrayList<>();
            List<Service> services = response.services();

            System.out.println("Get the first 10 services");
            int index = 1;
            for (Service service : services) {
                if (index == 11)
                    break;

                System.out.println("The Service name is: " + service.name());
                if (service.name().compareTo("Account") == 0)
                    serviceCode = service.code();

                // Get the Categories for this service.
                List<Category> categories = service.categories();
                for (Category cat : categories) {
                    System.out.println("The category name is: " + cat.name());
                    if (cat.name().compareTo("Security") == 0)
                        catName = cat.name();
                }
                index++;
            }

            // Push the two values to the list.
            sevCatList.add(serviceCode);
            sevCatList.add(catName);
            return sevCatList;

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
        return null;
    }
```

- Untuk detail API, lihat DescribeServicesdi Referensi AWS SDK for Java 2.x API.

Kotlin

SDK untuk Kotlin

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di AWS Repositori Contoh Kode.

```
// Return a List that contains a Service name and Category name.
suspend fun displayServices(): List<String> {
    var serviceCode = ""
    var catName = ""
    val sevCatList = mutableListOf<String>()
    val servicesRequest =
        DescribeServicesRequest {
            language = "en"
        }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.describeServices(servicesRequest)
        println("Get the first 10 services")
        var index = 1

        response.services?.forEach { service ->
            if (index == 11) {
                return@forEach
            }

            println("The Service name is ${service.name}")
            if (service.name == "Account") {
                serviceCode = service.code.toString()
            }

            // Get the categories for this service.
            service.categories?.forEach { cat ->
                println("The category name is ${cat.name}")
                if (cat.name == "Security") {
                    catName = cat.name!!
                }
            }
```

```
            index++
        }
    }

    // Push the two values to the list.
    serviceCode.let { sevCatList.add(it) }
    catName.let { sevCatList.add(it) }
    return sevCatList
}
```

- Untuk detail API, lihat DescribeServicesdi AWS SDK untuk referensi API Kotlin.

PowerShell

Alat untuk PowerShell

Contoh 1: Mengembalikan semua kode layanan, nama, dan kategori yang tersedia.

```
Get-ASAService
```

Contoh 2: Mengembalikan nama dan kategori untuk layanan dengan kode yang ditentukan.

```
Get-ASAService -ServiceCodeList "amazon-cloudfront"
```

Contoh 3: Mengembalikan nama dan kategori untuk kode layanan tertentu.

```
Get-ASAService -ServiceCodeList @("amazon-cloudfront", "amazon-cloudwatch")
```

Contoh 4: Mengembalikan nama dan kategori (dalam bahasa Jepang) untuk kode layanan yang ditentukan. Saat ini kode bahasa Inggris (“en”) dan Jepang (“ja”) didukung.

```
Get-ASAService -ServiceCodeList @("amazon-cloudfront", "amazon-cloudwatch") -
Language "ja"
```

- Untuk detail API, lihat DescribeServicesdi Referensi AWS Tools for PowerShell Cmdlet.

Python

SDK untuk Python (Boto3)

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di AWS Repositori Contoh Kode.

```
class SupportWrapper:
    """Encapsulates Support actions."""

    def __init__(self, support_client):
        """
        :param support_client: A Boto3 Support client.
        """
        self.support_client = support_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        support_client = boto3.client("support")
        return cls(support_client)


    def describe_services(self, language):
        """
        Get the descriptions of AWS services available for support for a
 language.

        :param language: The language for support services.
        Currently, only "en" (English) and "ja" (Japanese) are supported.
        :return: The list of AWS service descriptions.
        """
        try:
            response = self.support_client.describe_services(language=language)
            services = response["services"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
```

```
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't get Support services for language %s. Here's why:
%s: %s",
                    language,
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return services
```

- Untuk detail API, lihat DescribeServicesdi AWS SDK for Python (Boto3) Referensi API.

Untuk daftar lengkap panduan pengembang AWS SDK dan contoh kode, lihatMenggunakan AWS Support dengan AWS SDK. Topik ini juga mencakup informasi tentang memulai dan detail tentang versi SDK sebelumnya.

Gunakan **`DescribeSeverityLevels`** dengan AWS SDK atau CLI

Contoh kode berikut menunjukkan cara menggunakan`DescribeSeverityLevels`.

Contoh tindakan adalah kutipan kode dari program yang lebih besar dan harus dijalankan dalam konteks. Anda dapat melihat tindakan ini dalam konteks dalam contoh kode berikut:

- Memulai kasus

.NET

AWS SDK for .NET

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di AWS Repositori Contoh Kode.

```
    /// <summary>
    /// Get the descriptions of support severity levels.
    /// </summary>
    /// <param name="name">Optional language for severity levels.
    /// Currently Chinese (“zh”), English ("en"), Japanese ("ja") and Korean
(“ko”) are supported.</param>
    /// <returns>The list of support severity levels.</returns>
    public async Task<List<SeverityLevel>> DescribeSeverityLevels(string language
= "en")
    {
        var response = await _amazonSupport.DescribeSeverityLevelsAsync(
            new DescribeSeverityLevelsRequest()
            {
                Language = language
            });
        return response.SeverityLevels;
    }
```

- Untuk detail API, lihat DescribeSeverityLevel di Referensi AWS SDK for .NET API.

CLI

AWS CLI

Untuk daftar tingkat keparahan yang tersedia

`describe-severity-levels`Contoh berikut mencantumkan tingkat keparahan yang tersedia untuk kasus dukungan.

```
aws support describe-severity-levels
```

Output:

```
{
    "severityLevels": [
        {
            "code": "low",
            "name": "Low"
        },
        {
            "code": "normal",
            "name": "Normal"
        },
        {
            "code": "high",
            "name": "High"
        },
        {
            "code": "urgent",
            "name": "Urgent"
        },
        {
            "code": "critical",
            "name": "Critical"
        }
    ]
}
```

Untuk informasi selengkapnya, lihat Memilih tingkat keparahan di Panduan Pengguna AWS Support.

- Untuk detail API, lihat DescribeSeverityLevel di Referensi AWS CLI Perintah.

Java

SDK untuk Java 2.x

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di AWS Repositori Contoh Kode.

```
   public static String displaySevLevels(SupportClient supportClient) {
       try {
           DescribeSeverityLevelsRequest severityLevelsRequest =
DescribeSeverityLevelsRequest.builder()
                   .language("en")
                   .build();

           DescribeSeverityLevelsResponse response =
supportClient.describeSeverityLevels(severityLevelsRequest);
           List<SeverityLevel> severityLevels = response.severityLevels();
           String levelName = null;
           for (SeverityLevel sevLevel : severityLevels) {
               System.out.println("The severity level name is: " +
sevLevel.name());
               if (sevLevel.name().compareTo("High") == 0)
                   levelName = sevLevel.name();
           }
           return levelName;

       } catch (SupportException e) {
           System.out.println(e.getLocalizedMessage());
           System.exit(1);
       }
       return "";
   }
```

- Untuk detail API, lihat DescribeSeverityLevel di Referensi AWS SDK for Java 2.x API.

JavaScript

SDK untuk JavaScript (v3)

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di AWS Repositori Contoh Kode.

```
import { DescribeSeverityLevelsCommand } from "@aws-sdk/client-support";

import { client } from "../libs/client.js";

export const main = async () => {
  try {
    // Get the list of severity levels.
    // The available values depend on the support plan for the account.
    const response = await client.send(new DescribeSeverityLevelsCommand({}));
    console.log(response.severityLevels);
    return response;
  } catch (err) {
    console.error(err);
  }
};
```

- Untuk detail API, lihat DescribeSeverityLevel di Referensi AWS SDK for JavaScript API.

Kotlin

SDK untuk Kotlin

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di AWS Repositori Contoh Kode.

```
suspend fun displaySevLevels(): String {
```

```
    var levelName = ""
    val severityLevelsRequest =
        DescribeSeverityLevelsRequest {
            language = "en"
        }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response =
 supportClient.describeSeverityLevels(severityLevelsRequest)
        response.severityLevels?.forEach { sevLevel ->
            println("The severity level name is: ${sevLevel.name}")
            if (sevLevel.name == "High") {
                levelName = sevLevel.name!!
            }
        }
        return levelName
    }
}
```

- Untuk detail API, lihat DescribeSeverityLevel di AWS SDK untuk referensi API Kotlin.

PowerShell

Alat untuk PowerShell

Contoh 1: Mengembalikan daftar tingkat keparahan yang dapat ditetapkan ke kasus AWS Support.

```
Get-ASASeverityLevel
```

Contoh 2: Mengembalikan daftar tingkat keparahan yang dapat ditetapkan ke kasus AWS Support. Nama-nama level dikembalikan dalam bahasa Jepang.

```
Get-ASASeverityLevel -Language "ja"
```

- Untuk detail API, lihat DescribeSeverityLevel di Referensi AWS Tools for PowerShell Cmdlet.

Python

SDK untuk Python (Boto3)

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di AWS Repositori Contoh Kode.

```
class SupportWrapper:
    """Encapsulates Support actions."""

    def __init__(self, support_client):
        """
        :param support_client: A Boto3 Support client.
        """
        self.support_client = support_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        support_client = boto3.client("support")
        return cls(support_client)


    def describe_severity_levels(self, language):
        """
        Get the descriptions of available severity levels for support cases for a
 language.

        :param language: The language for support severity levels.
        Currently, only "en" (English) and "ja" (Japanese) are supported.
        :return: The list of severity levels.
        """
        try:
            response =
 self.support_client.describe_severity_levels(language=language)
            severity_levels = response["severityLevels"]
        except ClientError as err:
```

```
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't get severity levels for language %s. Here's why:
%s: %s",
                    language,
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return severity_levels
```

- Untuk detail API, lihat DescribeSeverityLevel dalam AWS SDK for Python (Boto3) Referensi API.

Untuk daftar lengkap panduan pengembang AWS SDK dan contoh kode, lihatMenggunakan AWS Support dengan AWS SDK. Topik ini juga mencakup informasi tentang memulai dan detail tentang versi SDK sebelumnya.

Gunakan **`DescribeTrustedAdvisorCheckRefreshStatuses`** dengan AWS SDK atau CLI

Contoh kode berikut menunjukkan cara menggunakan`DescribeTrustedAdvisorCheckRefreshStatuses`.

CLI

AWS CLI

Untuk mencantumkan status penyegaran pemeriksaan AWS Trusted Advisor

`describe-trusted-advisor-check-refresh-statuses`Contoh berikut mencantumkan status penyegaran untuk dua pemeriksaan Trusted Advisor: Izin Bucket Amazon S3 dan Penggunaan IAM.

```
aws support describe-trusted-advisor-check-refresh-statuses \
    --check-id "Pfx0RwqBli" "zXCkfM1nI3"
```

Output:

```
{
    "statuses": [
        {
            "checkId": "Pfx0RwqBli",
            "status": "none",
            "millisUntilNextRefreshable": 0
        },
        {
            "checkId": "zXCkfM1nI3",
            "status": "none",
            "millisUntilNextRefreshable": 0
        }
    ]
}
```

Untuk informasi selengkapnya, lihat AWS Trusted Advisor di Panduan Pengguna AWS Support.

- Untuk detail API, lihat DescribeTrustedAdvisorCheckRefreshStatusesdi Referensi AWS CLI Perintah.

PowerShell

Alat untuk PowerShell

Contoh 1: Mengembalikan status permintaan penyegaran saat ini untuk pemeriksaan yang ditentukan. Request-ASA TrustedAdvisorCheckRefresh dapat digunakan untuk meminta agar informasi status cek disegarkan.

```
Get-ASATrustedAdvisorCheckRefreshStatus -CheckId @("checkid1", "checkid2")
```

- Untuk detail API, lihat DescribeTrustedAdvisorCheckRefreshStatusesdi Referensi AWS Tools for PowerShell Cmdlet.

Untuk daftar lengkap panduan pengembang AWS SDK dan contoh kode, lihatMenggunakan AWS Support dengan AWS SDK. Topik ini juga mencakup informasi tentang memulai dan detail tentang versi SDK sebelumnya.

Gunakan **`DescribeTrustedAdvisorCheckResult`** dengan AWS SDK atau CLI

Contoh kode berikut menunjukkan cara menggunakan`DescribeTrustedAdvisorCheckResult`.

CLI

AWS CLI

Untuk mencantumkan hasil pemeriksaan AWS Trusted Advisor

`describe-trusted-advisor-check-result`Contoh berikut mencantumkan hasil pemeriksaan IAM Use.

```
aws support describe-trusted-advisor-check-result \
    --check-id "zXCkfM1nI3"
```

Output:

```
{
    "result": {
        "checkId": "zXCkfM1nI3",
        "timestamp": "2020-05-13T21:38:05Z",
        "status": "ok",
        "resourcesSummary": {
            "resourcesProcessed": 1,
            "resourcesFlagged": 0,
            "resourcesIgnored": 0,
            "resourcesSuppressed": 0
        },
        "categorySpecificSummary": {
            "costOptimizing": {
                "estimatedMonthlySavings": 0.0,
```

```
                "estimatedPercentMonthlySavings": 0.0
            }
        },
        "flaggedResources": [
            {
                "status": "ok",
                "resourceId": "47DEQpj8HBSa-_TImW-5JCeuQeRkm5NMpJWZEXAMPLE",
                "isSuppressed": false
            }
        ]
    }
}
```

Untuk informasi selengkapnya, lihat AWS Trusted Advisor di Panduan Pengguna AWS Support.

- Untuk detail API, lihat DescribeTrustedAdvisorCheckResult in AWS CLI Command Reference.

PowerShell

Alat untuk PowerShell

Contoh 1: Mengembalikan hasil pemeriksaan Trusted Advisor. Daftar cek Trusted Advisor yang tersedia dapat diperoleh dengan menggunakan Cek TrustedAdvisor Get-Asa. Outputnya adalah status keseluruhan pemeriksaan, stempel waktu di mana pemeriksaan terakhir dijalankan dan checkid unik untuk pemeriksaan tertentu. Untuk mendapatkan output hasil dalam bahasa Jepang, tambahkan parameter -Language “ja”.

```
Get-ASATrustedAdvisorCheckResult -CheckId "checkid1"
```

- Untuk detail API, lihat DescribeTrustedAdvisorCheckHasil dalam Referensi AWS Tools for PowerShell Cmdlet.

Untuk daftar lengkap panduan pengembang AWS SDK dan contoh kode, lihatMenggunakan AWS Support dengan AWS SDK. Topik ini juga mencakup informasi tentang memulai dan detail tentang versi SDK sebelumnya.

Gunakan **DescribeTrustedAdvisorCheckSummaries** dengan AWS SDK atau CLI

Contoh kode berikut menunjukkan cara menggunakan`DescribeTrustedAdvisorCheckSummaries`.

CLI

AWS CLI

Untuk membuat daftar ringkasan cek Trusted AWS Advisor

`describe-trusted-advisor-check-summaries`Contoh berikut mencantumkan hasil untuk dua pemeriksaan Trusted Advisor: Izin Bucket Amazon S3 dan Penggunaan IAM.

```
aws support describe-trusted-advisor-check-summaries \
    --check-ids "Pfx0RwqBli" "zXCkfM1nI3"
```

Output:

```
{
    "summaries": [
        {
            "checkId": "Pfx0RwqBli",
            "timestamp": "2020-05-13T21:38:12Z",
            "status": "ok",
            "hasFlaggedResources": true,
            "resourcesSummary": {
                "resourcesProcessed": 44,
                "resourcesFlagged": 0,
                "resourcesIgnored": 0,
                "resourcesSuppressed": 0
            },
            "categorySpecificSummary": {
                "costOptimizing": {
                    "estimatedMonthlySavings": 0.0,
                    "estimatedPercentMonthlySavings": 0.0
                }
            }
        },
        {
            "checkId": "zXCkfM1nI3",
```

```
            "timestamp": "2020-05-13T21:38:05Z",
            "status": "ok",
            "hasFlaggedResources": true,
            "resourcesSummary": {
                "resourcesProcessed": 1,
                "resourcesFlagged": 0,
                "resourcesIgnored": 0,
                "resourcesSuppressed": 0
            },
            "categorySpecificSummary": {
                "costOptimizing": {
                    "estimatedMonthlySavings": 0.0,
                    "estimatedPercentMonthlySavings": 0.0
                }
            }
        }
    ]
}
```

Untuk informasi selengkapnya, lihat AWS Trusted Advisor di Panduan Pengguna AWS Support.

- Untuk detail API, lihat DescribeTrustedAdvisorCheckRingkasan dalam Referensi AWS CLI Perintah.

PowerShell

Alat untuk PowerShell

Contoh 1: Mengembalikan ringkasan terbaru untuk pemeriksaan Trusted Advisor yang ditentukan.

```
Get-ASATrustedAdvisorCheckSummary -CheckId "checkid1"
```

Contoh 2: Mengembalikan ringkasan terbaru untuk pemeriksaan Trusted Advisor yang ditentukan.

```
Get-ASATrustedAdvisorCheckSummary -CheckId @("checkid1", "checkid2")
```

- Untuk detail API, lihat DescribeTrustedAdvisorCheckRingkasan di Referensi AWS Tools for PowerShell Cmdlet.

Untuk daftar lengkap panduan pengembang AWS SDK dan contoh kode, lihatMenggunakan AWS Support dengan AWS SDK. Topik ini juga mencakup informasi tentang memulai dan detail tentang versi SDK sebelumnya.

Gunakan **`DescribeTrustedAdvisorChecks`** dengan AWS SDK atau CLI

Contoh kode berikut menunjukkan cara menggunakan`DescribeTrustedAdvisorChecks`.

CLI

AWS CLI

Untuk daftar cek AWS Trusted Advisor yang tersedia

`describe-trusted-advisor-checks`Contoh berikut mencantumkan cek Trusted Advisor yang tersedia di akun Anda AWS . Informasi ini mencakup nama cek, ID, deskripsi, kategori, dan metadata. Perhatikan bahwa output dipersingkat agar mudah dibaca.

```
aws support describe-trusted-advisor-checks \
    --language "en"
```

Output:

```
{
    "checks": [
        {
            "id": "zXCkfM1nI3",
            "name": "IAM Use",
            "description": "Checks for your use of AWS Identity and Access
 Management (IAM). You can use IAM to create users, groups, and roles in
 AWS, and you can use permissions to control access to AWS resources. \n<br>
\n<br>\n<b>Alert Criteria</b><br>\nYellow: No IAM users have been created
 for this account.\n<br>\n<br>\n<b>Recommended Action</b><br>\nCreate one or
 more IAM users and groups in your account. You can then create additional
 users whose permissions are limited to perform specific tasks in your AWS
 environment. For more information, see <a href=\"https://docs.aws.amazon.com/
IAM/latest/UserGuide/IAMGettingStarted.html\" target=\"_blank\">Getting
 Started</a>. \n<br><br>\n<b>Additional Resources</b><br>\n<a href=\"https://
docs.aws.amazon.com/IAM/latest/UserGuide/IAM_Introduction.html\" target=\"_blank
\">What Is IAM?</a>",
            "category": "security",
            "metadata": []
```

```
        }
    ]
}
```

Untuk informasi selengkapnya, lihat AWS Trusted Advisor di Panduan Pengguna AWS Support.

- Untuk detail API, lihat DescribeTrustedAdvisorChecksdi Referensi AWS CLI Perintah.

PowerShell

Alat untuk PowerShell

Contoh 1: Mengembalikan koleksi cek Trusted Advisor. Anda harus menentukan parameter Bahasa yang dapat menerima “en” untuk output bahasa Inggris atau “ja” untuk output Jepang.

```
Get-ASATrustedAdvisorCheck -Language "en"
```

- Untuk detail API, lihat DescribeTrustedAdvisorChecksdi Referensi AWS Tools for PowerShell Cmdlet.

Untuk daftar lengkap panduan pengembang AWS SDK dan contoh kode, lihatMenggunakan AWS Support dengan AWS SDK. Topik ini juga mencakup informasi tentang memulai dan detail tentang versi SDK sebelumnya.

Gunakan **`RefreshTrustedAdvisorCheck`** dengan AWS SDK atau CLI

Contoh kode berikut menunjukkan cara menggunakan`RefreshTrustedAdvisorCheck`.

CLI

AWS CLI

Untuk me-refresh pemeriksaan AWS Trusted Advisor

`refresh-trusted-advisor-check`Contoh berikut menyegarkan cek Trusted Advisor Amazon S3 Bucket Permissions di akun Anda. AWS

```
aws support refresh-trusted-advisor-check \
```

```
    --check-id "Pfx0RwqBli"
```

Output:

```
{
    "status": {
        "checkId": "Pfx0RwqBli",
        "status": "enqueued",
        "millisUntilNextRefreshable": 3599992
    }
}
```

Untuk informasi selengkapnya, lihat AWS Trusted Advisor di Panduan Pengguna AWS Support.

- Untuk detail API, lihat RefreshTrustedAdvisorCheckdi Referensi AWS CLI Perintah.

PowerShell

Alat untuk PowerShell

Contoh 1: Meminta penyegaran untuk pemeriksaan Trusted Advisor yang ditentukan.

```
Request-ASATrustedAdvisorCheckRefresh -CheckId "checkid1"
```

- Untuk detail API, lihat RefreshTrustedAdvisorCheckdi Referensi AWS Tools for PowerShell Cmdlet.

Untuk daftar lengkap panduan pengembang AWS SDK dan contoh kode, lihatMenggunakan AWS Support dengan AWS SDK. Topik ini juga mencakup informasi tentang memulai dan detail tentang versi SDK sebelumnya.

Gunakan **`ResolveCase`** dengan AWS SDK atau CLI

Contoh kode berikut menunjukkan cara menggunakan`ResolveCase`.

Contoh tindakan adalah kutipan kode dari program yang lebih besar dan harus dijalankan dalam konteks. Anda dapat melihat tindakan ini dalam konteks dalam contoh kode berikut:

- Memulai kasus

.NET

AWS SDK for .NET

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di AWS Repositori Contoh Kode.

```
/// <summary>
/// Resolve a support case by caseId.
/// </summary>
/// <param name="caseId">Id for the support case.</param>
/// <returns>The final status of the case after resolving.</returns>
public async Task<string> ResolveCase(string caseId)
{
    var response = await _amazonSupport.ResolveCaseAsync(
        new ResolveCaseRequest()
        {
            CaseId = caseId
        });
    return response.FinalCaseStatus;
}
```

- Untuk detail API, lihat ResolveCasedi Referensi AWS SDK for .NET API.

CLI

AWS CLI

Untuk menyelesaikan kasus dukungan

`resolve-case`Contoh berikut menyelesaikan kasus dukungan di akun Anda AWS .

```
aws support resolve-case \
    --case-id "case-12345678910-2013-c4c1d2bf33c5cf47"
```

Output:

```
{
    "finalCaseStatus": "resolved",
    "initialCaseStatus": "work-in-progress"
}
```

Untuk informasi selengkapnya, lihat Manajemen kasus di AWS Support User Guide.

- Untuk detail API, lihat ResolveCasedi Referensi AWS CLI Perintah.

Java

SDK untuk Java 2.x

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di AWS Repositori Contoh Kode.

```
   public static void resolveSupportCase(SupportClient supportClient, String
caseId) {
       try {
           ResolveCaseRequest caseRequest = ResolveCaseRequest.builder()
                   .caseId(caseId)
                   .build();

           ResolveCaseResponse response =
supportClient.resolveCase(caseRequest);
           System.out.println("The status of case " + caseId + " is " +
response.finalCaseStatus());

       } catch (SupportException e) {
           System.out.println(e.getLocalizedMessage());
           System.exit(1);
       }
   }
```

- Untuk detail API, lihat ResolveCasedi Referensi AWS SDK for Java 2.x API.

JavaScript

SDK untuk JavaScript (v3)

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di AWS Repositori Contoh Kode.

```
import { ResolveCaseCommand } from "@aws-sdk/client-support";

import { client } from "../libs/client.js";

const main = async () => {
  try {
    const response = await client.send(
      new ResolveCaseCommand({
        caseId: "CASE_ID",
      }),
    );

    console.log(response.finalCaseStatus);
    return response;
  } catch (err) {
    console.error(err);
  }
};
```

- Untuk detail API, lihat ResolveCasedi Referensi AWS SDK for JavaScript API.

Kotlin

SDK untuk Kotlin

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di AWS Repositori Contoh Kode.

```
suspend fun resolveSupportCase(caseIdVal: String) {
    val caseRequest =
        ResolveCaseRequest {
            caseId = caseIdVal
        }
    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.resolveCase(caseRequest)
        println("The status of case $caseIdVal is ${response.finalCaseStatus}")
    }
}
```

- Untuk detail API, lihat ResolveCasedi AWS SDK untuk referensi API Kotlin.

PowerShell

Alat untuk PowerShell

Contoh 1: Mengembalikan keadaan awal dari kasus yang ditentukan dan keadaan saat ini setelah panggilan untuk menyelesaikannya selesai.

```
Resolve-ASACase -CaseId "case-12345678910-2013-c4c1d2bf33c5cf47"
```

- Untuk detail API, lihat ResolveCasedi Referensi AWS Tools for PowerShell Cmdlet.

Python

SDK untuk Python (Boto3)

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di AWS Repositori Contoh Kode.

```
class SupportWrapper:
    """Encapsulates Support actions."""

    def __init__(self, support_client):
        """
```

```
        :param support_client: A Boto3 Support client.
        """
        self.support_client = support_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        support_client = boto3.client("support")
        return cls(support_client)


    def resolve_case(self, case_id):
        """
        Resolve a support case by its caseId.

        :param case_id: The ID of the case to resolve.
        :return: The final status of the case.
        """
        try:
            response = self.support_client.resolve_case(caseId=case_id)
            final_status = response["finalCaseStatus"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't resolve case. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return final_status
```

- Untuk detail API, lihat ResolveCasedi AWS SDK for Python (Boto3) Referensi API.

Untuk daftar lengkap panduan pengembang AWS SDK dan contoh kode, lihatMenggunakan AWS Support dengan AWS SDK. Topik ini juga mencakup informasi tentang memulai dan detail tentang versi SDK sebelumnya.

Skenario untuk AWS Support menggunakan AWS SDK

Contoh kode berikut menunjukkan cara menerapkan skenario umum AWS Support dengan AWS SDK. Skenario ini menunjukkan kepada Anda bagaimana menyelesaikan tugas tertentu dengan memanggil beberapa fungsi di dalamnya AWS Support. Setiap skenario menyertakan tautan ke GitHub, di mana Anda dapat menemukan petunjuk tentang cara mengatur dan menjalankan kode.

Contoh

- Memulai AWS Support kasus menggunakan AWS SDK

Memulai AWS Support kasus menggunakan AWS SDK

Contoh kode berikut ini menunjukkan cara:

- Dapatkan dan tampilkan layanan yang tersedia dan tingkat keparahan untuk kasus.
- Buat kasus dukungan menggunakan layanan, kategori, dan tingkat keparahan yang dipilih.
- Dapatkan dan tampilkan daftar kasus terbuka untuk hari ini.
- Tambahkan set lampiran dan komunikasi ke kasus baru.
- Jelaskan keterikatan dan komunikasi baru untuk kasus ini.
- Selesaikan kasusnya.
- Dapatkan dan tampilkan daftar kasus yang diselesaikan untuk hari ini.

.NET

AWS SDK for .NET

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkap dan pelajari cara menyiapkan dan menjalankan di Repositori Contoh Kode AWS.

Jalankan skenario interaktif di penggugah/prompt perintah.

```
/// <summary>
/// Hello AWS Support example.
/// </summary>
public static class SupportCaseScenario
{
    /*
    Before running this .NET code example, set up your development environment,
 including your credentials.
    To use the AWS Support API, you must have one of the following AWS Support
 plans: Business, Enterprise On-Ramp, or Enterprise.

    This .NET example performs the following tasks:
    1.  Get and display services. Select a service from the list.
    2.  Select a category from the selected service.
    3.  Get and display severity levels and select a severity level from the
 list.
    4.  Create a support case using the selected service, category, and severity
 level.
    5.  Get and display a list of open support cases for the current day.
    6.  Create an attachment set with a sample text file to add to the case.
    7.  Add a communication with the attachment to the support case.
    8.  List the communications of the support case.
    9.  Describe the attachment set.
    10. Resolve the support case.
    11. Get a list of resolved cases for the current day.
   */

    private static SupportWrapper _supportWrapper = null!;

    static async Task Main(string[] args)
```

```
    {
        // Set up dependency injection for the AWS Support service.
        // Use your AWS profile name, or leave it blank to use the default
profile.
        using var host = Host.CreateDefaultBuilder(args)
            .ConfigureLogging(logging =>
                logging.AddFilter("System", LogLevel.Debug)
                    .AddFilter<DebugLoggerProvider>("Microsoft",
LogLevel.Information)
                    .AddFilter<ConsoleLoggerProvider>("Microsoft",
LogLevel.Trace))
            .ConfigureServices((_, services) =>
                services.AddAWSService<IAmazonAWSSupport>(new AWSOptions()
{ Profile = "default" })
                    .AddTransient<SupportWrapper>()
            )
            .Build();

        var logger = LoggerFactory.Create(builder =>
        {
            builder.AddConsole();
        }).CreateLogger(typeof(SupportCaseScenario));

        _supportWrapper = host.Services.GetRequiredService<SupportWrapper>();

        Console.WriteLine(new string('-', 80));
        Console.WriteLine("Welcome to the AWS Support case example scenario.");
        Console.WriteLine(new string('-', 80));

        try
        {
            var apiSupported = await _supportWrapper.VerifySubscription();
            if (!apiSupported)
            {
                logger.LogError("You must have a Business, Enterprise On-Ramp, or
Enterprise Support " +
                                "plan to use the AWS Support API. \n\tPlease
upgrade your subscription to run these examples.");
                return;
            }

            var service = await DisplayAndSelectServices();

            var category = DisplayAndSelectCategories(service);
```

```
            var severityLevel = await DisplayAndSelectSeverity();

            var caseId = await CreateSupportCase(service, category,
severityLevel);

            await DescribeTodayOpenCases();

            var attachmentSetId = await CreateAttachmentSet();

            await AddCommunicationToCase(attachmentSetId, caseId);

            var attachmentId = await ListCommunicationsForCase(caseId);

            await DescribeCaseAttachment(attachmentId);

            await ResolveCase(caseId);

            await DescribeTodayResolvedCases();

            Console.WriteLine(new string('-', 80));
            Console.WriteLine("AWS Support case example scenario complete.");
            Console.WriteLine(new string('-', 80));
        }
        catch (Exception ex)
        {
            logger.LogError(ex, "There was a problem executing the scenario.");
        }
    }

    /// <summary>
    /// List some available services from AWS Support, and select a service for
the example.
    /// </summary>
    /// <returns>The selected service.</returns>
    private static async Task<Service> DisplayAndSelectServices()
    {
        Console.WriteLine(new string('-', 80));
        var services = await _supportWrapper.DescribeServices();
        Console.WriteLine($"AWS Support client returned {services.Count}
services.");

        Console.WriteLine($"1. Displaying first 10 services:");
        for (int i = 0; i < 10 && i < services.Count; i++)
```

```
        {
            Console.WriteLine($"\t{i + 1}. {services[i].Name}");
        }

        var choiceNumber = 0;
        while (choiceNumber < 1 || choiceNumber > services.Count)
        {
            Console.WriteLine(
                "Select an example support service by entering a number from the
preceding list:");
            var choice = Console.ReadLine();
            Int32.TryParse(choice, out choiceNumber);
        }
        Console.WriteLine(new string('-', 80));

        return services[choiceNumber - 1];
    }

    /// <summary>
    /// List the available categories for a service and select a category for the
example.
    /// </summary>
    /// <param name="service">Service to use for displaying categories.</param>
    /// <returns>The selected category.</returns>
    private static Category DisplayAndSelectCategories(Service service)
    {
        Console.WriteLine(new string('-', 80));

        Console.WriteLine($"2. Available support categories for Service
\"{service.Name}\":");
        for (int i = 0; i < service.Categories.Count; i++)
        {
            Console.WriteLine($"\t{i + 1}. {service.Categories[i].Name}");
        }

        var choiceNumber = 0;
        while (choiceNumber < 1 || choiceNumber > service.Categories.Count)
        {
            Console.WriteLine(
                "Select an example support category by entering a number from the
preceding list:");
            var choice = Console.ReadLine();
            Int32.TryParse(choice, out choiceNumber);
        }
```

```
        Console.WriteLine(new string('-', 80));

        return service.Categories[choiceNumber - 1];
    }

    /// <summary>
    /// List available severity levels from AWS Support, and select a level for
the example.
    /// </summary>
    /// <returns>The selected severity level.</returns>
    private static async Task<SeverityLevel> DisplayAndSelectSeverity()
    {
        Console.WriteLine(new string('-', 80));
        var severityLevels = await _supportWrapper.DescribeSeverityLevels();

        Console.WriteLine($"3. Get and display available severity levels:");
        for (int i = 0; i < 10 && i < severityLevels.Count; i++)
        {
            Console.WriteLine($"\t{i + 1}. {severityLevels[i].Name}");
        }

        var choiceNumber = 0;
        while (choiceNumber < 1 || choiceNumber > severityLevels.Count)
        {
            Console.WriteLine(
                "Select an example severity level by entering a number from the
preceding list:");
            var choice = Console.ReadLine();
            Int32.TryParse(choice, out choiceNumber);
        }
        Console.WriteLine(new string('-', 80));

        return severityLevels[choiceNumber - 1];
    }

    /// <summary>
    /// Create an example support case.
    /// </summary>
    /// <param name="service">Service to use for the new case.</param>
    /// <param name="category">Category to use for the new case.</param>
    /// <param name="severity">Severity to use for the new case.</param>
    /// <returns>The caseId of the new support case.</returns>
    private static async Task<string> CreateSupportCase(Service service,
```

```
        Category category, SeverityLevel severity)
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"4. Create an example support case" +
                          $" with the following settings:" +
                          $" \n\tService: {service.Name}, Category:
{category.Name} " +
                          $"and Severity Level: {severity.Name}.");
        var caseId = await _supportWrapper.CreateCase(service.Code,
category.Code, severity.Code,
            "Example case for testing, ignore.", "This is my example support
case.");

        Console.WriteLine($"\tNew case created with ID {caseId}");

        Console.WriteLine(new string('-', 80));

        return caseId;
    }

    /// <summary>
    /// List open cases for the current day.
    /// </summary>
    /// <returns>Async task.</returns>
    private static async Task DescribeTodayOpenCases()
    {
        Console.WriteLine($"5. List the open support cases for the current
day.");
        // Describe the cases. If it is empty, try again and allow time for the
new case to appear.
        List<CaseDetails> currentOpenCases = null!;
        while (currentOpenCases == null || currentOpenCases.Count == 0)
        {
            Thread.Sleep(1000);
            currentOpenCases = await _supportWrapper.DescribeCases(
                new List<string>(),
                null,
                false,
                false,
                DateTime.UtcNow.Date,
                DateTime.UtcNow);
        }

        foreach (var openCase in currentOpenCases)
```

```
        {
            Console.WriteLine($"\tCase: {openCase.CaseId} created
 {openCase.TimeCreated}");
        }

        Console.WriteLine(new string('-', 80));
    }

    /// <summary>
    /// Create an attachment set for a support case.
    /// </summary>
    /// <returns>The attachment set id.</returns>
    private static async Task<string> CreateAttachmentSet()
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"6. Create an attachment set for a support case.");
        var fileName = "example_attachment.txt";

        // Create the file if it does not already exist.
        if (!File.Exists(fileName))
        {
            await using StreamWriter sw = File.CreateText(fileName);
            await sw.WriteLineAsync(
                "This is a sample file for attachment to a support case.");
        }

        await using var ms = new MemoryStream(await
 File.ReadAllBytesAsync(fileName));

        var attachmentSetId = await _supportWrapper.AddAttachmentToSet(
            ms,
            fileName);

        Console.WriteLine($"\tNew attachment set created with id: \n
\t{attachmentSetId.Substring(0, 65)}...");

        Console.WriteLine(new string('-', 80));

        return attachmentSetId;
    }

    /// <summary>
    /// Add an attachment set and communication to a case.
    /// </summary>
```

```
    /// <param name="attachmentSetId">Id of the attachment set.</param>
    /// <param name="caseId">Id of the case to receive the attachment set.</
param>
    /// <returns>Async task.</returns>
    private static async Task AddCommunicationToCase(string attachmentSetId,
 string caseId)
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"7. Add attachment set and communication to
 {caseId}.");

        await _supportWrapper.AddCommunicationToCase(
            caseId,
            "This is an example communication added to a support case.",
            attachmentSetId);

        Console.WriteLine($"\tNew attachment set and communication added to
 {caseId}");

        Console.WriteLine(new string('-', 80));
    }

    /// <summary>
    /// List the communications for a case.
    /// </summary>
    /// <param name="caseId">Id of the case to describe.</param>
    /// <returns>An attachment id.</returns>
    private static async Task<string> ListCommunicationsForCase(string caseId)
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"8. List communications for case {caseId}.");

        var communications = await
 _supportWrapper.DescribeCommunications(caseId);
        var attachmentId = "";
        foreach (var communication in communications)
        {
            Console.WriteLine(
                $"\tCommunication created on: {communication.TimeCreated} has
 {communication.AttachmentSet.Count} attachments.");
            if (communication.AttachmentSet.Any())
            {
                attachmentId = communication.AttachmentSet.First().AttachmentId;
            }
```

```
        }

        Console.WriteLine(new string('-', 80));
        return attachmentId;
    }

    /// <summary>
    /// Describe an attachment by id.
    /// </summary>
    /// <param name="attachmentId">Id of the attachment to describe.</param>
    /// <returns>Async task.</returns>
    private static async Task DescribeCaseAttachment(string attachmentId)
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"9. Describe the attachment set.");

        var attachment = await _supportWrapper.DescribeAttachment(attachmentId);
        var data = Encoding.ASCII.GetString(attachment.Data.ToArray());
        Console.WriteLine($"\tAttachment includes {attachment.FileName} with
data: \n\t{data}");

        Console.WriteLine(new string('-', 80));
    }

    /// <summary>
    /// Resolve the support case.
    /// </summary>
    /// <param name="caseId">Id of the case to resolve.</param>
    /// <returns>Async task.</returns>
    private static async Task ResolveCase(string caseId)
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"10. Resolve case {caseId}.");

        var status = await _supportWrapper.ResolveCase(caseId);
        Console.WriteLine($"\tCase {caseId} has final status {status}");

        Console.WriteLine(new string('-', 80));
    }

    /// <summary>
    /// List resolved cases for the current day.
    /// </summary>
    /// <returns>Async Task.</returns>
```

```
    private static async Task DescribeTodayResolvedCases()
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"11. List the resolved support cases for the current
 day.");
        var currentCases = await _supportWrapper.DescribeCases(
            new List<string>(),
            null,
            false,
            true,
            DateTime.UtcNow.Date,
            DateTime.UtcNow);

        foreach (var currentCase in currentCases)
        {
            if (currentCase.Status == "resolved")
            {
                Console.WriteLine(
                    $"\tCase: {currentCase.CaseId}: status
 {currentCase.Status}");
            }
        }

        Console.WriteLine(new string('-', 80));
    }
}
```

Metode pembungkus yang digunakan oleh skenario untuk AWS Support tindakan.

```
/// <summary>
/// Wrapper methods to use AWS Support for working with support cases.
/// </summary>
public class SupportWrapper
{
    private readonly IAmazonAWSSupport _amazonSupport;
    public SupportWrapper(IAmazonAWSSupport amazonSupport)
    {
        _amazonSupport = amazonSupport;
    }
```

```
    /// <summary>
    /// Get the descriptions of AWS services.
    /// </summary>
    /// <param name="name">Optional language for services.
    /// Currently Chinese (“zh”), English ("en"), Japanese ("ja") and Korean
(“ko”) are supported.</param>
    /// <returns>The list of AWS service descriptions.</returns>
    public async Task<List<Service>> DescribeServices(string language = "en")
    {
        var response = await _amazonSupport.DescribeServicesAsync(
            new DescribeServicesRequest()
            {
                Language = language
            });
        return response.Services;
    }



    /// <summary>
    /// Get the descriptions of support severity levels.
    /// </summary>
    /// <param name="name">Optional language for severity levels.
    /// Currently Chinese (“zh”), English ("en"), Japanese ("ja") and Korean
(“ko”) are supported.</param>
    /// <returns>The list of support severity levels.</returns>
    public async Task<List<SeverityLevel>> DescribeSeverityLevels(string language
= "en")
    {
        var response = await _amazonSupport.DescribeSeverityLevelsAsync(
            new DescribeSeverityLevelsRequest()
            {
                Language = language
            });
        return response.SeverityLevels;
    }



    /// <summary>
    /// Create a new support case.
    /// </summary>
    /// <param name="serviceCode">Service code for the new case.</param>
    /// <param name="categoryCode">Category for the new case.</param>
```

```
   /// <param name="severityCode">Severity code for the new case.</param>
   /// <param name="subject">Subject of the new case.</param>
   /// <param name="body">Body text of the new case.</param>
   /// <param name="language">Optional language support for your case.
   /// Currently Chinese (“zh”), English ("en"), Japanese ("ja") and Korean
(“ko”) are supported.</param>
   /// <param name="attachmentSetId">Optional Id for an attachment set for the
new case.</param>
   /// <param name="issueType">Optional issue type for the new case. Options are
"customer-service" or "technical".</param>
   /// <returns>The caseId of the new support case.</returns>
   public async Task<string> CreateCase(string serviceCode, string categoryCode,
string severityCode, string subject,
       string body, string language = "en", string? attachmentSetId = null,
string issueType = "customer-service")
   {
       var response = await _amazonSupport.CreateCaseAsync(
           new CreateCaseRequest()
           {
               ServiceCode = serviceCode,
               CategoryCode = categoryCode,
               SeverityCode = severityCode,
               Subject = subject,
               Language = language,
               AttachmentSetId = attachmentSetId,
               IssueType = issueType,
               CommunicationBody = body
           });
       return response.CaseId;
   }



   /// <summary>
   /// Add an attachment to a set, or create a new attachment set if one does
not exist.
   /// </summary>
   /// <param name="data">The data for the attachment.</param>
   /// <param name="fileName">The file name for the attachment.</param>
   /// <param name="attachmentSetId">Optional setId for the attachment. Creates
a new attachment set if empty.</param>
   /// <returns>The setId of the attachment.</returns>
   public async Task<string> AddAttachmentToSet(MemoryStream data, string
fileName, string? attachmentSetId = null)
```

```
    {
        var response = await _amazonSupport.AddAttachmentsToSetAsync(
            new AddAttachmentsToSetRequest
            {
                AttachmentSetId = attachmentSetId,
                Attachments = new List<Attachment>
                {
                    new Attachment
                    {
                        Data = data,
                        FileName = fileName
                    }
                }
            });
        return response.AttachmentSetId;
    }



    /// <summary>
    /// Get description of a specific attachment.
    /// </summary>
    /// <param name="attachmentId">Id of the attachment, usually fetched by
describing the communications of a case.</param>
    /// <returns>The attachment object.</returns>
    public async Task<Attachment> DescribeAttachment(string attachmentId)
    {
        var response = await _amazonSupport.DescribeAttachmentAsync(
            new DescribeAttachmentRequest()
            {
                AttachmentId = attachmentId
            });
        return response.Attachment;
    }



    /// <summary>
    /// Add communication to a case, including optional attachment set ID and CC
email addresses.
    /// </summary>
    /// <param name="caseId">Id for the support case.</param>
    /// <param name="body">Body text of the communication.</param>
    /// <param name="attachmentSetId">Optional Id for an attachment set.</param>
```

```
    /// <param name="ccEmailAddresses">Optional list of CC email addresses.</
param>
    /// <returns>True if successful.</returns>
    public async Task<bool> AddCommunicationToCase(string caseId, string body,
        string? attachmentSetId = null, List<string>? ccEmailAddresses = null)
    {
        var response = await _amazonSupport.AddCommunicationToCaseAsync(
            new AddCommunicationToCaseRequest()
            {
                CaseId = caseId,
                CommunicationBody = body,
                AttachmentSetId = attachmentSetId,
                CcEmailAddresses = ccEmailAddresses
            });
        return response.Result;
    }



    /// <summary>
    /// Describe the communications for a case, optionally with a date filter.
    /// </summary>
    /// <param name="caseId">The ID of the support case.</param>
    /// <param name="afterTime">The optional start date for a filtered search.</
param>
    /// <param name="beforeTime">The optional end date for a filtered search.</
param>
    /// <returns>The list of communications for the case.</returns>
    public async Task<List<Communication>> DescribeCommunications(string caseId,
 DateTime? afterTime = null, DateTime? beforeTime = null)
    {
        var results = new List<Communication>();
        var paginateCommunications =
 _amazonSupport.Paginators.DescribeCommunications(
            new DescribeCommunicationsRequest()
            {
                CaseId = caseId,
                AfterTime = afterTime?.ToString("s"),
                BeforeTime = beforeTime?.ToString("s")
            });
        // Get the entire list using the paginator.
        await foreach (var communications in
 paginateCommunications.Communications)
        {
```

```
            results.Add(communications);
        }
        return results;
    }



    /// <summary>
    /// Get case details for a list of case ids, optionally with date filters.
    /// </summary>
    /// <param name="caseIds">The list of case IDs.</param>
    /// <param name="displayId">Optional display ID.</param>
    /// <param name="includeCommunication">True to include communication.
 Defaults to true.</param>
    /// <param name="includeResolvedCases">True to include resolved cases.
 Defaults to false.</param>
    /// <param name="afterTime">The optional start date for a filtered search.</
param>
    /// <param name="beforeTime">The optional end date for a filtered search.</
param>
    /// <param name="language">Optional language support for your case.
    /// Currently Chinese (“zh”), English ("en"), Japanese ("ja") and Korean
 (“ko”) are supported.</param>
    /// <returns>A list of CaseDetails.</returns>
    public async Task<List<CaseDetails>> DescribeCases(List<string> caseIds,
 string? displayId = null, bool includeCommunication = true,
        bool includeResolvedCases = false, DateTime? afterTime = null, DateTime?
 beforeTime = null,
        string language = "en")
    {
        var results = new List<CaseDetails>();
        var paginateCases = _amazonSupport.Paginators.DescribeCases(
            new DescribeCasesRequest()
            {
                CaseIdList = caseIds,
                DisplayId = displayId,
                IncludeCommunications = includeCommunication,
                IncludeResolvedCases = includeResolvedCases,
                AfterTime = afterTime?.ToString("s"),
                BeforeTime = beforeTime?.ToString("s"),
                Language = language
            });
        // Get the entire list using the paginator.
        await foreach (var cases in paginateCases.Cases)
```

```
        {
            results.Add(cases);
        }
        return results;
    }



    /// <summary>
    /// Resolve a support case by caseId.
    /// </summary>
    /// <param name="caseId">Id for the support case.</param>
    /// <returns>The final status of the case after resolving.</returns>
    public async Task<string> ResolveCase(string caseId)
    {
        var response = await _amazonSupport.ResolveCaseAsync(
            new ResolveCaseRequest()
            {
                CaseId = caseId
            });
        return response.FinalCaseStatus;
    }



    /// <summary>
    /// Verify the support level for AWS Support API access.
    /// </summary>
    /// <returns>True if the subscription level supports API access.</returns>
    public async Task<bool> VerifySubscription()
    {
        try
        {
            var response = await _amazonSupport.DescribeServicesAsync(
                new DescribeServicesRequest()
                {
                    Language = "en"
                });
            return response.HttpStatusCode == HttpStatusCode.OK;
        }
        catch (Amazon.AWSSupport.AmazonAWSSupportException ex)
        {
            if (ex.ErrorCode == "SubscriptionRequiredException")
            {
                return false;
```

```
            }
            else throw;
        }
    }
}
```

- Untuk detail API, lihat topik berikut di Referensi API AWS SDK for .NET .
  - AddAttachmentsToSet
  - AddCommunicationToCase
  - CreateCase
  - DescribeAttachment
  - DescribeCases
  - DescribeCommunications
  - DescribeServices
  - DescribeSeverityLevel
  - ResolveCase

Java

SDK untuk Java 2.x

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di AWS Repositori Contoh Kode.

Jalankan berbagai AWS Support operasi.

```
import software.amazon.awssdk.core.SdkBytes;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.support.SupportClient;
import software.amazon.awssdk.services.support.model.AddAttachmentsToSetResponse;
import
 software.amazon.awssdk.services.support.model.AddCommunicationToCaseRequest;
import
 software.amazon.awssdk.services.support.model.AddCommunicationToCaseResponse;
```

```
import software.amazon.awssdk.services.support.model.Attachment;
import software.amazon.awssdk.services.support.model.AttachmentDetails;
import software.amazon.awssdk.services.support.model.CaseDetails;
import software.amazon.awssdk.services.support.model.Category;
import software.amazon.awssdk.services.support.model.Communication;
import software.amazon.awssdk.services.support.model.CreateCaseRequest;
import software.amazon.awssdk.services.support.model.CreateCaseResponse;
import software.amazon.awssdk.services.support.model.DescribeAttachmentRequest;
import software.amazon.awssdk.services.support.model.DescribeAttachmentResponse;
import software.amazon.awssdk.services.support.model.DescribeCasesRequest;
import software.amazon.awssdk.services.support.model.DescribeCasesResponse;
import
 software.amazon.awssdk.services.support.model.DescribeCommunicationsRequest;
import
 software.amazon.awssdk.services.support.model.DescribeCommunicationsResponse;
import software.amazon.awssdk.services.support.model.DescribeServicesRequest;
import software.amazon.awssdk.services.support.model.DescribeServicesResponse;
import
 software.amazon.awssdk.services.support.model.DescribeSeverityLevelsRequest;
import
 software.amazon.awssdk.services.support.model.DescribeSeverityLevelsResponse;
import software.amazon.awssdk.services.support.model.ResolveCaseRequest;
import software.amazon.awssdk.services.support.model.ResolveCaseResponse;
import software.amazon.awssdk.services.support.model.Service;
import software.amazon.awssdk.services.support.model.SeverityLevel;
import software.amazon.awssdk.services.support.model.SupportException;
import software.amazon.awssdk.services.support.model.AddAttachmentsToSetRequest;
import java.io.File;
import java.io.FileInputStream;
import java.io.FileNotFoundException;
import java.io.InputStream;
import java.time.Instant;
import java.time.temporal.ChronoUnit;
import java.util.ArrayList;
import java.util.List;

/**
 * Before running this Java (v2) code example, set up your development
 * environment, including your credentials.
 *
 * For more information, see the following documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
```

```
 *
 * In addition, you must have the AWS Business Support Plan to use the AWS
 * Support Java API. For more information, see:
 *
 * https://aws.amazon.com/premiumsupport/plans/
 *
 * This Java example performs the following tasks:
 *
 * 1. Gets and displays available services.
 * 2. Gets and displays severity levels.
 * 3. Creates a support case by using the selected service, category, and
 * severity level.
 * 4. Gets a list of open cases for the current day.
 * 5. Creates an attachment set with a generated file.
 * 6. Adds a communication with the attachment to the support case.
 * 7. Lists the communications of the support case.
 * 8. Describes the attachment set included with the communication.
 * 9. Resolves the support case.
 * 10. Gets a list of resolved cases for the current day.
 */
public class SupportScenario {

    public static final String DASHES = new String(new char[80]).replace("\0",
 "-");

    public static void main(String[] args) {
        final String usage = """

                Usage:
                    <fileAttachment>Where:
                    fileAttachment - The file can be a simple saved .txt file to
 use as an email attachment.\s
                """;

        if (args.length != 1) {
            System.out.println(usage);
            System.exit(1);
        }

        String fileAttachment = args[0];
        Region region = Region.US_WEST_2;
        SupportClient supportClient = SupportClient.builder()
                .region(region)
                .build();
```

```
        System.out.println(DASHES);
        System.out.println("***** Welcome to the AWS Support case example
scenario.");
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("1. Get and display available services.");
        List<String> sevCatList = displayServices(supportClient);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("2. Get and display Support severity levels.");
        String sevLevel = displaySevLevels(supportClient);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("3. Create a support case using the selected service,
category, and severity level.");
        String caseId = createSupportCase(supportClient, sevCatList, sevLevel);
        if (caseId.compareTo("") == 0) {
            System.out.println("A support case was not successfully created!");
            System.exit(1);
        } else
            System.out.println("Support case " + caseId + " was successfully
created!");
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("4. Get open support cases.");
        getOpenCase(supportClient);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("5. Create an attachment set with a generated file to
add to the case.");
        String attachmentSetId = addAttachment(supportClient, fileAttachment);
        System.out.println("The Attachment Set id value is" + attachmentSetId);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("6. Add communication with the attachment to the
support case.");
        addAttachSupportCase(supportClient, caseId, attachmentSetId);
```

```
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("7. List the communications of the support case.");
        String attachId = listCommunications(supportClient, caseId);
        System.out.println("The Attachment id value is" + attachId);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("8. Describe the attachment set included with the
communication.");
        describeAttachment(supportClient, attachId);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("9. Resolve the support case.");
        resolveSupportCase(supportClient, caseId);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("10. Get a list of resolved cases for the current
day.");
        getResolvedCase(supportClient);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("***** This Scenario has successfully completed");
        System.out.println(DASHES);
    }

    public static void getResolvedCase(SupportClient supportClient) {
        try {
            // Specify the start and end time.
            Instant now = Instant.now();
            java.time.LocalDate.now();
            Instant yesterday = now.minus(1, ChronoUnit.DAYS);

            DescribeCasesRequest describeCasesRequest =
DescribeCasesRequest.builder()
                    .maxResults(30)
                    .afterTime(yesterday.toString())
                    .beforeTime(now.toString())
                    .includeResolvedCases(true)
                    .build();
```

```
            DescribeCasesResponse response =
supportClient.describeCases(describeCasesRequest);
            List<CaseDetails> cases = response.cases();
            for (CaseDetails sinCase : cases) {
                if (sinCase.status().compareTo("resolved") == 0)
                    System.out.println("The case status is " + sinCase.status());
            }

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }

    public static void resolveSupportCase(SupportClient supportClient, String
caseId) {
        try {
            ResolveCaseRequest caseRequest = ResolveCaseRequest.builder()
                    .caseId(caseId)
                    .build();

            ResolveCaseResponse response =
supportClient.resolveCase(caseRequest);
            System.out.println("The status of case " + caseId + " is " +
response.finalCaseStatus());

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }

    public static void describeAttachment(SupportClient supportClient, String
attachId) {
        try {
            DescribeAttachmentRequest attachmentRequest =
DescribeAttachmentRequest.builder()
                    .attachmentId(attachId)
                    .build();

            DescribeAttachmentResponse response =
supportClient.describeAttachment(attachmentRequest);
```

```
            System.out.println("The name of the file is " +
response.attachment().fileName());

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }

    public static String listCommunications(SupportClient supportClient, String
caseId) {
        try {
            String attachId = null;
            DescribeCommunicationsRequest communicationsRequest =
DescribeCommunicationsRequest.builder()
                    .caseId(caseId)
                    .maxResults(10)
                    .build();

            DescribeCommunicationsResponse response =
supportClient.describeCommunications(communicationsRequest);
            List<Communication> communications = response.communications();
            for (Communication comm : communications) {
                System.out.println("the body is: " + comm.body());

                // Get the attachment id value.
                List<AttachmentDetails> attachments = comm.attachmentSet();
                for (AttachmentDetails detail : attachments) {
                    attachId = detail.attachmentId();
                }
            }
            return attachId;

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
        return "";
    }

    public static void addAttachSupportCase(SupportClient supportClient, String
caseId, String attachmentSetId) {
        try {
```

```
            AddCommunicationToCaseRequest caseRequest =
AddCommunicationToCaseRequest.builder()
                    .caseId(caseId)
                    .attachmentSetId(attachmentSetId)
                    .communicationBody("Please refer to attachment for details.")
                    .build();

            AddCommunicationToCaseResponse response =
supportClient.addCommunicationToCase(caseRequest);
            if (response.result())
                System.out.println("You have successfully added a communication
to an AWS Support case");
            else
                System.out.println("There was an error adding the communication
to an AWS Support case");

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }

    public static String addAttachment(SupportClient supportClient, String
fileAttachment) {
        try {
            File myFile = new File(fileAttachment);
            InputStream sourceStream = new FileInputStream(myFile);
            SdkBytes sourceBytes = SdkBytes.fromInputStream(sourceStream);

            Attachment attachment = Attachment.builder()
                    .fileName(myFile.getName())
                    .data(sourceBytes)
                    .build();

            AddAttachmentsToSetRequest setRequest =
AddAttachmentsToSetRequest.builder()
                    .attachments(attachment)
                    .build();

            AddAttachmentsToSetResponse response =
supportClient.addAttachmentsToSet(setRequest);
            return response.attachmentSetId();

        } catch (SupportException | FileNotFoundException e) {
```

```
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
        return "";
    }

    public static void getOpenCase(SupportClient supportClient) {
        try {
            // Specify the start and end time.
            Instant now = Instant.now();
            java.time.LocalDate.now();
            Instant yesterday = now.minus(1, ChronoUnit.DAYS);

            DescribeCasesRequest describeCasesRequest =
DescribeCasesRequest.builder()
                    .maxResults(20)
                    .afterTime(yesterday.toString())
                    .beforeTime(now.toString())
                    .build();

            DescribeCasesResponse response =
supportClient.describeCases(describeCasesRequest);
            List<CaseDetails> cases = response.cases();
            for (CaseDetails sinCase : cases) {
                System.out.println("The case status is " + sinCase.status());
                System.out.println("The case Id is " + sinCase.caseId());
                System.out.println("The case subject is " + sinCase.subject());
            }

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }

    public static String createSupportCase(SupportClient supportClient,
List<String> sevCatList, String sevLevel) {
        try {
            String serviceCode = sevCatList.get(0);
            String caseCat = sevCatList.get(1);
            CreateCaseRequest caseRequest = CreateCaseRequest.builder()
                    .categoryCode(caseCat.toLowerCase())
                    .serviceCode(serviceCode.toLowerCase())
                    .severityCode(sevLevel.toLowerCase())
```

```
                    .communicationBody("Test issue with " +
serviceCode.toLowerCase())
                    .subject("Test case, please ignore")
                    .language("en")
                    .issueType("technical")
                    .build();

            CreateCaseResponse response = supportClient.createCase(caseRequest);
            return response.caseId();

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
        return "";
    }

    public static String displaySevLevels(SupportClient supportClient) {
        try {
            DescribeSeverityLevelsRequest severityLevelsRequest =
DescribeSeverityLevelsRequest.builder()
                    .language("en")
                    .build();

            DescribeSeverityLevelsResponse response =
supportClient.describeSeverityLevels(severityLevelsRequest);
            List<SeverityLevel> severityLevels = response.severityLevels();
            String levelName = null;
            for (SeverityLevel sevLevel : severityLevels) {
                System.out.println("The severity level name is: " +
sevLevel.name());
                if (sevLevel.name().compareTo("High") == 0)
                    levelName = sevLevel.name();
            }
            return levelName;

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
        return "";
    }

    // Return a List that contains a Service name and Category name.
```

```
   public static List<String> displayServices(SupportClient supportClient) {
       try {
           DescribeServicesRequest servicesRequest =
DescribeServicesRequest.builder()
                   .language("en")
                   .build();

           DescribeServicesResponse response =
supportClient.describeServices(servicesRequest);
           String serviceCode = null;
           String catName = null;
           List<String> sevCatList = new ArrayList<>();
           List<Service> services = response.services();

           System.out.println("Get the first 10 services");
           int index = 1;
           for (Service service : services) {
               if (index == 11)
                   break;

               System.out.println("The Service name is: " + service.name());
               if (service.name().compareTo("Account") == 0)
                   serviceCode = service.code();

               // Get the Categories for this service.
               List<Category> categories = service.categories();
               for (Category cat : categories) {
                   System.out.println("The category name is: " + cat.name());
                   if (cat.name().compareTo("Security") == 0)
                       catName = cat.name();
               }
               index++;
           }

           // Push the two values to the list.
           sevCatList.add(serviceCode);
           sevCatList.add(catName);
           return sevCatList;

       } catch (SupportException e) {
           System.out.println(e.getLocalizedMessage());
           System.exit(1);
       }
       return null;
```

```
    }
}
```

- Untuk detail API, lihat topik berikut di Referensi API AWS SDK for Java 2.x .
  - AddAttachmentsToSet
  - AddCommunicationToCase
  - CreateCase
  - DescribeAttachment
  - DescribeCases
  - DescribeCommunications
  - DescribeServices
  - DescribeSeverityLevel
  - ResolveCase

JavaScript

SDK untuk JavaScript (v3)

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di AWS Repositori Contoh Kode.

Jalankan skenario interaktif di terminal.

```
import {
  AddAttachmentsToSetCommand,
  AddCommunicationToCaseCommand,
  CreateCaseCommand,
  DescribeAttachmentCommand,
  DescribeCasesCommand,
  DescribeCommunicationsCommand,
  DescribeServicesCommand,
  DescribeSeverityLevelsCommand,
  ResolveCaseCommand,
  SupportClient,
```

```
} from "@aws-sdk/client-support";
import * as inquirer from "@inquirer/prompts";
import { retry } from "@aws-doc-sdk-examples/lib/utils/util-timers.js";

const wrapText = (text, char = "=") => {
  const rule = char.repeat(80);
  return `${rule}\n    ${text}\n${rule}\n`;
};

const client = new SupportClient({ region: "us-east-1" });

// Verify that the account has a Support plan.
export const verifyAccount = async () => {
  const command = new DescribeServicesCommand({});

  try {
    await client.send(command);
  } catch (err) {
    if (err.name === "SubscriptionRequiredException") {
      throw new Error(
        "You must be subscribed to the AWS Support plan to use this feature.",
      );
    } else {
      throw err;
    }
  }
};

/**
 * Select a service from the list returned from DescribeServices.
 */
export const getService = async () => {
  const { services } = await client.send(new DescribeServicesCommand({}));
  const selectedService = await inquirer.select({
    message:
      "Select a service. Your support case will be created for this service. The
 list of services is truncated for readability.",
    choices: services.slice(0, 10).map((s) => ({ name: s.name, value: s })),
  });
  return selectedService;
};

/**
 * @param {{ categories: import('@aws-sdk/client-support').Category[]}} service
```

```
 */
export const getCategory = async (service) => {
  const selectedCategory = await inquirer.select({
    message: "Select a category.",
    choices: service.categories.map((c) => ({ name: c.name, value: c })),
  });
  return selectedCategory;
};

// Get the available severity levels for the account.
export const getSeverityLevel = async () => {
  const command = new DescribeSeverityLevelsCommand({});
  const { severityLevels } = await client.send(command);
  const selectedSeverityLevel = await inquirer.select({
    message: "Select a severity level.",
    choices: severityLevels.map((s) => ({ name: s.name, value: s })),
  });
  return selectedSeverityLevel;
};

/**
 * Create a new support case
 * @param {{
 *  selectedService: import('@aws-sdk/client-support').Service
 *  selectedCategory: import('@aws-sdk/client-support').Category
 *  selectedSeverityLevel: import('@aws-sdk/client-support').SeverityLevel
 * }} selections
 * @returns
 */
export const createCase = async ({
  selectedService,
  selectedCategory,
  selectedSeverityLevel,
}) => {
  const command = new CreateCaseCommand({
    subject: "IGNORE: Test case",
    communicationBody: "This is a test. Please ignore.",
    serviceCode: selectedService.code,
    categoryCode: selectedCategory.code,
    severityCode: selectedSeverityLevel.code,
  });
  const { caseId } = await client.send(command);
  return caseId;
};
```

```
// Get a list of open support cases created today.
export const getTodaysOpenCases = async () => {
  const d = new Date();
  const startOfToday = new Date(d.getFullYear(), d.getMonth(), d.getDate());
  const command = new DescribeCasesCommand({
    includeCommunications: false,
    afterTime: startOfToday.toISOString(),
  });

  const { cases } = await client.send(command);

  if (cases.length === 0) {
    throw new Error(
      "Unexpected number of cases. Expected more than 0 open cases.",
    );
  }
  return cases;
};

// Create an attachment set.
export const createAttachmentSet = async () => {
  const command = new AddAttachmentsToSetCommand({
    attachments: [
      {
        fileName: "example.txt",
        data: new TextEncoder().encode("some example text"),
      },
    ],
  });
  const { attachmentSetId } = await client.send(command);
  return attachmentSetId;
};

export const linkAttachmentSetToCase = async (attachmentSetId, caseId) => {
  const command = new AddCommunicationToCaseCommand({
    attachmentSetId,
    caseId,
    communicationBody: "Adding attachment set to case.",
  });
  await client.send(command);
};

// Get all communications for a support case.
```

```
export const getCommunications = async (caseId) => {
  const command = new DescribeCommunicationsCommand({
    caseId,
  });
  const { communications } = await client.send(command);
  return communications;
};

/**
 * @param {import('@aws-sdk/client-support').Communication[]} communications
 */
export const getFirstAttachment = (communications) => {
  const firstCommWithAttachment = communications.find(
    (c) => c.attachmentSet.length > 0,
  );
  return firstCommWithAttachment?.attachmentSet[0].attachmentId;
};

// Get an attachment.
export const getAttachment = async (attachmentId) => {
  const command = new DescribeAttachmentCommand({
    attachmentId,
  });
  const { attachment } = await client.send(command);
  return attachment;
};

// Resolve the case matching the given case ID.
export const resolveCase = async (caseId) => {
  const shouldResolve = await inquirer.confirm({
    message: `Do you want to resolve ${caseId}?`,
  });

  if (shouldResolve) {
    const command = new ResolveCaseCommand({
      caseId: caseId,
    });

    await client.send(command);
    return true;
  }
  return false;
};
```

```
/**
 * Find a specific case in the list of provided cases by case ID.
 * If the case is not found, and the results are paginated, continue
 * paging through the results.
 * @param {{
 *   caseId: string,
 *   cases: import('@aws-sdk/client-support').CaseDetails[]
 *   nextToken: string
 * }} options
 * @returns
 */
export const findCase = async ({ caseId, cases, nextToken }) => {
  const foundCase = cases.find((c) => c.caseId === caseId);

  if (foundCase) {
    return foundCase;
  }

  if (nextToken) {
    const response = await client.send(
      new DescribeCasesCommand({
        nextToken,
        includeResolvedCases: true,
      }),
    );
    return findCase({
      caseId,
      cases: response.cases,
      nextToken: response.nextToken,
    });
  }

  throw new Error(`${caseId} not found.`);
};

// Get all cases created today.
export const getTodaysResolvedCases = async (caseIdToWaitFor) => {
  const d = new Date("2023-01-18");
  const startOfToday = new Date(d.getFullYear(), d.getMonth(), d.getDate());
  const command = new DescribeCasesCommand({
    includeCommunications: false,
    afterTime: startOfToday.toISOString(),
    includeResolvedCases: true,
  });
```

```
  const { cases, nextToken } = await client.send(command);
  await findCase({ cases, caseId: caseIdToWaitFor, nextToken });
  return cases.filter((c) => c.status === "resolved");
};

const main = async () => {
  let caseId;
  try {
    console.log(wrapText("Welcome to the AWS Support basic usage scenario."));

    // Verify that the account is subscribed to support.
    await verifyAccount();

    // Provided a truncated list of services and prompt the user to select one.
    const selectedService = await getService();

    // Provided the categories for the selected service and prompt the user to
 select one.
    const selectedCategory = await getCategory(selectedService);

    // Provide the severity available severity levels for the account and prompt
 the user to select one.
    const selectedSeverityLevel = await getSeverityLevel();

    // Create a support case.
    console.log("\nCreating a support case.");
    caseId = await createCase({
      selectedService,
      selectedCategory,
      selectedSeverityLevel,
    });
    console.log(`Support case created: ${caseId}`);

    // Display a list of open support cases created today.
    const todaysOpenCases = await retry(
      { intervalInMs: 1000, maxRetries: 15 },
      getTodaysOpenCases,
    );
    console.log(
      `\nOpen support cases created today: ${todaysOpenCases.length}`,
    );
    console.log(todaysOpenCases.map((c) => `${c.caseId}`).join("\n"));

    // Create an attachment set.
```

```
    console.log("\nCreating an attachment set.");
    const attachmentSetId = await createAttachmentSet();
    console.log(`Attachment set created: ${attachmentSetId}`);

    // Add the attachment set to the support case.
    console.log(`\nAdding attachment set to ${caseId}`);
    await linkAttachmentSetToCase(attachmentSetId, caseId);
    console.log(`Attachment set added to ${caseId}`);

    // List the communications for a support case.
    console.log(`\nListing communications for ${caseId}`);
    const communications = await getCommunications(caseId);
    console.log(
      communications
        .map(
          (c) =>
            `Communication created on ${c.timeCreated}. Has
${c.attachmentSet.length} attachments.`,
        )
        .join("\n"),
    );

    // Describe the first attachment.
    console.log(`\nDescribing attachment ${attachmentSetId}`);
    const attachmentId = getFirstAttachment(communications);
    const attachment = await getAttachment(attachmentId);
    console.log(
      `Attachment is the file '${
        attachment.fileName
      }' with data: \n${new TextDecoder().decode(attachment.data)}`,
    );

    // Confirm that the support case should be resolved.
    const isResolved = await resolveCase(caseId);
    if (isResolved) {
      // List the resolved cases and include the one previously created.
      // Resolved cases can take a while to appear.
      console.log(
        "\nWaiting for case status to be marked as resolved. This can take some
time.",
      );
      const resolvedCases = await retry(
        { intervalInMs: 20000, maxRetries: 15 },
        () => getTodaysResolvedCases(caseId),
```

```
      );
      console.log("Resolved cases:");
      console.log(resolvedCases.map((c) => c.caseId).join("\n"));
    }
  } catch (err) {
    console.error(err);
  }
};
```

- Untuk detail API, lihat topik berikut di Referensi API AWS SDK for JavaScript .
  - AddAttachmentsToSet
  - AddCommunicationToCase
  - CreateCase
  - DescribeAttachment
  - DescribeCases
  - DescribeCommunications
  - DescribeServices
  - DescribeSeverityLevel
  - ResolveCase

Kotlin

SDK untuk Kotlin

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkap dan pelajari cara menyiapkan dan menjalankan di Repositori Contoh Kode AWS.

```
/**
Before running this Kotlin code example, set up your development environment,
including your credentials.

For more information, see the following documentation topic:
```

```
https://docs.aws.amazon.com/sdk-for-kotlin/latest/developer-guide/setup.html
In addition, you must have the AWS Business Support Plan to use the AWS Support
 Java API. For more information, see:

https://aws.amazon.com/premiumsupport/plans/

This Kotlin example performs the following tasks:
1. Gets and displays available services.
2. Gets and displays severity levels.
3. Creates a support case by using the selected service, category, and severity
 level.
4. Gets a list of open cases for the current day.
5. Creates an attachment set with a generated file.
6. Adds a communication with the attachment to the support case.
7. Lists the communications of the support case.
8. Describes the attachment set included with the communication.
9. Resolves the support case.
10. Gets a list of resolved cases for the current day.
*/

suspend fun main(args: Array<String>) {
    val usage = """
    Usage:
        <fileAttachment>
    Where:
         fileAttachment - The file can be a simple saved .txt file to use as an
 email attachment.
    """

    if (args.size != 1) {
        println(usage)
        exitProcess(0)
    }

    val fileAttachment = args[0]
    println("***** Welcome to the AWS Support case example scenario.")
    println("***** Step 1. Get and display available services.")
    val sevCatList = displayServices()

    println("***** Step 2. Get and display Support severity levels.")
    val sevLevel = displaySevLevels()

    println("***** Step 3. Create a support case using the selected service,
 category, and severity level.")
```

```
    val caseIdVal = createSupportCase(sevCatList, sevLevel)
    if (caseIdVal != null) {
        println("Support case $caseIdVal was successfully created!")
    } else {
        println("A support case was not successfully created!")
        exitProcess(1)
    }

    println("***** Step 4. Get open support cases.")
    getOpenCase()

    println("***** Step 5. Create an attachment set with a generated file to add
 to the case.")
    val attachmentSetId = addAttachment(fileAttachment)
    println("The Attachment Set id value is $attachmentSetId")

    println("***** Step 6. Add communication with the attachment to the support
 case.")
    addAttachSupportCase(caseIdVal, attachmentSetId)

    println("***** Step 7. List the communications of the support case.")
    val attachId = listCommunications(caseIdVal)
    println("The Attachment id value is $attachId")

    println("***** Step 8. Describe the attachment set included with the
 communication.")
    describeAttachment(attachId)

    println("***** Step 9. Resolve the support case.")
    resolveSupportCase(caseIdVal)

    println("***** Step 10. Get a list of resolved cases for the current day.")
    getResolvedCase()
    println("***** This Scenario has successfully completed")
}

suspend fun getResolvedCase() {
    // Specify the start and end time.
    val now = Instant.now()
    LocalDate.now()
    val yesterday = now.minus(1, ChronoUnit.DAYS)
    val describeCasesRequest =
        DescribeCasesRequest {
            maxResults = 30
```

```
            afterTime = yesterday.toString()
            beforeTime = now.toString()
            includeResolvedCases = true
        }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.describeCases(describeCasesRequest)
        response.cases?.forEach { sinCase ->
            println("The case status is ${sinCase.status}")
            println("The case Id is ${sinCase.caseId}")
            println("The case subject is ${sinCase.subject}")
        }
    }
}

suspend fun resolveSupportCase(caseIdVal: String) {
    val caseRequest =
        ResolveCaseRequest {
            caseId = caseIdVal
        }
    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.resolveCase(caseRequest)
        println("The status of case $caseIdVal is ${response.finalCaseStatus}")
    }
}

suspend fun describeAttachment(attachId: String?) {
    val attachmentRequest =
        DescribeAttachmentRequest {
            attachmentId = attachId
        }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.describeAttachment(attachmentRequest)
        println("The name of the file is ${response.attachment?.fileName}")
    }
}

suspend fun listCommunications(caseIdVal: String?): String? {
    val communicationsRequest =
        DescribeCommunicationsRequest {
            caseId = caseIdVal
            maxResults = 10
        }
```

```
    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response =
 supportClient.describeCommunications(communicationsRequest)
        response.communications?.forEach { comm ->
            println("the body is: " + comm.body)
            comm.attachmentSet?.forEach { detail ->
                return detail.attachmentId
            }
        }
    }
    return ""
}

suspend fun addAttachSupportCase(
    caseIdVal: String?,
    attachmentSetIdVal: String?
) {
    val caseRequest =
        AddCommunicationToCaseRequest {
            caseId = caseIdVal
            attachmentSetId = attachmentSetIdVal
            communicationBody = "Please refer to attachment for details."
        }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.addCommunicationToCase(caseRequest)
        if (response.result) {
            println("You have successfully added a communication to an AWS
 Support case")
        } else {
            println("There was an error adding the communication to an AWS
 Support case")
        }
    }
}

suspend fun addAttachment(fileAttachment: String): String? {
    val myFile = File(fileAttachment)
    val sourceBytes = (File(fileAttachment).readBytes())
    val attachmentVal =
        Attachment {
            fileName = myFile.name
            data = sourceBytes
```

```
        }

    val setRequest =
        AddAttachmentsToSetRequest {
            attachments = listOf(attachmentVal)
        }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.addAttachmentsToSet(setRequest)
        return response.attachmentSetId
    }
}

suspend fun getOpenCase() {
    // Specify the start and end time.
    val now = Instant.now()
    LocalDate.now()
    val yesterday = now.minus(1, ChronoUnit.DAYS)
    val describeCasesRequest =
        DescribeCasesRequest {
            maxResults = 20
            afterTime = yesterday.toString()
            beforeTime = now.toString()
        }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.describeCases(describeCasesRequest)
        response.cases?.forEach { sinCase ->
            println("The case status is ${sinCase.status}")
            println("The case Id is ${sinCase.caseId}")
            println("The case subject is ${sinCase.subject}")
        }
    }
}

suspend fun createSupportCase(
    sevCatListVal: List<String>,
    sevLevelVal: String
): String? {
    val serCode = sevCatListVal[0]
    val caseCategory = sevCatListVal[1]
    val caseRequest =
        CreateCaseRequest {
            categoryCode = caseCategory.lowercase(Locale.getDefault())
```

```
            serviceCode = serCode.lowercase(Locale.getDefault())
            severityCode = sevLevelVal.lowercase(Locale.getDefault())
            communicationBody = "Test issue with
 ${serCode.lowercase(Locale.getDefault())}"
            subject = "Test case, please ignore"
            language = "en"
            issueType = "technical"
        }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.createCase(caseRequest)
        return response.caseId
    }
}

suspend fun displaySevLevels(): String {
    var levelName = ""
    val severityLevelsRequest =
        DescribeSeverityLevelsRequest {
            language = "en"
        }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response =
 supportClient.describeSeverityLevels(severityLevelsRequest)
        response.severityLevels?.forEach { sevLevel ->
            println("The severity level name is: ${sevLevel.name}")
            if (sevLevel.name == "High") {
                levelName = sevLevel.name!!
            }
        }
        return levelName
    }
}

// Return a List that contains a Service name and Category name.
suspend fun displayServices(): List<String> {
    var serviceCode = ""
    var catName = ""
    val sevCatList = mutableListOf<String>()
    val servicesRequest =
        DescribeServicesRequest {
            language = "en"
        }
```

```
    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.describeServices(servicesRequest)
        println("Get the first 10 services")
        var index = 1

        response.services?.forEach { service ->
            if (index == 11) {
                return@forEach
            }

            println("The Service name is ${service.name}")
            if (service.name == "Account") {
                serviceCode = service.code.toString()
            }

            // Get the categories for this service.
            service.categories?.forEach { cat ->
                println("The category name is ${cat.name}")
                if (cat.name == "Security") {
                    catName = cat.name!!
                }
            }
            index++
        }
    }

    // Push the two values to the list.
    serviceCode.let { sevCatList.add(it) }
    catName.let { sevCatList.add(it) }
    return sevCatList
}
```

- Untuk detail API, lihat topik berikut di referensi API SDK untuk Kotlin AWS .
  - AddAttachmentsToSet
  - AddCommunicationToCase
  - CreateCase
  - DescribeAttachment
  - DescribeCases
  - DescribeCommunications

- DescribeServices
- DescribeSeverityLevel
- ResolveCase

Python

SDK untuk Python (Boto3)

> **Note**
>
> Ada lebih banyak tentang GitHub. Temukan contoh lengkap dan pelajari cara menyiapkan dan menjalankan di Repositori Contoh Kode AWS.

Jalankan skenario interaktif di penggugah/prompt perintah.

```
class SupportCasesScenario:
    """Runs an interactive scenario that shows how to get started using AWS
 Support."""

    def __init__(self, support_wrapper):
        """
        :param support_wrapper: An object that wraps AWS Support actions.
        """
        self.support_wrapper = support_wrapper

    def display_and_select_service(self):
        """
        Lists support services and prompts the user to select one.

        :return: The support service selected by the user.
        """
        print("-" * 88)
        services_list = self.support_wrapper.describe_services("en")
        print(f"AWS Support client returned {len(services_list)} services.")
        print("Displaying first 10 services:")

        service_choices = [svc["name"] for svc in services_list[:10]]
        selected_index = q.choose(
            "Select an example support service by entering a number from the
 preceding list:",
```

```
            service_choices,
        )
        selected_service = services_list[selected_index]
        print("-" * 88)
        return selected_service

    def display_and_select_category(self, service):
        """
        Lists categories for a support service and prompts the user to select
one.

        :param service: The service of the categories.
        :return: The selected category.
        """
        print("-" * 88)
        print(
            f"Available support categories for Service {service['name']}
{len(service['categories'])}:"
        )
        categories_choices = [category["name"] for category in
service["categories"]]
        selected_index = q.choose(
            "Select an example support category by entering a number from the
preceding list:",
            categories_choices,
        )
        selected_category = service["categories"][selected_index]
        print("-" * 88)
        return selected_category

    def display_and_select_severity(self):
        """
        Lists available severity levels and prompts the user to select one.

        :return: The selected severity level.
        """
        print("-" * 88)
        severity_levels_list =
self.support_wrapper.describe_severity_levels("en")
        print(f"Available severity levels:")
        severity_choices = [level["name"] for level in severity_levels_list]
        selected_index = q.choose(
            "Select an example severity level by entering a number from the
preceding list:",
```

```
            severity_choices,
        )
        selected_severity = severity_levels_list[selected_index]
        print("-" * 88)
        return selected_severity

    def create_example_case(self, service, category, severity_level):
        """
        Creates an example support case with the user's selections.

        :param service: The service for the new case.
        :param category: The category for the new case.
        :param severity_level: The severity level for the new case.
        :return: The caseId of the new support case.
        """
        print("-" * 88)
        print(f"Creating new case for service {service['name']}.")
        case_id = self.support_wrapper.create_case(service, category,
severity_level)
        print(f"\tNew case created with ID {case_id}.")
        print("-" * 88)
        return case_id

    def list_open_cases(self):
        """
        List the open cases for the current day.
        """
        print("-" * 88)
        print("Let's list the open cases for the current day.")
        start_time = str(datetime.utcnow().date())
        end_time = str(datetime.utcnow().date() + timedelta(days=1))
        open_cases = self.support_wrapper.describe_cases(start_time, end_time,
False)
        for case in open_cases:
            print(f"\tCase: {case['caseId']}: status {case['status']}.")
        print("-" * 88)

    def create_attachment_set(self):
        """
        Create an attachment set with a sample file.

        :return: The attachment set ID of the new attachment set.
        """
        print("-" * 88)
```

```
        print("Creating attachment set with a sample file.")
        attachment_set_id = self.support_wrapper.add_attachment_to_set()
        print(f"\tNew attachment set created with ID {attachment_set_id}.")
        print("-" * 88)
        return attachment_set_id

    def add_communication(self, case_id, attachment_set_id):
        """
        Add a communication with an attachment set to the case.

        :param case_id: The ID of the case for the communication.
        :param attachment_set_id: The ID of the attachment set to
        add to the communication.
        """
        print("-" * 88)
        print(f"Adding a communication and attachment set to the case.")
        self.support_wrapper.add_communication_to_case(attachment_set_id,
case_id)
        print(
            f"Added a communication and attachment set {attachment_set_id} to the
case {case_id}."
        )
        print("-" * 88)

    def list_communications(self, case_id):
        """
        List the communications associated with a case.

        :param case_id: The ID of the case.
        :return: The attachment ID of an attachment.
        """
        print("-" * 88)
        print("Let's list the communications for our case.")
        attachment_id = ""
        communications =
self.support_wrapper.describe_all_case_communications(case_id)
        for communication in communications:
            print(
                f"\tCommunication created on {communication['timeCreated']} "
                f"has {len(communication['attachmentSet'])} attachments."
            )
            if len(communication["attachmentSet"]) > 0:
                attachment_id = communication["attachmentSet"][0]["attachmentId"]
        print("-" * 88)
```

```
        return attachment_id

    def describe_case_attachment(self, attachment_id):
        """
        Describe an attachment associated with a case.

        :param attachment_id: The ID of the attachment.
        """
        print("-" * 88)
        print("Let's list the communications for our case.")
        attached_file = self.support_wrapper.describe_attachment(attachment_id)
        print(f"\tAttachment includes file {attached_file}.")
        print("-" * 88)

    def resolve_case(self, case_id):
        """
        Shows how to resolve an AWS Support case by its ID.

        :param case_id: The ID of the case to resolve.
        """
        print("-" * 88)
        print(f"Resolving case with ID {case_id}.")
        case_status = self.support_wrapper.resolve_case(case_id)
        print(f"\tFinal case status is {case_status}.")
        print("-" * 88)

    def list_resolved_cases(self):
        """
        List the resolved cases for the current day.
        """
        print("-" * 88)
        print("Let's list the resolved cases for the current day.")
        start_time = str(datetime.utcnow().date())
        end_time = str(datetime.utcnow().date() + timedelta(days=1))
        resolved_cases = self.support_wrapper.describe_cases(start_time,
end_time, True)
        for case in resolved_cases:
            print(f"\tCase: {case['caseId']}: status {case['status']}.")
        print("-" * 88)

    def run_scenario(self):
        logging.basicConfig(level=logging.INFO, format="%(levelname)s:
%(message)s")
```

```
        print("-" * 88)
        print("Welcome to the AWS Support get started with support cases demo.")
        print("-" * 88)

        selected_service = self.display_and_select_service()
        selected_category = self.display_and_select_category(selected_service)
        selected_severity = self.display_and_select_severity()
        new_case_id = self.create_example_case(
            selected_service, selected_category, selected_severity
        )
        wait(10)
        self.list_open_cases()
        new_attachment_set_id = self.create_attachment_set()
        self.add_communication(new_case_id, new_attachment_set_id)
        new_attachment_id = self.list_communications(new_case_id)
        self.describe_case_attachment(new_attachment_id)
        self.resolve_case(new_case_id)
        wait(10)
        self.list_resolved_cases()

        print("\nThanks for watching!")
        print("-" * 88)


if __name__ == "__main__":
    try:
        scenario = SupportCasesScenario(SupportWrapper.from_client())
        scenario.run_scenario()
    except Exception:
        logging.exception("Something went wrong with the demo.")
```

Tentukan kelas yang membungkus tindakan klien dukungan.

```
class SupportWrapper:
    """Encapsulates Support actions."""

    def __init__(self, support_client):
        """
        :param support_client: A Boto3 Support client.
        """
        self.support_client = support_client
```

```
    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        support_client = boto3.client("support")
        return cls(support_client)


    def describe_services(self, language):
        """
        Get the descriptions of AWS services available for support for a
language.

        :param language: The language for support services.
        Currently, only "en" (English) and "ja" (Japanese) are supported.
        :return: The list of AWS service descriptions.
        """
        try:
            response = self.support_client.describe_services(language=language)
            services = response["services"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't get Support services for language %s. Here's why:
%s: %s",
                    language,
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return services


    def describe_severity_levels(self, language):
```

```
        """
        Get the descriptions of available severity levels for support cases for a
language.

        :param language: The language for support severity levels.
        Currently, only "en" (English) and "ja" (Japanese) are supported.
        :return: The list of severity levels.
        """
        try:
            response =
self.support_client.describe_severity_levels(language=language)
            severity_levels = response["severityLevels"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't get severity levels for language %s. Here's why:
%s: %s",
                    language,
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return severity_levels


    def create_case(self, service, category, severity):
        """
        Create a new support case.

        :param service: The service to use for the new case.
        :param category: The category to use for the new case.
        :param severity: The severity to use for the new case.
        :return: The caseId of the new case.
        """
        try:
```

```
            response = self.support_client.create_case(
                subject="Example case for testing, ignore.",
                serviceCode=service["code"],
                severityCode=severity["code"],
                categoryCode=category["code"],
                communicationBody="Example support case body.",
                language="en",
                issueType="customer-service",
            )
            case_id = response["caseId"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't create case. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return case_id


    def add_attachment_to_set(self):
        """
        Add an attachment to a set, or create a new attachment set if one does
not exist.

        :return: The attachment set ID.
        """
        try:
            response = self.support_client.add_attachments_to_set(
                attachments=[
                    {
                        "fileName": "attachment_file.txt",
                        "data": b"This is a sample file for attachment to a
support case.",
```

```
                    }
                ]
            )
            new_set_id = response["attachmentSetId"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't add attachment. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return new_set_id


    def add_communication_to_case(self, attachment_set_id, case_id):
        """
        Add a communication and an attachment set to a case.

        :param attachment_set_id: The ID of an existing attachment set.
        :param case_id: The ID of the case.
        """
        try:
            self.support_client.add_communication_to_case(
                caseId=case_id,
                communicationBody="This is an example communication added to a
support case.",
                attachmentSetId=attachment_set_id,
            )
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
```

```
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't add communication. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise


    def describe_all_case_communications(self, case_id):
        """
        Describe all the communications for a case using a paginator.

        :param case_id: The ID of the case.
        :return: The communications for the case.
        """
        try:
            communications = []
            paginator =
self.support_client.get_paginator("describe_communications")
            for page in paginator.paginate(caseId=case_id):
                communications += page["communications"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't describe communications. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return communications
```

```
    def describe_attachment(self, attachment_id):
        """
        Get information about an attachment by its attachmentID.

        :param attachment_id: The ID of the attachment.
        :return: The name of the attached file.
        """
        try:
            response = self.support_client.describe_attachment(
                attachmentId=attachment_id
            )
            attached_file = response["attachment"]["fileName"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't get attachment description. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return attached_file


    def resolve_case(self, case_id):
        """
        Resolve a support case by its caseId.

        :param case_id: The ID of the case to resolve.
        :return: The final status of the case.
        """
        try:
            response = self.support_client.resolve_case(caseId=case_id)
            final_status = response["finalCaseStatus"]
```

```
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't resolve case. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return final_status


    def describe_cases(self, after_time, before_time, resolved):
        """
        Describe support cases over a period of time, optionally filtering
        by status.

        :param after_time: The start time to include for cases.
        :param before_time: The end time to include for cases.
        :param resolved: True to include resolved cases in the results,
            otherwise results are open cases.
        :return: The final status of the case.
        """
        try:
            cases = []
            paginator = self.support_client.get_paginator("describe_cases")
            for page in paginator.paginate(
                afterTime=after_time,
                beforeTime=before_time,
                includeResolvedCases=resolved,
                language="en",
            ):
                cases += page["cases"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
```

```
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't describe cases. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            if resolved:
                cases = filter(lambda case: case["status"] == "resolved", cases)
            return cases
```

- Untuk detail API, lihat topik berikut ini adalah Referensi API SDK untuk Python (Boto3)AWS .
  - AddAttachmentsToSet
  - AddCommunicationToCase
  - CreateCase
  - DescribeAttachment
  - DescribeCases
  - DescribeCommunications
  - DescribeServices
  - DescribeSeverityLevel
  - ResolveCase

Untuk daftar lengkap panduan pengembang AWS SDK dan contoh kode, lihatMenggunakan AWS Support dengan AWS SDK. Topik ini juga mencakup informasi tentang memulai dan detail tentang versi SDK sebelumnya.

Pemantauan dan loggingAWS Support

Pemantauan adalah bagian penting dari pemeliharaan keandalan, ketersediaan, dan kinerja AWS Support dan solusi AWS lain Anda. AWS menyediakan alat pemantauan berikut untuk memantau AWS Support, melaporkan jika ada yang salah, dan mengambil tindakan otomatis jika diperlukan:

- Amazon EventBridge memberikan aliran sistem secara hampir waktu-nyata yang menjelaskan perubahan dalamAWS sumber daya. EventBridge memungkinkan komputasi berbasis peristiwa otomatis, karena Anda dapat menulis peraturan yang mengawasi peristiwa tertentu dan memicu tindakan otomatis dalamAWS layanan lainnya saat peristiwa ini terjadi. Untuk informasi selengkapnya, lihat Panduan EventBridge Pengguna Amazon Amazon.
- AWS CloudTrail merekam panggilan API dan peristiwa terkait yang dilakukan oleh atau atas nama akun AWS Anda dan mengirimkan berkas 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 informasi selengkapnya, lihat Panduan Pengguna AWS CloudTrail.

Topik

Memantau AWS Support kasus dengan Amazon EventBridge

Anda dapat menggunakan Amazon EventBridge untuk mendeteksi dan bereaksi terhadap perubahan untuk AWS Support kasus Anda. Kemudian, berdasarkan aturan yang Anda buat, EventBridge memanggil satu atau beberapa tindakan target saat peristiwa cocok dengan nilai yang Anda tentukan dalam aturan.

Bergantung pada acara, Anda dapat mengirim pemberitahuan, menangkap informasi acara, mengambil tindakan korektif, memulai acara, atau mengambil tindakan lain. Misalnya, Anda bisa mendapatkan pemberitahuan setiap kali tindakan berikut terjadi di akun Anda:

- Membuat kasus dukungan
- Tambahkan korespondensi kasus ke kasus dukungan yang ada

- Menyelesaikan kasus dukungan
- Buka kembali kasus dukungan

> **Note**
>
> AWS Supportmemberikan acara atas dasar upaya terbaik. Acara tidak selalu dijamin akan dikirimkan ke EventBridge.

Membuat EventBridge aturan untuk AWS Support kasus

Anda dapat membuat EventBridge aturan untuk mendapatkan pemberitahuan untuk peristiwa AWS Support kasus. Aturan akan memantau pembaruan untuk kasus dukungan di akun Anda, termasuk tindakan yang dilakukan oleh Anda, pengguna IAM, atau agen dukungan. Sebelum Anda membuat aturan untuk peristiwa AWS Support kasus, lakukan hal berikut:

- Biasakan diri Anda dengan acara, aturan, dan target di EventBridge. Untuk informasi selengkapnya, lihat Apa itu Amazon EventBridge? di Panduan EventBridge Pengguna Amazon.
- Buat target untuk digunakan dalam aturan acara Anda. Misalnya, Anda dapat membuat topik Amazon Simple Notification Service (Amazon SNS) sehingga setiap kali kasus dukungan diperbarui, Anda akan menerima pesan teks atau email. Untuk informasi lebih lanjut, lihat EventBridgetarget.

> **Note**
>
> AWS Support adalah layanan global. Untuk menerima pembaruan untuk kasus dukungan Anda, Anda dapat menggunakan salah satu wilayah berikut: Wilayah AS Timur (Virginia N.), Wilayah AS Barat (Oregon) atau Wilayah Eropa (Irlandia).

Untuk membuat EventBridge aturan untuk peristiwa AWS Support kasus

1. Buka EventBridge konsol Amazon di https://console.aws.amazon.com/events/.
2. Jika Anda belum melakukannya, gunakan pemilih Wilayah di sudut kanan atas halaman dan pilih US East (Virginia N.).
3. Di panel navigasi, pilih Aturan.

4. Pilih Buat aturan.
5. Pada halaman Tentukan detail aturan, masukkan nama dan deskripsi untuk aturan Anda.
6. Simpan nilai default untuk bus Acara dan tipe Aturan, lalu pilih Berikutnya.
7. Pada halaman pola acara Build, untuk sumber acara, pilih AWSacara atau acara EventBridge mitra.
8. Di bawah pola Peristiwa, pertahankan nilai default untuk Layanan AWS.
9. Untuk Layanan AWS, pilih Support.
10. Untuk jenis Event, pilih Support Case Update.
11. Pilih Selanjutnya.
12. Di bagian Pilih target, pilih target yang Anda buat untuk aturan ini, lalu konfigurasikan opsi tambahan apa pun yang diperlukan untuk jenis tersebut. Misalnya, jika Anda memilih Amazon SNS, pastikan topik SNS Anda dikonfigurasi dengan benar sehingga Anda akan diberi tahu melalui email atau SMS.
13. Pilih Selanjutnya.
14. (Opsional) Pada halaman Konfigurasi tag, tambahkan tag apa pun lalu pilih Berikutnya.
15. Pada halaman Tinjau dan buat, tinjau pengaturan aturan Anda dan pastikan aturan tersebut memenuhi persyaratan pemantauan acara Anda.
16. Pilih Buat aturan. Aturan Anda sekarang akan memantau kejadian AWS Support kasus dan kemudian mengirimkannya ke target yang Anda tentukan.

Catatan

- Ketika Anda menerima acara, Anda dapat menggunakan `origin` parameter untuk menentukan apakah Anda atau AWS Support agen menambahkan korespondensi kasus ke kasus dukungan. Nilai untuk `origin` bisa salah satu `CUSTOMER` atau`AWS`.

  Saat ini, hanya peristiwa untuk `AddCommunicationToCase` tindakan yang memiliki nilai ini.
- Untuk informasi selengkapnya tentang membuat pola peristiwa, lihat Pola acara di Panduan EventBridge Pengguna Amazon.
- Anda juga dapat membuat aturan lain untuk AWSAPI Call melalui jenis CloudTrail acara. Aturan ini akan memantau AWS CloudTrail log untuk panggilan AWS Support API di akun Anda.

Contoh AWS Support peristiwa

Peristiwa berikut dibuat saat tindakan dukungan terjadi di akun Anda.

Example : Buat kasus dukungan

Peristiwa berikut dibuat ketika kasus dukungan dibuat.


```
{
    "version": "0",
    "id": "3433df007-9285-55a3-f6d1-536944be45d7",
    "detail-type": "Support Case Update",
    "source": "aws.support",
    "account": "111122223333",
    "time": "2022-02-21T15:51:19Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "case-id": "case-111122223333-muen-2022-7118885805350839",
        "display-id": "1234563851",
        "communication-id": "",
        "event-name": "CreateCase",
        "origin": ""
    }
}
```


Example : Perbarui kasus dukungan

Peristiwa berikut dibuat saat AWS Support membalas kasus dukungan.


```
{
    "version": "0",
    "id": "f90cb8cb-32be-1c91-c0ba-d50b4ca5e51b",
    "detail-type": "Support Case Update",
    "source": "aws.support",
    "account": "111122223333",
    "time": "2022-02-21T15:51:31Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "case-id": "case-111122223333-muen-2022-7118885805350839",
        "display-id": "1234563851",
```

```
        "communication-id": "ekko:us-east-1:12345678-268a-424b-be08-54613cab84d2",
        "event-name": "AddCommunicationToCase",
        "origin": "AWS"
    }
}
```

Example : Selesaikan kasus dukungan

Peristiwa berikut dibuat ketika kasus dukungan diselesaikan.

```
{
    "version": "0",
    "id": "1aa4458d-556f-732e-ddc1-4a5b2fbd14a5",
    "detail-type": "Support Case Update",
    "source": "aws.support",
    "account": "111122223333",
    "time": "2022-02-21T15:51:31Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "case-id": "case-111122223333-muen-2022-7118885805350839",
        "display-id": "1234563851",
        "communication-id": "",
        "event-name": "ResolveCase",
        "origin": ""
    }
}
```

Example : Buka kembali kasus dukungan

Peristiwa berikut dibuat ketika kasus dukungan dibuka kembali.

```
{
    "version": "0",
    "id": "3bb9d8fe-6089-ad27-9508-804209b233ad",
    "detail-type": "Support Case Update",
    "source": "aws.support",
    "account": "111122223333",
    "time": "2022-02-21T15:47:19Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "case-id": "case-111122223333-muen-2021-27f40618fe0303ea",
```

```
        "display-id": "1234563851",
        "communication-id": "",
        "event-name": "ReopenCase",
        "origin": ""
    }
}
```

Lihat juga

Untuk informasi selengkapnya tentang cara menggunakannya EventBridge AWS Support, lihat sumber daya berikut:

- Cara mengotomatiskan AWS Support API dengan Amazon EventBridge
- AWS Supportnotifier aktivitas kasus aktif GitHub

Mencatat panggilan API AWS Support dengan AWS CloudTrail

AWS Supportterintegrasi denganAWS CloudTrail, layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atauAWS layanan diAWS Support. CloudTrail merekam panggilan untukAWS Support sebagai peristiwa. Panggilan yang direkam mencakup panggilan dari AWS Support konsol dan panggilan kode ke operasi API AWS Support ini.

Jika membuat jejak, Anda dapat mengaktifkan pengiriman berkelanjutan CloudTrail kejadian ke bucket Amazon Simple Storage Service (Amazon Simple Simple Storage Service (Amazon S3), termasuk peristiwa untukAWS Support. Jika Anda tidak mengonfigurasi jejak, Anda masih dapat melihat tindakan terbaru di CloudTrail konsol di Riwayat tindakan.

Menggunakan informasi yang dikumpulkan oleh CloudTrail, Anda dapat menentukan permintaan yang dibuatAWS Support, alamat IP asal permintaan tersebut dibuat, siapa yang membuat permintaan, kapan permintaan dibuat, dan detail lainnya.

Untuk mempelajari lebih lanjut CloudTrail, termasuk cara mengonfigurasi dan mengaktifkannya, lihat PanduanAWS CloudTrail Pengguna.

AWS Supportinformasi dalam CloudTrail

CloudTrail diaktifkan padaAWS akun Anda saat Anda membuat akun. Saat aktivitas peristiwa yang didukung terjadi diAWS Support, aktivitas tersebut dicatat di CloudTrail peristiwa lainnyaAWS di

Riwayat tindakan. Anda dapat melihat, mencari, dan mengunduh peristiwa terbaru di akun AWS Anda. Untuk informasi lebih lanjut, lihat peristiwa dengan riwayat CloudTrail peristiwa.

Untuk catatan berkelanjutan tentang peristiwa di akun AWS Anda, termasuk peristiwa untuk AWS Support, buat jejak. Jejak memungkinkan CloudTrail untuk mengirim file log ke bucket Amazon S3. Secara default, saat Anda membuat jejak di dalam konsol tersebut, jejak diterapkan ke semua Wilayah AWS. Jejak mencatat peristiwa dari semua Wilayah di partisi AWS dan mengirimkan file log ke bucket Amazon S3 yang Anda tentukan. Selain itu, Anda dapat mengonfigurasiAWS layanan lainnya untuk menganalisis lebih lanjut dan bertindak berdasarkan data peristiwa yang dikumpulkan di CloudTrail log. Untuk informasi selengkapnya, lihat yang berikut:

- Gambaran umum untuk membuat jejak
- CloudTrail Layanan yang didukung dan integrasi
- Mengonfigurasi notifikasi Amazon SNS untuk CloudTrail
- Menerima berkas log CloudTrail dari beberapa wilayah dan Menerima berkas log CloudTrail dari beberapa akun

SemuaAWS Support operasi dicatat oleh CloudTrail dan didokumentasikan dalam ReferensiAWS Support API.

Misalnya, panggilan ke`CreateCase`,`DescribeCases` dan`ResolveCase` operasi menghasilkan entri dalam file CloudTrail log.

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 .

Anda juga dapat mengagregatkan file log AWS Support dari beberapa Wilayah AWS dan beberapa akun AWS ke dalam satu bucket Amazon S3.

AWS Trusted Advisorinformasi dalam CloudTrail logging

Trusted Advisor adalah layanan AWS Support yang dapat Anda gunakan untuk memeriksa akun AWS untuk cara menghemat biaya, meningkatkan keamanan, dan mengoptimalkan akun Anda.

SemuaTrusted Advisor operasi dicatat oleh CloudTrail dan didokumentasikan dalam ReferensiAWS Support API.

Misalnya, panggilan ke`DescribeTrustedAdvisorCheckRefreshStatuses`,`DescribeTrustedAdvisorCheckResult` dan`RefreshTrustedAdvisorCheck` operasi menghasilkan entri dalam file CloudTrail log.

> **Note**
>
> CloudTrail juga mencatat tindakanTrusted Advisor konsol. Lihat Mencatat tindakan AWS Trusted Advisor konsol dengan AWS CloudTrail.

Memahami entri file log AWS Support

Jejak adalah konfigurasi yang memungkinkan pengiriman peristiwa sebagai berkas log ke bucket Amazon S3 yang Anda tentukan. CloudTrail File log berisi satu atau beberapa entri log. Peristiwa menunjukkan satu permintaan dari sumber mana pun. Setiap peristiwa mencakup informasi tentang operasi yang diminta, tanggal dan waktu operasi, parameter permintaan, dan sebagainya. CloudTrail Berkas log bukan jejak tumpukan terurut dari panggilan API, sehingga berkas tersebut tidak muncul dalam urutan tertentu.

Example : Entri log untuk CreateCase

Contoh berikut menunjukkan entri CloudTrail log untuk CreateCaseoperasi.

```
{
   "Records": [
      {
         "eventVersion": "1.04",
         "userIdentity": {
            "type": "IAMUser",
            "principalId": "AIDACKCEVSQ6C2EXAMPLE",
            "arn": "arn:aws:iam::111122223333:user/janedoe",
```

```
            "accountId": "111122223333",
            "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
            "userName": "janedoe",
            "sessionContext": {
               "attributes": {
                  "mfaAuthenticated": "false",
                  "creationDate": "2016-04-13T17:51:37Z"
               }
            },
            "invokedBy": "signin.amazonaws.com"
         },
         "eventTime": "2016-04-13T18:05:53Z",
         "eventSource": "support.amazonaws.com",
         "eventName": "CreateCase",
         "awsRegion": "us-east-1",
         "sourceIPAddress": "198.51.100.15",
         "userAgent": "signin.amazonaws.com",
         "requestParameters": {
            "severityCode": "low",
            "categoryCode": "other",
            "language": "en",
            "serviceCode": "support-api",
            "issueType": "technical"
         },
         "responseElements": {
            "caseId": "case-111122223333-muen-2016-c3f2077e504940f2"
         },
         "requestID": "58c257ef-01a2-11e6-be2a-01c031063738",
         "eventID": "5aa34bfc-ad5b-4fb1-8a55-2277c86e746a",
         "eventType": "AwsApiCall",
         "recipientAccountId": "111122223333"
      }
   ],
   ...
}
```

Example : Entri log untuk RefreshTrustedAdvisorCheck

Contoh berikut menunjukkan entri CloudTrail log untuk RefreshTrustedAdvisorCheckoperasi.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
```

```
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::111122223333:user/Admin",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Admin"
    },
    "eventTime": "2020-10-21T16:34:13Z",
    "eventSource": "support.amazonaws.com",
    "eventName": "RefreshTrustedAdvisorCheck",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "72.21.198.67",
    "userAgent": "signin.amazonaws.com",
    "requestParameters": {
        "checkId": "Pfx0RwqBli"
    },
    "responseElements": null,
    "requestID": "4c4d5fc8-c403-4f82-9544-41f820e0fa01",
    "eventID": "2f4630ac-5c27-4f0d-b93f-63742d6fc85e",
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```


LoggingAWS Support App di Slack API panggilan menggunakanAWS CloudTrail

AWS SupportAplikasi di Slack terintegrasi denganAWS CloudTrail. CloudTrail menyediakan catatan tindakan yang diambil oleh pengguna, peran, atauLayanan AWS diAWS Support Aplikasi. Untuk membuat catatan ini, CloudTrail menangkap semua panggilan API publik untukAWS Support App sebagai peristiwa. Panggilan yang direkam mencakup panggilan dari konsolAWS Support Aplikasi, dan panggilan kode ke operasi API publikAWS Support Aplikasi. Jika Anda membuat jejak, Anda dapat mengaktifkan pengiriman berkelanjutan dari CloudTrail kejadian ke bucket Amazon S3. Ini termasuk acara untukAWS Support App. Jika Anda tidak mengonfigurasi jejak, Anda masih bisa melihat kejadian terbaru di CloudTrail konsol di Riwayat peristiwa. Anda dapat menggunakan informasi yang CloudTrail dikumpulkan untuk menentukan bahwa permintaan yang dibuat keAWS Support Aplikasi. Anda juga dapat mempelajari alamat IP untuk membuat permintaan, siapa yang membuat permintaan, kapan itu dibuat, dan detail tambahan.

Untuk mempelajari lebih lanjut CloudTrail, lihat PanduanAWS CloudTrail Pengguna.

AWS SupportInformasi aplikasi di CloudTrail

Saat Anda membuatAkun AWS, ini akan aktif CloudTrail di akun. Saat aktivitas API publik terjadi diAWS Support Aplikasi, aktivitas tersebut dicatat, bersama CloudTrail peristiwaAWS layanan lainnya di Riwayat peristiwa. Anda dapat melihat, mencari, dan mengunduh peristiwa terbaru di Akun AWS Anda. Untuk informasi selengkapnya, lihat Melihat peristiwa dengan Riwayat CloudTrail peristiwa.

Untuk catatan berkelanjutan tentang peristiwa di AndaAkun AWS, termasuk peristiwa untukAWS Support Aplikasi, buat jejak. 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 lainnyaLayanan AWS untuk menganalisis lebih lanjut data peristiwa yang dikumpulkan di CloudTrail log dan bertindak berdasarkan data. Untuk informasi selengkapnya, lihat yang berikut:

- Gambaran umum untuk membuat jejak
- CloudTrail Layanan yang didukung dan integrasi
- Mengonfigurasi notifikasi Amazon SNS untuk CloudTrail
- Menerima berkas CloudTrail log dari beberapa akun dan Menerima berkas CloudTrail log dari beberapa akun

CloudTrail log semua tindakanAWS Support App publik. Tindakan ini juga didokumentasikan dalam AWS SupportApp in Slack API Reference. Misalnya, panggilan ke`CreateSlackChannelConfiguration`,`GetAccountAlias` dan`UpdateSlackChannelConfiguration` tindakan menghasilkan entri dalam file CloudTrail log.

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.
- Apakah permintaan dibuat oleh orang lainLayanan AWS.

Untuk informasi selengkapnya, lihat Elemen userIdentity CloudTrail .

AWS SupportMemahami entri berkas log

Jejak adalah konfigurasi yang memungkinkan pengiriman peristiwa sebagai berkas log ke bucket Amazon S3 yang Anda tentukan. CloudTrail berkas log berisi satu atau beberapa entri log. Sebuah peristiwa mewakili permintaan tunggal dari sumber apa pun dan mencakup informasi tentang tindakan yang diminta, tanggal dan waktu tindakan, parameter permintaan, dan sebagainya. CloudTrail Berlog bukan merupakan pelacakan tumpukan berurutan dari panggilan API publik. Ini berarti bahwa log tidak ditampilkan dalam urutan tertentu.

Example : Log contoh untuk**`CreateSlackChannelConfiguration`**

Contoh berikut menunjukkan entri CloudTrail log untuk CreateSlackChannelConfigurationoperasi.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE:JaneDoe",
        "arn": "arn:aws:sts::111122223333:assumed-role/Administrator/JaneDoe",
        "accountId": "111122223333",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Administrator",
                "accountId": "111122223333",
                "userName": "Administrator"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-02-26T01:37:57Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-02-26T01:48:20Z",
    "eventSource": "supportapp.amazonaws.com",
    "eventName": "CreateSlackChannelConfiguration",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "205.251.233.183",
    "userAgent": "aws-cli/1.3.23 Python/2.7.6 Linux/2.6.18-164.el5",
    "requestParameters": {
```

```
        "notifyOnCreateOrReopenCase": true,
        "teamId": "T012ABCDEFG",
        "notifyOnAddCorrespondenceToCase": true,
        "notifyOnCaseSeverity": "all",
        "channelName": "troubleshooting-channel",
        "notifyOnResolveCase": true,
        "channelId": "C01234A5BCD",
        "channelRoleArn": "arn:aws:iam::111122223333:role/AWSSupportAppRole"
    },
    "responseElements": null,
    "requestID": "d06df6ca-c233-4ffb-bbff-63470c5dc255",
    "eventID": "0898ce29-a396-444a-899d-b068f390c361",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Example : Log contoh untuk**`ListSlackChannelConfigurations`**

Contoh berikut menunjukkan entri CloudTrail log untuk ListSlackChannelConfigurationsoperasi.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE:AWSSupportAppRole",
        "arn": "arn:aws:sts::111122223333:assumed-role/AWSSupportAppRole",
        "accountId": "111122223333",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/AWSSupportAppRole",
                "accountId": "111122223333",
                "userName": "AWSSupportAppRole"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-03-01T20:06:32Z",
                "mfaAuthenticated": "false"
            }
```

```
        }
    },
    "eventTime": "2022-03-01T20:06:46Z",
    "eventSource": "supportapp.amazonaws.com",
    "eventName": "ListSlackChannelConfigurations",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "72.21.217.131",
    "userAgent": "aws-cli/1.3.23 Python/2.7.6 Linux/2.6.18-164.el5",
    "requestParameters": null,
    "responseElements": null,
    "requestID": "20f81d63-31c5-4351-bd02-9eda7f76e7b8",
    "eventID": "70acb7fe-3f84-47cd-8c28-cc148ad06d21",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Example : Log contoh untuk**`GetAccountAlias`**

Contoh berikut menunjukkan entri CloudTrail log untuk GetAccountAliasoperasi.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE:devdsk",
        "arn": "arn:aws:sts::111122223333:assumed-role/AWSSupportAppRole/devdsk",
        "accountId": "111122223333",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/AWSSupportAppRole",
                "accountId": "111122223333",
                "userName": "AWSSupportAppRole"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-03-01T20:31:27Z",
                "mfaAuthenticated": "false"
            }
```

```
        }
    },
    "eventTime": "2022-03-01T20:31:47Z",
    "eventSource": "supportapp.amazonaws.com",
    "eventName": "GetAccountAlias",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "72.21.217.142",
    "userAgent": "aws-cli/1.3.23 Python/2.7.6 Linux/2.6.18-164.el5",
    "requestParameters": null,
    "responseElements": null,
    "requestID": "a225966c-0906-408b-b8dd-f246665e6758",
    "eventID": "79ebba8d-3285-4023-831a-64af7de8d4ad",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Pemantauan dan pencatatan untukAWS Support Rencana

Pemantauan adalah bagian penting dari pemeliharaan keandalan, ketersediaan, dan kinerja Rencana Support danAWS solusi Anda lainnya. AWSmenyediakan alat pemantauan berikut untuk mengawasi Rencana Support, melaporkan saat terjadi kesalahan, dan mengambil tindakan otomatis jika diperlukan:

- AWS CloudTrail merekam panggilan API dan peristiwa terkait yang dilakukan oleh atau atas nama akun AWS Anda dan mengirimkan berkas 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 informasi selengkapnya, lihat Panduan Pengguna AWS CloudTrail.

Topik

LoggingAWS Support Rencana panggilan API denganAWS CloudTrail

AWS SupportPaket terintegrasi denganAWS CloudTrail, layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atauLayanan AWS. CloudTrailmerekam panggilan API untukAWS Support Paket sebagai peristiwa. Panggilan yang direkam mencakup panggilan dari konsolAWS Support Paket dan panggilan kode ke operasiAWS Support Rencana API.

Jika membuat jejak, Anda dapat mengaktifkan pengiriman berkelanjutanCloudTrail peristiwa ke bucket Amazon Simple Storage Service (Amazon S3), termasuk peristiwa untukAWS Support Paket. Jika Anda tidak membuat konfigurasi jejak, Anda masih dapat melihat kejadian terbaru dalam konsol CloudTrail di Riwayat peristiwa.

Menggunakan informasi yang dikumpulkan olehCloudTrail, Anda dapat menentukan permintaan yang dibuat keAWS Support Rencana, alamat IP asal permintaan tersebut dibuat, siapa yang membuat permintaan, kapan permintaan dibuat, dan detail lainnya.

Untuk mempelajari selengkapnyaCloudTrail, termasuk cara mengonfigurasi dan mengaktifkannya, lihat PanduanAWS CloudTrail Pengguna.

AWS SupportRencana informasi diCloudTrail

CloudTraildiaktifkan pada AndaAkun AWS saat Anda membuat akun. Saat aktivitas peristiwa yang didukung terjadi diAWS Support Paket, aktivitas tersebut dicatat diCloudTrail peristiwa bersamaLayanan AWS peristiwa lainnya di Riwayat peristiwa. Anda dapat melihat, mencari, dan mengunduh peristiwa terbaru di akun Anda. Untuk informasi lebih lanjut, lihat Menampilkan peristiwa dengan riwayat peristiwa CloudTrail.

Untuk catatan peristiwa yang sedang berlangsung di akun Anda, termasuk peristiwa untukAWS Support Paket, buat jejak. Jejak memungkinkan CloudTrail untuk mengirim 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 lainnyaLayanan AWS untuk dianalisis lebih lanjut dan bertindak berdasarkan data peristiwa yang dikumpulkan diCloudTrail log. Untuk informasi selengkapnya, lihat yang berikut:

- Gambaran umum untuk membuat jejak
- CloudTrailLayanan yang didukung dan integrasi
- Mengonfigurasi notifikasi Amazon SNS untukCloudTrail
- Menerima berkas log CloudTrail dari beberapa wilayah dan Menerima berkas log CloudTrail dari beberapa akun

Semua operasiAWS Support Rencana API dicatat olehCloudTrail. 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.
- Apakah permintaan dibuat oleh orang lainLayanan AWS.

Untuk informasi selengkapnya, lihat Elemen userIdentity CloudTrail.

Anda juga dapat mengagregasi berkas logAWS Support Paket dari beberapaWilayah AWS dan beberapa akun ke dalam satu bucket Amazon S3.

AWS SupportMemahami entri berkas log

Jejak adalah konfigurasi yang memungkinkan pengiriman peristiwa sebagai berkas log ke bucket Amazon S3 yang telah Anda tentukan. File log CloudTrail berisi satu atau lebih entri log. Peristiwa menunjukkan satu permintaan dari sumber mana pun. Setiap peristiwa mencakup informasi tentang operasi yang diminta, tanggal dan waktu operasi, parameter permintaan, dan sebagainya. Berkas log CloudTrail bukan jejak tumpukan terurut dari panggilan API publik, sehingga berkas tersebut tidak muncul dalam urutan tertentu.

Example : Entri log untuk**`GetSupportPlan`**

Contoh berikut menunjukkan entriCloudTrail log untuk`GetSupportPlan` operasi.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:sts::111122223333:user/janedoe",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-06-29T16:30:04Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-06-29T16:39:11Z",
    "eventSource": "supportplans.amazonaws.com",
    "eventName": "GetSupportPlan",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "205.251.233.183",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101
 Firefox/91.0",
```

```
    "requestParameters": null,
    "responseElements": null,
    "requestID": "7665c39a-d6bf-4d0d-8010-2f59740b8ecb",
    "eventID": "b711bc30-16a5-4579-8f0d-9ada8fe6d1ce",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Example : Entri log untuk**`GetSupportPlanUpdateStatus`**

Contoh berikut menunjukkan entriCloudTrail log untuk`GetSupportPlanUpdateStatus` operasi.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:sts::111122223333:user/janedoe",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-06-29T16:30:04Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-06-29T16:39:02Z",
    "eventSource": "supportplans.amazonaws.com",
    "eventName": "GetSupportPlanUpdateStatus",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "205.251.233.183",
```

```
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101
 Firefox/91.0",
    "requestParameters": {
        "supportPlanUpdateArn":
 "arn:aws:supportplans::111122223333:supportplanupdate/7f03b7a233a0e87ebc79e56d4d2bcaf19e976c37
    },
    "responseElements": null,
    "requestID": "75e5c767-8703-4ed3-b01e-4dda28020322",
    "eventID": "28d1c0e3-ccb6-4fd1-8793-65be010114cc",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Example : Entri log untuk**`StartSupportPlanUpdate`**

Contoh berikut menunjukkan entriCloudTrail log untuk`StartSupportPlanUpdate` operasi.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:sts::111122223333:user/janedoe",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-06-29T16:30:04Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-06-29T16:38:55Z",
```

```
    "eventSource": "supportplans.amazonaws.com",
    "eventName": "StartSupportPlanUpdate",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "205.251.233.183",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101
 Firefox/91.0",
    "requestParameters": {
        "clientToken": "98add111-dcc9-464d-8722-438d697fe242",
        "update": {
            "supportLevel": "BASIC"
        }
    },
    "responseElements": {
        "Access-Control-Expose-Headers": "x-amzn-RequestId,x-amzn-ErrorType,x-amzn-
ErrorMessage,Date",
        "supportPlanUpdateArn":
 "arn:aws:supportplans::111122223333:supportplanupdate/7f03b7a233a0e87ebc79e56d4d2bcaf19e976c37
    },
    "requestID": "e5ff9382-5fb8-4764-9993-0f33fb0b1e17",
    "eventID": "5dba89f8-2e5b-42b9-9b8f-395580c52962",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Example : Entri log untuk**`CreateSupportPlanSchedule`**

Contoh berikut menunjukkan entriCloudTrail log untuk`CreateSupportPlanSchedule` operasi.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:sts::111122223333:user/janedoe",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Admin",
```

```
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-05-09T16:30:04Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-05-09T16:30:04Z",
    "eventSource": "supportplans.amazonaws.com",
    "eventName": "CreateSupportPlanSchedule",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "205.251.233.183",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101
 Firefox/91.0",
    "requestParameters": {
        "clientToken": "b998de5e-ad1c-4448-90db-2bf86d6d9e9a",
        "scheduleCreationDetails": {
            "startLevel": "BUSINESS",
            "startOffer": "TrialPlan7FB93B",
            "startTimestamp": "2023-06-03T17:23:56.109Z",
            "endLevel": "BUSINESS",
            "endOffer": "StandardPlan2074BB",
            "endTimestamp": "2023-09-03T17:23:55.109Z"
        }
    },
    "responseElements": {
        "Access-Control-Expose-Headers": "x-amzn-RequestId,x-amzn-ErrorType,x-amzn-
ErrorMessage,Date",
        "supportPlanUpdateArn":
 "arn:aws:supportplans::111122223333:supportplanschedule/
b9a9a4336a3974950a6e670f7dab79b77a4b104db548a0d57050ce4544721d4b"
    },
    "requestID": "150450b8-e61a-4b15-93a8-c3b557a1ca48",
    "eventID": "a2a1ba44-610d-4dc8-bf16-29f1635b57a9",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Mencatat perubahan ke paket AWS Support Anda

> **Important**
>
> Mulai 3 Agustus 2022, operasi berikut tidak berlaku lagi dan tidak akan muncul diCloudTrail log baru Anda. Untuk daftar operasi yang didukung, lihatAWS SupportMemahami entri berkas log.

- `DescribeSupportLevelSummary` – Tindakan ini muncul di log Anda ketika Anda membuka halaman Paket dukungan.
- `UpdateProbationAutoCancellation` – Setelah Anda mendaftar untuk Dukungan Developer atau Dukungan Bisnis dan kemudian mencoba membatalkan dalam waktu 30 hari, paket Anda akan dibatalkan secara otomatis pada akhir periode tersebut. Tindakan ini muncul di log Anda saat Anda memilih Opt out of automatic cancellation (Memilih untuk tidak menerima pembatalan otomatis) pada banner yang muncul di halaman Paket dukungan. Anda akan melanjutkan paket untuk Dukungan Developer atau Bisnis.
- `UpdateSupportLevel`— Tindakan ini muncul di log Anda saat Anda mengubah paket dukungan Anda.

> **Note**
>
> Bidang `eventSource` memiliki namespace `support-subscription.amazonaws.com` untuk tindakan ini.

Example : Entri log untukDescribeSupportLevelSummary

Contoh berikut menunjukkan entriCloudTrail log untuk`DescribeSupportLevelSummary` tindakan.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "Root",
    "principalId": "111122223333",
    "arn": "arn:aws:iam::111122223333:root",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
```

```
    "sessionContext": {
      "sessionIssuer": {},
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-01-07T22:08:05Z"
      }
    }
  },
  "eventTime": "2021-01-07T22:08:07Z",
  "eventSource": "support-subscription.amazonaws.com",
  "eventName": "DescribeSupportLevelSummary",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "100.127.8.67",
  "userAgent": "AWS-SupportPlansConsole, aws-internal/3",
  "requestParameters": {
    "lang": "en"
  },
  "responseElements": null,
  "requestID": "b423b84d-829b-4090-a239-2b639b123abc",
  "eventID": "e1eeda0e-d77c-487b-a7e5-4014f7123abc",
  "readOnly": true,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "111122223333"
}
```

Example : Entri log untukUpdateProbationAutoCancellation

Contoh berikut menunjukkan entriCloudTrail log untuk`UpdateProbationAutoCancellation` tindakan.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "Root",
    "principalId": "111122223333",
    "arn": "arn:aws:iam::111122223333:root",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE"
  },
  "eventTime": "2021-01-07T23:28:43Z",
```

```
  "eventSource": "support-subscription.amazonaws.com",
  "eventName": "UpdateProbationAutoCancellation",
  "awsRegion": "us-east-1", "sourceIPAddress": "100.127.8.67",
  "userAgent": "AWS-SupportPlansConsole, aws-internal/3",
  "requestParameters": {
    "lang": "en"
  },
  "responseElements": null,
  "requestID": "5492206a-e200-4c33-9fcf-4162d4123abc",
  "eventID": "f4a58c09-0bb0-4ba2-a8d3-df6909123abc",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "111122223333"
}
```

Example : Entri log untukUpdateSupportLevel

Contoh berikut menunjukkan entriCloudTrail log untuk`UpdateSupportLevel` tindakan untuk mengubah ke Support Developer.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "Root",
    "principalId": "111122223333",
    "arn": "arn:aws:iam::111122223333:root",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {},
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-01-07T22:08:05Z"
      }
    }
  },
  "eventTime": "2021-01-07T22:08:43Z",
  "eventSource": "support-subscription.amazonaws.com",
  "eventName": "UpdateSupportLevel",
  "awsRegion": "us-east-1",
```

```
  "sourceIPAddress": "100.127.8.247",
  "userAgent": "AWS-SupportPlansConsole, aws-internal/3",
  "requestParameters": {
    "supportLevel": "new_developer"
  },
  "responseElements": {
    "aispl": false,
    "supportLevel": "new_developer"
  },
  "requestID": "5df3da3a-61cd-4a3c-8f41-e5276b123abc",
  "eventID": "c69fb149-c206-47ce-8766-8df6ec123abc",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "111122223333"
}
```

Pemantauan dan loggingAWS Trusted Advisor

Pemantauan adalah bagian penting dari pemeliharaan keandalan, ketersediaan, dan kinerja Trusted Advisor dan solusi AWS lain Anda. AWS menyediakan alat pemantauan berikut untuk memantau Trusted Advisor, melaporkan jika ada yang salah, dan mengambil tindakan otomatis jika diperlukan:

- Amazon EventBridge memberikan pengaliran sistem secara hampir waktu-nyata yang menjelaskan perubahan dalamAWS sumber daya. EventBridge memungkinkan komputasi berbasis peristiwa otomatis, karena Anda dapat menulis peraturan yang mengawasi peristiwa tertentu dan memicu tindakan otomatis dalamAWS layanan lainnya saat peristiwa ini terjadi.

  Misalnya, Trusted Advisor menyediakan pemeriksaan Amazon S3 Bucket Permissions (Izin Bucket Amazon S3). Pemeriksaan ini mengidentifikasi jika Anda memiliki bucket yang memiliki izin akses terbuka atau mengizinkan akses ke setiap pengguna AWS terautentikasi. Jika izin bucket berubah, status berubah untukTrusted Advisor pemeriksaan. EventBridge mendeteksi kejadian ini, lalu mengirimkan notifikasi sehingga Anda dapat mengambil tindakan. Untuk informasi selengkapnya, lihat Panduan EventBridge Pengguna Amazon.
- Pemeriksaan AWS Trusted Advisor mengidentifikasi cara bagi Anda untuk mengurangi biaya, meningkatkan kinerja, dan meningkatkan keamanan untuk akun AWS. Anda dapat menggunakan EventBridge untuk memantau statusTrusted Advisor pemeriksaan. Anda kemudian dapat menggunakan Amazon CloudWatch untuk membuat alarm diTrusted Advisor metrik. Alarm ini memberi tahu Anda saat status berubah untuk pemeriksaan Trusted Advisor, seperti sumber daya yang diperbarui atau service quotas yang tercapai.
- AWS CloudTrail merekam panggilan API dan peristiwa terkait yang dilakukan oleh atau atas nama akun AWS Anda dan mengirimkan berkas 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 informasi selengkapnya, lihat Panduan Pengguna AWS CloudTrail.

Topik

Memantau hasil AWS Trusted Advisor pemeriksaan dengan Amazon EventBridge

Anda dapat menggunakan EventBridge untuk mendeteksi ketika Anda memeriksa status Trusted Advisor perubahan. Kemudian, berdasarkan aturan yang Anda buat, EventBridge memanggil satu atau beberapa tindakan target saat status berubah menjadi nilai yang Anda tentukan dalam aturan.

Bergantung pada perubahan status, Anda dapat mengirim pemberitahuan, menangkap informasi status, mengambil tindakan korektif, memulai acara, atau mengambil tindakan lain. Misalnya, Anda dapat menentukan jenis target berikut jika pemeriksaan mengubah status dari tidak ada masalah yang terdeteksi (hijau) ke tindakan yang disarankan (merah).

- Gunakan AWS Lambda fungsi untuk meneruskan notifikasi ke saluran Slack.
- Dorong data tentang pemeriksaan ke aliran Amazon Kinesis untuk mendukung pemantauan status yang komprehensif dan real-time.
- Kirim topik Layanan Pemberitahuan Sederhana Amazon ke email Anda.
- Dapatkan pemberitahuan dengan tindakan CloudWatch alarm Amazon.

Untuk informasi selengkapnya tentang cara menggunakan EventBridge dan fungsi Lambda untuk mengotomatiskan responsTrusted Advisor, lihat Trusted Advisor alat di. GitHub

> **Catatan**
>
> - Trusted Advisormemberikan acara atas dasar upaya terbaik. Acara tidak selalu dijamin akan dikirimkan ke EventBridge.
> - Anda harus memiliki AWS Support rencana Bisnis, Enterprise On-Ramp, atau Enterprise untuk membuat aturan untuk Trusted Advisor pemeriksaan. Untuk informasi selengkapnya, lihat Mengubah AWS Support Rencana.
> - Seperti Trusted Advisor layanan Global, semua Acara dipancarkan ke EventBridge Wilayah AS Timur (Virginia N.).

Ikuti prosedur ini untuk membuat EventBridge aturan untukTrusted Advisor. Sebelum Anda membuat aturan acara, lakukan hal berikut:

- Biasakan diri Anda dengan acara, aturan, dan target di EventBridge. Untuk informasi lebih lanjut, lihat Apa itu Amazon EventBridge? di Panduan EventBridge Pengguna Amazon.
- Buat target yang akan Anda gunakan dalam aturan acara Anda.

Untuk membuat EventBridge aturan untuk Trusted Advisor

1. Buka EventBridge konsol Amazon di https://console.aws.amazon.com/events/.
2. Untuk mengubah Region, gunakan pemilih Region di sudut kanan atas halaman dan pilih US East (Virginia N.).
3. Di panel navigasi, pilih Aturan.
4. Pilih Buat aturan.
5. Pada halaman Tentukan detail aturan, masukkan nama dan deskripsi untuk aturan Anda.
6. Simpan nilai default untuk bus Acara dan tipe Aturan, lalu pilih Berikutnya.
7. Pada halaman pola acara Build, untuk sumber acara, pilih AWSacara atau acara EventBridge mitra.
8. Di bawah pola Peristiwa, pertahankan nilai default untuk Layanan AWS.
9. Untuk Layanan AWS, pilih Trusted Advisor.
10. Untuk jenis Acara, pilih Periksa Status Penyegaran Item.
11. Pilih salah satu opsi berikut untuk memeriksa status:
    - Pilih Status apa pun untuk membuat aturan yang memantau perubahan status apa pun.
    - Pilih Status spesifik, lalu pilih nilai yang ingin dipantau oleh aturan Anda.
        - ERROR — Trusted Advisor merekomendasikan tindakan untuk pemeriksaan.
        - INFO — tidak Trusted Advisor dapat menentukan status cek.
        - OK - Trusted Advisor tidak mendeteksi masalah untuk pemeriksaan.
        - PERINGATAN — Trusted Advisor mendeteksi kemungkinan masalah untuk pemeriksaan dan merekomendasikan penyelidikan.
12. Pilih salah satu opsi berikut untuk pemeriksaan Anda:
    - Pilih Cek apa saja.
    - Pilih Centang khusus, lalu pilih satu atau beberapa nama centang dari daftar.
13. Pilih salah satu opsi berikut untuk AWS sumber daya:
    - Pilih ID sumber daya apa pun untuk membuat aturan yang memantau semua sumber daya.

- Pilih ID sumber daya tertentu menurut ARN, lalu masukkan Nama Sumber Daya Amazon (ARN) yang Anda inginkan.

14. Pilih Selanjutnya.
15. Di halaman Pilih target, pilih jenis target yang Anda buat untuk aturan ini, lalu konfigurasikan opsi tambahan apa pun yang diperlukan untuk jenis tersebut. Misalnya, Anda dapat mengirim acara ke antrean Amazon SQS atau topik Amazon SNS.
16. Pilih Selanjutnya.
17. (Opsional) Pada halaman Konfigurasi tag, tambahkan tag apa pun lalu pilih Berikutnya.
18. Pada halaman Tinjau dan buat, tinjau pengaturan aturan Anda dan pastikan aturan tersebut memenuhi persyaratan pemantauan acara Anda.
19. Pilih Buat aturan. Aturan Anda sekarang akan memantau Trusted Advisor pemeriksaan dan kemudian mengirim acara ke target yang Anda tentukan.

Membuat CloudWatch alarm Amazon untuk memantauAWS Trusted Advisor metrik

SaatAWS Trusted Advisor menyegarkan pemeriksaan Anda,Trusted Advisor menerbitkan metrik tentang hasil pemeriksaan Anda CloudWatch. Anda dapat melihat metrik di CloudWatch. Anda juga dapat membuat alarm untuk mendeteksi perubahan status pemeriksaan Trusted Advisor dan perubahan status sumber daya, dan penggunaan service quotas (sebelumnya disebut sebagai batas). Misalnya, Anda dapat membuat alarm untuk melacak perubahan status untuk pemeriksaan di kategori Service Limits. Alarm kemudian akan memberi tahu Anda saat Anda mencapai atau melebihi service quotas untuk akun AWS.

Ikuti prosedur ini untuk membuat CloudWatch alarm untukTrusted Advisor metrik tertentu.

Topik

Prasyarat

Sebelum Anda membuat CloudWatch alarm untukTrusted Advisor metrik, tinjau informasi berikut:

- Pahami cara CloudWatch menggunakan metrik dan alarm. Untuk informasi selengkapnya, lihat Cara CloudWatch kerjanya di Panduan CloudWatch Pengguna Amazon.
- Gunakan konsol Trusted Advisor atau API AWS Support untuk menyegarkan pemeriksaan Anda dan mendapatkan hasil pemeriksaan terbaru. Untuk informasi selengkapnya, lihat Menyegarkan hasil pemeriksaan.

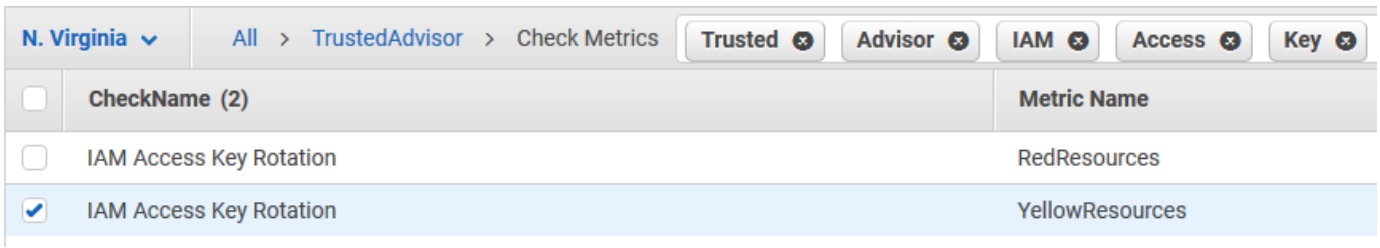
Membuat CloudWatch alarm untukTrusted Advisor metrik

1. Buka CloudWatch konsol di https://console.aws.amazon.com/cloudwatch/.
2. Gunakan Region selector (Pemilih wilayah) dan pilih Wilayah US East (N. Virginia) AWS.
3. Di panel navigasi, pilih Alarm.
4. Pilih Buat alarm.
5. Pilih Pilih metrik.
6. Untuk Metrics (Metrik), masukkan satu atau beberapa nilai dimensi untuk memfilter daftar metrik. Misalnya, Anda dapat memasukkan nama metrik ServiceLimitUsageatau dimensi, seperti namaTrusted Advisor pemeriksaan.

   > **Tip**
   >
   > - Anda dapat mencari **`Trusted Advisor`** untuk mencantumkan semua metrik untuk layanan.
   > - Untuk daftar nama metrik dan dimensi, lihat Metrik dan dimensi Trusted Advisor.

7. Dalam tabel hasil, pilih kotak centang untuk metrik.

   Pada contoh berikut, nama centang adalah IAM Access Key Rotation dan nama metriknya YellowResources.



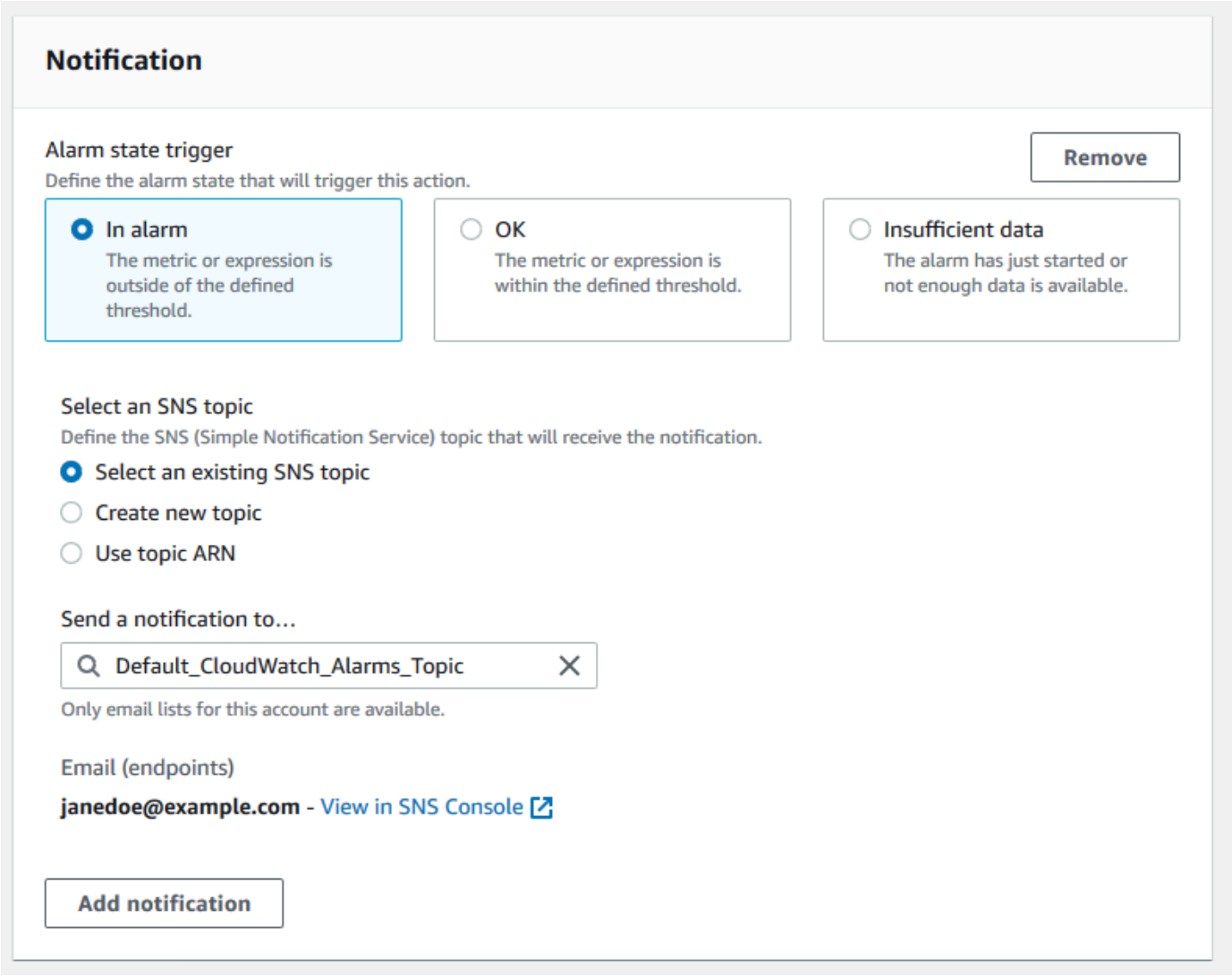
8. Pilih Pilih metrik.

9. Pada halaman Tentukan metrik dan kondisi, verifikasi bahwa nama Metrik dan CheckNameyang Anda pilih muncul di halaman.
10. Untuk Period (Jangka waktu), Anda dapat menentukan jangka waktu yang Anda inginkan alarm untuk dimulai ketika status pemeriksaan berubah, seperti 5 menit.
11. Di bawah Conditions (Syarat), pilih Static (Statis), lalu tentukan syarat ketika alarm harus dimulai.

    Misalnya, jika Anda memilih Lebih Besar/Sama >=ambang dan memasukkan **1** untuk nilai ambang batas, ini berarti bahwa alarm dimulai ketika Trusted Advisor mendeteksi setidaknya satu access key IAM yang belum dirotasi dalam 90 hari terakhir.

    > **Catatan**
    >
    > - Untuk GreenChecks,, RedChecks, YellowChecksRedResources, dan YellowResourcesmetrik, Anda dapat menentukan ambang batas yang merupakan bilangan bulat yang lebih besar dari atau sama dengan nol.
    > - Trusted Advisortidak mengirim metrik untuk GreenResources, yang merupakan sumber daya yangTrusted Advisor belum mendeteksi masalah apa pun.

12. Pilih Selanjutnya.
13. Pada halaman Configure actions (Mengonfigurasi tindakan), untuk Alarm state trigger (Pemicu keadaan alarm), pilihIn alarm (Dalam alarm).
14. Untuk Select an SNS topic (Pilih topik SNS), pilih topik Amazon Simple Notification Service (Amazon SNS) yang sudah ada atau buat baru.



15. Pilih Selanjutnya.
16. Untuk Name and description (Nama dan deskripsi), masukkan nama dan deskripsi untuk alarm Anda.
17. Pilih Selanjutnya.
18. Pada Preview and create (Pratinjau dan buat), tinjau detail alarm Anda, lalu pilihCreate alarm (Buat alarm).

    Ketika status untuk pemeriksaan IAM Access Key Rotation (Rotasi Access Key IAM) berubah menjadi merah selama 5 menit, alarm akan mengirimkan notifikasi ke topik SNS Anda.

Example : Pemberitahuan email untuk CloudWatch alarm

Pesan email berikut menunjukkan bahwa alarm mendeteksi perubahan untuk pemeriksaan IAM Access Key Rotation (Rotasi Access Key IAM).

```
You are receiving this email because your Amazon CloudWatch Alarm
 "IAMAcessKeyRotationCheckAlarm" in the US East (N. Virginia) region has entered the
 ALARM state,
because "Threshold Crossed: 1 out of the last 1 datapoints [9.0 (26/03/21 22:44:00)]
 was greater than or equal to the threshold (1.0) (minimum 1 datapoint for OK -> ALARM
 transition)." at "Friday 26 March, 2021 22:49:42 UTC".

View this alarm in the AWS Management Console:
https://us-east-1.console.aws.amazon.com/cloudwatch/home?region=us-
east-1#s=Alarms&alarm=IAMAcessKeyRotationCheckAlarm

Alarm Details:
- Name:                       IAMAcessKeyRotationCheckAlarm
- Description:                This alarm starts when one or more AWS access keys in my
 AWS account have not been rotated in the last 90 days.
- State Change:               INSUFFICIENT_DATA -> ALARM
- Reason for State Change:    Threshold Crossed: 1 out of the last 1 datapoints [9.0
 (26/03/21 22:44:00)] was greater than or equal to the threshold (1.0) (minimum 1
 datapoint for OK -> ALARM transition).
- Timestamp:                  Friday 26 March, 2021 22:49:42 UTC
- AWS Account:                123456789012
- Alarm Arn:                  arn:aws:cloudwatch:us-
east-1:123456789012:alarm:IAMAcessKeyRotationCheckAlarm

Threshold:
- The alarm is in the ALARM state when the metric is GreaterThanOrEqualToThreshold 1.0
 for 300 seconds.

Monitored Metric:
- MetricNamespace:                    AWS/TrustedAdvisor
- MetricName:                         RedResources
- Dimensions:                         [CheckName = IAM Access Key Rotation]
- Period:                             300 seconds
- Statistic:                          Average
- Unit:                               not specified
- TreatMissingData:                   missing


State Change Actions:
```

```
- OK:
- ALARM: [arn:aws:sns:us-east-1:123456789012:Default_CloudWatch_Alarms_Topic]
- INSUFFICIENT_DATA:
```

CloudWatch metrik untukTrusted Advisor

Anda dapat menggunakan CloudWatch konsol atauAWS Command Line Interface (AWS CLI) untuk menemukan metrik yang tersediaTrusted Advisor.

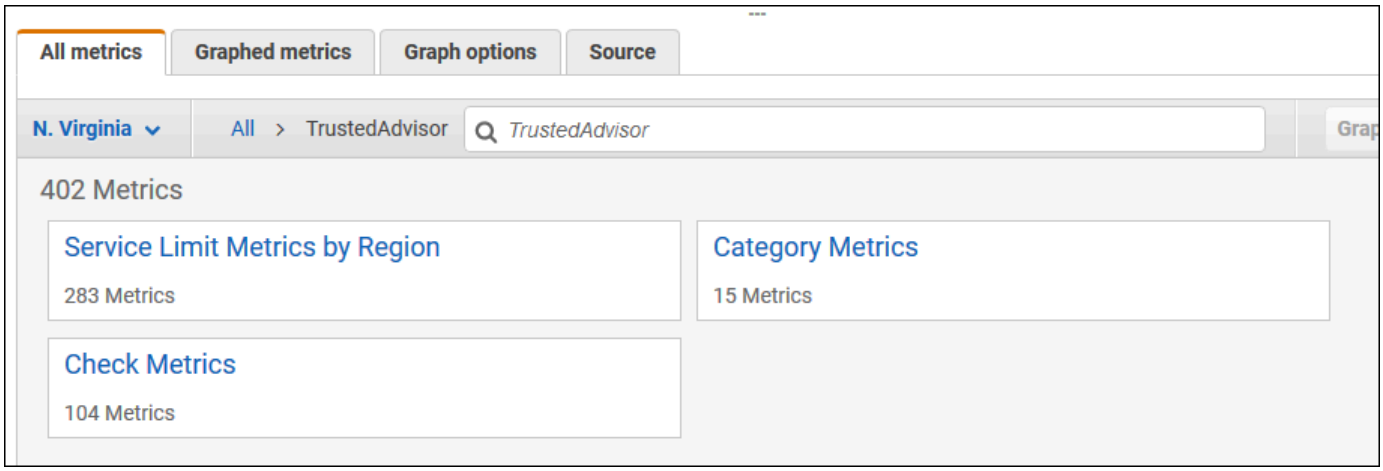
Untuk daftar namespace, metrik, dan dimensi untuk semua layanan yang menerbitkan metrik, lihat AWSlayanan yang menerbitkan CloudWatch metrik dalam Panduan CloudWatch Pengguna Amazon.

Lihat metrik Trusted Advisor (konsol)

Anda dapat masuk ke CloudWatch konsol dan melihat metrik yang tersedia untukTrusted Advisor.

Untuk melihat metrik Trusted Advisor yang tersedia (konsol)

1. Buka CloudWatch konsol di https://console.aws.amazon.com/cloudwatch/.
2. Gunakan Region selector (Pemilih wilayah) dan pilih Wilayah US East (N. Virginia) AWS.
3. Di panel navigasi, pilih Metrik.
4. Masukkan namespace metrik, seperti **`TrustedAdvisor`**.
5. Pilih dimensi metrik, seperti Check Metrics (Metrik Pemeriksaan).



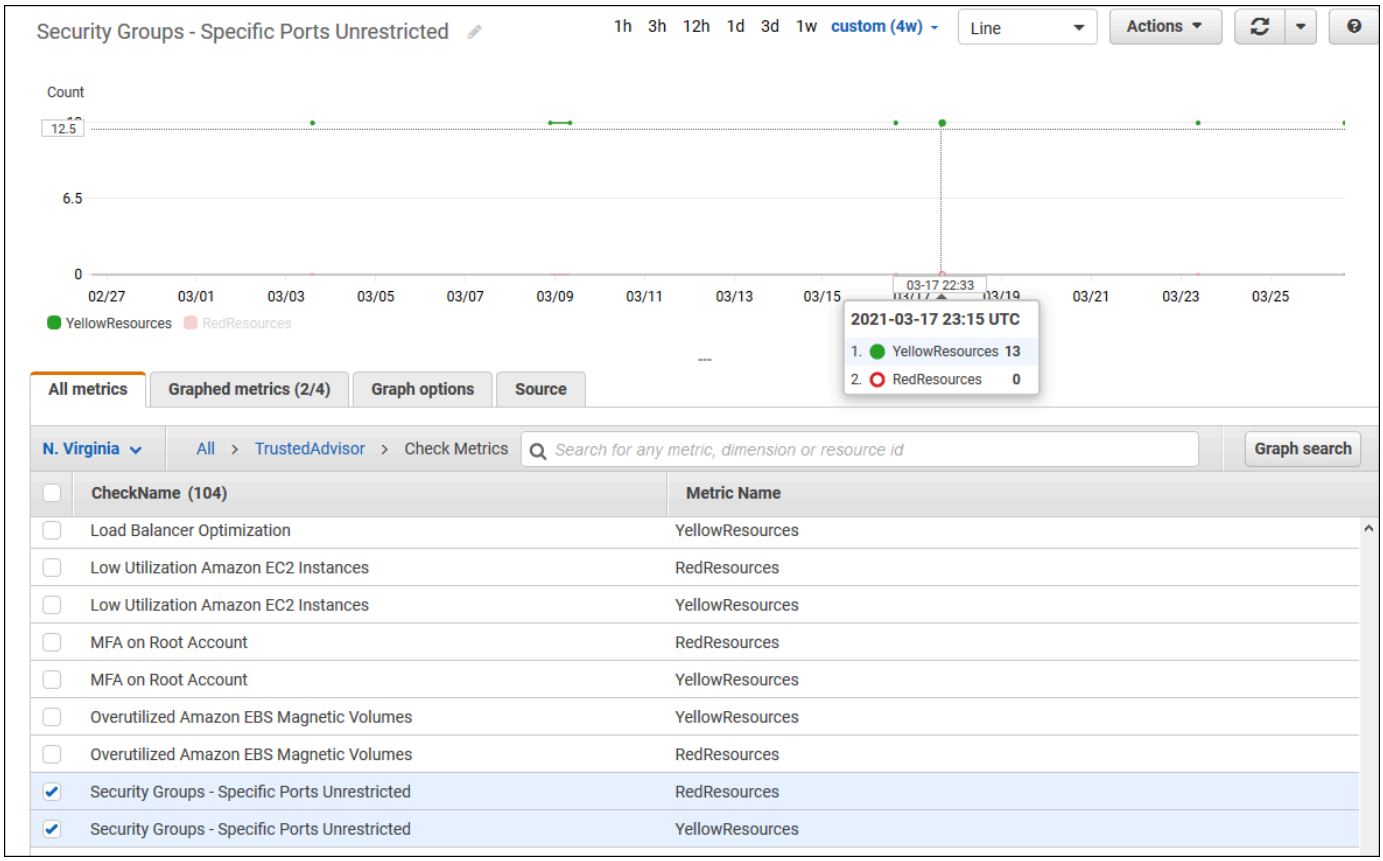
6. Tab All metrics (Semua metrik) menampilkan semua metrik untuk dimensi tersebut di namespace. Anda dapat melakukan hal berikut:

   a. Untuk menyortir tabel, pilih judul kolom.

b. Untuk membuat grafik metrik, pilih kotak centang di samping metrik. Untuk memilih semua metrik, pilih kotak centang di baris judul tabel.

c. Untuk memfilter berdasarkan metrik, pilih nama metrik, kemudian pilih Tambahkan ke pencarian.

Contoh berikut menunjukkan hasil untuk pemeriksaan Security Groups - Specific Ports Unrestricted (Grup Keamanan - Port Tertentu Tak Terbatas). Pemeriksaan mengidentifikasi 13 sumber daya yang berwarna kuning. Trusted Advisor merekomendasikan bahwa Anda menyelidiki pemeriksaan yang berwarna kuning.



7. (Opsional) Untuk menambahkan grafik ini ke CloudWatch dasbor, pilih Tindakan, lalu pilih Tambahkan ke dasbor.

Untuk informasi selengkapnya tentang cara membuat grafik untuk melihat metrik, lihat Membuat grafik metrik dalam Panduan CloudWatch Pengguna Amazon.

Lihat metrik Trusted Advisor (CLI)

Anda dapat menggunakan perintah AWS CLI daftar-metrik untuk melihat metrik yang tersedia untuk Trusted Advisor.

Example : Daftar semua metrik untuk Trusted Advisor

Contoh berikut menentukan namespace `AWS/TrustedAdvisor` untuk melihat semua metrik untuk Trusted Advisor.

```
aws cloudwatch list-metrics --namespace AWS/TrustedAdvisor
```

Output Anda mungkin terlihat seperti berikut ini.

```
{
    "Metrics": [
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "ServiceName",
                    "Value": "EBS"
                },
                {
                    "Name": "ServiceLimit",
                    "Value": "Magnetic (standard) volume storage (TiB)"
                },
                {
                    "Name": "Region",
                    "Value": "ap-northeast-2"
                }
            ],
            "MetricName": "ServiceLimitUsage"
        },
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "CheckName",
                    "Value": "Overutilized Amazon EBS Magnetic Volumes"
                }
            ],
            "MetricName": "YellowResources"
```

```
        },
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "ServiceName",
                    "Value": "EBS"
                },
                {
                    "Name": "ServiceLimit",
                    "Value": "Provisioned IOPS"
                },
                {
                    "Name": "Region",
                    "Value": "eu-west-1"
                }
            ],
            "MetricName": "ServiceLimitUsage"
        },
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "ServiceName",
                    "Value": "EBS"
                },
                {
                    "Name": "ServiceLimit",
                    "Value": "Provisioned IOPS"
                },
                {
                    "Name": "Region",
                    "Value": "ap-south-1"
                }
            ],
            "MetricName": "ServiceLimitUsage"
        },
    ...
  ]
}
```

Example : Daftar semua metrik untuk dimensi

Contoh berikut menentukan namespace `AWS/TrustedAdvisor` dan dimensi `Region` untuk melihat metrik yang tersedia untuk Wilayah AWS yang ditentukan.

```
aws cloudwatch list-metrics --namespace AWS/TrustedAdvisor --dimensions
 Name=Region,Value=us-east-1
```

Output Anda mungkin terlihat seperti berikut ini.

```
{
    "Metrics": [
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "ServiceName",
                    "Value": "SES"
                },
                {
                    "Name": "ServiceLimit",
                    "Value": "Daily sending quota"
                },
                {
                    "Name": "Region",
                    "Value": "us-east-1"
                }
            ],
            "MetricName": "ServiceLimitUsage"
        },
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "ServiceName",
                    "Value": "AutoScaling"
                },
                {
                    "Name": "ServiceLimit",
                    "Value": "Launch configurations"
                },
                {
                    "Name": "Region",
```

```
                    "Value": "us-east-1"
                }
            ],
            "MetricName": "ServiceLimitUsage"
        },
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "ServiceName",
                    "Value": "CloudFormation"
                },
                {
                    "Name": "ServiceLimit",
                    "Value": "Stacks"
                },
                {
                    "Name": "Region",
                    "Value": "us-east-1"
                }
            ],
            "MetricName": "ServiceLimitUsage"
        },
    ...
  ]
}
```

Example : Daftar metrik untuk nama metrik tertentu

Contoh berikut menentukan namespace `AWS/TrustedAdvisor` dan nama metrik `RedResources` untuk melihat hasil hanya untuk metrik yang ditentukan.

```
aws cloudwatch list-metrics --namespace AWS/TrustedAdvisor --metric-name RedResources
```

Output Anda mungkin terlihat seperti berikut ini.

```
{
    "Metrics": [
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "CheckName",
```

```
                    "Value": "Amazon RDS Security Group Access Risk"
                }
            ],
            "MetricName": "RedResources"
        },
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "CheckName",
                    "Value": "Exposed Access Keys"
                }
            ],
            "MetricName": "RedResources"
        },
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "CheckName",
                    "Value": "Large Number of Rules in an EC2 Security Group"
                }
            ],
            "MetricName": "RedResources"
        },
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "CheckName",
                    "Value": "Auto Scaling Group Health Check"
                }
            ],
            "MetricName": "RedResources"
        },
    ...
  ]
}
```

Metrik dan dimensi Trusted Advisor

Lihat tabel berikut untukTrusted Advisor metrik dan dimensi yang dapat digunakan untuk CloudWatch alarm dan grafik.

Metrik pemeriksaan-tingkat Trusted Advisor

Anda dapat menggunakan metrik berikut untuk pemeriksaan Trusted Advisor.

Metrik	Deskripsi
`RedResources`	Jumlah sumber daya yang berada dalam keadaan merah (tindakan dianjurkan).
`YellowResources`	Jumlah sumber daya yang berada dalam keadaan kuning (investigasi disarankan).

Metrik kategori-tingkat Trusted Advisor

Anda dapat menggunakan metrik berikut untuk kategori Trusted Advisor.

Metrik	Deskripsi
`GreenChecks`	Jumlah pemeriksaan Trusted Advisor yang berada dalam keadaan hijau (tidak ada masalah terdeteksi).
`RedChecks`	Jumlah pemeriksaan Trusted Advisor yang berada dalam keadaan merah (tindakan dianjurkan).
`YellowChecks`	Jumlah pemeriksaan Trusted Advisor yang berada dalam keadaan kuning (investigasi dianjurkan).

Metrik tingkat service quotas Trusted Advisor

Anda dapat menggunakan metrik berikut untukLayanan AWS quotas.

Metrik	Deskripsi
`ServiceLimitUsage`	Persentase penggunaan sumber daya terhadap service quotas (sebelumnya disebut sebagai batas).

Dimensi untuk metrik pemeriksaan-tingkat

Anda dapat menggunakan dimensi berikut untuk pemeriksaan Trusted Advisor.

Dimensi	Deskripsi
`CheckName`	Nama pemeriksaan Trusted Advisor. Anda dapat menemukan semua nama cek di Trusted Advisorkonsol atauAWS Trusted Advisor periksa referensi.

Dimensi untuk metrik kategori-tingkat

Anda dapat menggunakan dimensi berikut untuk kategori pemeriksaan Trusted Advisor.

Dimensi	Deskripsi
`Category`	Nama kategori pemeriksaan Trusted Advisor. Anda dapat menemukan semua kategori pemeriksaan di konsol Trusted Advisor atau halaman Melihat kategori pemeriksaan.

Dimensi untuk metrik service quotas

Anda dapat menggunakan dimensi berikut untuk metrik service quotas Trusted Advisor.

Dimensi	Deskripsi
`Region`	Wilayah AWSUntuk service quotas.
`ServiceName`	Nama Layanan AWS.
`ServiceLimit`	Nama kuota layanan. Untuk informasi lebih lanjut tentang service quotas, lihat Layanan AWSquotas dalam Referensi Umum AWS.

Mencatat tindakan AWS Trusted Advisor konsol dengan AWS CloudTrail

Trusted Advisor terintegrasi dengan AWS CloudTrail, layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atau AWS layanan di Trusted Advisor. CloudTrail menangkap tindakan untuk Trusted Advisor sebagai acara. Panggilan yang diambil termasuk panggilan dari Trusted Advisor konsol. Jika Anda membuat jejak, Anda dapat mengaktifkan pengiriman CloudTrail acara secara terus menerus ke bucket Amazon Simple Storage Service (Amazon S3), termasuk acara untuk. Trusted Advisor 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 Trusted Advisor, alamat IP dari mana permintaan dibuat, siapa yang membuat permintaan, kapan dibuat, dan detail tambahan.

Untuk mempelajari selengkapnya CloudTrail, termasuk cara mengonfigurasi dan mengaktifkannya, lihat Panduan AWS CloudTrail Pengguna.

Trusted Advisor informasi di CloudTrail

CloudTrail diaktifkan di AWS akun Anda saat Anda membuat akun. Ketika aktivitas peristiwa yang didukung terjadi di Trusted Advisor konsol, aktivitas tersebut direkam dalam suatu CloudTrail peristiwa bersama dengan peristiwa AWS layanan lainnya dalam riwayat Acara. Anda dapat melihat, mencari, dan mengunduh acara terbaru di AWS akun Anda. Untuk informasi selengkapnya, lihat Melihat Acara dengan Riwayat CloudTrail Acara.

Untuk catatan peristiwa yang sedang berlangsung di AWS akun Anda, termasuk acara untuk Trusted Advisor, buat jejak. Jejak memungkinkan CloudTrail untuk mengirimkan file log ke bucket Amazon S3. Secara default, saat Anda membuat jejak di konsol tersebut, jejak diterapkan ke semua Wilayah AWS . Jejak mencatat peristiwa dari semua Wilayah di AWS partisi dan mengirimkan file 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 berikut ini:

- Ikhtisar untuk Membuat Jejak
- CloudTrail Layanan dan Integrasi yang Didukung
- Mengkonfigurasi Notifikasi Amazon SNS untuk CloudTrail

- Menerima File CloudTrail Log dari Beberapa Wilayah dan Menerima File CloudTrail Log dari Beberapa Akun

Trusted Advisor mendukung pencatatan subset dari tindakan Trusted Advisor konsol sebagai peristiwa dalam file CloudTrail log. CloudTrail mencatat tindakan berikut:

- BatchUpdateRecommendationResourceExclusion
- CreateEngagement
- CreateEngagementAttachment
- CreateEngagementCommunication
- CreateExcelReport
- DescribeAccount
- DescribeAccountAccess
- DescribeCheckItems
- DescribeCheckRefreshStatuses
- DescribeCheckSummaries
- DescribeChecks
- DescribeNotificationPreferences
- DescribeOrganization
- DescribeOrganizationAccounts
- DescribeReports
- DescribeServiceMetadata
- ExcludeCheckItems
- GenerateReport
- GetEngagement
- GetEngagementAttachment
- GetEngagementType
- GetExcelReport
- GetOrganizationRecommendation
- GetRecommendation

- IncludeCheckItems
- ListAccountsForParent
- ListChecks
- ListEngagementCommunications
- ListEngagementTypes
- ListEngagements
- ListOrganizationRecommendationAccounts
- ListOrganizationRecommendationResources
- ListOrganizationRecommendations
- ListOrganizationalUnitsForParent
- ListRecommendationResources
- ListRecommendations
- ListRoots
- RefreshCheck
- SetAccountAccess
- SetOrganizationAccess
- UpdateEngagement
- UpdateEngagementStatus
- UpdateNotificationPreferences
- UpdateOrganizationRecommendationLifecycle
- UpdateRecommendationLifecycle

Untuk daftar lengkap tindakan Trusted Advisor konsol, lihatTrusted Advisor tindakan.

> **Note**
>
> CloudTrail juga mencatat operasi Trusted Advisor API di Referensi AWS Support API. Untuk informasi selengkapnya, lihat Mencatat panggilan API AWS Support dengan AWS CloudTrail.

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

- Apakah permintaan itu dibuat dengan kredenal pengguna root atau AWS Identity and Access Management (IAM).
- Apakah permintaan tersebut dibuat dengan kredensial keamanan sementara untuk satu peran atau pengguna terfederasi.
- Apakah permintaan itu dibuat oleh AWS layanan lain.

Untuk informasi selengkapnya, lihat Elemen CloudTrail UserIdentity.

Contoh: Entri Berkas Trusted Advisor Log

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, jadi file tersebut tidak muncul dalam urutan tertentu.

Example : Entri log untuk RefreshCheck

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan `RefreshCheck` tindakan untuk pemeriksaan (ID) Amazon S3 Bucket Versioning. R365s2Qddf


```
{
        "eventVersion":"1.04",
        "userIdentity":{
        "type":"IAMUser",
        "principalId":"AIDACKCEVSQ6C2EXAMPLE",
        "arn":"arn:aws:iam::123456789012:user/janedoe",
        "accountId":"123456789012",
        "accessKeyId":"AKIAIOSFODNN7EXAMPLE",
        "userName":"janedoe",
        "sessionContext":{
        "attributes":{
        "mfaAuthenticated":"false",
        "creationDate":"2020-10-21T22:06:18Z"
        }
        }
        },
        "eventTime":"2020-10-21T22:06:33Z",
        "eventSource":"trustedadvisor.amazonaws.com",
        "eventName":"RefreshCheck",
```

```
        "awsRegion":"us-east-1",
        "sourceIPAddress":"100.127.34.136",
        "userAgent":"signin.amazonaws.com",
        "requestParameters":{
        "checkId":"R365s2Qddf"
        },
        "responseElements":{
        "status":{
        "checkId":"R365s2Qddf",
        "status":"enqueued",
        "millisUntilNextRefreshable":3599993
        }
        },
        "requestID":"d23ec729-8995-494c-8054-dedeaEXAMPLE",
        "eventID":"a49d5202-560f-4a4e-b38a-02f1cEXAMPLE",
        "eventType":"AwsApiCall",
        "recipientAccountId":"123456789012"
        }
```


Example : Entri log untuk UpdateNotificationPreferences

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


```
{
        "eventVersion":"1.04",
        "userIdentity":{
        "type":"IAMUser",
        "principalId":"AIDACKCEVSQ6C2EXAMPLE",
        "arn":"arn:aws:iam::123456789012:user/janedoe",
        "accountId":"123456789012",
        "accessKeyId":"AKIAIOSFODNN7EXAMPLE",
        "userName":"janedoe",
        "sessionContext":{
        "attributes":{
        "mfaAuthenticated":"false",
        "creationDate":"2020-10-21T22:06:18Z"
        }
        }
        },
        "eventTime":"2020-10-21T22:09:49Z",
        "eventSource":"trustedadvisor.amazonaws.com",
```

```
        "eventName":"UpdateNotificationPreferences",
        "awsRegion":"us-east-1",
        "sourceIPAddress":"100.127.34.167",
        "userAgent":"signin.amazonaws.com",
        "requestParameters":{
        "contacts":[
        {
        "id":"billing",
        "type":"email",
        "active":false
        },
        {
        "id":"operational",
        "type":"email",
        "active":false
        },
        {
        "id":"security",
        "type":"email",
        "active":false
        }
        ],
        "language":"en"
        },
        "responseElements":null,
        "requestID":"695295f3-c81c-486e-9404-fa148EXAMPLE",
        "eventID":"5f923d8c-d210-4037-bd32-997c6EXAMPLE",
        "eventType":"AwsApiCall",
        "recipientAccountId":"123456789012"
        }
```

Example : Entri log untuk GenerateReport

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan `GenerateReport` tindakan. Tindakan ini membuat laporan untuk organisasi AWS Anda.

```
{
        "eventVersion":"1.04",
        "userIdentity":{
        "type":"IAMUser",
        "principalId":"AIDACKCEVSQ6C2EXAMPLE",
        "arn":"arn:aws:iam::123456789012:user/janedoe",
```

```
        "accountId":"123456789012",
        "accessKeyId":"AKIAIOSFODNN7EXAMPLE",
        "userName":"janedoe",
        "sessionContext":{
        "attributes":{
        "mfaAuthenticated":"false",
        "creationDate":"2020-11-03T13:03:10Z"
        }
        }
        },
        "eventTime":"2020-11-03T13:04:29Z",
        "eventSource":"trustedadvisor.amazonaws.com",
        "eventName":"GenerateReport",
        "awsRegion":"us-east-1",
        "sourceIPAddress":"100.127.36.171",
        "userAgent":"signin.amazonaws.com",
        "requestParameters":{
        "refresh":false,
        "includeSuppressedResources":false,
        "language":"en",
        "format":"JSON",
        "name":"organizational-view-report",
        "preference":{
        "accounts":[

        ],
        "organizationalUnitIds":[
        "r-j134"
        ],
        "preferenceName":"organizational-view-report",
        "format":"json",
        "language":"en"
        }
        },
        "responseElements":{
        "status":"ENQUEUED"
        },
        "requestID":"bb866dc1-60af-47fd-a660-21498EXAMPLE",
        "eventID":"2606c89d-c107-47bd-a7c6-ec92fEXAMPLE",
        "eventType":"AwsApiCall",
        "recipientAccountId":"123456789012"
        }
```

Sumber daya pemecahan masalah

Untuk jawaban terhadap pertanyaan pemecahan masalah umum, kunjungi Pusat Pengetahuan AWS Support.

Untuk Windows, Amazon EC2 menawarkan EC2Rescue, yang dapat digunakan pelanggan untuk memeriksa instance Windows mereka guna membantu mengidentifikasi masalah umum, mengumpulkan file log, dan membantu AWS Support memecahkan masalah Anda. Anda juga dapat menggunakan EC2Rescue untuk menganalisis volume boot dari contoh nonfungsional. Untuk informasi lebih lanjut, lihat Bagaimana cara menggunakan EC2Rescue untuk memecahkan masalah dan memperbaiki masalah umum pada instans Windows EC2 saya?

Pemecahan masalah khusus layanan

Sebagian besar Layanan AWS dokumentasi berisi topik pemecahan masalah yang dapat membantu Anda memulai sebelum menghubungi. AWS Support Tabel berikut menyediakan tautan ke topik pemecahan masalah, disusun menurut layanan.

> **Note**
>
> Tabel berikut menyediakan daftar layanan yang paling umum. Untuk mencari topik pemecahan masalah lainnya, gunakan kotak teks pencarian di halaman landing AWS Dokumentasi.

Layanan	Tautan
Amazon Web Services	Memecahkan masalah kesalahan AWS Tanda Tangan Versi 4
Amazon API Gateway	Memecahkan masalah dengan API HTTP
Amazon AppStream	Memecahkan masalah Amazon AppStream
Amazon Athena	Memecahkan masalah di Athena
Amazon Aurora MySQL	Memecahkan masalah untuk Amazon Aurora
Amazon Aurora PostgreSQL	Memecahkan masalah untuk Amazon Aurora

Layanan	Tautan
Amazon EC2 Auto Scaling	Pemecahan Masalah Auto Scaling
AWS Certificate Manager (ACM)	Pemecahan Masalah
AWS CloudFormation	Pemecahan masalah AWS CloudFormation
Amazon CloudFront	Pemecahan Masalah | Pemecahan masalah distribusi RTMP
AWS CloudHSM	Pemecahan Masalah
Amazon CloudSearch	Memecahkan Masalah Amazon CloudSearch
AWS CodeDeploy	Pemecahan masalah AWS CodeDeploy
Amazon CloudWatch	Pemecahan masalah
AWS Database Migration Service	Memecahkan masalah tugas migrasi di AWS Database Migration Service
AWS Data Pipeline	Pemecahan Masalah
AWS Direct Connect	Pemecahan masalah AWS Direct Connect
AWS Directory Service	Memecahkan masalah administrasi AWS Directory Service
Amazon DynamoDB	Pemecahan masalah | Memecahkan masalah pembuatan koneksi SSL/TLS
AWS Elastic Beanstalk	Pemecahan Masalah
Amazon Elastic Compute Cloud (Amazon EC2)	Pemecahan masalah instans | Pemecahan masalah instans Windows | Pemecahan masalah VM Import/Export | Pemecahan masalah eror permintaan API | Pemecahan masalah paket manajemen AWS | Pemecahan masalah AWS Systems Manager untuk Microsoft SCVMM | Diagnostik AWS untuk server Microsoft Windows

Layanan	Tautan
Layanan Amazon Elastic Container (Amazon ECS)	Pemecahan masalah Amazon ECS
Amazon Elastic Kubernetes Service (Amazon EKS)	Pemecahan masalah Amazon EKS
Penyeimbang Beban Elastis	Memecahkan masalah Application Load Balancer | Memecahkan masalah Classic Load Balancer
Amazon ElastiCache untuk Memcached	Aplikasi pemecahan masalah
Amazon ElastiCache untuk Redis	Aplikasi pemecahan masalah
Amazon EMR	Memecahkan masalah klaster
AWS Flow Framework	Kiat pemecahan masalah dan debugging
AWS Glue	Pemecahan Masalah AWS Glue
AWS Glue DataBrew	Memecahkan masalah identitas dan akses di AWS Glue DataBrew
AWS GovCloud (US)	Pemecahan Masalah
AWS Identity and Access Management (IAM)	Pemecahan Masalah IAM
Amazon Keyspaces (untuk Apache Cassandra)	Memecahkan Masalah Amazon Keyspaces (untuk Apache Cassandra)
Amazon Kinesis Data Streams	Pemecahan Masalah Produsen Amazon Kinesis Data Streams | Memecahkan Masalah Amazon Kinesis Data Streams konsumen
Layanan Terkelola Amazon untuk Apache Flink	Pemecahan Masalah Kinerja | Pemecahan Masalah Amazon Managed Service untuk Apache Flink untuk Aplikasi SQL

Layanan	Tautan
Amazon Data Firehose	Memecahkan Masalah Amazon Data Firehose
AWS Lambda	Pemecahan masalah dan pemantauan AWS Lambda fungsi dengan CloudWatch
OpenSearch Layanan Amazon	Memecahkan Masalah Layanan Amazon OpenSearch
AWS OpsWorks	Panduan debugging dan pemecahan masalah
Amazon Personalize	Pemecahan Masalah
Amazon QLDB	Memecahkan Masalah Amazon QLDB
Amazon QuickSight	Memecahkan masalah Amazon QuickSight | Memecahkan masalah kesalahan baris yang dilewati
AWS Resource Access Manager (AWS RAM)	Memecahkan masalah dengan AWS RAM
Amazon Redshift	Memecahkan masalah kueri | Memecahkan masalah beban data | Memecahkan masalah koneksi di Amazon Redshift | Memecahkan masalah pencatatanaudit Amazon Redshift | Memecahkan masalah kueri di Amazon Redshift Spectrum
Amazon Relational Database Service (Amazon RDS)	Pemecahan masalah | Pemecahan masalah aplikasi di Amazon RDS | Memecahkan masalah DB untuk Amazon RDS Custom
Amazon Route 53	Memecahkan Masalah Amazon Route 53
Amazon SageMaker	Memecahkan masalah kesalahan | Memecahkan masalah Amazon Studio SageMaker
Amazon Silk	Pemecahan Masalah
Amazon Simple Email Service (Amazon SES)	Memecahkan Masalah Amazon SES

Layanan	Tautan
Amazon Simple Storage Service (Amazon S3)	Pemecahan masalah
Amazon Simple Workflow Service (Amazon SWF)	AWS Framework flow untuk Java: Tips pemecahan masalah dan debugging | framework AWS flow untuk Ruby: Pemecahan masalah dan debugging alur kerja
AWS Storage Gateway	Memecahkan masalah gateway Anda
AWS Systems Manager	Pemecahan Masalah Agen SSM
Amazon Virtual Private Cloud (Amazon VPC)	Pemecahan Masalah
AWS Virtual Private Network (AWS VPN)	Memecahkan masalah perangkat gateway pelanggan Anda
AWS WAF	Menguji dan menyetel perlindungan Anda AWS WAF
Amazon WorkMail	Memecahkan masalah aplikasi web Amazon WorkMail
Amazon WorkSpaces	Memecahkan masalah Amazon | Memecahkan WorkSpaces masalah klien Amazon WorkSpaces

Riwayat dokumen

Tabel berikut menjelaskan perubahan penting pada dokumentasi sejak rilis terakhir AWS Support layanan.

- AWS Support Versi API: 15-4-2013
- AWS Support Versi API Aplikasi: 2021-08-20

Tabel berikut menjelaskan pembaruan penting pada AWS Support dan AWS Trusted Advisor dokumentasi, mulai 10 Mei 2021. Anda dapat berlangganan ke umpan RSS untuk menerima pemberitahuan tentang pembaruan.

Perubahan	Deskripsi	Tanggal
Dokumentasi diperbarui untuk AWSTrustedAdvisorServiceRolePolicy	Menambahkan tindakan IAM baruaccess-analyzer:ListAnalyzers ,cloudwatch:ListMetrics ,dax:DescribeClusters ,ec2:DescribeNatGateways ,ec2:DescribeRouteTables ,,ec2:DescribeVpcEndpoints ,ec2:GetManagedPrefixListEntries , elasticloadbalancing:DescribeTargetHealth iam:ListSAMLProviders , kafka:DescribeClusterV2 network-firewall:ListFirewalls network-f	Juni 11, 2024

	`irewall:DescribeFirewall` dan `sqs:GetQueueAttributes` untuk onboard cek baru. Untuk informasi selengkapnya, lihat kebijakan AWS terkelola : AWSTrustedAdvisorServiceRolePolicy.	
Ditambahkan dokumentasi untuk AWS Support Rekomendasi	Ditambahkan dokumentasi untuk AWS Support Rekomendasi.	22 Mei 2024
Dihapus 5 AWS Trusted Advisor cek dari dokumentasi	Menghapus 5 AWS Trusted Advisor cek yang sekarang tidak digunakan lagi. Untuk informasi selengkapnya, lihat Mengubah log untuk AWS Trusted Advisor pemeriksaan.	15 Mei 2024
Ditambahkan 1 pemeriksaan AWS Trusted Advisor Keamanan baru untuk dokumentasi	Ditambahkan 1 pemeriksaan AWS Trusted Advisor Keamanan baru untuk dokumentasi. Untuk informasi selengkapnya, lihat Mengubah log untuk AWS Trusted Advisor pemeriksaan.	15 Mei 2024
Dihapus 3 pemeriksaan Toleransi Kesalahan dari dokumentasi	Dihapus 3 pemeriksaan Toleransi Kesalahan yang sekarang tidak digunakan lagi. Untuk informasi selengkapnya, lihat Mengubah log untuk AWS Trusted Advisor pemeriksaan.	April 25, 2024

Diperbarui Toleransi Kesalahan dan dokumentasi pemeriksaan Keamanan	Ditambahkan 1 pemeriksaan toleransi kesalahan baru. Diperbarui 1 toleransi kesalahan dan 1 pemeriksaan keamanan. Untuk informasi selengkapnya, lihat Mengubah log untuk AWS Trusted Advisor pemeriksaan.	Maret 29, 2024
Dokumentasi diperbarui untuk `AWSSupportServiceRolePolicy`	Menambahkan izin baru untuk menyediakan layanan penagihan, administratif, dan dukungan untuk peran terkait layanan. Untuk informasi selengkapnya, lihat kebijakan AWS terkelola: AWSSupportServiceRolePolicy.	Maret 22, 2024
Dokumentasi diperbarui untuk AWS Support rencana	Pembaruan Fitur AWS Support Paket. Untuk informasi lebih lanjut, lihat AWS Support paket.	Maret 11, 2024
Dokumentasi diperbarui untuk Trusted Advisor	Ditambahkan 1 pemeriksaan toleransi kesalahan. Untuk informasi selengkapnya, lihat Mengubah log untuk AWS Trusted Advisor pemeriksaan.	Februari 29, 2024
Dokumentasi diperbarui untuk Trusted Advisor	Ditambahkan 1 pemeriksaan toleransi kesalahan. Untuk informasi selengkapnya, lihat Mengubah log untuk AWS Trusted Advisor pemeriksaan.	Januari 31, 2024

Dokumentasi diperbarui untuk AWSTrustedAdvisorServiceRolePolicy	Menambahkan tindakan IAM barucloudtrail:GetTrail ,,cloudtrail:ListTrails ,cloudtrail:GetEventSelectors ,outposts:GetOutpost , outposts:ListAssets dan outposts:ListOutposts untuk onboard cek baru. Untuk informasi selengkapnya, lihat kebijakan AWS terkelola: AWSTrustedAdvisorServiceRolePolicy.	Januari 18, 2024
Dokumentasi diperbarui untuk AWSSupportServiceRolePolicy	Menambahkan izin baru untuk menyediakan layanan penagihan, administratif, dan dukungan untuk peran terkait layanan. Untuk informasi selengkapnya, lihat kebijakan AWS terkelola: AWSSupportServiceRolePolicy.	Januari 17, 2024
Dokumentasi diperbarui untuk Trusted Advisor	Diperbarui 1 pemeriksaan toleransi kesalahan untuk mengubah judul dan deskripsi. Untuk informasi selengkapnya, lihat Mengubah log untuk AWS Trusted Advisor pemeriksaan.	8 Januari 2024

Dokumentasi diperbarui untuk Trusted Advisor	Memperbarui 1 pemeriksaan keamanan untuk mencermin kan perubahan dalam periode penghentian. Untuk informasi selengkapnya, lihat Mengubah log untuk AWS Trusted Advisor pemeriksaan.	21 Desember 2023
Dokumentasi diperbarui untuk Trusted Advisor	Ditambahkan 2 pemeriksaan keamanan dan 2 pemeriksa an kinerja. Untuk informasi selengkapnya, lihat Mengubah log untuk AWS Trusted Advisor pemeriksaan.	20 Desember 2023
Dokumentasi diperbarui untuk Trusted Advisor	Ditambahkan 1 pemeriksaan keamanan. Untuk informasi selengkapnya, lihat Mengubah log untuk AWS Trusted Advisor pemeriksaan.	15 Desember 2023
Dokumentasi yang diperbarui untuk Trusted Advisor Engage	Diperbarui dokumentasi Trusted Advisor Engage dengan perubahan untuk opsi pemberitahuan email.	14 Desember 2023
Dokumentasi yang diperbarui untuk Trusted Advisor Engage	Dokumentasi Trusted Advisor Engage yang diperbarui dengan perubahan untuk keterlibatan terjadwal.	Desember 11, 2023
Dokumentasi diperbarui untuk Trusted Advisor	Ditambahkan 2 pemeriksaan toleransi kesalahan baru dan 1 pemeriksaan optimasi biaya. Untuk informasi selengkapnya, lihat Mengubah log untuk AWS Trusted Advisor pemeriksaan.	Desember 7, 2023

Dokumentasi diperbarui untuk `AWSSupportServiceRolePolicy`	Menambahkan izin baru untuk menyediakan layanan penagihan, administratif, dan dukungan untuk peran terkait layanan. Untuk informasi selengkapnya, lihat kebijakan AWS terkelola: AWSSupportServiceRolePolicy.	6 Desember 2023
Kebijakan AWS terkelola yang diperbarui untuk Trusted Advisor	Memperbarui `AWSTrustedAdvisorPriorityFullAccess` dan `AWSTrustedAdvisorPriorityReadOnlyAccess` AWS mengelola kebijakan untuk menyertakan ID pernyataan. Untuk informasi selengkapnya, lihat kebijakan AWS terkelola untuk AWS Trusted Advisor.	6 Desember 2023
Dokumentasi diperbarui untuk Trusted Advisor	Ditambahkan 3 pemeriksaan toleransi kesalahan baru. Untuk informasi selengkapnya, lihat Mengubah log untuk AWS Trusted Advisor pemeriksaan.	17 November 2023
Dokumentasi diperbarui untuk Trusted Advisor	Menambahkan 37 cek baru untuk Amazon RDS. Untuk informasi selengkapnya, lihat Mengubah log untuk AWS Trusted Advisor pemeriksaan.	15 November 2023

Dokumentasi diperbarui untuk AWSTrustedAdvisorServiceRolePolicy	Menambahkan tindakan IAM baruec2:DescribeRegions ,s3:GetLifecycleConfiguration , ecs:DescribeTaskDefinition dan ecs:ListTaskDefinitions untuk onboard cek baru. Untuk informasi selengkapnya, lihat kebijakan AWS terkelola: AWSTrustedAdvisorServiceRolePolicy.	9 November 2023
Dokumentasi diperbarui untuk AWSSupportServiceRolePolicy	Menambahkan izin baru untuk menyediakan layanan penagihan, administratif, dan dukungan untuk peran terkait layanan. Untuk informasi selengkapnya, lihat kebijakan AWS terkelola: AWSSupportServiceRolePolicy.	Oktober 27, 2023
Dokumentasi diperbarui untuk Trusted Advisor	Menambahkan 64 cek baru terintegrasi dari AWS Config. Untuk informasi selengkapnya, lihat Mengubah log untuk AWS Trusted Advisor pemeriksaan.	26 Oktober 2023
Dokumentasi diperbarui untuk Trusted Advisor	Menambahkan enam pemeriksaan toleransi kesalahan baru Trusted Advisor. Untuk informasi selengkapnya, lihat log Perubahan untuk AWS Trusted Advisor pemeriksaan.	12 Oktober 2023

Dokumentasi diperbarui untuk AWSTrustedAdvisorServiceRolePolicy	Menambahkan tindakan IAM baru `route53resolver:ListResolverEndpoints`, `route53resolver:ListResolverEndpointIpAddresses`, `ec2:DescribeSubnets`, `kafka:ListClustersV2` dan `kafka:ListNodes` untuk melakukan pemeriksaan ketahanan baru. Untuk informasi selengkapnya, lihat kebijakan AWS terkelola: AWSTrustedAdvisorServiceRolePolicy.	14 September 2023
Dokumentasi diperbarui untuk AWSSupportServiceRolePolicy	Menambahkan izin baru untuk menyediakan layanan penagihan, administratif, dan dukungan untuk peran terkait layanan. Untuk informasi selengkapnya, lihat kebijakan AWS terkelola: AWSSupportServiceRolePolicy.	28 Agustus 2023
Dokumentasi diperbarui untuk Trusted Advisor	Ditambahkan 1 pemeriksaan batas layanan baru untuk AWS Lambda. Untuk informasi selengkapnya, lihat log Perubahan untuk AWS Trusted Advisor pemeriksaan.	17 Agustus 2023

Dokumentasi diperbarui untuk Trusted Advisor	Ditambahkan 1 pemeriksaan toleransi kesalahan baru untuk Lambda. Untuk informasi selengkapnya, lihat log Perubahan untuk AWS Trusted Advisor pemeriksaan.	3 Agustus 2023
Dokumentasi yang diperbarui untuk Trusted Advisor Engage	Dokumentasi Trusted Advisor Engage yang diperbarui dengan perubahan pada formulir untuk membuat dan mengedit keterlibatan. Ditambahkan halaman dengan Contoh Kebijakan Kontrol Layanan untuk AWS Trusted Advisor.	Juli 27, 2023
Dokumentasi diperbarui untuk `AWSSupportServiceRolePolicy`	Menambahkan izin baru untuk menyediakan layanan penagihan, administratif, dan dukungan untuk peran terkait layanan. Untuk informasi selengkapnya, lihat kebijakan AWS terkelola: AWSSupportServiceRolePolicy.	26 Juni 2023
Dokumentasi diperbarui untuk Trusted Advisor	Menambahkan dua pemeriksaan toleransi kesalahan baru untuk Amazon MQ. Menambahkan satu pemeriksaan toleransi kesalahan baru dan satu pemeriksaan kinerja baru untuk Amazon Elastic File System. Untuk informasi selengkapnya, lihat log Perubahan untuk AWS Trusted Advisor pemeriksaan.	1 Juni 2023

Dokumentasi diperbarui untuk Trusted Advisor	Menambahkan dua pemeriksaan toleransi kesalahan baru untuk NAT Gateway. Untuk informasi selengkapnya, lihat log Perubahan untuk AWS Trusted Advisor pemeriksaan.	16 Mei 2023
Dokumentasi diperbarui untuk AWS Support Rencana	Menambahkan izin dan CloudTrail dokumentasi baru untuk pembuatan jadwal rencana dukungan. Untuk informasi selengkapnya, lihat Mengelola akses ke AWS Support Paket, kebijakan AWS terkelola untuk panggilan API AWS SupportAWS Support Paket, dan Logging Plans dengan AWS CloudTrail.	8 Mei 2023
Dokumentasi diperbarui untuk `AWSSupportServiceRolePolicy`	Menambahkan izin baru untuk menyediakan layanan penagihan, administratif, dan dukungan untuk peran terkait layanan. Untuk informasi selengkapnya, lihat kebijakan AWS terkelola: AWSSupportServiceRolePolicy.	2 Mei 2023
Dokumentasi yang diperbarui untuk Trusted Advisor Engage dan Trusted Advisor Prioritas	Prasyarat yang diklarifikasi untuk Terlibat dan Prioritas . Trusted Advisor Trusted Advisor Menambahkan contoh kebijakan IAM dengan kemampuan untuk menggunakan Trusted Advisor Engage dan untuk mengaktifkan akses tepercaya ke Trusted Advisor.	28 April 2023

Dokumentasi diperbarui untuk Trusted Advisor	Menambahkan dua pemeriksaan toleransi kesalahan baru untuk AWS Resilience Hub dan Manajer Insiden. Untuk informasi selengkapnya, lihat log Perubahan untuk AWS Trusted Advisor pemeriksaan.	27 April 2023
Ditambahkan dokumentasi untuk Trusted Advisor Engage	Anda dapat menggunakan AWS Trusted Advisor Engage untuk mendapatkan hasil maksimal dari AWS Support Rencana Anda dengan memudahkan Anda melihat, meminta, dan melacak semua keterlibatan proaktif Anda, dan berkomunikasi dengan Akun AWS tim Anda tentang keterlibatan yang sedang berlangsung. Untuk informasi selengkapnya, lihat Memulai dengan AWS Trusted Advisor Engage.	6 April 2023
Dokumentasi diperbarui untuk Trusted Advisor	Menambahkan dua pemeriksaan toleransi kesalahan baru untuk Amazon ECS. Untuk informasi selengkapnya, lihat log Perubahan untuk AWS Trusted Advisor pemeriksaan.	30 Maret 2023

Dokumentasi diperbarui untuk `AWSSupportServiceRolePolicy`	Menambahkan izin baru untuk menyediakan layanan penagihan, administratif, dan dukungan untuk peran terkait layanan. Untuk informasi selengkapnya, lihat kebijakan AWS terkelola: AWSSupportServiceRolePolicy.	16 Maret 2023
Ditambahkan dokumentasi untuk Trusted Advisor Prioritas	Memperbarui konsol Trusted Advisor Prioritas: • Tombol Acknowledge and Dismiss telah menggantikan tombol Terima dan Tolak. • Anda tidak perlu memasukkan jabatan atau nama pekerjaan Anda untuk mengakui, menyelesaikan, memberhentikan, atau membuka kembali rekomendasi. Untuk informasi selengkapnya, lihat Memulai dengan Trusted Advisor Prioritas.	16 Februari 2023

Contoh kode yang diperbarui untuk AWS Support	Menambahkan contoh kode .NET, Java, dan Kotlin yang menunjukkan cara menggunakan AWS Support kit pengembangan AWS perangkat lunak (SDK). Untuk informasi selengkapnya, lihat Contoh kode untuk AWS Support menggunakan AWS SDK.	Januari 16, 2023
Dokumentasi diperbarui untuk `AWSSupportServiceRolePolicy`	Menambahkan izin baru untuk menyediakan layanan penagihan, administratif, dan dukungan untuk peran terkait layanan. Untuk informasi selengkapnya, lihat kebijakan AWS terkelola: AWSSupportServiceRolePolicy.	10 Januari 2023
Dokumentasi yang diperbarui untuk AWS Support App	Anda dapat mencari kasus dukungan di Slack dengan menggunakan opsi filter atau mencari berdasarkan ID kasus. Untuk informasi selengkapnya, lihat Mencari kasus dukungan di Slack.	Desember 29, 2022
Dokumentasi yang diperbarui untuk AWS Support App	Anda juga dapat menggunakan Terraform untuk membuat sumber daya Anda untuk Aplikasi. AWS Support Untuk informasi selengkapnya, lihat Membuat resource AWS Support Aplikasi menggunakan Terraform.	22 Desember 2022

Dokumentasi diperbarui untuk Trusted Advisor	Ditambahkan tiga pemeriksaan toleransi kesalahan baru untuk Amazon MemoryDB ElastiCache, Amazon, dan. AWS CloudHSM Untuk informasi selengkapnya, lihat log Perubahan untuk AWS Trusted Advisor pemeriksaan.	Desember 15, 2022
Dokumentasi yang diperbarui untuk AWS Support Aplikasi di Slack	Anda sekarang dapat meminta dukungan obrolan langsung untuk opsi berikut: • Kasus dukungan akun dan penagihan. • Dukungan bahasa Jepang untuk kasus dukungan teknis. • Untuk informasi selengkapnya, lihat Membuat kasus dukungan di saluran Slack.	14 Desember 2022
Dokumentasi diperbarui untuk AWS Support	Menambahkan dokumentasi tentang titik akhir baru untuk AWS Support API. Untuk informasi selengkapnya, lihat Tentang AWS Support API.	14 Desember 2022

Menambahkan dokumentasi untuk AWS CloudFormation template yang akan digunakan untuk AWS Support Aplikasi di Slack	Anda dapat menggunakan CloudFormation template untuk membuat ruang kerja dan saluran konfigurasi Slack untuk Akun AWS masuk. AWS Organizations Untuk informasi selengkapnya, lihat Membuat sumber daya AWS Support Aplikasi dengan AWS CloudFormation.	Desember 5, 2022
Dokumentasi diperbarui untuk Trusted Advisor	Menambahkan dua pemeriksaan toleransi kesalahan baru untuk AWS Resilience Hub. Untuk informasi selengkapnya, lihat log Perubahan untuk AWS Trusted Advisor pemeriksaan.	17 November 2022
Menambahkan dokumentasi untuk AWS Security Hub temuan Anda di Trusted Advisor	Temuan Anda dari kontrol Security Hub dihapus dari yang Trusted Advisor lebih cepat. Untuk informasi selengkapnya, lihat log Perubahan untuk AWS Trusted Advisor pemeriksaan.	17 November 2022
Dokumentasi diperbarui untuk AWS Trusted Advisor	Ditambahkan dokumentasi untuk Trusted Advisor Rekomendasi. Untuk informasi selengkapnya, lihat log Perubahan untuk AWS Trusted Advisor pemeriksaan.	16 November 2022

Dokumentasi yang diperbarui untuk AWS Support Aplikasi di Slack	Ditambahkan dokumentasi untuk dukungan bahasa Jepang. Untuk informasi selengkapnya, lihat Membuat kasus dukungan di saluran Slack.	11 November 2022
Dokumentasi diperbarui untuk AWS Support Rencana	Menambahkan informasi pemecahan masalah untuk memungkinkan Support Plans mengakses di organisasi. Untuk informasi selengkapnya, lihat Pemecahan Masalah.	9 November 2022
Dokumentasi yang diperbarui untuk AWS Support Aplikasi di Slack	Ditambahkan dokumentasi untuk `supportapp` izin. Untuk informasi selengkapnya, lihat Izin yang diperlukan agar AWS Support Aplikasi dapat terhubung ke Slack.	1 November 2022
Dokumentasi yang diperbarui untuk AWS Support Aplikasi di Slack	Anda dapat menggunakan operasi `RegisterSlackWorkspaceForOrganization` API untuk mendaftarkan ruang kerja Slack untuk Anda. Akun AWS Untuk memanggil API ini, akun Anda harus menjadi bagian dari organisasi di AWS Organizations. Untuk informasi selengkapnya, lihat AWS Support Aplikasi di Referensi API Slack.	Oktober 19, 2022

Dokumentasi diperbarui untuk AWSSupportServiceRolePolicy	Menambahkan izin baru untuk menyediakan layanan penagihan, administratif, dan dukungan untuk peran terkait layanan. Untuk informasi selengkapnya, lihat kebijakan AWS terkelola: AWSSupportServiceRolePolicy.	4 Oktober 2022
Dokumentasi yang diperbarui untuk Support Plans	Anda sekarang dapat menggunakan AWS Identity and Access Management (IAM) untuk mengelola izin untuk mengubah paket dukungan untuk Anda. Akun AWS Untuk informasi selengkapnya, lihat topik berikut. • Mengelola akses untuk AWS Support Rencana • AWS kebijakan terkelola untuk AWS Support Rencana • Mengubah AWS Support Rencana • Panggilan API AWS Support Rencana Logging dengan AWS CloudTrail	29 September 2022

Dokumentasi yang diperbarui untuk AWS Support Aplikasi di Slack	Menambahkan dokumentasi tentang cara mengonfigurasi saluran publik atau pribadi untuk digunakan dengan AWS Support Aplikasi. Untuk informasi selengkapnya, lihat Mengonfigurasi saluran Slack.	September 22, 2022
Dokumentasi diperbarui untuk AWS Support	Menambahkan bagian baru tentang keamanan untuk kasus dukungan Anda. Untuk informasi selengkapnya, lihat Keamanan untuk AWS Support kasus Anda.	9 September 2022
Dokumentasi diperbarui untuk Trusted Advisor	Menambahkan pemeriksa an keamanan baru untuk Amazon EC2. Untuk informasi selengkapnya, lihat log Perubahan untuk AWS Trusted Advisor pemeriksaan.	September 1, 2022

Dokumentasi yang diperbarui untuk AWS Support Aplikasi di Slack	Lihat topik berikut: Anda dapat menggunakan AWS Support Aplikasi untuk mengelola kasus dukungan, meminta peningkatan kuota layanan, dan mengobrol dengan agen dukungan langsung di saluran Slack Anda. Untuk informasi selengkapnya, lihat dokumentasi AWS Support App in Slack. Anda dapat melampirkan kebijakan AWS terkelola ke peran IAM Anda untuk menggunakan AWS Support Aplikasi. Untuk informasi selengkapnya, lihat kebijakan AWS terkelola untuk AWS Support Aplikasi di Slack. Referensi API baru untuk AWS Support Aplikasi. Lihat Referensi API AWS Support Aplikasi.	Agustus 24, 2022
Dokumentasi diperbarui untuk `AWSSupportServiceRolePolicy`	Menambahkan izin baru untuk menyediakan layanan penagihan, administratif, dan dukungan untuk peran terkait layanan. Untuk informasi selengkapnya, lihat kebijakan AWS terkelola: AWSSupportServiceRolePolicy.	17 Agustus 2022

Ditambahkan dokumentasi untuk Trusted Advisor Prioritas	Trusted Advisor Prioritas menambahkan dukungan untuk fitur-fitur berikut: • Administrator yang didelegasikan • Pemberitahuan email harian dan mingguan untuk ringkasan rekomendasi • Buka kembali rekomenda si yang diselesaikan atau ditolak • AWS kebijakan terkelola Untuk informasi selengkapnya, lihat Memulai dengan Trusted Advisor Prioritas.	17 Agustus 2022
Dokumentasi diperbarui untuk Trusted Advisor	Halaman Preferensi di Trusted Advisor konsol telah diperbaru i. Untuk informasi selengkap nya, lihat Memulai dengan AWS Trusted Advisor.	15 Juli 2022

Dokumentasi diperbarui untuk Trusted Advisor	Memperbarui cek untuk menyertakan informasi berikut: • Kriteria Peringatan • Tindakan yang Direkomendasikan • Sumber Daya Tambahan • Laporkan kolom Untuk informasi lebih lanjut, lihat referensi AWS Trusted Advisor cek.	Juli 7, 2022
Dokumentasi diperbarui untuk AWS Support	Menambahkan dokumentasi yang menjelaskan cara mengelola kasus dukungan Anda. • Memperbarui kasus dukungan yang ada • Pemecahan Masalah	Juni 28, 2022
Dokumentasi diperbarui untuk `AWSSupportServiceRolePolicy`	Izin yang diperbarui untuk menyediakan layanan penagihan, administratif, dan dukungan untuk peran terkait layanan. Untuk informasi selengkapnya, lihat kebijakan AWS terkelola: AWSSupportServiceRolePolicy.	Juni 23, 2022

Dokumentasi diperbarui untuk Trusted Advisor	Trusted Advisor mendukung kontrol standar keamanan AWS Foundational Security Best Practices tambahan yang bersumber dari. AWS Security Hub Untuk informasi selengkapnya, lihat log Perubahan untuk AWS Trusted Advisor pemeriksaan.	Juni 23, 2022
Dokumentasi diperbarui untuk Trusted Advisor	Menambahkan informasi tentang cara meminta kuota layanan meningkat. Untuk informasi selengkapnya, lihat Batas layanan.	21 Juni 2022
Dokumentasi diperbarui untuk AWS Support	Pengalaman membuat case telah diperbarui di Support Center Console. Untuk informasi selengkapnya, lihat Membuat kasus dukungan dan manajemen kasus.	Mei 18, 2022
Dokumentasi diperbarui untuk Trusted Advisor	Menambahkan empat cek untuk Amazon EBS dan AWS Lambda. Untuk informasi selengkapnya, lihat Memilih AWS Compute Optimizer untuk menambahkan Trusted Advisor cek.	4 Mei, 2022

Dokumentasi diperbarui untuk AWSSupportServiceRolePolicy	Menambahkan izin baru untuk menyediakan layanan penagihan, administratif, dan dukungan untuk peran terkait layanan. Untuk informasi selengkapnya, lihat kebijakan AWS terkelola: AWSSupportServiceRolePolicy.	27 April 2022
Dokumentasi yang diperbarui untuk pemeriksaan Exposed Access Keys	Pemeriksaan ini sekarang secara otomatis disegarkan untuk Anda. Untuk informasi selengkapnya, lihat Mengubah log untuk AWS Trusted Advisor pemeriksaan.	April 25, 2022
Dokumentasi diperbarui untuk Trusted Advisor	AWS Direct Connect Cek dalam kategori toleransi kesalahan diperbarui. Untuk informasi selengkapnya, lihat Mengubah log untuk AWS Trusted Advisor pemeriksaan.	29 Maret 2022
Dokumentasi diperbarui untuk AWSSupportServiceRolePolicy	Menambahkan izin baru untuk menyediakan layanan penagihan, administratif, dan dukungan untuk peran terkait layanan. Untuk informasi selengkapnya, lihat kebijakan AWS terkelola: AWSSupportServiceRolePolicy.	Maret 14, 2022

Ditambahkan dokumentasi untuk Trusted Advisor Prioritas	Anda dapat menggunakan Trusted Advisor Priority untuk melihat daftar rekomenda si yang diprioritaskan dari manajer akun teknis (TAM) Anda. Untuk informasi selengkapnya, lihat Memulai dengan Trusted Advisor Prioritas.	28 Februari 2022
Dokumentasi yang diperbarui untuk menggunakan Amazon EventBridge untuk Trusted Advisor	Anda dapat membuat EventBridge aturan untuk memantau perubahan pada Trusted Advisor cek Anda. Untuk informasi selengkapnya, lihat Memantau hasil AWS Trusted Advisor pemeriksaan dengan EventBridge.	Februari 21, 2022
Dokumentasi baru untuk menggunakan Amazon EventBridge untuk memantau AWS Support kasus	Anda dapat membuat EventBridge aturan untuk memantau dan menerima pemberitahuan tentang kasus dukungan Anda. Untuk informasi selengkapnya, lihat Memantau AWS Support k asus dengan EventBridge.	Februari 21, 2022
Dokumentasi diperbarui untuk `AWSSupportServiceR olePolicy`	Menambahkan izin baru untuk menyediakan layanan penagihan, administratif, dan dukungan untuk peran terkait layanan. Untuk informasi selengkapnya, lihat kebijakan AWS terkelola: AWSSuppor tServiceRolePolicy.	Februari 17, 2022

Ditambahkan dokumentasi untuk mengintegrasikan dengan AWS Security Hub	Di Trusted Advisor konsol, Anda sekarang dapat melihat temuan untuk kontrol Security Hub yang merupakan bagian dari standar keamanan Praktik Terbaik Keamanan AWS Dasar. Untuk informasi selengkapnya, lihat Melihat AWS Security Hub kontrol di AWS Trusted Advisor konsol.	18 Januari 2022
Dokumentasi diperbarui untuk Trusted Advisor	Menambahkan tiga pemeriksaan baru untuk instans Amazon EC2 yang menjalankan Microsoft SQL Server. • Amazon EC2 Instans Konsolidasi untuk Microsoft SQL Server • Instans Amazon EC2 disediakan secara berlebihan untuk Microsoft SQL Server • Instans Amazon EC2 dengan dukungan akhir Microsoft SQL Server Untuk informasi lebih lanjut, lihat referensi AWS Trusted Advisor cek.	Desember 20, 2021

Dokumentasi diperbarui untuk Trusted Advisor	Trusted Advisor menambahkan empat cek baru untuk AWS Well-Architected • AWS Well-Architectedmasalah risiko tinggi untuk optimalisasi biaya • AWS Well-Architectedmasalah risiko tinggi untuk kinerja • AWS Well-Architectedmasalah risiko tinggi untuk keamanan • AWS Well-Architectedmasalah risiko tinggi untuk keandalan Untuk informasi lebih lanjut, lihat referensi AWS Trusted Advisor cek.	Desember 20, 2021
Dokumentasi diperbarui	Jika Anda memiliki paket Enterprise On-Ramp Support, Anda memiliki akses ke semua Trusted Advisor pemeriksaan dan API. AWS Support	24 November 2021
Dokumentasi diperbarui untuk Trusted Advisor	Trusted Advisor menambahkan dua cek baru untuk Amazon Comprehend. Untuk informasi lebih lanjut, lihat referensi AWS Trusted Advisor cek.	29 September 2021

Dokumentasi diperbarui untuk Trusted Advisor	Nama cek untuk Amazon OpenSearch Service Reserved Instance Optimization telah diperbarui. Untuk informasi selengkapnya, lihat Mengubah log untuk AWS Trusted Advisor pemeriksaan.	8 September 2021
Dokumentasi yang diperbarui untuk Trusted Advisor pemeriksaan	Menambahkan topik referensi untuk semua Trusted Advisor pemeriksaan. Untuk informasi lebih lanjut, lihat referensi AWS Trusted Advisor cek.	1 September 2021
Dokumentasi yang diperbarui untuk kebijakan Trusted Advisor terkelola	Dokumentasi yang diperbarui untuk kebijakan Trusted Advisor terkelola. Untuk informasi selengkapnya, lihat kebijakan AWS terkelola untuk AWS Support dan AWS Trusted Advisor.	Agustus 10, 2021
Dokumentasi diperbarui untuk Trusted Advisor	Dokumentasi yang diperbarui untuk Trusted Advisor konsol. Untuk informasi selengkapnya, lihat Memulai dengan AWS Trusted Advisor.	16 Juli 2021
Dokumentasi diperbarui untuk membuat AWS Support kasus	Menambahkan dokumentasi tentang cara membuat kasus dukungan terkait untuk kasus yang ditutup secara permanen. Untuk informasi selengkapnya, lihat Membuka kembali kasus tertutup dan Membuat kasus terkait.	8 Juni 2021

Dokumentasi diperbarui untuk Trusted Advisor	Trusted Advisor menambahkan dua cek baru untuk penyimpanan volume Amazon Elastic Block Store (Amazon EBS) EBS). Untuk informasi selengkapnya, lihat Mengubah log untuk AWS Trusted Advisor pemeriksaan.	8 Juni 2021
Dokumentasi diperbarui	Memperbarui topik berikut: • Prosedur yang diperbarui dan menambahkan konten ke CloudWatch alarm Membuat Amazon untuk memantau topik AWS Trusted Advisor metrik • Menambahkan kuota Layanan untuk bagian AWS Support API	12 Mei 2021

Pembaruan sebelumnya

Perubahan	Deskripsi	Tanggal
Dokumentasi diperbarui untuk Trusted Advisor	Menambahkan dokumentasi untuk memfilter, menyegarkan, dan mengunduh hasil pemeriksaan. Untuk informasi lebih lanjut, lihat bagian berikut: • Memfilter pemeriksaan Anda • Menyegarkan hasil pemeriksaan • Mengunduh hasil pemeriksaan	16 Maret 2021
Dokumentasi yang diperbarui tentang	Menambahkan informasi tentang kebijakan `AWSSupportServiceRolePolicy` AWS	16 Maret 2021

Perubahan	Deskripsi	Tanggal
kebijakan AWS terkelola	terkelola. Untuk informasi selengkapnya, lihat Menggunakan peran terkait layanan untuk AWS Support.	
Ditambahkan cek untuk AWS Lambda	Menambahkan empat AWS Trusted Advisor cek untuk Lambda di. Ubah log untuk AWS Trusted Advisor	8 Maret 2021
Memperbarui pemeriksaan service limits untuk Amazon Elastic Block Store	Memperbarui lima AWS Trusted Advisor pemeriksaan untuk Amazon EBS di. Ubah log untuk AWS Trusted Advisor	5 Maret 2021
Dokumentasi yang diperbarui untuk CloudTrail logging	CloudTrail mendukung pencatatan untuk tindakan konsol saat Anda mengubah AWS Support paket. Untuk informasi selengkap nya, lihat Mencatat perubahan ke paket AWS Support Anda.	9 Februari 2021
Dokumentasi diperbarui untuk Trusted Advisor	Memperbarui topik Memulai dengan Trusted Advisor Rekomendasi.	29 Januari 2021
Dokumentasi yang diperbarui untuk Trusted Advisor laporan	Menambahkan Pemecahan Masalah bagian untuk menggunakan Trusted Advisor laporan dengan AWS layanan lain.	4 Desember 2020
Ditambahkan AWS Trusted Advisor dukungan untuk AWS CloudTrail logging	CloudTrail mendukung pencatatan untuk subset tindakan Trusted Advisor konsol. Untuk informasi selengkapnya, lihat Mencatat tindakan AWS Trusted Advisor konsol dengan AWS CloudTrail.	23 November 2020
Menambahkan topik log perubahan	Lihat perubahan pada AWS Trusted Advisor pemeriksaan dan kategori diUbah log untuk AWS Trusted Advisor.	18 November 2020

Perubahan	Deskripsi	Tanggal
Menambahkan dukungan untuk unit organisasi	Anda sekarang dapat membuat laporan untuk Trusted Advisor pemeriksaan unit organisasi (OU). Untuk informasi selengkapnya, lihat Membuat laporan tampilan organisasi.	17 November 2020
Memperbarui logging dengan AWS CloudTrail topik	Menambahkan entri log contoh untuk operasi Trusted Advisor API. Lihat AWS Trusted Advisorinformasi dalam CloudTrail logging.	22 Oktober 2020
Menambahkan AWS Support kuota	Menambahkan informasi tentang kuota saat ini dan pembatasan untuk AWS Support. Lihat AWS Support titik akhir dan kuota di. Referensi Umum AWS	4 Agustus 2020
Pandangan organisasi untuk AWS Trusted Advisor	Anda sekarang dapat membuat laporan untuk Trusted Advisor cek untuk akun yang merupakan bagian dari AWS Organizations. Lihat Tampilan organisasi untuk AWS Trusted Advisor.	17 Juli 2020
Keamanan dan AWS Support	Informasi terbaru tentang pertimbangan keamanan saat menggunakan AWS Support dan Trusted Advisor. Lihat Keamanan di AWS Support	5 Mei 2020
Keamanan dan AWS Support	Menambahkan informasi tentang pertimbangan keamanan saat menggunakan AWS Support.	10 Januari 2020
Menggunakan Trusted Advisor sebagai layanan web	Menambahkan instruksi yang diperbarui untuk menyegarkan Trusted Advisor data setelah mendapatkan daftar Trusted Advisor cek.	1 November 2018
Menggunakan peran terkait Layanan	Menambahkan bagian baru.	11 Juli 2018
Memulai: Pemecahan Masalah	Menambahkan tautan pemecahan masalah untuk Route 53 dan AWS Certificate Manager.	1 September 2017

Perubahan	Deskripsi	Tanggal
Contoh Manajemen Kasus: Membuat Kasus	Menambahkan catatan tentang kotak CC untuk pengguna yang memiliki paket Basic Support.	1 Agustus 2017
Memantau Hasil Trusted Advisor Pemeriksaan dengan CloudWatch Acara	Menambahkan bagian baru.	18 November 2016
Manajemen Kasus	Memperbarui nama-nama tingkat kepelikan kasus.	27 Oktober 2016
Logging AWS Support Panggilan dengan AWS CloudTrail	Menambahkan bagian baru.	21 April 2016
Memulai: Pemecahan Masalah	Menambahkan tautan pemecahan masalah lainnya.	19 Mei 2015
Memulai: Pemecahan Masalah	Menambahkan tautan pemecahan masalah lainnya.	18 November 2014
Memulai: Manajemen Kasus	Diperbarui untuk mencerminkan Service Catalog di AWS Management Console.	30 Oktober 2014
Pemrograman Kehidupan Sebuah AWS Support Kasus	Menambahkan informasi tentang elemen API baru untuk menambahkan lampiran ke kasus dan untuk menghilangkan komunikasi kasus saat mengambil riwayat kasus.	16 Juli 2014
Mengakses AWS Support	Menghapus kontak dukungan bernama sebagai metode akses.	28 Mei 2014
Memulai	Menambahkan bagian Memulai.	13 Desember 2013
Publikasi awal	AWS Support Layanan baru dirilis.	30 April 2013

AWSGlosarium

Untuk AWS terminologi terbaru, lihat AWSglosarium di Referensi. Glosarium AWS

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