aws

Panduan Pengguna

AWS Audit Manager

AWS Audit Manager: Panduan Pengguna

Table of Contents

Apakah AWS Audit Manager itu?

Selamat datang di Panduan AWS Audit Manager Pengguna.

AWS Audit Managermembantu Anda terus mengaudit AWS penggunaan Anda untuk menyederhanakan cara Anda mengelola risiko dan kepatuhan terhadap peraturan dan standar industri. Audit Manager mengotomatiskan pengumpulan bukti sehingga Anda dapat lebih mudah menilai apakah kebijakan, prosedur, dan aktivitas Anda — juga dikenal sebagai kontrol — beroperasi secara efektif. Saat tiba waktunya untuk audit, Audit Manager membantu Anda mengelola tinjauan pemangku kepentingan atas kontrol Anda. Ini berarti Anda dapat membuat laporan siap audit dengan upaya manual yang jauh lebih sedikit.

Audit Manager menyediakan kerangka kerja bawaan yang menyusun dan mengotomatiskan penilaian untuk standar atau peraturan kepatuhan tertentu. Kerangka kerja mencakup kumpulan kontrol bawaan dengan deskripsi dan prosedur pengujian. Kontrol ini dikelompokkan sesuai dengan persyaratan standar atau peraturan kepatuhan yang ditentukan. Anda juga dapat menyesuaikan kerangka kerja dan kontrol untuk mendukung audit internal sesuai dengan kebutuhan spesifik Anda.

Anda dapat membuat penilaian dari kerangka kerja apa pun. Saat Anda membuat penilaian, Audit Manager secara otomatis menjalankan penilaian sumber daya. Penilaian ini mengumpulkan data untuk layanan Akun AWS dan layanan yang Anda definisikan sebagai cakupan audit Anda. Data yang dikumpulkan secara otomatis diubah menjadi bukti yang ramah audit. Kemudian, itu dilampirkan ke kontrol yang relevan untuk membantu Anda menunjukkan kepatuhan dalam keamanan, manajemen perubahan, kelangsungan bisnis, dan lisensi perangkat lunak. Proses pengumpulan bukti ini sedang berlangsung, dan dimulai saat Anda membuat penilaian. Setelah Anda menyelesaikan audit dan Anda tidak lagi memerlukan Audit Manager untuk mengumpulkan bukti, Anda dapat menghentikan pengumpulan bukti. Untuk melakukan ini, ubah status penilaian Anda menjadi tidak aktif.

Fitur Audit Manager

DenganAWS Audit Manager, Anda dapat melakukan tugas-tugas berikut:

- Mulailah dengan cepat — Buat penilaian pertama Anda dengan memilih dari galeri kerangka kerja bawaan yang mendukung berbagai standar dan peraturan kepatuhan. Kemudian, mulailah pengumpulan bukti otomatis untuk mengaudit Layanan AWS penggunaan Anda.

- Unggah dan kelola bukti dari lingkungan hybrid atau multicloud — Selain bukti yang dikumpulkan Audit Manager dari AWS lingkungan Anda, Anda juga dapat mengunggah dan mengelola bukti secara terpusat dari lingkungan lokal atau multicloud Anda.
- Mendukung standar dan peraturan kepatuhan umum — Pilih salah satu kerangka kerja AWS Audit Manager standar. Kerangka kerja ini menyediakan pemetaan kontrol bawaan untuk standar dan peraturan kepatuhan umum. Ini termasuk Tolok Ukur Yayasan CIS, PCI DSS, GDPR, HIPAA, SOC2, GxP, dan praktik terbaik operasional. AWS
- Pantau penilaian aktif Anda — Gunakan dasbor Audit Manager untuk melihat data analitik untuk penilaian aktif Anda, dan dengan cepat mengidentifikasi bukti yang tidak sesuai yang perlu diperbaiki.
- Cari bukti — Gunakan fitur pencari bukti untuk menemukan bukti yang relevan dengan kueri penelusuran Anda dengan cepat. Anda dapat membuat laporan penilaian dari hasil penelusuran, atau mengekspor hasil pencarian Anda dalam format CSV.
- Buat kontrol khusus - Buat kontrol Anda sendiri dari awal atau sesuaikan kontrol yang ada untuk memenuhi kebutuhan Anda. Anda juga dapat menggunakan fitur kontrol khusus untuk membuat pertanyaan penilaian risiko dan menyimpan tanggapan atas pertanyaan tersebut sebagai bukti manual.
- Kustomisasi kerangka kerja — Buat kerangka kerja Anda sendiri dengan kontrol standar atau kustom berdasarkan persyaratan spesifik Anda untuk audit internal.
- Bagikan kerangka kerja kustom — Bagikan kerangka kerja Audit Manager kustom Anda dengan yang lainAkun AWS, atau tiru ke yang lain Wilayah AWS di bawah akun Anda sendiri.
- Support kolaborasi lintas tim - Delegasikan set kontrol ke ahli materi pelajaran yang dapat meninjau bukti terkait, menambahkan komentar, dan memperbarui status setiap kontrol.
- Buat laporan untuk auditor — Buat laporan penilaian yang merangkum bukti relevan yang dikumpulkan untuk audit Anda dan tautkan ke folder yang berisi bukti terperinci.
- Pastikan integritas bukti — Simpan bukti di lokasi yang aman, di mana ia tetap tidak berubah.

> **Note**
>
> AWS Audit Managermembantu mengumpulkan bukti yang relevan untuk memverifikasi kepatuhan terhadap standar dan peraturan kepatuhan tertentu. Namun, itu tidak menilai kepatuhan Anda sendiri. AWS Audit ManagerOleh karena itu, bukti yang dikumpulkan mungkin tidak mencakup semua informasi tentang AWS penggunaan Anda yang diperlukan untuk audit. AWS Audit Managerbukan pengganti penasihat hukum atau pakar kepatuhan.

Harga untuk Audit Manager

Untuk informasi selengkapnya tentang harga, lihat AWS Audit Manager Harga.

Apakah Anda pengguna pertama kali Audit Manager?

Jika Anda adalah pengguna Audit Manager pertama kali, kami sarankan Anda memulai dengan halaman berikut:

1. AWS Audit Managerkonsep dan terminologi - Pelajari tentang konsep dan istilah kunci yang digunakan dalam Audit Manager, seperti penilaian, kerangka kerja, dan kontrol.
2. Cara AWS Audit Manager mengumpulkan bukti — Pelajari cara Audit Manager mengumpulkan bukti untuk penilaian sumber daya.
3. Menyiapkan — Pelajari tentang persyaratan penyiapan untuk Audit Manager.
4. Memulai — Ikuti tutorial untuk membuat penilaian Audit Manager pertama Anda.
5. AWS Audit ManagerReferensi API — Biasakan diri Anda dengan tindakan dan tipe data Audit Manager API.

Sumber daya Audit Manager lainnya

Jelajahi sumber daya berikut untuk mempelajari lebih lanjut tentang Audit Manager.

- Kumpulkan Bukti dan Kelola Data Audit Menggunakan AWS Audit Manager
- Konfigurasikan penilaian Audit Manager kustom secara manual dari AWSLokakarya
- Integrasikan di seluruh Model Tiga Garis (Bagian 2): Ubah paket AWS Config kesesuaian menjadi AWS Audit Manager penilaian dari Blog Manajemen & Tata Kelola AWS

AWS Audit Managerkonsep dan terminologi

Untuk membantu Anda memulai, halaman ini mendefinisikan istilah dan menjelaskan beberapa konsep AWS Audit Manager kunci.

A

A| B | C | D E | F | | G | H | I | J | K | L | M | N | O | P R | T S | T | U | W | X | Y | Z

Penilaian

Anda dapat menggunakan penilaian Audit Manager untuk secara otomatis mengumpulkan bukti yang relevan untuk audit.

Penilaian didasarkan pada kerangka kerja, yang merupakan pengelompokan kontrol yang terkait dengan audit Anda. Bergantung pada kebutuhan bisnis Anda, Anda dapat membuat penilaian dari kerangka kerja standar atau kerangka kerja khusus. Kerangka kerja standar berisi set kontrol bawaan yang mendukung standar atau peraturan kepatuhan tertentu. Sebaliknya, kerangka kerja khusus berisi kontrol yang dapat Anda sesuaikan dan kelompokkan sesuai dengan persyaratan audit internal Anda. Menggunakan kerangka kerja sebagai titik awal, Anda dapat membuat penilaian yang menentukan Akun AWS dan layanan yang ingin Anda sertakan dalam lingkup audit Anda.

Saat Anda membuat penilaian, Audit Manager secara otomatis mulai menilai sumber daya di Akun AWS dan layanan Anda berdasarkan kontrol yang ditentukan dalam kerangka kerja. Selanjutnya, ia mengumpulkan bukti yang relevan dan mengubahnya menjadi format yang ramah auditor. Setelah melakukan ini, kemudian melampirkan bukti ke kontrol dalam penilaian Anda. Ketika tiba waktunya untuk audit, Anda—atau delegasi pilihan Anda—dapat meninjau bukti yang dikumpulkan dan kemudian menambahkannya ke laporan penilaian. Laporan penilaian ini membantu Anda menunjukkan bahwa kontrol Anda berfungsi sebagaimana mestinya.

Pengumpulan bukti adalah proses berkelanjutan yang dimulai saat Anda membuat penilaian. Anda dapat menghentikan pengumpulan bukti dengan mengubah status penilaian menjadi tidak aktif. Atau, Anda dapat menghentikan pengumpulan bukti di tingkat kontrol. Anda dapat melakukan ini dengan mengubah status kontrol tertentu dalam penilaian Anda menjadi tidak aktif.

Untuk petunjuk tentang cara membuat dan mengelola penilaian, lihatPenilaian di AWS Audit Manager.

Laporan penilaian

Laporan penilaian adalah dokumen final yang dihasilkan dari penilaian Audit Manager. Laporan ini merangkum bukti relevan yang dikumpulkan untuk audit Anda. Mereka menautkan ke folder bukti yang relevan. Folder diberi nama dan diatur sesuai dengan kontrol yang ditentukan dalam penilaian Anda. Untuk setiap penilaian, Anda dapat meninjau bukti yang dikumpulkan Audit Manager, dan memutuskan bukti mana yang ingin Anda sertakan dalam laporan penilaian.

Untuk mempelajari lebih lanjut tentang laporan penilaian, lihatLaporan penilaian. Untuk mempelajari cara membuat laporan penilaian, lihatMenghasilkan laporan penilaian.

Tujuan laporan penilaian

Tujuan laporan penilaian adalah bucket S3 default tempat Audit Manager menyimpan laporan penilaian Anda. Untuk mempelajari selengkapnya, lihat Tujuan laporan penilaian (opsional).

Audit

Audit adalah pemeriksaan independen terhadap aset, operasi, atau integritas bisnis organisasi Anda. Audit teknologi informasi (TI) secara khusus memeriksa kontrol dalam sistem informasi organisasi Anda. Tujuan dari audit TI adalah untuk menentukan apakah sistem informasi melindungi aset, beroperasi secara efektif, dan menjaga integritas data. Semua ini penting untuk memenuhi persyaratan peraturan yang diamanatkan oleh standar atau peraturan kepatuhan.

Pemilik audit

Istilah pemilik audit memiliki dua arti yang berbeda tergantung pada konteksnya.

Dalam konteks Audit Manager, pemilik audit adalah pengguna atau peran yang mengelola penilaian dan sumber daya terkait. Tanggung jawab persona Audit Manager ini meliputi membuat penilaian, meninjau bukti, dan menghasilkan laporan penilaian. Audit Manager adalah layanan kolaboratif, dan pemilik audit mendapat manfaat ketika pemangku kepentingan lain berpartisipasi dalam penilaian mereka. Misalnya, Anda dapat menambahkan pemilik audit lain ke penilaian Anda untuk berbagi tugas manajemen. Atau, jika Anda adalah pemilik audit dan Anda memerlukan bantuan untuk menafsirkan bukti yang dikumpulkan untuk kontrol, Anda dapat mendelegasikan kontrol itu kepada pemangku kepentingan yang memiliki keahlian materi pelajaran di bidang tersebut. Orang seperti itu dikenal sebagai persona delegasi.

Dalam istilah bisnis, pemilik audit adalah seseorang yang mengoordinasikan dan mengawasi upaya kesiapan audit perusahaan mereka, dan menyajikan bukti kepada auditor. Biasanya, ini adalah profesional tata kelola, risiko, dan kepatuhan (GRC), seperti Petugas Kepatuhan atau Petugas Perlindungan Data GDPR. Profesional GRC memiliki keahlian dan wewenang untuk mengelola persiapan audit. Lebih khusus lagi, mereka memahami persyaratan kepatuhan, dan dapat menganalisis, menafsirkan, dan menyiapkan data pelaporan. Namun, peran bisnis lainnya juga dapat mengasumsikan persona Audit Manager dari pemilik audit — tidak hanya profesional GRC yang mengambil peran ini. Misalnya, Anda dapat memilih agar penilaian Audit Manager disiapkan dan dikelola oleh pakar teknis dari salah satu tim berikut:

- SecOps
- IT/ DevOps
- Pusat Operasi Keamanan/Respon Insiden

- Tim serupa yang memiliki, mengembangkan, memulihkan, dan menyebarkan aset cloud, serta memahami infrastruktur cloud organisasi Anda

Siapa yang Anda pilih untuk ditetapkan sebagai pemilik audit dalam penilaian Audit Manager Anda sangat bergantung pada organisasi Anda. Itu juga tergantung pada bagaimana Anda menyusun operasi keamanan Anda dan spesifikasi audit. Dalam Audit Manager, individu yang sama dapat mengasumsikan persona pemilik audit dalam satu penilaian, dan persona delegasi di penilaian lain.

Tidak peduli bagaimana Anda memilih untuk menggunakan Audit Manager, Anda dapat mengelola pemisahan tugas di seluruh organisasi Anda menggunakan persona pemilik audit/delegasi dan memberikan kebijakan IAM khusus kepada setiap pengguna. Melalui pendekatan dua langkah ini, Audit Manager memastikan bahwa Anda memiliki kendali penuh atas semua spesifikasi penilaian individu. Untuk informasi selengkapnya, lihat Kebijakan yang disarankan untuk persona pengguna di AWS Audit Manager.

C

A| B | C | D E | F | | G | H | I | J | K | L | M | N | O | P R | T S | T | U | W | X | Y | Z

Changelog

Untuk setiap kontrol dalam penilaian, Audit Manager menangkap changelog untuk melacak aktivitas pengguna untuk kontrol tersebut. Anda kemudian dapat meninjau jejak audit aktivitas yang terkait dengan kontrol tertentu. Untuk informasi selengkapnya tentang aktivitas pengguna yang ditangkap di changelog, lihat. Tab Changelog

Kepatuhan cloud

Kepatuhan cloud adalah prinsip umum bahwa sistem yang dikirim cloud harus sesuai dengan standar yang dihadapi oleh pelanggan cloud.

Peraturan kepatuhan

Peraturan kepatuhan adalah hukum, aturan, atau perintah lain yang ditentukan oleh otoritas, biasanya untuk mengatur perilaku. Salah satu contohnya adalah GDPR.

Standar kepatuhan

Standar kepatuhan adalah seperangkat pedoman terstruktur yang merinci proses organisasi untuk mempertahankan sesuai dengan peraturan, spesifikasi, atau undang-undang yang ditetapkan. Contohnya termasuk PCI DSS dan HIPAA.

Pengendalian

Kontrol adalah perlindungan atau penanggulangan yang ditentukan untuk sistem informasi atau organisasi. Kontrol dirancang untuk melindungi kerahasiaan, integritas, dan ketersediaan informasi Anda, dan untuk memenuhi serangkaian persyaratan keamanan yang ditetapkan. Mereka memberikan jaminan bahwa sumber daya Anda beroperasi sebagaimana dimaksud, data Anda dapat diandalkan, dan organisasi Anda mematuhi hukum dan peraturan yang berlaku.

Dalam Audit Manager, kontrol juga dapat mewakili pertanyaan dalam kuesioner penilaian risiko vendor. Dalam hal ini, kontrol adalah pertanyaan spesifik yang menanyakan informasi tentang keamanan dan postur kepatuhan organisasi.

Kontrol mengumpulkan bukti secara terus-menerus saat mereka aktif dalam penilaian Audit Manager Anda. Anda juga dapat menambahkan bukti secara manual ke kontrol apa pun. Setiap bukti menjadi catatan yang membantu Anda menunjukkan kepatuhan terhadap persyaratan kontrol.

Ada dua jenis kontrol di Audit Manager:

- Kontrol standar — Ini adalah kontrol bawaan yang terkait dengan kerangka kerja tertentu di Audit Manager. Gunakan kontrol standar untuk membantu Anda dengan persiapan audit untuk berbagai standar kepatuhan dan peraturan.
- Kontrol kustom — Ini adalah kontrol khusus yang Anda tentukan sebagai pengguna Audit Manager. Gunakan kontrol khusus untuk membantu Anda memenuhi persyaratan kepatuhan khusus untuk audit internal atau penilaian risiko vendor.

Untuk informasi selengkapnya, lihat Contoh AWS Audit Manager kontrol. Untuk petunjuk tentang cara membuat dan mengelola kontrol, lihatPustaka kontrol.

Domain kontrol

Anda dapat menganggap domain kontrol sebagai kategori umum kontrol yang tidak spesifik untuk satu kerangka kerja. Pengelompokan domain kontrol adalah salah satu fitur paling canggih dari dasbor Audit Manager. Audit Manager menyoroti kontrol dalam penilaian Anda yang memiliki bukti yang tidak sesuai, dan mengelompokkannya berdasarkan domain kontrol. Ini memungkinkan Anda untuk memfokuskan upaya remediasi Anda pada domain subjek tertentu saat Anda mempersiapkan audit.

> **Note**
>
> Domain kontrol berbeda dengan set kontrol. Set kontrol adalah pengelompokan kontrol khusus kerangka kerja yang biasanya ditentukan oleh badan pengatur. Misalnya, kerangka kerja PCI DSS memiliki set kontrol bernama Persyaratan 8: Identifikasi dan otentikasi akses ke komponen sistem. Set kontrol ini berada di bawah domain kontrol Identitas dan manajemen akses.

Audit Manager mengkategorikan kontrol di bawah domain kontrol berikut.

Kontrol nama domain	Deskripsi tentang apa yang diatur oleh kontrol ini
Kelangsungan bisnis dan perencanaan kontingensi	Bagaimana Anda menetapkan proses yang melindungi operasi bisnis penting dari efek gangguan sistem dan jaringan utama.
Manajemen perubahan	Bagaimana Anda menguji, menyetujui, menerapkan, dan mendokumentasikan perubahan pada infrastruktur cloud Anda.
Keamanan dan privasi data	Bagaimana Anda mengamankan privasi, ketersediaan, dan integritas data Anda.
Pengembangan dan manajemen konfigurasi	Bagaimana Anda memelihara infrastruktur cloud Anda dalam keadaan yang diinginkan dan konsisten.
Tata kelola dan pengawasan	Bagaimana Anda menyelaraskan penggunaan komputasi awan dengan kewajiban hukum, peraturan, dan etika Anda.
Pengelolaan identitas dan akses	Bagaimana Anda memastikan bahwa pengguna yang tepat memiliki akses yang tepat ke sumber daya teknologi Anda.
Manajemen insiden	Bagaimana Anda menetapkan tanggung jawab dan prosedur yang memastikan respons yang cepat dan efektif terhadap insiden keamanan.

Kontrol nama domain	Deskripsi tentang apa yang diatur oleh kontrol ini
Pencatatan dan pemantauan	Bagaimana Anda meninjau aktivitas pengguna untuk indikasi bahwa aktivitas yang tidak sah telah dicoba atau dilakukan.
Manajemen jaringan	Bagaimana Anda mengelola dan mengoperasikan jaringan data Anda menggunakan sistem manajemen jaringan.
Manajemen personalia	Bagaimana Anda menilai dan mengelola risiko keamanan personel di tingkat organisasi
Keamanan fisik	Bagaimana Anda mendeteksi dan mencegah masalah keamanan fisik di fasilitas Anda.
Manajemen risiko	Bagaimana Anda mengevaluasi potensi risiko dan kerugian, dan bagaimana Anda mengurangi atau menghilangkan ancaman tersebut.
Manajemen rantai pasokan	Bagaimana Anda mengidentifikasi, menilai, dan mengurangi risiko yang terkait dengan produk TI, vendor, dan rantai pasokan.
Manajemen perangkat pengguna	Bagaimana Anda mengurangi risiko bahwa perangkat keras TI karyawan Anda hilang, rusak, atau terganggu.
Manajemen kerentanan	Bagaimana Anda mendefinisikan, menilai, dan memulihkan semua kerentanan yang diketahui untuk aset dalam infrastruktur cloud Anda.

D

A| B | C | D E | F | | G | H | I | J | K | L | M | N | O | P R | T S | T | U | W | X | Y | Z

Sumber data

Audit Manager menggunakan sumber data untuk mengumpulkan bukti untuk kontrol. Terminologi berikut menjelaskan apa itu sumber data dan cara kerjanya.

- Tipe sumber data menentukan dari mana Audit Manager mengumpulkan bukti untuk kontrol. Jika Anda mengunggah bukti Anda sendiri, tipe sumber datanya adalah Manual. Jika Audit Manager mengumpulkan bukti atas nama Anda, tipe sumber data adalah salah satu dari

yang berikut: AWS Security Hub,, AWS ConfigAWS CloudTrail, atau panggilan AWS API. Audit Manager API mengacu pada tipe sumber data sebagai SourceType (tunggal) atau ControlSources (jamak).

- Pemetaan adalah kata kunci spesifik yang berhubungan dengan tipe sumber data. Misalnya, ini mungkin nama CloudTrail acara atau AWS Config nama. Audit Manager API mengacu pada ini sebagai SourceKeyword (tunggal) atau controlMappingSources(jamak).
- Nama sumber data adalah nama yang diberikan ke sumber data. Dengan kata lain, nama sumber data memberi label kombinasi tipe sumber data dan pemetaan. Untuk kontrol standar, Audit Manager menyediakan nama sumber data default (seperti Sumber data 1 dan Sumber data 2). Untuk kontrol kustom, Anda dapat memberikan nama sumber data Anda sendiri. Ini mungkin membantu Anda membedakan antara beberapa pemetaan yang termasuk dalam tipe sumber data yang sama. Audit Manager API mengacu pada nama sumber data sebagai SourceName.

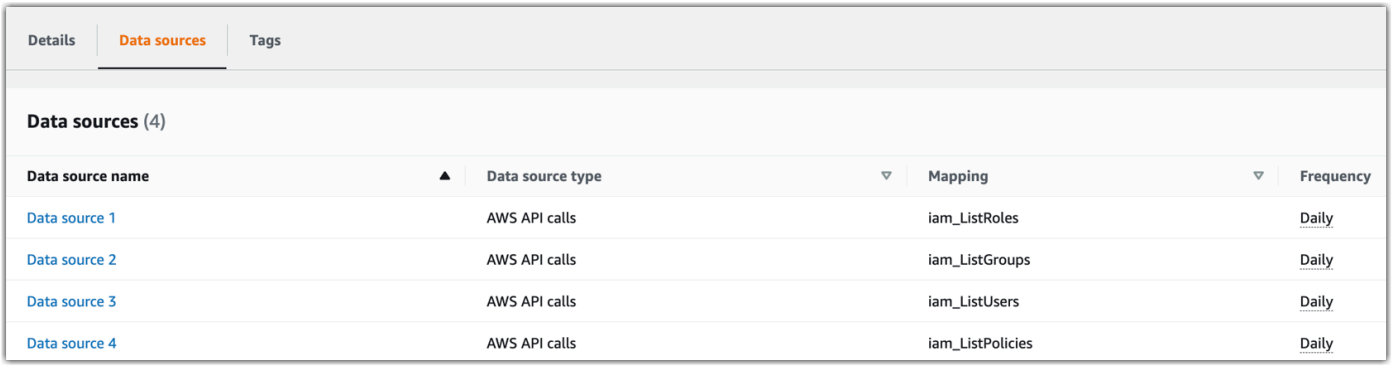
Kontrol tunggal dapat memiliki beberapa tipe sumber data dan beberapa pemetaan. Misalnya, satu kontrol mungkin mengumpulkan bukti dari campuran tipe sumber data (seperti AWS Config dan Security Hub). Kontrol lain AWS Config mungkin memiliki satu-satunya tipe sumber data, dengan beberapa AWS Config aturan sebagai pemetaan.

Tabel berikut mencantumkan tipe sumber data otomatis dan menunjukkan contoh beberapa pemetaan yang sesuai.

Jenis sumber data	Deskripsi	Contoh pemetaan
AWS Security Hub	Gunakan tipe sumber data ini untuk menangkap snapshot dari postur keamanan sumber daya Anda. Audit Manager menggunakan nama kontrol Security Hub sebagai kata kunci pemetaan, dan melaporkan hasil pemeriksaan keamanan tersebut langsung dari Security Hub.	`1.1 – Avoid the use of the "root" account`

Jenis sumber data	Deskripsi	Contoh pemetaan
AWS Config	Gunakan tipe sumber data ini untuk menangkap snapshot dari postur keamanan sumber daya Anda. Audit Manager menggunak an nama AWS Config aturan sebagai kata kunci pemetaan, dan melaporka n hasil pemeriksaan aturan tersebut langsung dariAWS Config.	`EC2_INSTANCE_MANAG ED_BY_SSM`
AWS CloudTrail	Gunakan tipe sumber data ini untuk melacak aktivitas pengguna tertentu yang diperlukan dalam audit Anda. Audit Manager menggunakan nama CloudTrail acara sebagai kata kunci pemetaan, dan mengumpulkan aktivitas pengguna terkait dari log Anda CloudTrail .	`CreateAccessKey`
AWSPanggilan API	Gunakan tipe sumber data ini untuk mengambil snapshot konfigurasi sumber daya Anda melalui panggilan API ke yang spesifikLayanan AWS. Audit Manager menggunakan nama panggilan API sebagai kata kunci pemetaan, dan mengumpulkan respons API.	`ec2_DescribeSecuri tyGroups`

Gambar berikut menunjukkan contoh sumber data yang berbeda seperti yang terlihat di konsol Audit Manager.



> **Note**
>
> Meskipun beberapa tipe sumber dataLayanan AWS, tipe sumber data berbeda dengan layanan dalam lingkup. Untuk informasi selengkapnya, lihat Apa perbedaan antara layanan dalam lingkup dan tipe sumber data? di bagian Pemecahan Masalah dari panduan ini.

Mendelegasikan

Delegasi adalah AWS Audit Manager pengguna dengan izin terbatas. Delegasi biasanya memiliki keahlian bisnis atau teknis khusus. Misalnya, keahlian ini mungkin dalam kebijakan penyimpanan data, rencana pelatihan, infrastruktur jaringan, atau manajemen identitas. Delegasi membantu pemilik audit meninjau bukti yang dikumpulkan untuk kontrol yang berada di bidang keahlian mereka. Delegasi dapat meninjau set kontrol dan bukti terkait mereka, menambahkan komentar, mengunggah bukti tambahan, dan memperbarui status setiap kontrol yang Anda tetapkan kepada mereka untuk ditinjau.

Pemilik audit menetapkan set kontrol khusus untuk delegasi, bukan seluruh penilaian. Akibatnya, delegasi memiliki akses terbatas ke penilaian. Untuk petunjuk tentang cara mendelegasikan set kontrol, lihatDelegasi diAWS Audit Manager.

E

A| B | C | D E | F | | G | H | I | J | K | L | M | N | O | P R | T S | T | U | W | X | Y | Z

Bukti

Bukti adalah catatan yang berisi informasi yang diperlukan untuk menunjukkan kepatuhan terhadap persyaratan kontrol. Contoh bukti termasuk aktivitas perubahan yang dipanggil oleh pengguna, dan snapshot konfigurasi sistem.

Ada dua jenis bukti utama dalam Audit Manager: bukti otomatis dan bukti manual.

- Bukti otomatis — Ini adalah bukti yang dikumpulkan oleh Audit Manager secara otomatis. Ini termasuk tiga kategori bukti otomatis berikut:
  - Pemeriksaan kepatuhan — Hasil pemeriksaan kepatuhan diambil dariAWS Security Hub,AWS Config, atau keduanya. Contoh pemeriksaan kepatuhan termasuk hasil pemeriksaan keamanan dari Security Hub untuk kontrol PCI DSS, dan evaluasi AWS Config aturan untuk kontrol HIPAA. Untuk informasi selengkapnya, lihat AWS ConfigAturan yang didukung oleh AWS Audit Manager dan AWS Security Hubkontrol yang didukung oleh AWS Audit Manager.
  - Aktivitas pengguna — Aktivitas pengguna yang mengubah konfigurasi sumber daya diambil dari CloudTrail log saat aktivitas tersebut terjadi. Contoh aktivitas pengguna termasuk pembaruan tabel rute, perubahan setelan cadangan instans Amazon RDS, dan perubahan kebijakan enkripsi bucket S3. Untuk informasi selengkapnya, lihat nama AWS CloudTrail acara yang didukung oleh AWS Audit Manager.
  - Data konfigurasi — Sebuah snapshot dari konfigurasi sumber daya diambil langsung dari setiap hari, mingguan, atau bulanan. Layanan AWS Contoh snapshot konfigurasi mencakup daftar rute untuk tabel rute VPC, setelan cadangan instans Amazon RDS, dan kebijakan enkripsi bucket S3. Untuk informasi selengkapnya, lihat panggilan API yang didukung oleh AWS Audit Manager.
- Bukti manual — Ini adalah bukti yang Anda tambahkan ke Audit Manager sendiri. Ada tiga cara untuk menambahkan bukti Anda sendiri:
  - Impor file dari Amazon S3
  - Unggah file dari browser Anda
  - Masukkan respons teks untuk pertanyaan penilaian risiko

  Untuk informasi selengkapnya, lihat Menambahkan bukti manual di AWS Audit Manager.

Pengumpulan bukti otomatis dimulai saat Anda membuat penilaian. Ini adalah proses yang berkelanjutan, dan Audit Manager mengumpulkan bukti pada frekuensi yang berbeda tergantung pada jenis bukti dan sumber data yang mendasarinya. Untuk informasi lebih lanjut tentang

pengumpulan bukti, lihatBagaimana AWS Audit Manager mengumpulkan bukti. Untuk petunjuk tentang cara meninjau bukti dalam penilaian, lihatMeninjau bukti dalam penilaian.

Metode pengumpulan bukti

Ada dua cara kontrol dapat mengumpulkan bukti.

- Kontrol otomatis secara otomatis mengumpulkan bukti dari sumber AWS data. Bukti otomatis ini dapat membantu Anda menunjukkan kepatuhan penuh atau sebagian terhadap kontrol.
- Kontrol manual mengharuskan Anda untuk mengunggah bukti Anda sendiri untuk menunjukkan kepatuhan terhadap kontrol.

> **Note**
>
> Anda dapat melampirkan bukti manual ke kontrol otomatis apa pun. Dalam banyak kasus, kombinasi bukti otomatis dan manual diperlukan untuk menunjukkan kepatuhan penuh terhadap kontrol. Meskipun Audit Manager dapat memberikan bukti otomatis yang bermanfaat dan relevan, beberapa bukti otomatis mungkin hanya menunjukkan kepatuhan sebagian. Dalam hal ini, Anda dapat melengkapi bukti otomatis yang diberikan Audit Manager dengan bukti Anda sendiri.
>
> Sebagai contoh:
>
> - Kerangka praktik terbaik AI AWS generatif berisi kontrol yang disebut`Error analysis`. Kontrol ini mengharuskan Anda untuk mengidentifikasi kapan ketidakakuratan terdeteksi dalam penggunaan model Anda. Ini juga mengharuskan Anda untuk melakukan analisis kesalahan menyeluruh untuk memahami akar penyebab dan mengambil tindakan korektif.
> - Untuk mendukung kontrol ini, Audit Manager mengumpulkan bukti otomatis yang menunjukkan jika CloudWatch alarm diaktifkan untuk Akun AWS tempat penilaian Anda berjalan. Anda dapat menggunakan bukti ini untuk menunjukkan kepatuhan sebagian terhadap kontrol dengan membuktikan bahwa alarm dan pemeriksaan Anda dikonfigurasi dengan benar.
> - Untuk menunjukkan kepatuhan penuh, Anda dapat melengkapi bukti otomatis dengan bukti manual. Misalnya, Anda dapat mengunggah kebijakan atau prosedur yang menunjukkan proses analisis kesalahan, ambang batas untuk eskalasi dan pelaporan, dan hasil analisis akar penyebab Anda. Anda dapat menggunakan bukti manual ini untuk menunjukkan bahwa kebijakan yang ditetapkan sudah ada, dan bahwa tindakan korektif diambil saat diminta.
>
> Untuk contoh yang lebih rinci, lihat Kontrol dengan sumber data campuran.

Tujuan ekspor

Tujuan ekspor adalah bucket S3 default tempat Audit Manager menyimpan file yang Anda ekspor dari pencari bukti. Untuk mempelajari selengkapnya, lihat Tujuan ekspor (opsional).

F

A| B | C | D E | F | | G | H | I | J | K | L | M | N | O | P R | T S | T | U | W | X | Y | Z

Kerangka

Kerangka kerja Audit Manager adalah file yang digunakan untuk menyusun dan mengotomatiskan penilaian untuk standar atau prinsip tata kelola risiko tertentu. Kerangka kerja ini membantu memetakan AWS sumber daya Anda ke persyaratan dalam kontrol. Mereka termasuk kumpulan kontrol prebuilt atau yang ditentukan pelanggan. Koleksi memiliki deskripsi dan prosedur pengujian untuk setiap kontrol. Kontrol ini diatur dan dikelompokkan berdasarkan persyaratan standar atau peraturan kepatuhan yang ditentukan. Contohnya termasuk PCI DSS, dan GDPR.

Ada dua jenis kerangka kerja di Audit Manager:

- Kerangka kerja standar — Kerangka kerja bawaan yang didasarkan pada praktik AWS terbaik untuk berbagai standar dan peraturan kepatuhan. Anda dapat menggunakan kerangka kerja ini untuk membantu persiapan audit.
- Kerangka kerja khusus - Kerangka kerja khusus yang Anda tentukan sebagai pengguna Audit Manager. Anda dapat menggunakan kerangka kerja ini untuk membantu persiapan audit sesuai dengan kepatuhan spesifik atau persyaratan tata kelola risiko Anda.

Untuk petunjuk tentang cara membuat dan mengelola kerangka kerja, lihatPustaka kerangka kerja.

> **Note**
>
> AWS Audit Managermembantu mengumpulkan bukti yang relevan untuk memverifikasi kepatuhan terhadap standar dan peraturan kepatuhan tertentu. Namun, itu tidak menilai kepatuhan Anda sendiri. AWS Audit ManagerOleh karena itu, bukti yang dikumpulkan mungkin tidak mencakup semua informasi tentang AWS penggunaan Anda yang diperlukan untuk audit. AWS Audit Managerbukan pengganti penasihat hukum atau pakar kepatuhan.

Berbagi kerangka

Anda dapat menggunakan fitur berbagi kerangka kerja kustom Audit Manager untuk membagikan kerangka kerja kustom Anda dengan cepat di seluruh Akun AWS dan Wilayah. Untuk berbagi kerangka kustom, Anda membuat permintaan berbagi. Penerima permintaan saham kemudian memiliki waktu 120 hari untuk menerima atau menolak permintaan tersebut. Ketika mereka menerima, Audit Manager mereplikasi kerangka kustom bersama ke dalam pustaka kerangka kerja mereka. Selain mereplikasi kerangka kustom, Audit Manager juga mereplikasi setiap set kontrol kustom dan kontrol yang terkandung dalam framework tersebut. Kontrol kustom ini ditambahkan ke pustaka kontrol penerima. Audit Manager tidak mereplikasi kerangka kerja atau kontrol standar. Ini karena sumber daya ini sudah tersedia secara default di setiap akun dan Wilayah.

R

A| B | C | D E | F | | G | H | I | J | K | L | M | N | O | P R | T S | T | U | W | X | Y | Z

Sumber

Sumber daya adalah aset fisik atau informasi yang dinilai dalam audit. Contoh sumber AWS daya termasuk instans Amazon EC2, instans Amazon RDS, bucket Amazon S3, dan subnet Amazon VPC.

Penilaian sumber daya

Penilaian sumber daya adalah proses menilai sumber daya individu. Penilaian ini didasarkan pada persyaratan kontrol. Sementara penilaian aktif, Audit Manager menjalankan penilaian sumber daya untuk setiap sumber daya individu dalam lingkup penilaian. Penilaian sumber daya menjalankan serangkaian tugas berikut:

1. Mengumpulkan bukti termasuk konfigurasi sumber daya, log peristiwa, dan temuan
2. Menerjemahkan dan memetakan bukti ke kontrol
3. Menyimpan dan melacak garis keturunan bukti untuk memungkinkan integritas

Kepatuhan sumber daya

Kepatuhan sumber daya mengacu pada status evaluasi sumber daya yang dinilai saat mengumpulkan bukti pemeriksaan kepatuhan.

Audit Manager mengumpulkan bukti pemeriksaan kepatuhan untuk kontrol yang menggunakan AWS Config dan Security Hub sebagai tipe sumber data. Beberapa sumber daya dapat dinilai

selama pengumpulan bukti ini. Akibatnya, satu bagian bukti pemeriksaan kepatuhan dapat mencakup satu atau lebih sumber daya.

Anda dapat menggunakan filter kepatuhan sumber daya di pencari bukti untuk menjelajahi status kepatuhan di tingkat sumber daya. Setelah penelusuran selesai, Anda kemudian dapat melihat pratinjau sumber daya yang cocok dengan kueri penelusuran Anda.

Dalam pencari bukti, ada tiga nilai yang mungkin untuk kepatuhan sumber daya:

- Non-compliant — Ini mengacu pada sumber daya dengan masalah pemeriksaan kepatuhan. Hal ini terjadi jika Security Hub melaporkan hasil Gagal untuk sumber daya, atau jika AWS Config melaporkan hasil yang tidak sesuai.
- Compliant — Ini mengacu pada sumber daya yang tidak memiliki masalah pemeriksaan kepatuhan. Hal ini terjadi jika Security Hub melaporkan hasil Pass untuk sumber daya, atau jika AWS Config melaporkan hasil Compliant.
- Tidak meyakinkan — Ini mengacu pada sumber daya yang pemeriksaan kepatuhan tidak tersedia atau berlaku. Ini terjadi jika AWS Config atau Security Hub adalah tipe sumber data yang mendasarinya, tetapi layanan tersebut tidak diaktifkan. Ini juga terjadi jika tipe sumber data yang mendasarinya tidak mendukung pemeriksaan kepatuhan (seperti bukti manual, panggilan AWS API, atau CloudTrail).

S

A| B | C | D E | F | | G | H | I | J | K | L | M | N | O | P R | T S | T | U | W | X | Y | Z

Layanan dalam lingkup

Ini adalah Layanan AWS yang termasuk dalam ruang lingkup penilaian Anda. Ketika Anda menentukan layanan sebagai disertakan dalam lingkup penilaian Anda, Audit Manager menilai sumber daya layanan tersebut. Audit Manager dapat menilai berbagai macam sumber daya dari layanan dalam lingkup. Beberapa contoh sumber daya meliputi yang berikut:

- Instans Amazon EC2
- Ember S3
- Pengguna atau peran
- Tabel DynamoDB
- Komponen jaringan seperti Amazon Virtual Private Cloud (VPC), grup keamanan, atau tabel daftar kontrol akses jaringan (ACL)

Saat Anda menggunakan konsol Audit Manager untuk membuat atau memperbarui penilaian dari kerangka kerja standar, daftar lingkup Layanan AWS dalam dipilih sebelumnya secara default. Daftar ini tidak dapat diedit. Ini karena Audit Manager secara otomatis memetakan dan memilih sumber data dan layanan untuk Anda. Pemilihan ini dibuat sesuai dengan persyaratan kerangka standar. Jika kerangka kerja standar yang hanya berisi kontrol manual, tidak Layanan AWS ada dalam cakupan penilaian Anda, dan Anda tidak dapat menambahkan layanan apa pun ke penilaian Anda.

Jika Anda perlu mengedit daftar layanan dalam lingkup untuk kerangka kerja standar, Anda dapat melakukannya dengan menggunakan operasi CreateAssessmentatau UpdateAssessmentAPI. Atau, Anda dapat menyesuaikan kerangka kerja standar dan kemudian membuat penilaian dari kerangka kerja khusus.

> **Note**
>
> Perlu diingat bahwa layanan dalam lingkup berbeda dengan tipe sumber data, yang juga bisa berupa Layanan AWS atau sesuatu yang lain. Untuk informasi selengkapnya, lihat Apa perbedaan antara layanan dalam lingkup dan tipe sumber data? di bagian Pemecahan Masalah dari panduan ini.

Bagaimana AWS Audit Manager mengumpulkan bukti

Setiap penilaian aktif secara AWS Audit Manager otomatis mengumpulkan bukti dari berbagai sumber data. Setiap penilaian memiliki ruang lingkup yang ditentukan yang menentukan Layanan AWS dan akun tempat Audit Manager mengumpulkan data. Masing-masing layanan dan akun yang ditentukan dalam lingkup ini berisi banyak sumber daya, dan setiap sumber daya adalah inventaris aset sistem yang Anda miliki. Pengumpulan bukti di Audit Manager melibatkan penilaian setiap sumber daya dalam lingkup. Ini disebut sebagai penilaian sumber daya.

Langkah-langkah berikut menjelaskan bagaimana Audit Manager mengumpulkan bukti untuk setiap penilaian sumber daya:

1. Menilai sumber daya dari sumber data

Untuk memulai pengumpulan bukti, Audit Manager menilai sumber daya dalam lingkup dari sumber data. Ini dilakukan dengan menangkap snapshot konfigurasi, hasil pemeriksaan kepatuhan terkait, dan aktivitas pengguna apa pun. Kemudian menjalankan analisis untuk menentukan kontrol mana

yang didukung data ini. Hasil penilaian sumber daya kemudian disimpan dan diubah menjadi bukti. Untuk informasi lebih lanjut tentang berbagai jenis bukti, lihat Bukti di bagian AWS Audit Managerkonsep dan terminologi panduan ini.

2. Mengubah hasil penilaian menjadi bukti

Hasil penilaian sumber daya berisi data asli yang diambil dari sumber daya tersebut, dan metadata yang menunjukkan kontrol mana yang didukung data. AWS Audit Managermengubah data asli menjadi format yang ramah auditor. Data dan metadata yang dikonversi kemudian disimpan sebagai bukti Audit Manager sebelum dilampirkan ke kontrol.

3. Melampirkan bukti ke kontrol terkait

Audit Manager membaca metadata bukti. Kemudian, ia melampirkan bukti yang disimpan ke kontrol terkait dalam penilaian. Bukti terlampir menjadi terlihat di Audit Manager. Ini melengkapi siklus penilaian sumber daya.

> **Note**
>
> Bergantung pada konfigurasi kontrol, bukti yang sama dapat, dalam beberapa kasus, dilampirkan ke beberapa kontrol dari beberapa penilaian Audit Manager. Ketika bukti yang sama dilampirkan ke beberapa kontrol, Audit Manager mengukur penilaian sumber daya tepat sekali. Ini karena bukti yang sama dikumpulkan tepat hanya sekali. Namun, satu kontrol dalam penilaian Audit Manager dapat memiliki banyak bukti dari berbagai sumber data.

Frekuensi pengumpulan bukti

Pengumpulan bukti adalah proses berkelanjutan yang dimulai saat Anda membuat penilaian. AWS Audit Managermengumpulkan bukti dari berbagai sumber data pada frekuensi yang berbeda-beda. Akibatnya, tidak ada one-size-fits-all jawaban untuk seberapa sering bukti dikumpulkan. Frekuensi pengumpulan bukti didasarkan pada jenis bukti dan sumber datanya, seperti yang dijelaskan di bawah ini.

- Pemeriksaan kepatuhan — Audit Manager mengumpulkan jenis bukti ini dari AWS Security Hub danAWS Config.
  - UntukAWS Security Hub, frekuensi pengumpulan bukti mengikuti jadwal pemeriksaan Security Hub Anda. Untuk informasi selengkapnya tentang jadwal pemeriksaan Security Hub, lihat

Menjadwalkan untuk menjalankan pemeriksaan keamanan di Panduan AWS Security Hub Pengguna. Untuk informasi selengkapnya tentang pemeriksaan Security Hub yang didukung oleh Audit Manager, lihatAWS Security Hub kontrol yang didukung oleh AWS Audit Manager.

  - KarenaAWS Config, frekuensi pengumpulan bukti mengikuti pemicu yang ditentukan dalam AWS Config aturan Anda. Untuk informasi selengkapnya tentang pemicu AWS Config aturan, lihat Jenis pemicu di Panduan AWS Config Pengguna. Untuk informasi selengkapnya tentang Aturan AWS Config yang didukung oleh Audit Manager, lihatAturan AWS Config didukung oleh AWS Audit Manager.

- Aktivitas pengguna — Audit Manager mengumpulkan jenis bukti ini dari AWS CloudTrail secara terus-menerus. Frekuensi ini terus menerus karena aktivitas pengguna dapat terjadi kapan saja sepanjang hari. Untuk informasi selengkapnya, lihat AWS CloudTrail nama acara yang didukung oleh AWS Audit Manager.
- Data konfigurasi — Audit Manager mengumpulkan jenis bukti ini menggunakan panggilan API deskripsi ke panggilan lain Layanan AWS seperti Amazon EC2, Amazon S3, atau IAM. Anda dapat memilih tindakan API mana yang akan dipanggil. Anda juga mengatur frekuensi sebagai harian, mingguan, atau bulanan di Audit Manager. Anda dapat menentukan frekuensi ini saat membuat atau mengedit kontrol di pustaka kontrol. Untuk petunjuk tentang cara mengedit atau membuat kontrol, lihatPustaka kontrol. Untuk informasi selengkapnya tentang cara Audit Manager menggunakan panggilan API untuk membuat bukti, lihatPanggilan API didukung oleh AWS Audit Manager.

Terlepas dari frekuensi pengumpulan bukti untuk sumber data, bukti baru dikumpulkan secara otomatis selama kontrol dan penilaian aktif.

Contoh AWS Audit Manager kontrol

Anda dapat meninjau contoh di halaman ini untuk mempelajari lebih lanjut tentang cara kerja kontrolAWS Audit Manager. Contoh-contoh ini menjelaskan seperti apa kontrol itu, bagaimana Audit Manager menghasilkan bukti untuk kontrol tersebut, dan langkah selanjutnya yang dapat Anda ambil untuk menunjukkan kepatuhan.

> **Tip**
>
> Kami menyarankan Anda mengaktifkan AWS Config dan AWS Security Hub untuk pengalaman optimal di Audit Manager. Saat Anda mengaktifkan layanan ini, layanan tersebut dapat digunakan sebagai tipe sumber data untuk kontrol dalam penilaian Audit Manager

Anda. Dengan kata lain, Audit Manager dapat menggunakan temuan Security Hub dan Aturan AWS Config untuk menghasilkan bukti otomatis.

- Setelah mengaktifkan AWS Security Hub, pastikan Anda juga mengaktifkan semua standar keamanan dan mengaktifkan pengaturan temuan kontrol terkonsolidasi. Langkah ini memastikan bahwa Audit Manager dapat mengimpor temuan untuk semua standar kepatuhan yang didukung.
- Setelah mengaktifkan AWS Config, pastikan Anda juga mengaktifkan yang relevan Aturan AWS Config atau menerapkan paket kesesuaian untuk standar kepatuhan yang terkait dengan audit Anda. Langkah ini memastikan bahwa Audit Manager dapat mengimpor temuan untuk semua yang didukung Aturan AWS Config yang Anda aktifkan.

Contoh tersedia untuk masing-masing jenis kontrol berikut:

Topik

Kontrol otomatis yang digunakan AWS Security Hub sebagai tipe sumber data

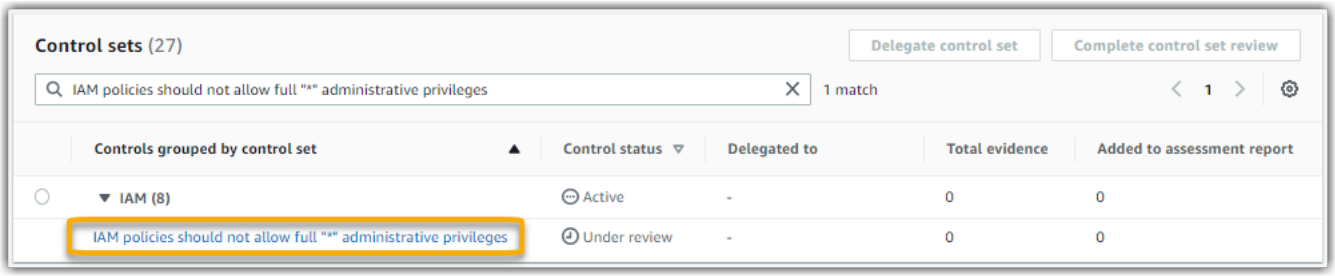
Contoh ini menunjukkan kontrol yang menggunakan AWS Security Hub sebagai tipe sumber datanya. Ini adalah kontrol standar yang diambil dari kerangka AWSFoundational Security Best Practices (FSBP). Audit Manager menggunakan kontrol ini untuk menghasilkan bukti yang dapat membantu membawa AWS lingkungan Anda sejalan dengan persyaratan FSBP.

Contoh detail kontrol

- Nama kontrol - `IAM policies should not allow full "*" administrative privileges`

- Set kontrol - Kontrol ini milik set `IAM` kontrol. Ini adalah pengelompokan kontrol yang berhubungan dengan identitas dan manajemen akses.
- Jenis sumber data — AWS Security Hub
- Jenis bukti - Pemeriksaan kepatuhan

Dalam contoh berikut, kontrol ini berada dalam penilaian Audit Manager yang dibuat dari kerangka FSBP.



Penilaian menunjukkan status kontrol. Ini juga menunjukkan berapa banyak bukti yang dikumpulkan untuk kontrol ini sejauh ini dan berapa banyak bukti yang dimasukkan dalam laporan penilaian Anda. Dari sini, Anda dapat mendelegasikan set kontrol untuk ditinjau atau menyelesaikan ulasan sendiri. Memilih nama kontrol membuka halaman detail dengan informasi lebih lanjut, termasuk bukti untuk kontrol itu.

Apa yang dilakukan kontrol ini

Audit Manager dapat menggunakan kontrol ini untuk memeriksa apakah kebijakan IAM Anda terlalu luas untuk memenuhi persyaratan FSBP. Lebih khusus lagi, ini dapat memeriksa apakah kebijakan IAM yang dikelola pelanggan Anda memiliki akses administrator yang menyertakan pernyataan wildcard berikut: `"Effect": "Allow"` dengan `"Action": "*"` over. `"Resource": "*"`

Bagaimana Audit Manager mengumpulkan bukti untuk kontrol ini

Audit Manager mengambil langkah-langkah berikut untuk mengumpulkan bukti untuk kontrol ini:

1. Untuk setiap kontrol, Audit Manager menilai sumber daya dalam ruang lingkup Anda. Hal ini dilakukan dengan menggunakan sumber data yang ditentukan dalam pengaturan kontrol. Dalam contoh ini, kebijakan IAM Anda adalah sumber daya, dan Security Hub dan AWS Config merupakan tipe sumber data. Audit Manager mencari hasil pemeriksaan Security Hub tertentu ([IAM.1]), yang pada gilirannya menggunakan AWS Config aturan untuk mengevaluasi kebijakan IAM Anda (-). iam-policy-no-statements with-admin-access

2. Hasil penilaian sumber daya disimpan dan diubah menjadi bukti ramah auditor. Audit Manager menghasilkan bukti pemeriksaan kepatuhan untuk kontrol yang menggunakan Security Hub sebagai tipe sumber data. Bukti ini berisi hasil pemeriksaan kepatuhan yang dilaporkan langsung dari Security Hub.
3. Audit Manager melampirkan bukti yang disimpan ke kontrol dalam penilaian Anda yang disebutkan namanya`IAM policies should not allow full "*" administrative privileges`.

Bagaimana Anda dapat menggunakan Audit Manager untuk menunjukkan kepatuhan terhadap kontrol ini

Setelah bukti dilampirkan pada kontrol, Anda — atau delegasi pilihan Anda — dapat meninjau bukti untuk melihat apakah ada perbaikan yang diperlukan.

Dalam contoh ini, Audit Manager mungkin menampilkan keputusan Gagal dari Security Hub. Ini dapat terjadi jika kebijakan IAM Anda berisi wildcard (*) dan terlalu luas untuk memenuhi kontrol. Dalam hal ini, Anda dapat memperbarui kebijakan IAM Anda sehingga mereka tidak mengizinkan hak administratif penuh. Untuk mencapai hal ini, Anda dapat menentukan tugas apa yang perlu dilakukan pengguna, dan kemudian membuat kebijakan yang memungkinkan pengguna hanya melakukan tugas-tugas tersebut. Tindakan korektif ini membantu membawa AWS lingkungan Anda sejalan dengan persyaratan FSBP.

Ketika kebijakan IAM Anda sejalan dengan kontrol, tandai kontrol sebagai Ditinjau dan tambahkan bukti ke laporan penilaian Anda. Anda kemudian dapat membagikan laporan ini dengan auditor untuk menunjukkan bahwa kontrol berfungsi sebagaimana dimaksud.

Kontrol otomatis yang digunakan AWS Config sebagai tipe sumber data

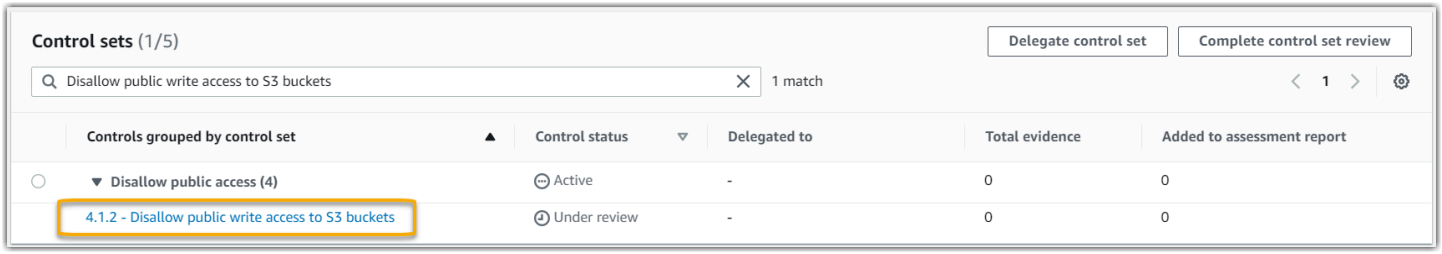
Contoh ini menunjukkan kontrol yang menggunakan AWS Config sebagai tipe sumber datanya. Ini adalah kontrol standar yang diambil dari kerangka AWS Control TowerGuardrails. Audit Manager menggunakan kontrol ini untuk menghasilkan bukti yang membantu membawa AWS lingkungan Anda sejalan dengan AWS Control Tower Guardrails.

Contoh detail kontrol

- Nama kontrol - `4.1.2 - Disallow public write access to S3 buckets`
- Set kontrol - Kontrol ini milik set `Disallow public access` kontrol. Ini adalah pengelompokan kontrol yang berhubungan dengan manajemen akses.
- Jenis sumber data — AWS Config

- Jenis bukti - Pemeriksaan kepatuhan

Dalam contoh berikut, kontrol ini berada dalam penilaian Audit Manager yang dibuat dari kerangka kerja AWS Control Tower Guardrails.



Penilaian menunjukkan status kontrol, berapa banyak bukti yang dikumpulkan untuk kontrol ini sejauh ini, dan berapa banyak bukti yang dimasukkan dalam laporan penilaian Anda. Dari sini, Anda dapat mendelegasikan set kontrol untuk ditinjau atau menyelesaikan ulasan sendiri. Memilih nama kontrol membuka halaman detail dengan informasi lebih lanjut, termasuk bukti untuk kontrol itu.

Apa yang dilakukan kontrol ini

Audit Manager dapat menggunakan kontrol ini untuk memeriksa apakah tingkat akses kebijakan bucket S3 Anda terlalu lunak untuk memenuhi persyaratan. AWS Control Tower Lebih khusus lagi, ini dapat memeriksa pengaturan Blokir Akses Publik, kebijakan bucket, dan daftar kontrol akses bucket (ACL) untuk mengonfirmasi bahwa bucket Anda tidak mengizinkan akses tulis publik.

Bagaimana Audit Manager mengumpulkan bukti untuk kontrol ini

Audit Manager mengambil langkah-langkah berikut untuk mengumpulkan bukti untuk kontrol ini:

1. Untuk setiap kontrol, Audit Manager menilai sumber daya dalam lingkup Anda menggunakan sumber data yang ditentukan dalam pengaturan kontrol. Dalam hal ini, bucket S3 Anda adalah sumber daya, dan AWS Config merupakan tipe sumber data. Audit Manager mencari hasil dari AWS Config Aturan tertentu (s3- bucket-public-write-prohibited) untuk mengevaluasi pengaturan, kebijakan, dan ACL dari masing-masing bucket S3 yang berada dalam lingkup penilaian Anda.
2. Hasil penilaian sumber daya disimpan dan diubah menjadi bukti ramah auditor. Audit Manager menghasilkan bukti pemeriksaan kepatuhan untuk kontrol yang digunakan AWS Config sebagai tipe sumber data. Bukti ini berisi hasil pemeriksaan kepatuhan yang dilaporkan langsung dariAWS Config.
3. Audit Manager melampirkan bukti yang disimpan ke kontrol dalam penilaian Anda yang disebutkan namanya`4.1.2 - Disallow public write access to S3 buckets`.

Bagaimana Anda dapat menggunakan Audit Manager untuk menunjukkan kepatuhan terhadap kontrol ini

Setelah bukti dilampirkan pada kontrol, Anda — atau delegasi pilihan Anda — dapat meninjau bukti untuk melihat apakah ada perbaikan yang diperlukan.

Dalam contoh ini, Audit Manager mungkin menampilkan putusan yang AWS Config menyatakan bahwa bucket S3 tidak sesuai. Ini bisa terjadi jika salah satu bucket S3 Anda memiliki setelan Blokir Akses Publik yang tidak membatasi kebijakan publik, dan kebijakan yang digunakan memungkinkan akses tulis publik. Untuk memulihkan ini, Anda dapat memperbarui pengaturan Blokir Akses Publik untuk membatasi kebijakan publik. Atau, Anda dapat menggunakan kebijakan bucket lain yang tidak mengizinkan akses penulisan publik. Tindakan korektif ini membantu membawa AWS lingkungan Anda sejalan dengan AWS Control Tower persyaratan.

Jika Anda puas bahwa tingkat akses bucket S3 sesuai dengan kontrol, Anda dapat menandai kontrol sebagai Ditinjau dan menambahkan bukti ke laporan penilaian Anda. Anda kemudian dapat membagikan laporan ini dengan auditor untuk menunjukkan bahwa kontrol berfungsi sebagaimana dimaksud.

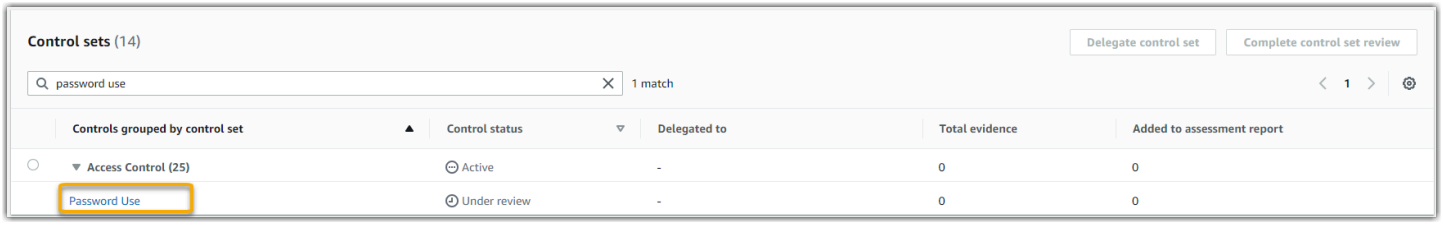
Kontrol otomatis yang menggunakan panggilan AWS API sebagai tipe sumber data

Contoh ini menunjukkan kontrol kustom yang menggunakan panggilan AWS API sebagai tipe sumber datanya. Audit Manager menggunakan kontrol ini untuk menghasilkan bukti yang dapat membantu membawa AWS lingkungan Anda sesuai dengan kebutuhan spesifik Anda.

Contoh detail kontrol

- Nama kontrol - `Password Use`
- Set kontrol - Kontrol ini milik set kontrol yang disebut`Access Control`. Ini adalah pengelompokan kontrol yang berhubungan dengan identitas dan manajemen akses.
- Jenis sumber data - Panggilan AWS API
- Jenis bukti - Data konfigurasi

Dalam contoh berikut, kontrol ini berada dalam penilaian Audit Manager yang dibuat dari kerangka kerja khusus.



Penilaian menunjukkan status kontrol. Ini juga menunjukkan berapa banyak bukti yang dikumpulkan untuk kontrol ini sejauh ini dan berapa banyak bukti yang dimasukkan dalam laporan penilaian Anda. Dari sini, Anda dapat mendelegasikan set kontrol untuk ditinjau atau menyelesaikan ulasan sendiri. Memilih nama kontrol membuka halaman detail dengan informasi lebih lanjut, termasuk bukti untuk kontrol itu.

Apa yang dilakukan kontrol ini

Audit Manager dapat menggunakan kontrol khusus ini untuk membantu Anda memastikan bahwa Anda memiliki kebijakan kontrol akses yang memadai. Kontrol ini mengharuskan Anda mengikuti praktik keamanan yang baik dalam pemilihan dan penggunaan kata sandi. Audit Manager dapat membantu Anda memvalidasi ini dengan mengambil daftar semua kebijakan kata sandi untuk prinsipal IAM yang berada dalam lingkup penilaian Anda.

Bagaimana Audit Manager mengumpulkan bukti untuk kontrol ini

Audit Manager mengambil langkah-langkah berikut untuk mengumpulkan bukti untuk kontrol kustom ini:

1. Untuk setiap kontrol, Audit Manager menilai sumber daya dalam lingkup Anda menggunakan sumber data yang ditentukan dalam pengaturan kontrol. Dalam hal ini, prinsip IAM Anda adalah sumber daya, dan panggilan AWS API adalah tipe sumber data. Audit Manager mencari hasil panggilan API IAM tertentu (GetAccountPasswordPolicy). Kemudian mengembalikan kebijakan kata sandi untuk Akun AWS yang berada dalam lingkup penilaian Anda.
2. Hasil penilaian sumber daya disimpan dan diubah menjadi bukti ramah auditor. Audit Manager menghasilkan bukti data konfigurasi untuk kontrol yang menggunakan panggilan API sebagai sumber data. Bukti ini berisi data asli yang diambil dari respons API, dan metadata tambahan yang menunjukkan kontrol mana yang mendukung data.
3. Audit Manager melampirkan bukti yang disimpan ke kontrol kustom dalam penilaian Anda yang diberi `Password Use` nama.

Bagaimana Anda dapat menggunakan Audit Manager untuk menunjukkan kepatuhan terhadap kontrol ini

Setelah bukti dilampirkan pada kontrol, Anda — atau delegasi pilihan Anda — dapat meninjau bukti untuk melihat apakah itu cukup atau apakah ada perbaikan yang diperlukan.

Dalam contoh ini, Anda dapat meninjau bukti untuk melihat tanggapan dari panggilan API. GetAccountPasswordPolicyRespons tersebut menjelaskan persyaratan kompleksitas dan periode rotasi wajib untuk kata sandi pengguna di akun Anda. Anda dapat menggunakan respons API ini sebagai bukti untuk menunjukkan bahwa Anda memiliki kebijakan kontrol akses kata sandi yang memadai untuk Akun AWS yang berada dalam lingkup penilaian Anda. Jika mau, Anda juga dapat memberikan komentar tambahan tentang kebijakan ini dengan menambahkan komentar ke kontrol.

Bila Anda puas bahwa kebijakan kata sandi kepala IAM Anda sejalan dengan kontrol kustom, Anda dapat menandai kontrol sebagai Ditinjau dan menambahkan bukti ke laporan penilaian Anda. Anda kemudian dapat membagikan laporan ini dengan auditor untuk menunjukkan bahwa kontrol berfungsi sebagaimana dimaksud.

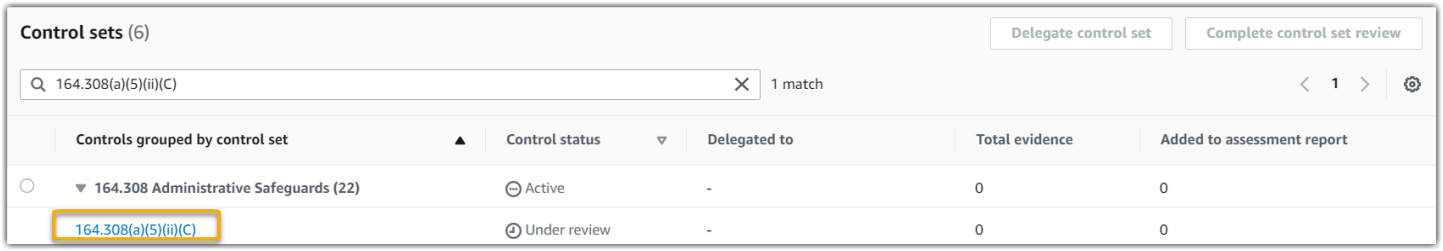
Kontrol otomatis yang digunakan AWS CloudTrail sebagai tipe sumber data

Contoh ini menunjukkan kontrol yang menggunakan AWS CloudTrail sebagai tipe sumber datanya. Ini adalah kontrol standar yang diambil dari kerangka HIPAA. Audit Manager menggunakan kontrol ini untuk menghasilkan bukti yang dapat membantu membawa AWS lingkungan Anda sejalan dengan persyaratan HIPAA.

Contoh detail kontrol

- Nama kontrol - `164.308(a)(5)(ii)(C)`
- Set kontrol - Kontrol ini milik set kontrol yang disebut`164.308 Administrative Safeguards`.
- Jenis sumber data — AWS CloudTrail
- Jenis bukti — Aktivitas pengguna

Berikut kontrol ini ditunjukkan dalam penilaian Audit Manager yang dibuat dari kerangka HIPAA:



Penilaian menunjukkan status kontrol. Ini juga menunjukkan berapa banyak bukti yang dikumpulkan untuk kontrol ini sejauh ini dan berapa banyak bukti yang dimasukkan dalam laporan penilaian Anda. Dari sini, Anda dapat mendelegasikan set kontrol untuk ditinjau atau menyelesaikan ulasan sendiri. Memilih nama kontrol membuka halaman detail dengan informasi lebih lanjut, termasuk bukti untuk kontrol itu.

Apa yang dilakukan kontrol ini

Kontrol ini memerlukan prosedur pemantauan untuk mendeteksi login yang tidak tepat. Contoh login yang tidak pantas adalah ketika seseorang memasukkan beberapa kombinasi nama pengguna atau kata sandi untuk mencoba mengakses sistem informasi. Audit Manager membantu Anda memvalidasi kontrol ini dengan memberikan daftar semua upaya masuk yang terdeteksi untuk sumber daya yang ada dalam lingkup penilaian Anda.

Bagaimana Audit Manager mengumpulkan bukti untuk kontrol ini

Audit Manager mengambil langkah-langkah berikut untuk mengumpulkan bukti untuk kontrol ini:

1. Untuk setiap kontrol, Audit Manager menilai sumber daya dalam lingkup Anda menggunakan sumber data yang ditentukan dalam pengaturan kontrol. Dalam hal ini, pengguna Anda adalah sumber daya, dan CloudTrail merupakan tipe sumber data. Audit Manager mencari hasil dari semua peristiwa masuk AWS Management Console yang dicatat oleh CloudTrail log. Kemudian mengembalikan log peristiwa yang relevan yang berada dalam lingkup penilaian Anda.
2. Hasil penilaian sumber daya disimpan dan diubah menjadi bukti ramah auditor. Audit Manager menghasilkan bukti aktivitas pengguna untuk kontrol yang digunakan CloudTrail sebagai tipe sumber data. Bukti ini berisi data asli yang diambil dari pengguna Anda, dan metadata tambahan yang menunjukkan kontrol mana yang mendukung data.
3. Audit Manager melampirkan bukti yang disimpan ke kontrol dalam penilaian Anda yang disebutkan namanya`164.308(a)(5)(ii)(C)`.

Bagaimana Anda dapat menggunakan Audit Manager untuk menunjukkan kepatuhan terhadap kontrol ini

Setelah bukti dilampirkan pada kontrol, Anda — atau delegasi pilihan Anda — dapat meninjau bukti untuk melihat apakah ada perbaikan yang diperlukan.

Dalam contoh ini, Anda dapat meninjau bukti untuk melihat peristiwa login yang dicatat oleh CloudTrail. Log ini menjelaskan aktivitas login konsol untuk pengguna Anda, yang mencakup informasi berikut:

- Setiap login yang berhasil
- Setiap upaya masuk yang gagal
- Verifikasi kapan otentikasi multi-faktor (MFA) diberlakukan
- Alamat IP dari setiap acara masuk

Anda dapat menggunakan log ini sebagai bukti untuk menunjukkan bahwa Anda memiliki prosedur pemantauan yang memadai untuk Akun AWS yang berada dalam lingkup penilaian Anda. Jika suka, Anda juga dapat memberikan komentar tambahan dengan menambahkan komentar ke kontrol. Misalnya, jika log menunjukkan perbedaan seperti beberapa upaya masuk yang gagal, Anda dapat menambahkan komentar yang menjelaskan cara Anda memperbaiki masalah. Pemantauan rutin login konsol membantu Anda mencegah masalah keamanan yang mungkin timbul dari perbedaan dan upaya masuk yang tidak tepat. Pada gilirannya, praktik terbaik ini membantu membawa AWS lingkungan Anda sejalan dengan persyaratan HIPAA.

Ketika Anda puas bahwa prosedur pemantauan Anda sejalan dengan kontrol, Anda dapat menandai kontrol sebagai Ditinjau dan menambahkan bukti ke laporan penilaian Anda. Anda kemudian dapat membagikan laporan ini dengan auditor untuk menunjukkan bahwa kontrol berfungsi sebagaimana dimaksud.

Kontrol manual

Beberapa kontrol tidak mendukung pengumpulan bukti otomatis. Ini termasuk kontrol yang bergantung pada penyediaan catatan fisik dan tanda tangan, selain pengamatan, wawancara, dan peristiwa lain yang tidak dihasilkan di cloud. Dalam kasus ini, Anda dapat mengunggah bukti secara manual untuk menunjukkan bahwa Anda memenuhi persyaratan kontrol.

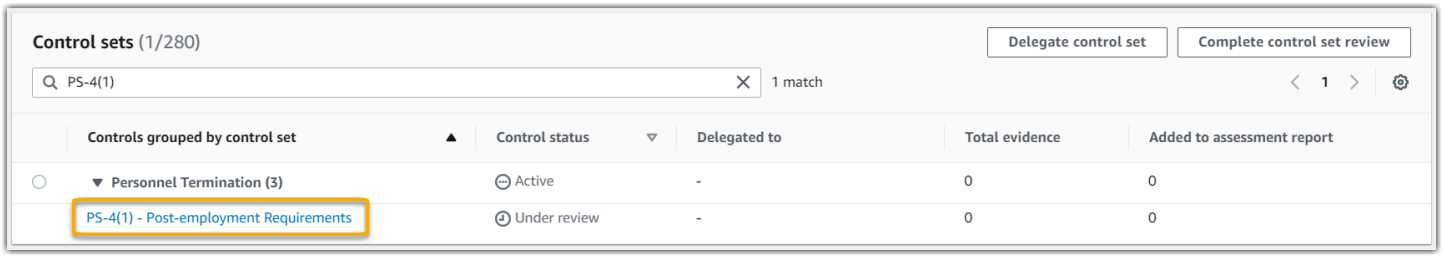
Contoh ini menunjukkan kontrol manual yang Audit Manager tidak mengumpulkan bukti otomatis. Ini adalah kontrol standar yang diambil dari kerangka kerja NIST 800-53 (Rev. 5). Anda dapat menggunakan Audit Manager untuk mengunggah dan menyimpan bukti yang menunjukkan kepatuhan terhadap kontrol ini.

Contoh detail kontrol

- Nama kontrol - `PS-4(1) - Post-employment Requirements`
- Set kontrol - Kontrol ini milik set `Personnel Termination` kontrol. Ini adalah pengelompokan kontrol yang berhubungan dengan keamanan informasi dalam konteks prosedur pemutusan hubungan kerja.

- Jenis sumber data — Manual
- Jenis bukti - Manual

Berikut kontrol ini ditunjukkan dalam penilaian Audit Manager yang dibuat dari kerangka kerja Low-Moderate-High NIST 800-53 (Rev. 5):



Penilaian menunjukkan status kontrol. Ini juga menunjukkan berapa banyak bukti yang dikumpulkan untuk kontrol ini sejauh ini dan berapa banyak bukti yang dimasukkan dalam laporan penilaian Anda. Dari sini, Anda dapat mendelegasikan set kontrol untuk ditinjau atau menyelesaikan ulasan sendiri. Memilih nama kontrol membuka halaman detail dengan informasi lebih lanjut, termasuk bukti untuk kontrol itu.

Apa yang dilakukan kontrol ini

Anda dapat menggunakan kontrol ini untuk mengonfirmasi bahwa Anda melindungi informasi organisasi jika karyawan diberhentikan. Secara khusus, Anda dapat menunjukkan bahwa Anda secara konsisten memberi tahu individu yang diberhentikan tentang persyaratan pasca-kerja yang berlaku dan mengikat secara hukum untuk perlindungan informasi organisasi. Selain itu, Anda dapat menunjukkan bahwa semua individu yang diberhentikan menandatangani pengakuan persyaratan pasca-kerja sebagai bagian dari proses pemutusan hubungan kerja untuk organisasi Anda.

Bagaimana Anda dapat mengunggah bukti secara manual untuk kontrol ini

Anda dapat mengambil langkah-langkah berikut untuk mengunggah bukti manual yang mendukung kontrol ini:

1. Tempatkan bukti manual yang ingin Anda unggah di bucket Amazon Simple Storage Service (S3) dan catat URI S3.
2. Dalam penilaian Audit Manager Anda, buka kontrol, buka tab folder bukti, dan unggah bukti dengan memasukkan URI S3. Untuk petunjuk, lihat Mengunggah bukti manual di AWS Audit Manager.

3. Audit Manager membuat folder bukti yang dinamai sesuai tanggal saat Anda mengunggah bukti. Kemudian melampirkan bukti yang diunggah ke kontrol dalam penilaian Anda yang disebutkan namanya. `PS-4(1) - Post-employment Requirements`

Bagaimana Anda dapat menggunakan Audit Manager untuk menunjukkan kepatuhan terhadap kontrol ini

Jika Anda memiliki dokumentasi yang mendukung kontrol ini, Anda dapat mengunggahnya sebagai bukti manual. Misalnya, Anda dapat mengunggah salinan terbaru persyaratan pasca-kerja yang mengikat secara hukum yang dikeluarkan departemen Sumber Daya Manusia Anda kepada karyawan yang diberhentikan. Jika ada individu yang dihentikan selama periode audit, Anda juga dapat mengunggah salinan bertanggal yang ditujukan kepada individu yang dihentikan tersebut.

Sama seperti dengan kontrol otomatis, Anda dapat mendelegasikan kontrol manual kepada pemangku kepentingan yang dapat membantu Anda meninjau bukti (atau, dalam hal ini, menyediakannya). Misalnya, ketika Anda meninjau kontrol ini, Anda mungkin menyadari bahwa Anda hanya memenuhi sebagian persyaratannya. Ini bisa terjadi jika Anda tidak memiliki surat pengakuan yang ditandatangani oleh individu yang dihentikan. Anda dapat mendelegasikan kontrol kepada pemangku kepentingan SDM, yang kemudian dapat mengunggah salinan surat yang ditandatangani. Atau, jika tidak ada karyawan yang diberhentikan selama periode audit, Anda dapat meninggalkan komentar yang menyatakan mengapa tidak ada surat yang ditandatangani yang dilampirkan pada kontrol.

Ketika Anda puas bahwa Anda sejalan dengan kontrol, Anda dapat menandainya sebagai Ditinjau dan menambahkan bukti ke laporan penilaian Anda. Anda kemudian dapat membagikan laporan ini dengan auditor untuk menunjukkan bahwa kontrol berfungsi sebagaimana dimaksud.

Kontrol dengan tipe sumber data campuran (otomatis dan manual)

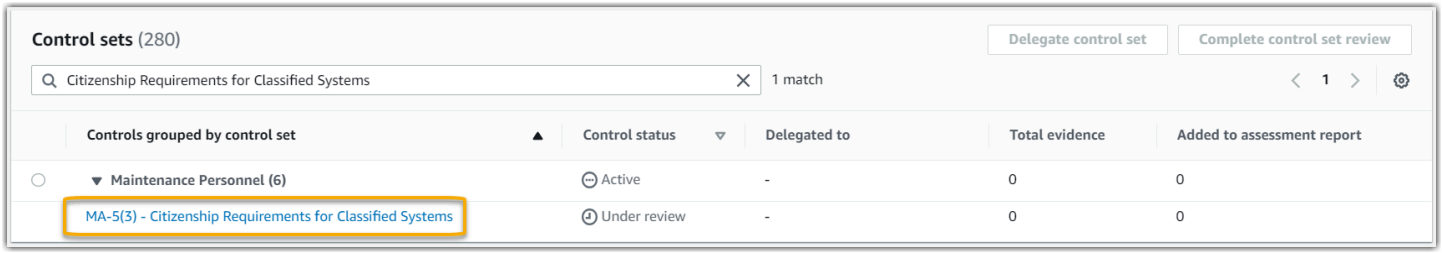
Dalam banyak kasus, kombinasi bukti otomatis dan manual diperlukan untuk memenuhi kontrol. Meskipun Audit Manager dapat memberikan bukti otomatis yang relevan dengan kontrol, Anda mungkin perlu melengkapi data ini dengan bukti manual yang Anda identifikasi dan unggah sendiri.

Contoh ini menunjukkan kontrol yang menggunakan kombinasi bukti manual dan bukti otomatis yang berasal dari panggilan AWS API. Ini adalah kontrol standar yang diambil dari kerangka kerja NIST 800-53 (Rev. 5). Audit Manager menggunakan kontrol ini untuk menghasilkan bukti yang dapat membantu membawa AWS lingkungan Anda sejalan dengan persyaratan NIST.

Contoh detail kontrol

- Nama kontrol - `MA-5(3) - Citizenship Requirements for Classified Systems`
- Set kontrol - Kontrol ini milik set `Maintenance Personnel` kontrol. Ini adalah pengelompokan kontrol yang berhubungan dengan individu yang melakukan pemeliharaan perangkat keras atau perangkat lunak pada sistem organisasi.
- Jenis sumber data — Panggilan AWS API, ditambah bukti manual tambahan
- Jenis bukti - Data konfigurasi

Berikut kontrol ini ditunjukkan dalam penilaian Audit Manager yang dibuat dari kerangka kerja NIST 800-53 (Rev. 5):



Penilaian menunjukkan status kontrol. Ini juga menunjukkan berapa banyak bukti yang dikumpulkan untuk kontrol ini sejauh ini dan berapa banyak bukti yang dimasukkan dalam laporan penilaian Anda. Dari sini, Anda dapat mendelegasikan set kontrol untuk ditinjau atau menyelesaikan ulasan sendiri. Memilih nama kontrol membuka halaman detail dengan informasi lebih lanjut, termasuk bukti untuk kontrol itu.

Apa yang dilakukan kontrol ini

Audit Manager dapat menggunakan kontrol ini untuk membantu Anda memastikan bahwa personel yang melakukan pemeliharaan dan kegiatan diagnostik Anda memiliki status kewarganegaraan yang diperlukan. Jika sistem Anda memproses, menyimpan, atau mengirimkan informasi rahasia, Anda harus menunjukkan bahwa personel pemeliharaan Anda adalah warga negara AS. Audit Manager membantu Anda memvalidasi ini. Ini dilakukan dengan mengembalikan daftar lengkap semua kebijakan dan prinsip IAM yang ada dalam lingkup penilaian Anda. Anda kemudian dapat memverifikasi dan menunjukkan bahwa daftar pengguna ini memiliki persyaratan kewarganegaraan yang diperlukan. Anda dapat melakukan ini dengan mengunggah bukti tambahan status kewarganegaraan mereka secara manual.

Bagaimana Audit Manager mengumpulkan bukti untuk kontrol ini

Audit Manager mengambil langkah-langkah berikut untuk mengumpulkan bukti untuk kontrol ini:

1. Untuk setiap kontrol, Audit Manager menilai sumber daya dalam lingkup Anda menggunakan sumber data yang ditentukan dalam pengaturan kontrol. Dalam hal ini, kebijakan dan prinsip IAM Anda adalah sumber daya, dan panggilan AWS API adalah sumber data. Audit Manager mencari hasil dari empat panggilan API IAM tertentu (ListUsers//ListRoles/ListGroups/ListPolicies) dan menampilkan daftar kebijakan dan prinsip IAM yang berada dalam lingkup penilaian Anda.
2. Hasil penilaian sumber daya disimpan dan diubah menjadi bukti ramah auditor. Audit Manager menghasilkan bukti data konfigurasi untuk kontrol yang menggunakan panggilan API sebagai tipe sumber data. Bukti ini berisi data asli yang diambil dari respons API, dan metadata tambahan yang menunjukkan kontrol mana yang mendukung data.
3. Audit Manager melampirkan bukti yang disimpan ke kontrol dalam penilaian Anda yang disebutkan namanya`MA-5(3) - Citizenship Requirements for Classified Systems`.

Bagaimana Anda dapat mengunggah bukti secara manual untuk kontrol ini

Anda dapat mengambil langkah-langkah berikut untuk mengunggah bukti manual yang melengkapi bukti otomatis:

1. Tempatkan dokumentasi kewarganegaraan di bucket Amazon Simple Storage Service (Amazon S3) dan catat URI S3.
2. Dalam penilaian Audit Manager Anda, buka kontrol, buka tab folder bukti, dan unggah bukti. Anda melakukan ini dengan memasukkan URI S3. Untuk petunjuk, lihat Menambahkan bukti manual di AWS Audit Manager.
3. Audit Manager melampirkan bukti yang diunggah ke kontrol dalam penilaian Anda yang disebutkan namanya. `MA-5(3) - Citizenship Requirements for Classified Systems`

Bagaimana Anda dapat menggunakan Audit Manager untuk menunjukkan kepatuhan terhadap kontrol ini

Setelah bukti dilampirkan pada kontrol, Anda — atau delegasi pilihan Anda — dapat meninjau bukti untuk melihat apakah itu cukup atau apakah ada perbaikan yang diperlukan.

Dalam contoh ini, Anda dapat meninjau bukti dan melihat daftar 20 pengguna. Jika Anda tidak yakin bagaimana mengidentifikasi pengguna mana yang merupakan personel pemeliharaan, atau kewarganegaraan pengguna tersebut, Anda dapat mendelegasikan kontrol kepada ahli materi pelajaran untuk validasi. Delegasi dapat mengkonfirmasi daftar personel pemeliharaan,

dan mengunggah bukti tambahan secara manual sebagai dokumentasi status kewarganegaraan mereka. Mengonfirmasi kewarganegaraan semua pengguna terdaftar yang relevan membantu membawa AWS lingkungan Anda sesuai dengan persyaratan NIST. Atau, jika sistem Anda tidak memproses, menyimpan, atau mengirimkan informasi rahasia, Anda dapat meninggalkan komentar yang menyatakan mengapa kontrol ini tidak berlaku.

Ketika Anda puas bahwa Anda sejalan dengan kontrol, tandai kontrol sebagai Ditinjau dan tambahkan bukti ke laporan penilaian Anda. Anda kemudian dapat membagikan laporan ini dengan auditor untuk menunjukkan bahwa kontrol berfungsi sebagaimana dimaksud.

Integrasi dengan terkait Layanan AWS

AWS Audit Managerterintegrasi dengan beberapa Layanan AWS untuk secara otomatis mengumpulkan bukti yang dapat Anda sertakan dalam laporan penilaian Anda.

AWS Security Hub

AWS Security Hubmemantau lingkungan Anda menggunakan pemeriksaan keamanan otomatis yang didasarkan pada praktik AWS terbaik dan standar industri. Audit Manager menangkap snapshot dari postur keamanan sumber daya Anda dengan melaporkan hasil pemeriksaan keamanan langsung dari Security Hub. Untuk informasi selengkapnya tentang Security Hub, lihat Apa ituAWS Security Hub? dalam AWS Security HubUser Guide.

AWS CloudTrail

AWS CloudTrailmembantu Anda memantau panggilan yang dilakukan ke AWS sumber daya di akun Anda. Ini termasuk panggilan yang dilakukan oleh AWS Management Console, AWS CLI, dan lainnya. Layanan AWS Audit Manager mengumpulkan data log CloudTrail secara langsung, dan mengubah log yang diproses menjadi bukti aktivitas pengguna. Untuk informasi lebih lanjut tentang CloudTrail, lihat Apa ituAWS CloudTrail? dalam AWS CloudTrailUser Guide.

AWS Config

AWS Config menyediakan tampilan detail dari konfigurasi sumber daya AWS dalam Akun AWS. Anda. Ini termasuk informasi tentang bagaimana sumber daya terkait satu sama lain dan bagaimana mereka dikonfigurasi di masa lalu. Audit Manager menangkap snapshot dari postur keamanan sumber daya Anda dengan melaporkan temuan langsung dari. AWS Config Untuk informasi lebih lanjut tentang AWS Config, lihat Apa itu AWS Config? di Panduan Pengguna AWS Config.

AWS License Manager

AWS License Manager menyederhanakan proses membawa lisensi vendor perangkat lunak ke cloud. Saat Anda membangun infrastruktur cloudAWS, Anda dapat menghemat biaya dengan menggunakan kembali inventaris lisensi yang ada untuk digunakan dengan sumber daya cloud. Audit Manager menyediakan kerangka kerja License Manager untuk membantu persiapan audit Anda. Kerangka kerja ini terintegrasi dengan License Manager untuk mengumpulkan informasi penggunaan lisensi berdasarkan aturan lisensi yang ditetapkan pelanggan. Untuk informasi selengkapnya tentang License Manager, lihat Apa ituAWS License Manager? dalam AWS License ManagerUser Guide.

AWS Control Tower

AWS Control Towermemberlakukan pagar pembatas preventif dan detektif untuk infrastruktur cloud. Audit Manager menyediakan kerangka kerja AWS Control Tower Guardrails untuk membantu Anda dengan persiapan audit Anda. Kerangka kerja ini berisi semua AWS Config aturan yang didasarkan pada pagar pembatas dari. AWS Control Tower Untuk informasi lebih lanjut tentang AWS Control Tower, lihat Apa itu AWS Control Tower? di Panduan Pengguna AWS Control Tower.

AWS Artifact

AWS Artifactadalah portal pengambilan artefak audit swalayan yang menyediakan akses sesuai permintaan ke dokumentasi kepatuhan dan sertifikasi untuk infrastruktur. AWS AWS Artifactmenawarkan bukti untuk membuktikan bahwa infrastruktur AWS Cloud memenuhi persyaratan kepatuhan. Sebaliknya, AWS Audit Manager membantu Anda mengumpulkan, meninjau, dan mengelola bukti untuk menunjukkan bahwa penggunaan Layanan AWS Anda sesuai. Untuk informasi lebih lanjut tentang AWS Artifact, lihat Apa itu AWS Artifact? di Panduan Pengguna AWS Artifact. Anda dapat mengunduh daftar AWS laporan diAWS Management Console.

Untuk daftar cakupan program kepatuhan tertentu, lihat Layanan AWSdi Lingkup berdasarkan Program Kepatuhan. Layanan AWS Untuk informasi lebih umum, lihat Program AWS Kepatuhan.

Integrasi dengan produk GRC pihak ketiga

AWS Audit Managermendukung integrasi dengan produk GRC mitra pihak ketiga yang tercantum di halaman ini.

Jika perusahaan Anda menggunakan model cloud hybrid atau model multicloud, kemungkinan Anda menggunakan produk GRC untuk mengelola bukti dari lingkungan tersebut. Ketika produk tersebut terintegrasi dengan Audit Manager, Anda dapat menarik bukti tentang AWS penggunaan Anda langsung ke lingkungan GRC Anda. Ini menyederhanakan cara Anda mengelola kepatuhan dengan

memberi Anda tempat terpusat untuk meninjau dan memulihkan bukti saat Anda mempersiapkan audit.

Baca halaman ini untuk ikhtisar produk GRC pihak ketiga yang dapat menyerap bukti dari Audit Manager. Anda juga dapat melihat referensi tindakan API Audit Manager mana yang dapat Anda ambil langsung di dalam produk tersebut.

Topik

Memahami cara kerja integrasi pihak ketiga dengan Audit Manager

Mitra GRC dapat menggunakan API publik Audit Manager untuk mengintegrasikan produk mereka dengan Audit Manager. Dengan integrasi ini, Anda dapat memetakan kontrol perusahaan di lingkungan GRC Anda ke kontrol yang disediakan Audit Manager.

Setelah menyelesaikan latihan pemetaan kontrol satu kali ini, Anda dapat membuat penilaian Audit Manager langsung di produk GRC. Tindakan ini memulai pengumpulan bukti tentang AWS penggunaan Anda. Anda kemudian dapat melihat AWS bukti ini bersama dengan bukti lain yang dikumpulkan dari lingkungan hibrida Anda, semuanya dalam konteks yang sama dari kontrol perusahaan Anda.

Saat Anda menggunakan integrasi Audit Manager dengan produk GRC pihak ketiga, ingatlah hal-hal berikut:

- Integrasi tersedia untuk semua Wilayah AWStempat Audit Manager didukung.
- Sumber daya Audit Manager apa pun yang Anda buat di produk mitra GRC juga tercermin dalam Audit Manager.
- Anda tunduk pada AWS Audit Managerharga selain harga produk GRC pihak ketiga.
- Bukti yang dikumpulkan oleh Audit Manager tidak dapat diubah. Bukti disajikan dengan cara yang persis sama dalam produk GRC pihak ketiga seperti di konsol Audit Manager. Namun, jika Anda menggunakan integrasi pihak ketiga, Anda mungkin dapat meningkatkan bukti ini dengan memberikan konteks tambahan dalam pelaporan Anda.
- Kuota yang sama yang berlaku untuk Audit Manager juga berlaku dalam produk GRC pihak ketiga. Misalnya, masing-masing Akun AWS dapat memiliki hingga 100 penilaian Audit Manager aktif. Kuota tingkat akun ini berlaku baik Anda membuat penilaian di konsol Audit Manager atau di

produk GRC pihak ketiga. Sebagian besar kuota Audit Manager, tetapi tidak semua, tercantum di bawah AWS Audit Manager namespace di konsol Service Quotas. Untuk mempelajari cara meminta peningkatan kuota, lihatMengelola kuota Audit Manager.

Jika Anda memiliki solusi kepatuhan dan Anda tertarik untuk berintegrasi dengan Audit Manager, kirim email`auditmanager-partners@amazon.com`.

Produk mitra GRC pihak ketiga yang terintegrasi dengan Audit Manager

Produk GRC pihak ketiga berikut dapat menyerap bukti dari Audit Manager.

MetricStream

Untuk menggunakan integrasi ini, hubungi akses MetricStreamdan pembelian perangkat lunak MetricStream GRC.

Dibangun di atas MetricStream Platform, solusi MetricStream Enterprise GRC memungkinkan pendekatan yang komprehensif dan kolaboratif untuk aktivitas dan proses GRC di seluruh perusahaan. Dengan memasukkan bukti dari Audit Manager ke dalam MetricStream, Anda dapat secara proaktif mengidentifikasi bukti yang tidak sesuai dari AWS lingkungan Anda dan meninjaunya bersama bukti dari sumber data lokal atau mitra cloud lainnya. Ini memberi Anda cara yang nyaman dan terpusat untuk meninjau dan meningkatkan keamanan cloud dan postur kepatuhan Anda saat Anda mempersiapkan audit.

Dengan integrasi MetricStream dan Audit Manager, Anda dapat melakukan operasi API berikut.

Tugas	Operasi API
Menyiapkan integrasi Audit Manager	• GetAccountStatus • GetOrganizationAdminAccount • GetSettings
Meninjau sumber daya Audit Manager	• GetAssessment • GetAssessmentFramework • GetControl • ListAssessmentFrameworks • ListControls

Tugas	Operasi API
Membuat sumber daya Audit Manager	• CreateAssessment • CreateAssessmentFramework
Memperbarui sumber daya Audit Manager	• UpdateAssessment • UpdateAssessmentControl • UpdateAssessmentStatus
Mengelola bukti	• StartQuery(AWS CloudTrailAPI) • GetQueryResults(AWS CloudTrailAPI)
Menghapus sumber daya Audit Manager	• DeleteAssessmentFramework

MetricStream Tautan terkait

- AWS Marketplacetautan
- Tautan produk
- Harga produk

Menggunakan Audit Manager dengan AWS SDK

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

Dokumentasi SDK	Dokumentasi khusus Audit Manager	Contoh kode	
AWS SDK for C++	AWS SDK for C++Referensi API untuk Audit Manager	contoh kode AWS SDK for C++	
AWS SDK for Go	AWS SDK for GoReferensi API untuk Audit Manager	contoh kode AWS SDK for Go	

Dokumentasi SDK	Dokumentasi khusus Audit Manager	Contoh kode	
AWS SDK for Java	AWS SDK for Java 2.xReferensi API untuk Audit Manager	contoh kode AWS SDK for Java	
AWS SDK for JavaScript	AWS SDK for JavaScriptReferensi API untuk Audit Manager	contoh kode AWS SDK for JavaScript	
AWS SDK for .NET	AWS SDK for .NETReferensi API untuk Audit Manager	contoh kode AWS SDK for .NET	
AWS SDK for PHP	AWS SDK for PHPReferensi API untuk Audit Manager	contoh kode AWS SDK for PHP	
AWS SDK for Python (Boto3)	AWS SDK for Python (Boto)Referensi API untuk Audit Manager	contoh kode AWS SDK for Python (Boto3)	
AWS SDK for Ruby	AWS SDK for RubyReferensi API untuk Audit Manager	contoh kode AWS SDK for Ruby	

Untuk contoh yang khusus untuk Audit Manager, lihat Contoh kode untuk AWS Audit Manager.

> **Note**
>
> Audit Manager tersedia dalam botocore versi 1.19.32 dan yang lebih baru untuk. AWS SDK for Python (Boto3) Sebelum Anda mulai menggunakan SDK, pastikan Anda menggunakan versi botocore yang sesuai.

Menyiapkan AWS Audit Manager

Sebelum mulai menggunakan Audit Manager, pastikan Anda menyelesaikan tugas penyiapan berikut.

Topik

- Prasyarat: Buat dan atur izin Akun AWS
- Aktifkan Audit Manager: Gunakan konsol, AWS CLI file, atau API untuk mengaktifkan Audit Manager
- Rekomendasi: Siapkan integrasi yang direkomendasikan dengan yang lain Layanan AWS

Prasyarat

Ikuti langkah-langkah ini untuk membuat Akun AWS dan pengguna administratif dengan hak penyiapan Audit Manager.

Langkah-langkah

- Daftar Akun AWS
- Membuat pengguna administratif
- Tambahkan izin yang diperlukan untuk mengakses dan mengaktifkan Audit Manager

> **Important**
>
> Jika Anda sudah mengatur dengan AWS dan IAM, Anda dapat melewati langkah 1 dan 2. Namun, Anda harus menyelesaikan langkah 3 untuk memastikan bahwa Anda memiliki izin yang diperlukan untuk menyiapkan Audit Manager.

Daftar Akun AWS

Jika Anda tidak memiliki Akun AWS, selesaikan langkah-langkah berikut untuk membuatnya.

Untuk mendaftar Akun AWS

1. Buka https://portal.aws.amazon.com/billing/signup.

2. Ikuti petunjuk secara online.

   Anda akan diminta untuk menerima panggilan telepon dan memasukkan kode verifikasi pada keypad telepon sebagai bagian dari prosedur pendaftaran.

   Saat Anda mendaftar Akun AWS, Pengguna root akun AWS dibuat. Pengguna root memiliki akses ke semua Layanan AWS dan sumber daya dalam akun. Sebagai praktik terbaik keamanan, tetapkan akses administratif ke pengguna administratif, dan hanya gunakan pengguna root untuk melakukan tugas yang memerlukan akses pengguna root.

AWS akan mengirimkan email konfirmasi kepada Anda setelah proses pendaftaran selesai. Anda dapat melihat aktivitas akun saat ini dan mengelola akun dengan mengunjungi https://aws.amazon.com/ dan memilih Akun Saya.

Membuat pengguna administratif

Setelah Anda mendaftarAkun AWS, amankanPengguna root akun AWS, aktifkanAWS IAM Identity Center, dan buat pengguna administratif sehingga Anda tidak menggunakan pengguna root untuk tugas sehari-hari.

Mengamankan Pengguna root akun AWS Anda

1. Masuk ke AWS Management Console sebagai pemilik akun dengan memilih Pengguna root dan memasukkan alamat email Akun AWS Anda. Pada halaman berikutnya, masukkan kata sandi Anda.

   Untuk bantuan masuk menggunakan pengguna root, lihat Masuk sebagai pengguna root dalam Panduan Pengguna AWS Sign-In.
2. Mengaktifkan autentikasi multi-faktor (MFA) untuk pengguna root Anda.

   Untuk petunjuk, lihat Mengaktifkan perangkat MFA virtual untuk pengguna root Akun AWS Anda (konsol) dalam Panduan Pengguna IAM.

Membuat pengguna administratif

1. Aktifkan Pusat Identitas IAM.

   Untuk petunjuk, lihat Mengaktifkan AWS IAM Identity Center di Panduan AWS IAM Identity Center Pengguna.

2. Di Pusat Identitas IAM, berikan akses administratif ke pengguna administratif.

   Untuk tutorial tentang menggunakan Direktori Pusat Identitas IAM sebagai sumber identitas Anda, lihat Mengkonfigurasi akses pengguna dengan default Direktori Pusat Identitas IAM di Panduan AWS IAM Identity Center Pengguna.

Masuk sebagai pengguna administratif

- Untuk masuk dengan pengguna Pusat Identitas IAM, gunakan URL masuk yang dikirim ke alamat email Anda saat Anda membuat pengguna Pusat Identitas IAM.

  Untuk bantuan masuk menggunakan pengguna Pusat Identitas IAM, lihat Masuk ke portal akses AWS dalam Panduan Pengguna AWS Sign-In.

Tambahkan izin yang diperlukan untuk mengakses dan mengaktifkan Audit Manager

Anda harus memberi pengguna izin yang diperlukan untuk mengaktifkan Audit Manager. Untuk pengguna yang membutuhkan akses penuh ke Audit Manager, gunakan kebijakan AWSAuditManagerAdministratorAccessterkelola. Ini adalah kebijakan AWS terkelola yang tersedia di AndaAkun AWS, dan ini adalah kebijakan yang direkomendasikan untuk administrator Audit Manager.

> **Tip**
>
> Sebagai praktik keamanan terbaik, kami menyarankan Anda memulai dengan kebijakan AWS terkelola dan kemudian beralih ke izin hak istimewa paling sedikit. AWSkebijakan terkelola memberikan izin untuk banyak kasus penggunaan umum. Namun, perlu diingat bahwa karena kebijakan AWS terkelola tersedia untuk digunakan oleh semua AWS pelanggan, kebijakan tersebut mungkin tidak memberikan izin hak istimewa paling sedikit untuk kasus penggunaan spesifik Anda. Oleh karena itu, kami menyarankan Anda mengurangi izin lebih lanjut dengan menentukan kebijakan terkelola pelanggan yang spesifik untuk kasus penggunaan Anda. Untuk informasi selengkapnya, lihat kebijakan AWS terkelola di Panduan AWS Identity and Access Management Pengguna.

Untuk memberikan akses, tambahkan izin ke pengguna, grup, atau peran Anda:

- Pengguna dan grup di AWS IAM Identity Center:

  Buat set izin. Ikuti instruksi di Buat set izin di Panduan Pengguna AWS IAM Identity Center.

- Pengguna yang dikelola di IAM melalui penyedia identitas:

  Buat peran untuk federasi identitas. Ikuti instruksi dalam Membuat peran untuk penyedia identitas pihak ketiga (federasi) di Panduan Pengguna IAM.

- Pengguna IAM:
  - Buat peran yang dapat diambil pengguna Anda. Ikuti instruksi dalam Membuat peran untuk pengguna IAM dalam Panduan Pengguna IAM.
  - (Tidak disarankan) Lampirkan kebijakan langsung ke pengguna atau tambahkan pengguna ke grup pengguna. Ikuti instruksi dalam Menambahkan izin ke pengguna (konsol) dalam Panduan Pengguna IAM.

Aktifkan AWS Audit Manager

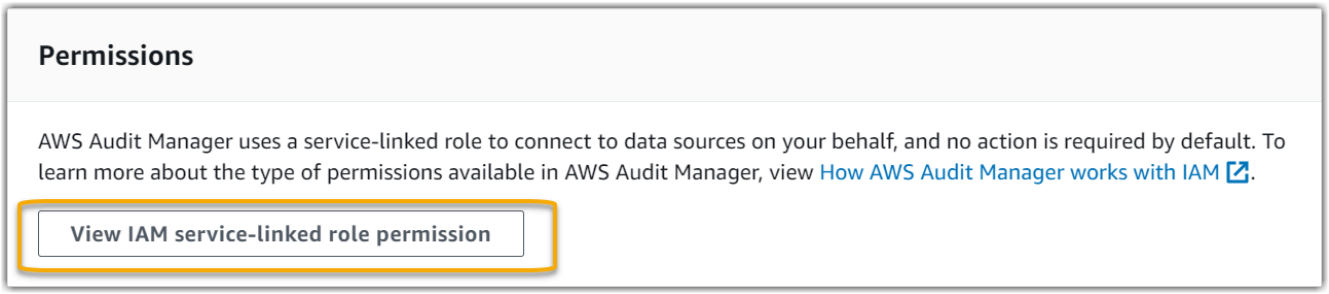
Anda dapat mengaktifkan Audit Manager menggunakanAWS Management Console, Audit Manager API, atau AWS Command Line Interface (AWS CLI).

Audit Manager console

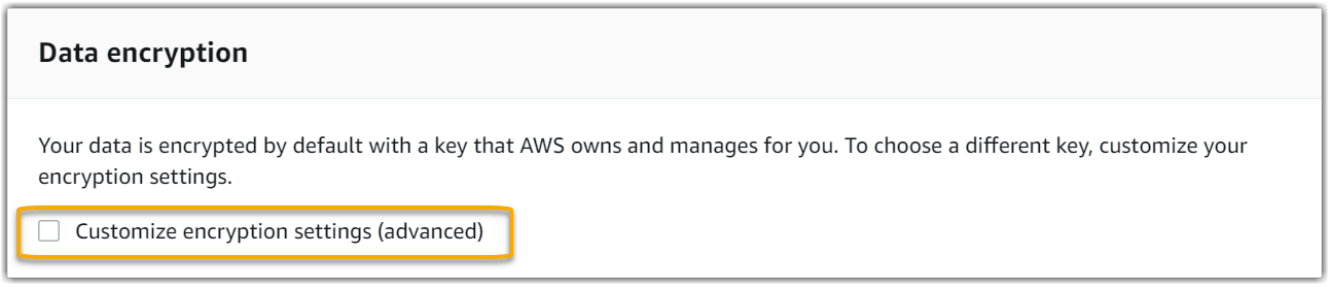
Untuk mengaktifkan Audit Manager menggunakan konsol

1. Buka konsol AWS Audit Manager di https://console.aws.amazon.com/auditmanager/home.
2. Gunakan kredensi identitas IAM Anda untuk masuk.
3. Pilih MenyiapkanAWS Audit Manager.

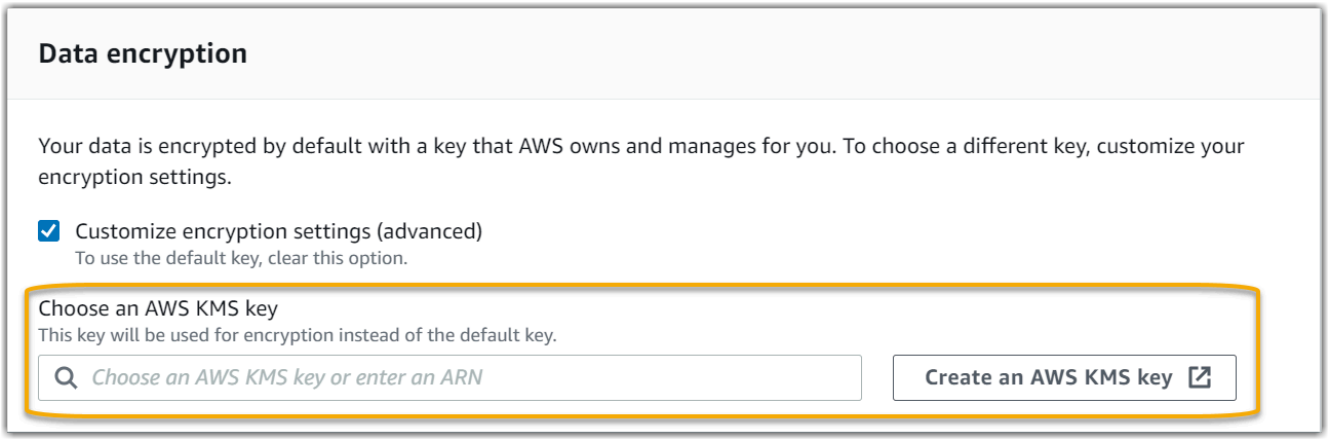
4. Di bawah Izin, tidak ada tindakan yang diperlukan. Ini karena Audit Manager menggunakan peran terkait layanan untuk terhubung ke sumber data atas nama Anda. Anda dapat meninjau peran terkait layanan dengan memilih Lihat izin peran terkait layanan IAM.



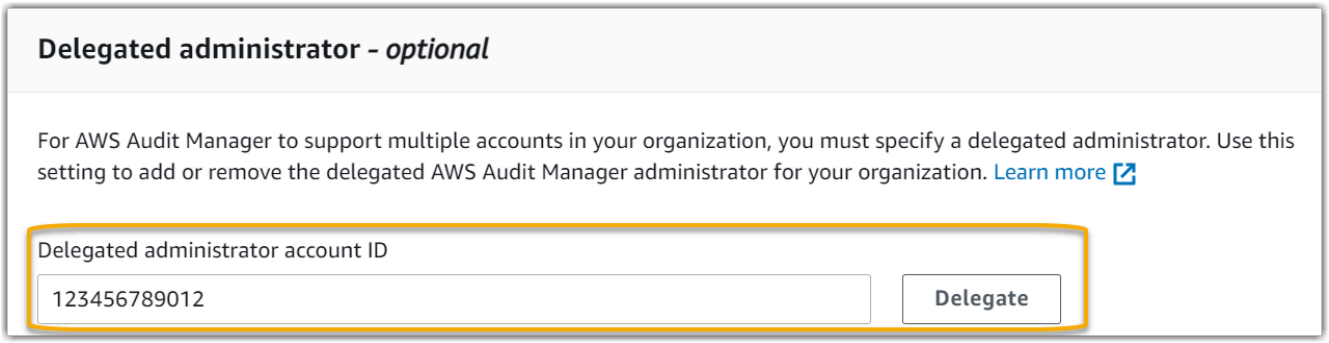
5. Di bawah Enkripsi data, opsi default adalah Audit Manager untuk membuat dan mengelola AWS KMS key untuk menyimpan data Anda dengan aman.



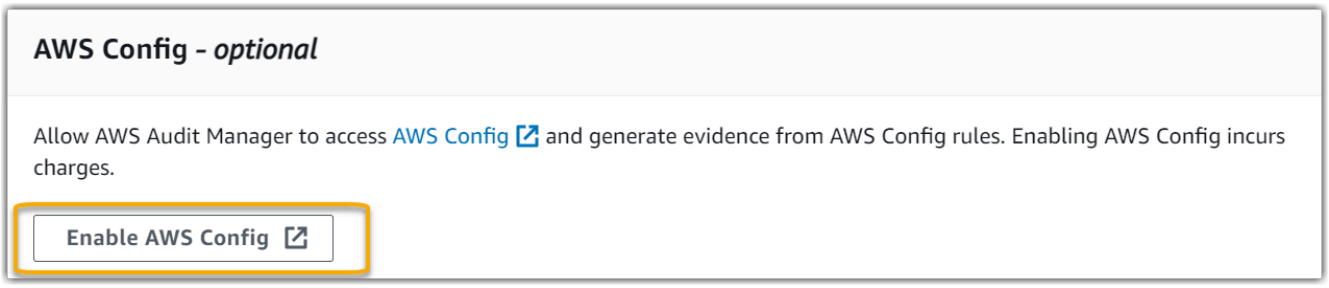
Jika Anda ingin menggunakan kunci terkelola pelanggan Anda sendiri untuk mengenkripsi data di Audit Manager, pilih kotak centang di samping Sesuaikan pengaturan enkripsi (lanjutan). Anda kemudian dapat memilih kunci KMS yang ada atau membuat yang baru.



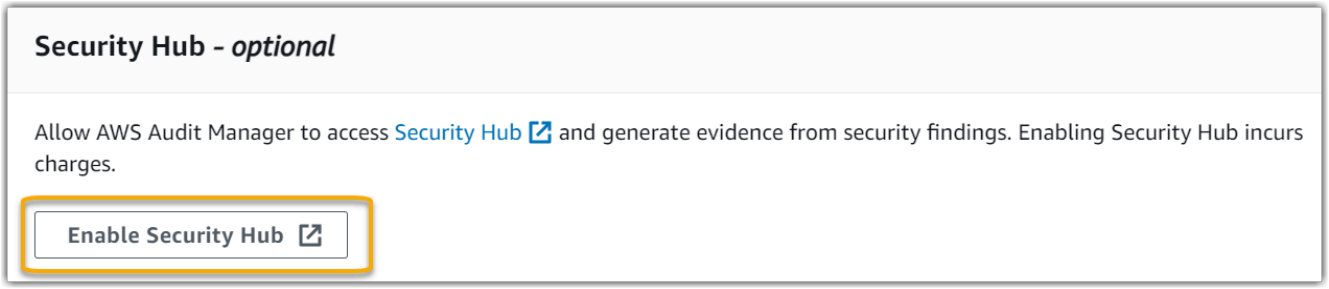
6. (Opsional) Di bawah Administrator yang didelegasikan - opsional, Anda dapat menentukan akun administrator yang didelegasikan jika Anda ingin Audit Manager menjalankan penilaian untuk beberapa akun. Untuk informasi dan rekomendasi selengkapnya, lihat Mengaktifkan dan menyiapkan AWS Organizations untuk digunakan dengan Audit Manager.



7. (Opsional) Di bawah AWS Config— opsional, kami menyarankan Anda mengaktifkan AWS Config untuk pengalaman yang optimal. Hal ini memungkinkan Audit Manager untuk menghasilkan bukti menggunakan AWS Config aturan. Untuk petunjuk dan setelan yang disarankan, lihat Mengaktifkan dan menyiapkan AWS Config untuk digunakan dengan Audit Manager.



8. (Opsional) Di bawah Security Hub — opsional, kami menyarankan Anda mengaktifkan Security Hub untuk pengalaman yang optimal. Hal ini memungkinkan Audit Manager untuk menghasilkan bukti menggunakan pemeriksaan Security Hub. Untuk petunjuk dan setelan yang disarankan, lihat Mengaktifkan dan menyiapkan AWS Security Hub untuk digunakan dengan Audit Manager.



9. Pilih Penyiapan lengkap untuk menyelesaikan proses penyiapan.

AWS CLI

Untuk mengaktifkan Audit Manager menggunakan AWS CLI

Di baris perintah, jalankan perintah register-account menggunakan parameter pengaturan berikut:

- `--kms-key`(opsional) — Gunakan parameter ini untuk mengenkripsi data Audit Manager Anda menggunakan kunci terkelola pelanggan Anda sendiri. Jika Anda tidak menentukan opsi di sini, Audit Manager membuat dan mengelola atas nama Anda untuk penyimpanan data yang aman. AWS KMS key
- `--delegated-admin-account`(opsional) — Gunakan parameter ini untuk menunjuk akun administrator yang didelegasikan organisasi Anda untuk Audit Manager. Jika Anda tidak menentukan opsi di sini, tidak ada administrator yang didelegasikan yang terdaftar.

Contoh masukan (ganti *`teks placeholder`* dengan informasi Anda sendiri):

```
aws auditmanager register-account \
--kms-key arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab \
--delegated-admin-account 111122224444
```

Contoh keluaran:

```
{
    "status": "ACTIVE"
}
```

Untuk informasi selengkapnya tentang AWS CLI dan untuk petunjuk tentang cara menginstal AWS CLI alat, lihat yang berikut ini di Panduan AWS Command Line Interface Pengguna.

- Panduan Pengguna Antarmuka Baris Perintah AWS
- Mendapatkan Set Up dengan AWS Command Line Interface

Audit Manager API

Untuk mengaktifkan Audit Manager menggunakan Audit Manager API

Gunakan RegisterAccountoperasi dengan parameter pengaturan berikut:

- KMSKey (opsional) - Gunakan parameter ini untuk mengenkripsi data Audit Manager Anda menggunakan kunci terkelola pelanggan Anda sendiri. Jika Anda tidak menentukan opsi di sini, Audit Manager membuat dan mengelola atas nama Anda untuk penyimpanan data yang aman. AWS KMS key
- delegatedAdminAccount(opsional) — Gunakan parameter ini untuk menentukan akun administrator yang didelegasikan organisasi Anda untuk Audit Manager. Jika Anda tidak menentukannya, tidak ada administrator yang didelegasikan yang terdaftar.

Contoh masukan (ganti *teks placeholder* dengan informasi Anda sendiri):

```
{
    "kmsKey":"arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "delegatedAdminAccount":"111122224444"
}
```

Contoh keluaran:

```
{
  "status": "ACTIVE"
}
```

Rekomendasi

Untuk pengalaman optimal di Audit Manager, kami sarankan Anda menyiapkan fitur-fitur berikut dan mengaktifkan yang berikut iniLayanan AWS.

Topik

- Siapkan fitur Audit Manager yang direkomendasikan
- Siapkan integrasi yang direkomendasikan dengan yang lain Layanan AWS

Siapkan fitur Audit Manager yang direkomendasikan

Setelah mengaktifkan Audit Manager, sebaiknya aktifkan fitur pencari bukti.

Pencari buktimenyediakan cara yang ampuh untuk mencari bukti di Audit Manager. Alih-alih menelusuri folder bukti yang sangat bersarang untuk menemukan apa yang Anda cari, Anda dapat

menggunakan pencari bukti untuk menanyakan bukti Anda dengan cepat. Jika Anda menggunakan pencari bukti sebagai administrator yang didelegasikan, Anda dapat mencari bukti di semua akun anggota di organisasi Anda. Dengan menggunakan kombinasi filter dan pengelompokan, Anda dapat semakin mempersempit ruang lingkup kueri penelusuran Anda. Misalnya, jika Anda menginginkan tampilan tingkat tinggi tentang kesehatan sistem Anda, lakukan penelusuran luas dan filter berdasarkan penilaian, rentang tanggal, dan kepatuhan sumber daya. Jika tujuan Anda adalah untuk memulihkan sumber daya tertentu, Anda dapat melakukan pencarian sempit untuk menargetkan bukti untuk kontrol atau ID sumber daya tertentu. Setelah menentukan filter, Anda dapat mengelompokkan lalu melihat pratinjau hasil penelusuran yang cocok sebelum membuat laporan penilaian.

Untuk menggunakan pencari bukti, Anda harus mengaktifkan fitur ini dari setelan Audit Manager. Untuk petunjuk, silakan lihat Pengaturan pencari bukti.

Siapkan integrasi yang direkomendasikan dengan yang lain Layanan AWS

Untuk pengalaman optimal di Audit Manager, kami sangat menyarankan agar Anda mengaktifkan hal-hal berikutLayanan AWS:

- AWS Organizations— Anda dapat menggunakan Organizations untuk menjalankan penilaian Audit Manager melalui beberapa akun dan mengkonsolidasikan bukti ke dalam akun administrator yang didelegasikan.
- AWS Security Hubdan AWS Config— Saat Anda mengaktifkan iniLayanan AWS, mereka dapat digunakan sebagai tipe sumber data untuk kontrol dalam penilaian Audit Manager Anda. Audit Manager kemudian dapat melaporkan hasil pemeriksaan kepatuhan langsung dari layanan ini.

Topik

Aktifkan dan atur AWS Config (opsional)

Banyak kontrol di Audit Manager digunakan AWS Config sebagai tipe sumber data. Untuk mendukung kontrol ini, Anda harus mengaktifkan AWS Config semua akun di masing-masing Wilayah AWS tempat Audit Manager diaktifkan. Jika Audit Manager mencoba mengumpulkan bukti

untuk kontrol yang digunakan AWS Config sebagai tipe sumber data, dan AWS Config aturan terkait tidak diaktifkan, tidak ada bukti yang dikumpulkan untuk kontrol tersebut.

Audit Manager tidak mengelola AWS Config untuk Anda. Anda dapat mengikuti langkah-langkah ini untuk mengaktifkan AWS Config dan mengonfigurasi pengaturannya.

Tugas untuk diintegrasikan AWS Config dengan Audit Manager

- Langkah 1: Aktifkan AWS Config
- Langkah 2: Konfigurasikan AWS Config pengaturan Anda untuk digunakan dengan Audit Manager

Langkah 1: Aktifkan AWS Config

Anda dapat mengaktifkan AWS Config menggunakan AWS Config konsol atau API. Untuk instruksi, lihat Memulai dengan AWS Config dalam Panduan Developer AWS Config.

Langkah 2: Konfigurasikan AWS Config pengaturan Anda untuk digunakan dengan Audit Manager

> **Important**
>
> Mengaktifkan AWS Config adalah rekomendasi opsional. Namun, jika Anda mengaktifkanAWS Config, pengaturan berikut diperlukan.

Setelah mengaktifkanAWS Config, pastikan Anda juga mengaktifkan AWS Config aturan atau menerapkan paket kesesuaian untuk standar kepatuhan yang terkait dengan audit Anda. Langkah ini memastikan bahwa Audit Manager dapat mengimpor temuan untuk AWS Config aturan yang Anda aktifkan.

Setelah Anda mengaktifkan AWS Config aturan, kami sarankan Anda meninjau parameter aturan itu. Anda kemudian harus memvalidasi parameter tersebut terhadap persyaratan kerangka kepatuhan yang Anda pilih. Jika diperlukan, Anda dapat memperbarui parameter aturan AWS Config untuk memastikan bahwa itu selaras dengan persyaratan kerangka kerja. Ini akan membantu memastikan bahwa penilaian Anda mengumpulkan bukti pemeriksaan kepatuhan yang benar untuk kerangka kerja tertentu.

Misalnya, anggaplah Anda membuat penilaian untuk CIS v1.2.0. Kerangka kerja ini memiliki kontrol bernama 1.4 — Pastikan kunci akses diputar setiap 90 hari atau kurang. DalamAWS Config, access-keys-rotatedaturan memiliki `maxAccessKeyAge` parameter dengan nilai default 90 hari. Akibatnya, aturan tersebut sejalan dengan persyaratan kontrol. Jika Anda tidak menggunakan nilai default,

pastikan bahwa nilai yang Anda gunakan sama dengan atau lebih besar dari persyaratan 90 hari dari CIS v1.2.0.

Anda dapat menemukan detail parameter default untuk setiap aturan terkelola dalam AWS Configdokumentasi. Untuk petunjuk tentang cara mengonfigurasi aturan, lihat Bekerja dengan Aturan AWS Config Terkelola.

Aktifkan dan atur AWS Security Hub (opsional)

Banyak kontrol di Audit Manager menggunakan Security Hub sebagai tipe sumber data. Untuk mendukung kontrol ini, Anda harus mengaktifkan Security Hub di semua akun di setiap Wilayah tempat Audit Manager diaktifkan. Jika Audit Manager mencoba mengumpulkan bukti untuk kontrol yang menggunakan Security Hub sebagai tipe sumber data, dan standar Security Hub terkait tidak diaktifkan, tidak ada bukti yang dikumpulkan untuk kontrol tersebut.

Audit Manager tidak mengelola Security Hub untuk Anda. Anda dapat mengikuti langkah-langkah ini untuk mengaktifkan Security Hub dan mengonfigurasi pengaturannya.

Tugas untuk diintegrasikan AWS Security Hub dengan Audit Manager

- Langkah 1: Aktifkan AWS Security Hub
- Langkah 2: Konfigurasikan pengaturan Security Hub Anda untuk digunakan dengan Audit Manager

Langkah 1: Aktifkan AWS Security Hub

Anda dapat mengaktifkan Security Hub menggunakan konsol atau API. Untuk petunjuk, lihat Menyiapkan AWS Security Hub di Panduan AWS Security Hub Pengguna.

Langkah 2: Konfigurasikan pengaturan Security Hub Anda untuk digunakan dengan Audit Manager

> **Important**
>
> Mengaktifkan Security Hub adalah rekomendasi opsional. Namun, jika Anda mengaktifkan Security Hub, pengaturan berikut diperlukan.

Setelah mengaktifkan Security Hub, pastikan Anda juga melakukan hal berikut:

- Mengaktifkan AWS Config dan mengonfigurasi perekaman sumber daya - Security Hub menggunakan AWS Config aturan terkait layanan untuk melakukan sebagian besar pemeriksaan

keamanannya untuk kontrol. Untuk mendukung kontrol ini, AWS Config harus diaktifkan dan dikonfigurasi untuk merekam sumber daya yang diperlukan untuk kontrol yang telah Anda aktifkan di setiap standar yang diaktifkan.

- Aktifkan semua standar keamanan - Langkah ini memastikan bahwa Audit Manager dapat mengimpor temuan untuk semua standar kepatuhan yang didukung.
- Aktifkan setelan temuan kontrol konsolidasi di Security Hub - Setelan ini diaktifkan secara default jika Anda mengaktifkan Security Hub pada atau setelah 23 Februari 2023.

> **Note**
>
> Saat Anda mengaktifkan temuan terkonsolidasi, Security Hub menghasilkan satu temuan untuk setiap pemeriksaan keamanan (bahkan ketika pemeriksaan yang sama digunakan di beberapa standar). Setiap temuan Security Hub dikumpulkan sebagai satu penilaian sumber daya unik di Audit Manager. Akibatnya, temuan konsolidasi menghasilkan penurunan total penilaian sumber daya unik yang dilakukan Audit Manager untuk temuan Security Hub. Untuk alasan ini, menggunakan temuan konsolidasi seringkali dapat mengakibatkan pengurangan biaya penggunaan Audit Manager Anda. Untuk informasi selengkapnya tentang menggunakan Security Hub sebagai tipe sumber data, lihatAWS Security Hub kontrol yang didukung oleh AWS Audit Manager. Untuk informasi selengkapnya tentang harga Audit Manager, lihat AWS Audit ManagerHarga.

Jika Anda menggunakan AWS Organizations dan ingin mengumpulkan bukti Security Hub dari akun anggota, Anda juga harus melakukan langkah-langkah berikut di Security Hub.

Untuk menyiapkan setelan Security Hub organisasi Anda

1. Masuk ke AWS Management Console dan buka AWS Security Hub konsol di https://console.aws.amazon.com/securityhub/.
2. Dengan menggunakan akun AWS Organizations manajemen Anda, tetapkan akun sebagai administrator yang didelegasikan untuk Security Hub. Untuk informasi selengkapnya, lihat Menetapkan akun administrator Security Hub di Panduan AWS Security Hub Pengguna.

> **Note**
>
> Pastikan akun administrator yang didelegasikan yang Anda tetapkan di Security Hub sama dengan yang Anda gunakan di Audit Manager.

3. Menggunakan akun administrator yang didelegasikan Organizations, buka Pengaturan, Akun, pilih semua akun, lalu tambahkan sebagai anggota dengan memilih Daftar otomatis. Untuk informasi selengkapnya, lihat Mengaktifkan akun anggota dari organisasi Anda di Panduan AWS Security Hub Pengguna.
4. Aktifkan AWS Config untuk setiap akun anggota organisasi. Untuk informasi selengkapnya, lihat Mengaktifkan akun anggota dari organisasi Anda di Panduan AWS Security Hub Pengguna.
5. Aktifkan standar keamanan PCI DSS untuk setiap akun anggota organisasi. Standar AWS CIS Foundations Benchmark dan standar Praktik Terbaik AWS Foundational sudah diaktifkan secara default. Untuk informasi selengkapnya, lihat Mengaktifkan standar keamanan di Panduan AWS Security Hub Pengguna.

Aktifkan AWS Organizations (opsional)

Audit Manager mendukung beberapa akun melalui integrasi denganAWS Organizations. Audit Manager dapat menjalankan penilaian melalui beberapa akun dan mengkonsolidasikan bukti ke dalam akun administrator yang didelegasikan. Administrator yang didelegasikan memiliki izin untuk membuat dan mengelola sumber daya Audit Manager dengan organisasi sebagai zona kepercayaan. Hanya akun manajemen yang dapat menunjuk administrator yang didelegasikan.

Tugas untuk diintegrasikan AWS Organizations dengan Audit Manager

- Langkah 1: Buat atau bergabung dengan organisasi
- Langkah 2: Aktifkan semua fitur di organisasi Anda
- Langkah 3: Tentukan administrator yang didelegasikan untuk Audit Manager

Langkah 1: Buat atau bergabung dengan organisasi

Jika Anda Akun AWS bukan bagian dari organisasi, Anda dapat membuat atau bergabung dengan organisasi. Untuk petunjuk, lihat Membuat dan mengelola organisasi di Panduan AWS Organizations Pengguna.

Langkah 2: Aktifkan semua fitur di organisasi Anda

Selanjutnya, Anda harus mengaktifkan semua fitur di organisasi Anda. Untuk petunjuk, lihat Mengaktifkan semua fitur di organisasi Anda di Panduan AWS Organizations Pengguna.

Langkah 3: Tentukan administrator yang didelegasikan untuk Audit Manager

Sebaiknya aktifkan Audit Manager menggunakan akun manajemen Organizations, lalu tentukan administrator yang didelegasikan. Setelah itu, Anda dapat menggunakan akun administrator yang didelegasikan untuk masuk dan menjalankan penilaian. Sebagai praktik terbaik, kami menyarankan Anda hanya membuat penilaian menggunakan akun administrator yang didelegasikan, bukan akun manajemen.

> ⚠ Warning
>
> Setelah menentukan administrator yang didelegasikan menggunakan akun manajemen Organizations, akun manajemen Anda tidak dapat lagi membuat penilaian tambahan di Audit Manager. Selain itu, pengumpulan bukti berhenti untuk setiap penilaian yang ada yang dibuat oleh akun manajemen. Sebagai gantinya, Audit Manager mengumpulkan dan melampirkan bukti ke administrator yang didelegasikan, yang merupakan akun utama untuk mengelola penilaian organisasi Anda.

Untuk menambah atau mengubah administrator yang didelegasikan setelah Anda mengaktifkan Audit Manager, lihat AWS Audit Managerpengaturan, Administrator yang didelegasikan.

Masalah yang perlu dipertimbangkan:

- Anda tidak dapat menggunakan akun manajemen sebagai administrator yang didelegasikan di Audit Manager.
- Jika Anda ingin mengaktifkan Audit Manager di lebih dari satuWilayah AWS, Anda harus menetapkan akun administrator yang didelegasikan secara terpisah di setiap Wilayah. Dalam pengaturan Audit Manager, Anda harus menetapkan akun administrator yang didelegasikan yang sama di semua Wilayah.
- Jika Anda memberikan kunci terkelola pelanggan saat mengaktifkan Audit Manager, pastikan akun administrator yang didelegasikan memiliki akses pada kunci KMS tersebut. Untuk meninjau dan mengubah setelan enkripsi Audit Manager, lihatEnkripsi data.
- Untuk solusi untuk masalah umum Organizations dan administrator yang didelegasikan di Audit Manager, lihatMemecahkan masalah administrator dan masalah yang didelegasikan AWS Organizations.

Apa yang harus saya lakukan selanjutnya?

Sekarang setelah Anda menyiapkan Audit Manager, Anda siap untuk memulai menggunakan layanan ini. Anda juga dapat mengunjungi halaman pengaturan konsol untuk memperbarui setelan apa pun yang Anda pilih saat menyiapkan Audit Manager.

Memulai Audit Manager

Anda dapat memulai Audit Manager dengan mengikuti tutorial yang memandu Anda melalui cara membuat penilaian pertama Anda. Untuk informasi selengkapnya, lihat Tutorial untuk Pemilik Audit: Membuat penilaian.

Memperbarui setelan Audit Manager

Anda dapat memperbarui pengaturan Anda kapan saja. Untuk informasi selengkapnya, lihat Pengaturan AWS Audit Manager.

Memulai dengan AWS Audit Manager

Gunakan step-by-step tutorial di bagian ini untuk mempelajari cara melakukan tugas menggunakanAWS Audit Manager.

> **Tip**
>
> Tutorial berikut dikategorikan berdasarkan audiens. Pilih tutorial yang sesuai untuk Anda berdasarkan peran Anda sebagai pemilik audit atau delegasi.
>
> - Pemilik audit adalah pengguna Audit Manager yang bertanggung jawab untuk membuat dan mengelola penilaian. Dalam dunia bisnis, pemilik audit biasanya merupakan profesional tata kelola, manajemen risiko, dan kepatuhan (GRC). Namun, dalam konteks Audit Manager, individu dari SecOps atau DevOps tim mungkin juga menganggap persona pengguna dari pemilik audit. Pemilik audit dapat meminta bantuan dari ahli materi pelajaran—juga dikenal sebagai delegasi—untuk meninjau kontrol spesifik dan memvalidasi bukti. Pemilik audit harus memiliki izin yang diperlukan untuk mengelola penilaian.
> - Delegasi adalah ahli materi pelajaran dengan keahlian teknis atau bisnis khusus. Meskipun mereka tidak memiliki atau mengelola penilaian Audit Manager, mereka tetap dapat berkontribusi kepada mereka. Delegasi membantu pemilik audit dengan tugas-tugas seperti memvalidasi bukti untuk kontrol yang berada di bawah bidang keahlian mereka. Delegasi memiliki izin terbatas di Audit Manager. Ini karena pemilik audit mendelegasikan set kontrol khusus untuk ditinjau, dan bukan keseluruhan penilaian.
>
> Untuk informasi selengkapnya tentang persona ini dan konsep Audit Manager lainnya, lihat Pemilik dan Delegasi Audit diAWS Audit Managerkonsep dan terminologi bagian panduan ini. Untuk informasi lebih lanjut tentang izin IAM yang disarankan untuk setiap persona, lihat Kebijakan yang disarankan untuk persona pengguna di AWS Audit Manager.

Tutorial Audit Manager

Membuat penilaian

Pemirsa: Pemilik Audit

Ikhtisar: Ikuti step-by-step petunjuk untuk membuat penilaian pertama Anda dan bangun dan berjalan cepat. Tutorial ini memandu Anda melalui bagaimana Anda dapat menggunakan satu kerangka kerja standar untuk membuat penilaian dan memulai pengumpulan bukti otomatis.

Meninjau set kontrol

Audience: Delegasi

Ikhtisar: Bantu pemilik audit dengan meninjau bukti untuk kontrol yang termasuk dalam bidang keahlian Anda. Pelajari cara meninjau set kontrol dan bukti terkait, menambahkan komentar, mengunggah bukti tambahan, dan memperbarui status kontrol.

Tutorial untuk Pemilik Audit: Membuat penilaian

Tutorial ini memberikan pengantarAWS Audit Manager. Dalam tutorial ini, Anda membuat penilaian menggunakan AWS Audit ManagerContoh Framework. Dengan membuat penilaian, Anda memulai proses pengumpulan bukti otomatis yang sedang berlangsung untuk kontrol dalam kerangka kerja tersebut.

Tutorial ini menunjukkan cara melakukan hal berikut:

- Pilih kerangka kerja standar untuk membuat penilaian
- TentukanAWS akun yang akan disertakan dalam penilaian Anda
- TentukanAWS layanan yang akan disertakan dalam penilaian Anda
- Tentukan pemilik audit untuk penilaian Anda
- Tinjau dan buat penilaian Anda

Sebelum Anda mulai tutorial ini, pastikan Anda terlebih dahulu memenuhi syarat berikut ini:

- Anda menyelesaikan semua prasyarat yang dijelaskan dalamMenyiapkan AWS Audit Manager. Anda harus menggunakanAWS akun Anda danAWS Audit Manager konsol untuk menyelesaikan tutorial ini.
- Identitas IAM Anda diberikan izin yang sesuai untuk membuat dan mengelola penilaian diAWS Audit Manager. Dua kebijakan yang disarankan yang memberikan izin ini adalah Contoh 2: Izinkan akses administrator penuh dan Contoh 3: Izinkan akses manajemen.
- Anda sudah familiar dengan terminologi dan fungsionalitas Audit Manager. Untuk gambaran umum, lihatApakah AWS Audit Manager itu? danAWS Audit Managerkonsep dan terminologi.

> **Note**
>
> AWS Audit Managermembantu mengumpulkan bukti yang relevan untuk memverifikasi kepatuhan terhadap kerangka kerja dan peraturan kepatuhan tertentu. Namun, itu tidak menilai kepatuhan Anda sendiri. Bukti yang dikumpulkan melaluiAWS Audit Manager karena itu mungkin tidak mencakup semua informasi tentangAWS penggunaan Anda yang diperlukan untuk audit. AWS Audit Managerbukan pengganti penasihat hukum atau pakar kepatuhan.

Langkah 1: Tentukan detail penilaian

Untuk langkah pertama, pilih kerangka kerja dan berikan informasi dasar untuk penilaian Anda.

Untuk menentukan rincian penilaian

1. Buka konsol AWS Audit Manager di https://console.aws.amazon.com/auditmanager/home.
2. Pilih LuncurkanAWS Audit Manager.
3. Di panel navigasi, pilih Memulai, dan kemudian pilih Mulai dengan kerangka kerja.
4. Pilih kerangka kerja yang Anda inginkan, lalu pilih Buat penilaian dari kerangka kerja. Contoh ini menggunakan KerangkaAWS Audit Manager Contoh.
5. Di bawah Nama penilaian Anda, masukkan nama untuk penilaian Anda.
6. (Opsional) Di bawah deskripsi penilaian Anda, masukkan deskripsi untuk penilaian Anda.
7. Di bawah tujuan laporan Penilaian, pilih bucket Amazon S3 tempat Anda ingin menyimpan laporan penilaian Anda.
8. Di bawah Frameworks, konfirmasikan bahwa AWS Audit ManagerContoh Framework (atau kerangka pilihan Anda) dipilih.
9. Di bawah Tag, pilih Tambahkan tag baru untuk mengaitkan tag dengan penilaian Anda. Anda dapat menentukan kunci dan nilai untuk setiap tanda. Kunci tag wajib dan dapat digunakan sebagai kriteria pencarian saat Anda mencari penilaian ini. Untuk informasi lebih lanjut tentang tanda diAWS Audit Manager, lihatPenandaan pada sumber daya AWS Audit Manager.
10. Pilih Selanjutnya.

Langkah 2: TentukanAWS akun di ruang lingkup

Selanjutnya, tentukanAWS akun yang ingin Anda sertakan dalam lingkup penilaian Anda.

AWS Audit Managerterintegrasi denganAWS Organizations, sehingga Anda dapat menjalankan penilaian Audit Manager di beberapa akun dan mengkonsolidasikan bukti ke dalam akun administrator yang didelegasikan. Untuk mengaktifkan Organizations di Audit Manager (jika Anda belum melakukannya), lihatAktifkan AWS Organizations (opsional) di halaman Menyiapkan panduan ini.

> **Note**
>
> Audit Manager dapat mendukung hingga sekitar 150 akun dalam lingkup penilaian. Jika Anda mencoba memasukkan lebih dari 150 akun, pembuatan penilaian mungkin gagal.

Untuk menentukan akun dalam lingkup

1. Di bawah AWSakun, pilihAWS akun yang ingin Anda sertakan dalam lingkup penilaian Anda.
   - Jika Anda mengaktifkan OrganizationsAWS Audit Manager, beberapa akun akan dicantumkan.
   - Jika Anda tidak mengaktifkan Organizations di Audit Manager, hanya akun Anda saat ini yang terdaftar.
2. Pilih Selanjutnya.

Langkah 3: TentukanAWS layanan di ruang lingkup

Kerangka kerja yang Anda pilih sebelumnya mendefinisikanAWS layanan yang dipantau dan dikumpulkan oleh Audit Manager.

Bila Anda menggunakan konsol Audit Manager untuk membuat penilaian dari kerangka kerja standar, daftar layanan dalam lingkup dipilih sebelumnya dan tidak dapat diedit. Ini karena Audit Manager secara otomatis memetakan dan memilih sumber data dan layanan untuk Anda. Pilihan ini dibuat sesuai dengan persyaratan kerangka standar. JikaAWS layanan yang tercantum tidak dipilih, Audit Manager tidak mengumpulkan bukti dari sumber daya yang terkait dengan layanan tersebut. Ini juga terjadi jika dipilih tetapi Anda belum berlangganan di lingkungan Anda.

Dalam langkah tutorial ini, Anda dapat meninjauAWS layanan mana yang berada dalam lingkup penilaian berdasarkan definisi kerangka kerja. Untuk mempelajari lebih lanjut tentang kerangka kerja dan cara mengakses dan memeriksanya, lihatPustaka kerangka kerja bagian panduan ini.

Untuk menentukanAWS layanan dalam lingkup

1. Di bawah AWSlayanan, tinjau daftar layanan yang berada dalam lingkup penilaian ini.
2. Pilih Selanjutnya.

> **Tip**
>
> Jika Anda perlu mengedit daftar layanan dalam lingkup, Anda dapat melakukannya dengan menggunakan CreateAssessmentAPI yang disediakan oleh Audit Manager.
> Atau, Anda dapat menyesuaikan kerangka kerja standar dan kemudian membuat penilaian dari kerangka kerja kustom.

Langkah 4: Tentukan pemilik audit

Pada langkah ini, Anda menentukan pemilik audit untuk penilaian Anda. Pemilik audit adalah individu di tempat kerja Anda—biasanya dari GRC, SecOps, atau DevOps tim—yang bertanggung jawab untuk mengelola penilaian Audit Manager. Kami menyarankan agar mereka menggunakan AWSAuditManagerAdministratorAccesskebijakan.

Untuk menentukan pemilik audit

1. Di bawah pemilik Audit, pilih pemilik audit untuk penilaian Anda. Untuk menemukan pemilik audit tambahan, gunakan bilah pencarian untuk mencari berdasarkan nama atauAWS akun.
2. Pilih Selanjutnya.

Langkah 5: Tinjau dan buat

Tinjau informasi untuk penilaian Anda. Untuk mengubah informasi selangkah, pilih Edit. Setelah selesai, pilih Buat penilaian untuk meluncurkan penilaian pertama Anda dan mulai pengumpulan bukti yang sedang berlangsung.

Setelah Anda membuat penilaian, pengumpulan bukti berlanjut hingga Anda mengubah status penilaian menjadi tidak aktif. Atau, Anda dapat menghentikan pengumpulan bukti untuk kontrol tertentu dengan mengubah status kontrol menjadi tidak aktif.

> **Note**
>
> Bukti otomatis tersedia 24 jam setelah Anda membuat penilaian. AWS Audit Managersecara otomatis mengumpulkan bukti dari berbagai sumber data, dan frekuensi pengumpulan bukti itu didasarkan pada jenis bukti. Untuk informasi lain, lihat Frekuensi pengumpulan bukti dalam panduan ini.

Apa yang saya lakukan selanjutnya?

Kami menyarankan Anda untuk terus mempelajari lebih lanjut tentang konsep dan alat yang diperkenalkan dalam tutorial ini. Anda dapat melakukannya dengan meninjau sumber daya berikut ini:

- Meninjau penilaian- Memperkenalkan Anda ke halaman penilaian tempat Anda dapat menjelajahi berbagai komponen penilaian Anda.
- Penilaian di AWS Audit Manager- Dibangun di atas tutorial ini dan memberikan informasi mendalam tentang konsep dan tugas untuk mengelola penilaian. Dalam dokumen ini, kami sangat menyarankan Anda memeriksa topik-topik berikut ini:
  - Cara membuat penilaian dari kerangka kerja yang berbeda
  - Cara meninjau bukti dalam penilaian dan menghasilkan laporan penilaian
  - Cara mengubah status penilaian atau menghapus penilaian
- Pustaka kerangka kerja- Memperkenalkan perpustakaan kerangka kerja dan menjelaskan cara membuat kerangka kerja khusus untuk kebutuhan kepatuhan spesifik Anda sendiri.
- Pustaka kontrol- Memperkenalkan pustaka kontrol dan menjelaskan cara membuat kontrol khusus untuk digunakan dalam kerangka kerja kustom Anda.
- AWS Audit Managerkonsep dan terminologi— Memberikan definisi untuk konsep dan terminologi yang digunakan di Audit Manager.
- [Video] Kumpulkan Bukti dan Kelola Penggunaan Data AuditAWS Audit Manager - Menunjukkan proses pembuatan penilaian yang dijelaskan dalam tutorial ini, dan tugas lain seperti meninjau kontrol dan membuat laporan penilaian.

Tutorial untuk Delegasi: Meninjau set kontrol

Tutorial ini menjelaskan cara meninjau set kontrol yang dibagikan dengan Anda oleh pemilik auditAWS Audit Manager.

Pemilik audit menggunakan Audit Manager untuk membuat penilaian dan mengumpulkan bukti untuk kontrol yang tercantum dalam penilaian tersebut. Terkadang pemilik audit mungkin memiliki pertanyaan atau memerlukan bantuan saat memvalidasi bukti untuk set kontrol. Dalam situasi ini, pemilik audit dapat mendelegasikan kontrol yang ditetapkan kepada ahli materi pelajaran untuk ditinjau.

Sebagai delegasi, Anda membantu pemilik audit untuk meninjau bukti yang dikumpulkan untuk kontrol yang termasuk dalam bidang keahlian Anda.

Tutorial ini menunjukkan cara melakukan hal berikut:

- Mengakses pemberitahuan yang dikirimkan kepada Anda oleh pemilik audit
- Tinjau set kontrol dan bukti terkait
- Unggah bukti manual untuk mendukung kontrol
- Tambahkan komentar untuk kontrol yang Anda tinjau
- Memperbarui status kontrol
- Kirimkan set kontrol yang ditinjau ke pemilik audit saat peninjauan Anda selesai

Sebelum Anda mulai tutorial ini, pastikan Anda terlebih dahulu memenuhi syarat berikut ini:

- AWSAkun Anda sudah diatur. Untuk menyelesaikan tutorial ini, Anda harus menggunakanAWS akun danAWS Audit Manager konsol Anda. Untuk informasi selengkapnya, lihat Menyiapkan AWS Audit Manager.
- Anda sudah familiar dengan terminologi dan fungsionalitas Audit Manager. Untuk ikhtisar umum Audit Manager, lihatApakah AWS Audit Manager itu? danAWS Audit Managerkonsep dan terminologi.

Langkah 1: Akses notifikasi Anda

Mulailah dengan masuk keAWS Audit Manager, di mana Anda dapat mengakses notifikasi untuk melihat set kontrol yang telah didelegasikan kepada Anda untuk ditinjau.

Untuk mengakses notifikasi

1. Buka konsol AWS Audit Manager di https://console.aws.amazon.com/auditmanager/home.
2. Di panel navigasi kiri, pilih Pemberitahuan. Atau, di bilah flash biru di bagian atas halaman, pilih Lihat notifikasi untuk membuka halaman notifikasi.
3. Pada halaman Notifikasi, Anda meninjau daftar set kontrol yang telah didelegasikan kepada Anda. Tabel notifikasi tersebut mencakup informasi berikut:
   - Tanggal - Tanggal ketika set kontrol didelegasikan.
   - Penilaian - Nama penilaian yang terkait dengan set kontrol. Anda dapat memilih nama penilaian untuk membuka halaman detail penilaian.
   - Set kontrol - Nama set kontrol yang didelegasikan kepada Anda untuk ditinjau.
   - Sumber - Pengguna atau peran yang mendelegasikan kontrol yang ditetapkan untuk Anda.
   - Deskripsi - Instruksi peninjauan yang diberikan oleh pemilik audit.

> **Tip**
>
> Anda juga dapat berlangganan topik SNS untuk menerima peringatan email saat set kontrol ditetapkan kepada Anda untuk ditinjau. Untuk informasi lebih lanjut, lihat Notifikasi di AWS Audit Manager.

Langkah 2: Tinjau set kontrol dan bukti terkait

Langkah selanjutnya adalah meninjau set kontrol yang didelegasikan oleh pemilik audit kepada Anda. Dengan memeriksa kontrol dan bukti mereka, Anda dapat menentukan apakah ada tindakan tambahan yang diperlukan untuk kontrol. Tindakan tambahan dapat mencakup pengunggahan bukti tambahan secara manual untuk menunjukkan kepatuhan atau meninggalkan komentar tentang kontrol tersebut.

Untuk meninjau set kontrol

1. Dari halaman Notifikasi, tinjau daftar set kontrol yang didelegasikan kepada Anda. Kemudian identifikasi mana yang ingin Anda tinjau dan pilih nama penilaian terkait.
2. Di bawah tab Kontrol pada halaman detail penilaian, gulir ke bawah ke tabel Set kontrol.

3. Di bawah kontrol dikelompokkan oleh kontrol set kolom, memperluas nama set kontrol untuk menunjukkan kontrolnya. Kemudian, pilih nama kontrol untuk membuka halaman detail kontrol.
4. (Opsional) Pilih Perbarui status kontrol untuk mengubah status kontrol. Saat ulasan sedang berlangsung, Anda dapat menandai status sebagai Dalam Tinjauan.
5. Tinjau informasi tentang kontrol di folder Bukti, Sumber data, Komentar, dan tab Changelog. Untuk informasi selengkapnya tentang masing-masing tab ini dan cara menafsirkan data yang dikandungnya, lihat Meninjau kontrol dalam penilaian.

Untuk meninjau bukti untuk kontrol

1. Dari halaman detail kontrol, pilih tab Folder bukti.
2. Arahkan ke tabel folder Bukti, di mana daftar folder yang berisi bukti untuk kontrol itu ditampilkan. Folder ini diatur dan diberi nama berdasarkan tanggal ketika bukti dalam folder itu dikumpulkan.
3. Pilih nama folder bukti untuk membukanya. Dari sini, Anda dapat meninjau ringkasan semua bukti yang dikumpulkan pada tanggal tersebut. Ringkasan ini juga mencakup jumlah total masalah pemeriksaan kepatuhan yang dilaporkan langsung dariAWS Security Hub,AWS Config, atau keduanya. Untuk petunjuk tentang cara menafsirkan data di halaman ini, lihat Meninjau folder bukti.
4. Dari halaman ringkasan folder bukti, arahkan ke tabel Bukti. Di bawah kolom Waktu, pilih item baris untuk membuka dan meninjau detail bukti yang dikumpulkan pada saat itu. Untuk petunjuk tentang cara menafsirkan data pada halaman detail bukti, lihat Meninjau bukti individu.

Langkah 3. Unggah bukti manual (opsional)

MeskipunAWS Audit Manager secara otomatis mengumpulkan bukti untuk banyak kontrol, dalam beberapa kasus Anda mungkin perlu memberikan bukti tambahan. Dalam kasus ini, Anda dapat mengunggah bukti secara manual yang membantu Anda menunjukkan kepatuhan terhadap kontrol tersebut.

Sebelum Anda dapat mengunggah bukti manual ke penilaian Anda, Anda harus terlebih dahulu menempatkan bukti di bucket S3. Untuk petunjuknya, lihat Membuat bucket dan Mengunggah objek di Panduan Pengguna Amazon Simple Storage Service.

> **Important**
>
> SetiapAWS akun hanya dapat mengunggah hingga 100 file bukti secara manual ke kontrol setiap hari. Melebihi kuota harian ini menyebabkan setiap upload manual tambahan gagal untuk kontrol tersebut. Jika Anda perlu mengunggah sejumlah besar bukti manual ke satu kontrol, unggah bukti Anda dalam batch selama beberapa hari.

Untuk mengunggah bukti manual ke kontrol

1. Buka konsol AWS Audit Manager di https://console.aws.amazon.com/auditmanager/home.
2. Dari halaman Notifikasi, Anda dapat melihat daftar set kontrol yang didelegasikan kepada Anda. Identifikasi set kontrol mana yang ingin Anda tambahkan bukti, dan pilih nama penilaian terkait untuk membuka halaman detail penilaian.
3. Pilih tab Controls, gulir ke bawah ke Control set, dan kemudian pilih nama kontrol untuk membukanya.
4. Pilih tab Folder bukti, lalu pilih Unggah bukti manual.
5. Di halaman berikutnya, masukkan URI S3 bukti. Anda dapat menemukan URI S3 dengan menavigasi ke objek di konsol Amazon S3 dan memilih URI Copy S3.
6. Pilih Unggah untuk mengunggah bukti manual.

> **Note**
>
> Saat kontrol dalam status tidak aktif, Anda tidak dapat mengunggah bukti manual untuk kontrol tersebut. Untuk mengunggah bukti manual, Anda harus terlebih dahulu mengubah status kontrol menjadi yang sedang ditinjau atau ditinjau. Untuk petunjuk cara mengubah status kontrol, lihatLangkah 5: Tandai kontrol sebagai ditinjau (opsional).

Langkah 4. Tambahkan komentar untuk kontrol (opsional)

Anda dapat menambahkan komentar untuk kontrol apa pun yang Anda tinjau. Komentar ini dapat dilihat oleh pemilik audit. Misalnya, Anda dapat meninggalkan komentar untuk memberikan pembaruan status dan mengonfirmasi bahwa Anda memperbaiki masalah apa pun dengan kontrol itu.

Menambahkan komentar ke kontrol

1. Dari halaman Notifikasi, tinjau daftar set kontrol yang didelegasikan kepada Anda. Temukan set kontrol yang ingin Anda tinggalkan komentar, dan pilih nama penilaian terkait.
2. Pilih tab Controls, gulir ke bawah ke tabel Control sets, dan kemudian pilih nama kontrol untuk membukanya.
3. Pilih tab Komentar.
4. Di bawah Kirim komentar, masukkan komentar Anda di kotak teks.
5. Pilih Kirim komentar untuk menambahkan komentar Anda. Komentar Anda sekarang muncul di bawah bagian Komentar sebelumnya dari halaman, bersama dengan komentar lain mengenai kontrol ini.

Langkah 5: Tandai kontrol sebagai ditinjau (opsional)

Mengubah status kontrol adalah opsional. Namun, kami menyarankan Anda mengubah status setiap kontrol menjadi Ditinjau saat Anda menyelesaikan tinjauan untuk kontrol tersebut. Terlepas dari status masing-masing kontrol individu, Anda masih dapat mengirimkan kontrol kepada pemilik audit.

Untuk menandai kontrol seperti yang ditinjau

1. Dari halaman Notifikasi, tinjau daftar set kontrol yang didelegasikan kepada Anda. Temukan set kontrol yang berisi kontrol yang ingin Anda tandai sebagai ditinjau. Kemudian, pilih nama penilaian terkait untuk membuka halaman detail penilaian.
2. Di bawah tab Kontrol pada halaman detail penilaian, gulir ke bawah ke tabel Set kontrol.
3. Di bawah kontrol dikelompokkan oleh kontrol set kolom, memperluas nama set kontrol untuk menunjukkan kontrolnya. Pilih nama kontrol untuk membuka halaman detail kontrol.
4. Pilih Perbarui status kontrol dan ubah status menjadi Diulas.
5. Di jendela pop-up yang muncul, pilih Perbarui status kontrol untuk mengonfirmasi bahwa Anda selesai meninjau kontrol.

Langkah 6. Kirimkan pengaturan kontrol yang ditinjau kembali ke pemilik audit

Setelah selesai meninjau semua kontrol, kirimkan kontrol yang ditetapkan kembali ke pemilik audit untuk memberi tahu mereka bahwa Anda telah menyelesaikan peninjauan.

Untuk mengirimkan kontrol yang ditinjau diatur kembali ke pemilik

1. Di halaman Pemberitahuan, tinjau daftar set kontrol yang ditetapkan untuk Anda. Temukan set kontrol yang ingin Anda kirimkan ke pemilik audit, dan pilih nama penilaian terkait.
2. Gulir ke bawah ke tabel Set kontrol, pilih set kontrol yang ingin Anda kirimkan kembali ke pemilik audit, lalu pilih Kirim untuk ditinjau.
3. Di jendela pop-up yang muncul, Anda dapat menambahkan komentar tingkat tinggi tentang set kontrol tersebut sebelum memilih Kirim untuk ditinjau.

Setelah Anda mengirimkan kontrol ke pemilik audit, pemilik audit dapat melihat komentar apa pun yang Anda tinggalkan untuk mereka.

Apa yang saya lakukan selanjutnya?

Anda dapat terus mempelajari lebih lanjut tentang konsep yang diperkenalkan dalam tutorial ini. Berikut ini adalah beberapa sumber daya yang direkomendasikan:

- Meninjau penilaian- Memperkenalkan Anda ke halaman penilaian, di mana Anda dapat menjelajahi berbagai komponen penilaian diAWS Audit Manager.
- Tinjau kontrol dalam penilaian dan Tinjau bukti dalam penilaian - Menyediakan definisi data untuk membantu Anda menafsirkan kontrol dan bukti untuk setiap penilaian.
- AWS Audit Managerkonsep dan terminologi- Memberikan definisi untuk konsep dan terminologi yang digunakan dalam Audit Manager.

Menggunakan dasbor Audit Manager

Dengan dasbor Audit Manager, Anda dapat memvisualisasikan bukti yang tidak sesuai dalam penilaian aktif Anda. Ini adalah cara yang mudah dan cepat untuk memantau penilaian Anda, tetap mendapat informasi, dan memperbaiki masalah secara proaktif. Secara default, dasbor menyediakan tampilan gabungan dari atas ke bawah dari semua penilaian aktif Anda. Dengan menggunakan tampilan ini, Anda dapat mengidentifikasi masalah secara visual dalam penilaian Anda tanpa terlebih dahulu perlu menyaring sejumlah besar bukti individu.

Dasbor adalah layar pertama yang Anda lihat saat masuk ke konsol Audit Manager. Ini berisi dua widget yang menunjukkan data dan indikator kinerja utama (KPI) yang paling relevan bagi Anda. Dengan menggunakan filter penilaian, Anda dapat menyempurnakan data ini agar fokus pada KPI untuk penilaian tertentu. Dari sana, Anda dapat meninjau pengelompokan domain kontrol untuk mengidentifikasi kontrol mana yang memiliki bukti paling tidak patuh. Kemudian, Anda dapat menjelajahi kontrol yang mendasarinya untuk memeriksa dan memperbaiki masalah.

> **Note**
>
> Jika Anda adalah pengguna Audit Manager pertama kali atau Anda tidak memiliki penilaian aktif, tidak ada data yang ditampilkan di dasbor. Untuk memulai, buat penilaian. Ini memulai pengumpulan bukti yang sedang berlangsung. Setelah periode 24 jam, data bukti agregat akan mulai muncul di dasbor. Anda dapat membaca bagian berikut untuk mempelajari cara memahami dan menafsirkan data ini.

Halaman ini mencakup topik berikut:

Topik

Konsep dan terminologi dasbor

Bagian ini mencakup hal-hal penting yang perlu diketahui tentang dasbor Audit Manager sebelum Anda mulai menggunakannya.

Izin dan visibilitas

Baik pemilik audit maupun delegasi memiliki akses ke dasbor. Ini berarti bahwa kedua persona ini dapat melihat metrik dan agregat untuk semua penilaian aktif di akun Anda. AWS Memiliki akses ke informasi yang sama memungkinkan semua tim Anda untuk fokus pada KPI dan tujuan yang sama.

Filter

Audit Manager menyediakan tingkat halaman the section called “Penilaian filter” yang dapat Anda terapkan ke semua widget di dasbor Anda.

Bukti yang tidak patuh

Dasbor menyoroti kontrol dalam penilaian Anda yang memiliki bukti pemeriksaan kepatuhan dengan kesimpulan yang tidak sesuai. Bukti pemeriksaan kepatuhan berkaitan dengan kontrol yang menggunakan AWS Config atau AWS Security Hub sebagai tipe sumber data. Untuk jenis bukti ini, Audit Manager melaporkan hasil pemeriksaan kepatuhan langsung dari layanan tersebut. Jika Security Hub melaporkan hasil Gagal, atau jika AWS Config melaporkan hasil yang tidak sesuai, Audit Manager akan mengklasifikasi bukti tersebut sebagai tidak patuh.

Bukti yang tidak meyakinkan

Bukti tidak meyakinkan jika pemeriksaan kepatuhan tidak tersedia atau berlaku. Akibatnya, tidak ada evaluasi kepatuhan yang dapat dilakukan. Ini adalah kasus jika kontrol menggunakan AWS Config atau AWS Security Hub sebagai jenis sumber data tetapi Anda tidak mengaktifkan layanan tersebut. Ini juga terjadi jika kontrol menggunakan tipe sumber data yang tidak mendukung pemeriksaan kepatuhan, seperti bukti manual, panggilan AWS API, atauAWS CloudTrail.

Jika bukti memiliki status pemeriksaan kepatuhan yang tidak berlaku di konsol, bukti tersebut diklasifikasikan sebagai tidak meyakinkan di dasbor.

Bukti yang patuh

Bukti sesuai jika pemeriksaan kepatuhan melaporkan tidak ada masalah. Hal ini terjadi jika Security Hub melaporkan hasil Pass, atau AWS Config melaporkan hasil Compliant.

Kontrol domain

Dasbor memperkenalkan konsep domain kontrol. Anda dapat menganggap domain kontrol sebagai kategori kontrol umum yang tidak spesifik untuk satu kerangka kerja. Pengelompokan domain kontrol adalah salah satu fitur paling kuat dari dasbor. Audit Manager menyoroti kontrol dalam penilaian Anda yang memiliki bukti yang tidak sesuai, dan mengelompokkannya berdasarkan domain kontrol. Dengan menggunakan fitur ini, Anda dapat memfokuskan upaya perbaikan pada domain subjek tertentu saat Anda mempersiapkan audit.

> **Note**
>
> Domain kontrol berbeda dengan set kontrol. Set kontrol adalah pengelompokan kontrol khusus kerangka kerja yang biasanya ditentukan oleh badan pengatur. Misalnya, framework PCI DSS memiliki set kontrol bernama Requirement 8: Identifikasi dan otentikasi akses ke komponen sistem. Set kontrol ini berada di bawah domain kontrol Identitas dan manajemen akses.

Audit Manager mengkategorikan kontrol di bawah domain kontrol berikut.

Kontrol nama domain	Deskripsi tentang apa yang diatur oleh kontrol ini
Kontinuitas bisnis dan perencanaan kontingensi	Bagaimana Anda membangun proses yang melindungi operasi bisnis penting dari efek gangguan sistem dan jaringan utama.
Manajemen perubahan	Cara Anda menguji, menyetujui, mengimplementasikan, dan mendokumentasikan perubahan pada infrastruktur cloud Anda.
Keamanan dan privasi data	Bagaimana Anda mengamankan privasi, ketersediaan, dan integritas data Anda.
Manajemen pengembangan dan konfigurasi	Bagaimana Anda mempertahankan infrastruktur cloud Anda dalam keadaan yang diinginkan dan konsisten.
Tata kelola dan pengawasan	Bagaimana Anda menyelaraskan penggunaan komputasi awan dengan kewajiban hukum, peraturan, dan etika Anda.

Kontrol nama domain	Deskripsi tentang apa yang diatur oleh kontrol ini
Manajemen identitas dan akses	Bagaimana Anda memastikan bahwa pengguna yang tepat memiliki akses yang sesuai ke sumber daya teknologi Anda.
Manajemen insident management	Bagaimana Anda menetapkan tanggung jawab dan prosedur yang memastikan respons yang cepat dan efektif terhadap insiden keamanan.
Pencatatan dan pemantauan	Cara meninjau aktivitas pengguna untuk indikasi bahwa aktivitas tidak sah dicoba atau dilakukan.
Manajemen jaringan	Bagaimana Anda mengelola dan mengoperasikan jaringan data Anda menggunakan sistem manajemen jaringan.
Manajemen personalia	Bagaimana Anda menilai dan mengelola risiko keamanan personel di tingkat organisasi.
Keamanan fisik	Bagaimana Anda mendeteksi dan mencegah masalah keamanan fisik di fasilitas Anda.
Pengelolaan Risiko	Bagaimana Anda mengevaluasi potensi risiko dan kerugian, dan bagaimana Anda mengurangi atau menghilangkan ancaman tersebut.
Manajemen rantai pasokan	Bagaimana Anda mengidentifikasi, menilai, dan mengurangi risiko yang terkait dengan produk TI, vendor, dan rantai pasokan.
Manajemen perangkat lunak pengguna	Bagaimana Anda mengurangi risiko bahwa perangkat keras TI karyawan Anda hilang, rusak, atau terganggu.
Manajemen kerentanan	Cara Anda menentukan, menilai, dan memulihkan semua kerentanan yang diketahui untuk aset dalam infrastruktur cloud Anda.

Konsistensi akhirnya data

Data dasbor pada akhirnya konsisten. Ini berarti bahwa, ketika Anda membaca data dari dasbor, mungkin tidak mencerminkan hasil operasi tulis atau pembaruan yang baru saja diselesaikan. Jika Anda memeriksa lagi dalam beberapa jam, dasbor harus mencerminkan data terbaru.

Data dari penilaian yang dihapus dan tidak aktif

Dasbor menampilkan data dari penilaian aktif. Jika Anda menghapus penilaian atau mengubah statusnya menjadi tidak aktif pada hari yang sama saat Anda melihat dasbor, data disertakan untuk penilaian tersebut sebagai berikut.

- Penilaian tidak aktif — Jika Audit Manager mengumpulkan bukti untuk penilaian Anda sebelum Anda mengubahnya menjadi tidak aktif, data bukti tersebut disertakan dalam jumlah dasbor untuk hari itu.
- Penilaian yang dihapus — Jika Audit Manager mengumpulkan bukti untuk penilaian Anda sebelum Anda menghapusnya, data bukti tersebut tidak disertakan dalam jumlah dasbor untuk hari itu.

Dasbor elemen dasbor

Bagian berikut mencakup berbagai komponen dasbor.

Topik

Penilaian filter

Anda dapat menggunakan filter penilaian untuk fokus pada penilaian aktif tertentu.

Secara default, dasbor menampilkan data agregat untuk semua penilaian aktif Anda. Jika Anda ingin melihat data untuk penilaian tertentu, Anda menerapkan filter penilaian. Ini adalah filter tingkat halaman yang berlaku untuk semua widget di dasbor.

Untuk menerapkan filter penilaian, pilih penilaian dari daftar drop-down di bagian atas dasbor. Daftar ini menampilkan hingga 10 penilaian aktif Anda. Penilaian yang paling baru dibuat muncul pertama kali. Jika Anda memiliki banyak penilaian aktif, Anda dapat mulai mengetik nama penilaian untuk menemukannya dengan cepat. Setelah Anda memilih penilaian, dasbor menampilkan data untuk penilaian tersebut saja.

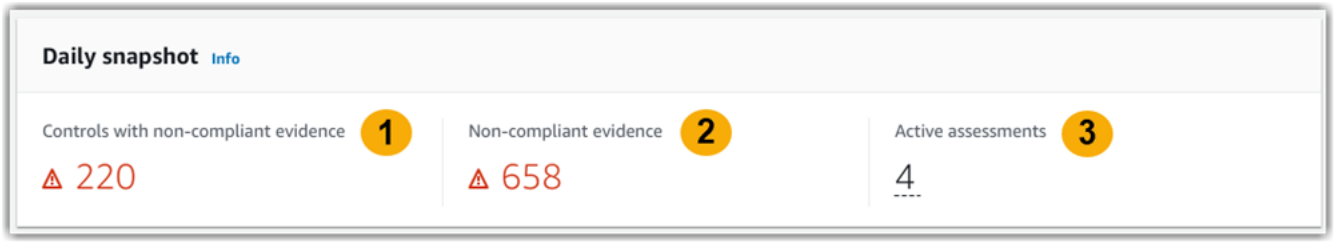
Snapshot harian

Widget ini menampilkan snapshot status kepatuhan saat ini dari penilaian aktif Anda.

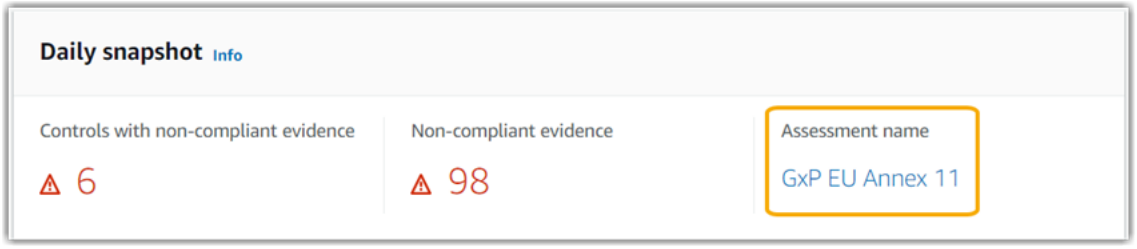
Snapshot harian mencerminkan data terbaru yang dikumpulkan pada tanggal di bagian atas dasbor. Tanggal dan waktu di dasbor diwakili dalam Waktu Universal Terkoordinasi (UTC). Penting untuk dipahami bahwa angka-angka ini adalah jumlah harian berdasarkan stempel waktu ini. Mereka bukan jumlah total sampai saat ini.

Secara default, snapshot harian menampilkan data berikut untuk semua penilaian aktif Anda:

1. Kontrol dengan bukti yang tidak patuh - Jumlah total kontrol yang terkait dengan bukti yang tidak patuh.
2. Bukti yang tidak patuh - Jumlah total bukti pemeriksaan kepatuhan dengan kesimpulan yang tidak sesuai.
3. Penilaian aktif - Jumlah total penilaian aktif Anda. Pilih nomor ini untuk melihat tautan ke penilaian ini.



Data snapshot harian berubah berdasarkan the section called “Penilaian filter” yang Anda terapkan. Saat Anda menentukan penilaian, data mencerminkan jumlah harian untuk penilaian itu saja. Dalam hal ini, snapshot harian menunjukkan nama penilaian yang Anda tentukan. Anda dapat memilih nama penilaian untuk membukanya.

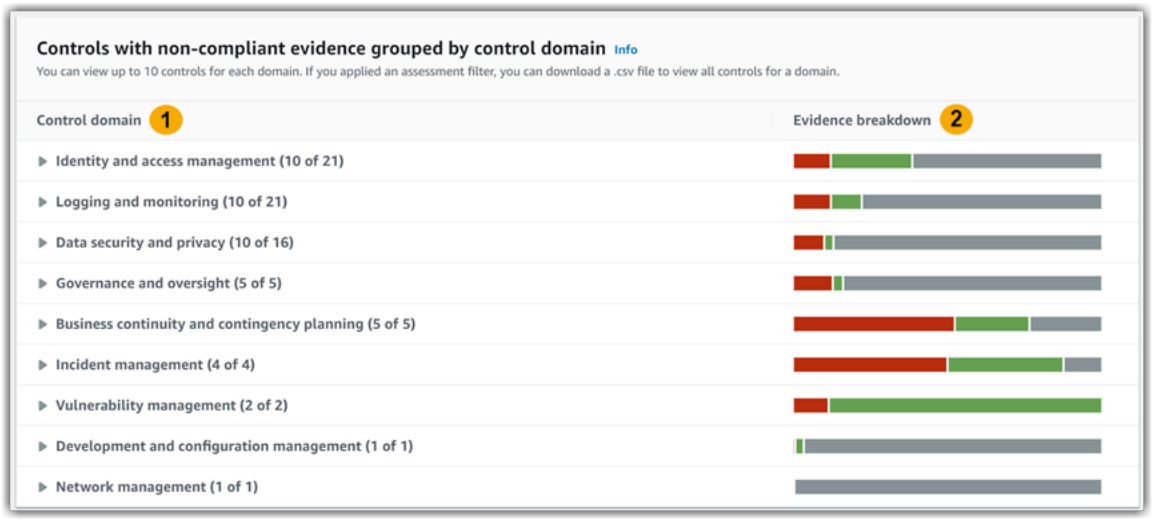


Kontrol dengan bukti yang tidak sesuai dikelompokkan berdasarkan domain kontrol

Anda dapat menggunakan widget ini untuk mengidentifikasi kontrol mana yang memiliki bukti yang paling tidak sesuai.

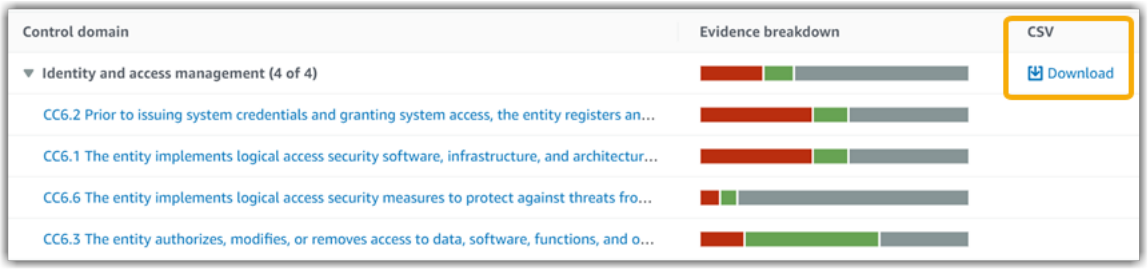
Secara default, widget menampilkan data berikut untuk semua penilaian aktif Anda:

1. Domain kontrol — Daftar control domains yang terkait dengan penilaian aktif Anda.
2. Rincian bukti - Bagan batang yang menunjukkan rincian status kepatuhan bukti.



Untuk memperluas domain kontrol, pilih tanda panah di samping namanya. Saat diperluas, konsol menampilkan hingga 10 kontrol untuk setiap domain. Kontrol ini diberi peringkat sesuai dengan jumlah total bukti non-compliant tertinggi.

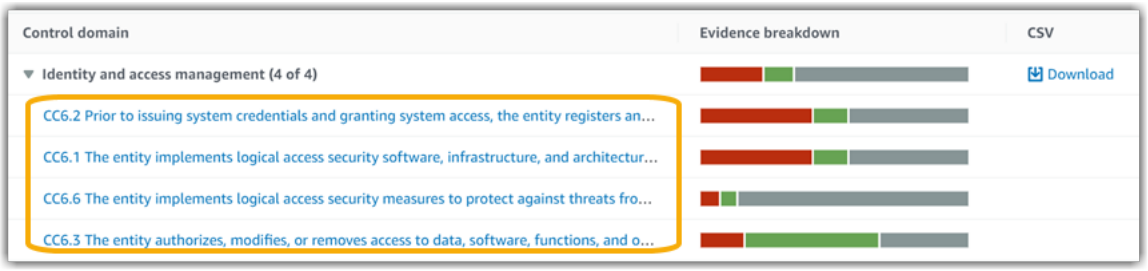
Data dalam widget ini berubah berdasarkan the section called “Penilaian filter” yang Anda terapkan. Saat menentukan penilaian, Anda hanya melihat data untuk penilaian tersebut. Selain itu, Anda juga dapat mengunduh file.csv untuk setiap domain kontrol yang tersedia dalam penilaian.



Berkas.csv menyertakan daftar lengkap kontrol di domain yang terkait dengan bukti yang tidak patuh. Contoh berikut menunjukkan kolom data.csv dengan nilai-nilai fiksi.

	A	B	C	D	E	F	G
1	Date and Time	AssessmentID	AsessmentName	ControlId	ControlName	ControlDescription	DataSource
2	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	abcdefgh-1234-bcde-5678-cdefghijklmn	Control 1	Description of control 1	Manual
3	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	12345678-abcd-9012-bcde-345678901234	Control 2	Description of control 2	Manual
4	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	bcdefghi-2345-cdef-3456-defghijklmno	Control 3	Description of control 3	AWS Config, AWS Security Hub
5	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	23456789-bcde-0123-cdef-456789012345	Control 4	Description of control 4	Manual
6	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	cdefghij-3456-defg-4567-efghijklmnop	Control 5	Description of control 5	AWS Config
7	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	34567890-cdef-1234-defg-567890123456	Control 6	Description of control 6	Manual
8	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	defghijk-4567-efgh-5678-fghijklmnopq	Control 7	Description of control 7	AWS Config
9	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	45678901-defg-2345-efgh-678901234567	Control 8	Description of control 8	AWS Security Hub
10	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	efghijkl-5678-fghi-6789-ghijklmnopqr	Control 9	Description of control 9	Manual
11	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	56789012-efgh-3456-fghi-789012345678	Control 10	Description of control 10	Manual
12	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	fghijklm-6789-ghij-7890-hijklmnopqrs	Control 11	Description of control 11	Manual
13	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	67890123-fghi-4567-ghij-890123456789	Control 12	Description of control 12	Manual
14	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	ghijklmn-7890-hijk-8901-ijklmnopqrst	Control 13	Description of control 13	AWS Config, AWS Security Hub
15	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	78901234-ghij-5678-hijk-901234567890	Control 14	Description of control 14	Manual
16							

Terakhir, saat Anda menerapkan filter penilaian, nama kontrol di bawah setiap domain akan di-hyperlink. Pilih kontrol apa pun untuk membuka halaman detail kontrol dalam penilaian yang ditentukan.



Tip

Dengan menggunakan halaman detail kontrol sebagai titik awal Anda, Anda dapat berpindah dari satu tingkat detail ke tingkat berikutnya.

1. Halaman rincian kontrol - Pada halaman ini, tab folder bukti mencantumkan folder harian bukti yang dikumpulkan oleh Audit Manager untuk kontrol itu. Untuk detail lebih lanjut, pilih folder.
2. Folder bukti - Selanjutnya, Anda dapat meninjau ringkasan folder dan daftar bukti di folder itu. Untuk detail lebih lanjut, pilih item bukti individu.

3. Bukti individu - Terakhir, Anda dapat menjelajahi detail bukti individu. Ini termasuk atribut yang berlaku dan data sumber daya untuk bukti. Ini adalah tingkat data bukti yang paling terperinci.

Apa yang harus saya lakukan selanjutnya?

Berikut adalah beberapa langkah selanjutnya yang dapat Anda ambil setelah meninjau dasbor.

- Unduh file.csv — Temukan domain penilaian dan kontrol yang ingin Anda fokuskan, dan unduh daftar lengkap kontrol terkait dengan bukti yang tidak sesuai.
- Tinjau kontrol - Setelah Anda mengidentifikasi kontrol yang perlu diperbaiki, Anda dapat meninjau kontrol.
- Delegasikan kontrol untuk ditinjau - Jika Anda memerlukan bantuan untuk meninjau kontrol, Anda dapat mendelegasikan set kontrol untuk ditinjau.
- Edit penilaian Anda - Jika Anda ingin mengubah ruang lingkup penilaian aktif, Anda dapat mengedit penilaian.
- Perbarui status penilaian Anda - Jika Anda ingin berhenti mengumpulkan bukti untuk penilaian, Anda dapat mengubah penilaian menjadi tidak aktif.

Pemecahan Masalah

Untuk menemukan jawaban atas pertanyaan dan masalah umum, lihat Memecahkan masalah dasbor di bagian Pemecahan Masalah pada panduan ini.

Penilaian di AWS Audit Manager

Penilaian Audit Manager didasarkan pada kerangka kerja, yang merupakan pengelompokan kontrol. Menggunakan kerangka kerja sebagai titik awal, Anda dapat membuat penilaian yang mengumpulkan bukti untuk kontrol dalam kerangka kerja itu. Dalam penilaian Anda, Anda juga dapat menentukan ruang lingkup audit Anda. Ini termasuk menentukan Akun AWS dan layanan yang ingin Anda kumpulkan buktinya.

Anda dapat membuat penilaian dari kerangka kerja apa pun. Anda dapat menggunakan kerangka kerja standar yang disediakan oleh Audit Manager. Atau, Anda dapat membuat penilaian dari kerangka kerja khusus yang Anda buat sendiri. Kerangka kerja standar berisi set kontrol bawaan yang mendukung standar atau peraturan kepatuhan tertentu. Sebaliknya, kerangka kerja khusus berisi kontrol yang dapat Anda sesuaikan dan kelompokkan sesuai dengan persyaratan audit internal Anda. Untuk informasi selengkapnya tentang perbedaan antara kerangka kerja standar dan kustom, lihat Kerangka kerja di bagian Konsep dan terminologi panduan ini.

Saat Anda membuat penilaian, ini memulai pengumpulan bukti yang sedang berlangsung. Ketika tiba waktunya untuk audit, Anda atau delegasi dapat meninjau bukti ini dan kemudian menambahkannya ke laporan penilaian.

> **Note**
>
> AWS Audit Managermembantu mengumpulkan bukti yang relevan untuk memverifikasi kepatuhan terhadap standar dan peraturan kepatuhan tertentu. Namun, itu tidak menilai kepatuhan Anda sendiri. AWS Audit ManagerOleh karena itu, bukti yang dikumpulkan mungkin tidak mencakup semua informasi tentang AWS penggunaan Anda yang diperlukan untuk audit. AWS Audit Managerbukan pengganti penasihat hukum atau pakar kepatuhan.

Topik

- Meninjau bukti dalam penilaian
- Menambahkan bukti manual di AWS Audit Manager
- Menghasilkan laporan penilaian
- Mengubah status penilaian menjadi tidak aktif
- Menghapus penilaian

Membuat penilaian

Topik ini didasarkan pada tutorial Memulai: Membuat penilaian. Ini berisi instruksi terperinci tentang cara membuat penilaian dari kerangka kerja. Ikuti langkah-langkah ini untuk membuat penilaian dan memulai pengumpulan bukti yang sedang berlangsung.

Tugas

- Langkah 1: Tentukan detail penilaian
- Langkah 2: Tentukan Akun AWS dalam ruang lingkup
- Langkah 3: Tentukan Layanan AWS dalam ruang lingkup
- Langkah 4: Tentukan pemilik audit
- Langkah 5: Tinjau dan buat
- Apa yang bisa saya lakukan selanjutnya?

Langkah 1: Tentukan detail penilaian

Mulailah dengan memilih kerangka kerja dan memberikan informasi dasar untuk penilaian Anda.

Untuk menentukan detail penilaian

1. Buka konsol AWS Audit Manager di https://console.aws.amazon.com/auditmanager/home.
2. Di panel navigasi, pilih Penilaian, lalu pilih Buat penilaian.
    - Atau, di panel navigasi, pilih Memulai, lalu pilih Buat penilaian.
3. Di bawah nama Penilaian, masukkan nama untuk penilaian Anda.
4. (Opsional) Di bawah deskripsi Penilaian, masukkan deskripsi untuk penilaian Anda.
5. Di bagian tujuan laporan Penilaian, pilih bucket Amazon S3 yang sudah ada tempat Anda ingin menyimpan laporan penilaian.

> **Tip**
>
> Tujuan laporan penilaian default didasarkan pada setelan Audit Manager Anda. Untuk informasi selengkapnya, lihat AWS Audit Managersetelan, Tujuan laporan penilaian. Jika mau, Anda dapat membuat dan menggunakan beberapa bucket S3 untuk membantu Anda mengatur laporan penilaian Anda.

6. Di bawah Frameworks, pilih kerangka kerja yang ingin Anda buat penilaian. Anda juga dapat menggunakan bilah pencarian untuk mencari kerangka kerja berdasarkan nama, atau dengan standar kepatuhan atau peraturan.

> **Tip**
>
> Untuk mempelajari lebih lanjut tentang kerangka kerja, pilih nama kerangka kerja. Ini membuka halaman ringkasan kerangka kerja. Di halaman ini, Anda dapat meninjau isi kerangka kerja itu. Ini termasuk kontrol dan sumber data kerangka kerja.

7. Di bawah Tag, pilih Tambahkan tag baru untuk mengaitkan tag dengan penilaian Anda. Anda dapat menentukan kunci dan nilai untuk setiap tag. Kunci tag wajib dan dapat digunakan sebagai kriteria pencarian saat Anda mencari penilaian ini. Untuk informasi selengkapnya tentang tag di Audit Manager, lihatPenandaan pada sumber daya AWS Audit Manager.
8. Pilih Berikutnya.

> **Note**
>
> Penting untuk memastikan bahwa penilaian Anda mengumpulkan bukti yang benar untuk kerangka kerja tertentu. Sebelum Anda memulai pengumpulan bukti, kami sarankan Anda meninjau persyaratan untuk kerangka kerja yang Anda pilih. Kemudian, validasi persyaratan ini terhadap parameter AWS Config aturan Anda saat ini. Untuk memastikan bahwa parameter aturan Anda selaras dengan persyaratan kerangka kerja, Anda dapat memperbarui aturan di AWS Config.
> Misalnya, Anda membuat penilaian untuk CIS v1.2.0. Kerangka kerja ini memiliki kontrol bernama 1.9 — Pastikan kebijakan kata sandi IAM membutuhkan panjang minimum 14 atau lebih. DalamAWS Config, iam-password-policyaturan memiliki `MinimumPasswordLength` parameter yang memeriksa panjang kata sandi. Nilai default untuk parameter ini adalah 14 karakter. Akibatnya, aturan tersebut sejalan dengan persyaratan kontrol. Jika Anda

tidak menggunakan nilai parameter default, pastikan bahwa nilai yang Anda gunakan sama dengan atau lebih besar dari persyaratan 14 karakter dari CIS v1.2.0. Anda dapat menemukan detail parameter default untuk setiap aturan terkelola dalam AWS Configdokumentasi.

Langkah 2: Tentukan Akun AWS dalam ruang lingkup

Anda dapat menentukan beberapa Akun AWS untuk berada dalam lingkup penilaian. Audit Manager mendukung beberapa akun melalui integrasi denganAWS Organizations. Ini berarti bahwa penilaian Audit Manager dapat dijalankan melalui beberapa akun, dengan bukti yang dikumpulkan dikonsolidasikan ke dalam akun administrator yang didelegasikan. Untuk mengaktifkan Organizations in Audit Manager, lihatAktifkan AWS Organizations (opsional).

> **Note**
>
> Audit Manager dapat mendukung hingga sekitar 150 akun dalam lingkup penilaian. Jika Anda mencoba memasukkan lebih dari 150 akun, pembuatan penilaian mungkin gagal.

Untuk menentukan Akun AWS dalam ruang lingkup

1. Di bawah Akun AWS, pilih Akun AWS yang ingin Anda sertakan dalam lingkup penilaian Anda.
   - Jika Anda mengaktifkan Organizations di Audit Manager, beberapa akun akan ditampilkan. Anda dapat memilih satu atau beberapa akun dari daftar. Atau, Anda juga dapat mencari akun berdasarkan nama akun, ID, atau email.
   - Jika Anda tidak mengaktifkan Organizations in Audit Manager, hanya yang terdaftar saat Akun AWS ini.
2. Pilih Berikutnya.

> **Note**
>
> Ketika akun dalam cakupan dihapus dari organisasi Anda, Audit Manager tidak lagi mengumpulkan bukti untuk akun tersebut. Namun, akun terus ditampilkan dalam penilaian Anda di bawah Akun AWStab. Untuk menghapus akun dari daftar akun dalam ruang lingkup,

Anda dapat mengedit penilaian. Akun yang dihapus tidak lagi ditampilkan dalam daftar selama pengeditan, dan Anda dapat menyimpan perubahan tanpa cakupan akun itu.

Langkah 3: Tentukan Layanan AWS dalam ruang lingkup

Framework yang Anda pilih sebelumnya mendefinisikan Audit Manager Layanan AWS yang memantau dan mengumpulkan bukti untuk. Jika daftar Layanan AWS tidak dipilih, atau dipilih tetapi Anda tidak mengaktifkannya di lingkungan Anda, Audit Manager tidak mengumpulkan bukti dari sumber daya yang terkait dengan layanan tersebut.

Anda dapat menentukan Layanan AWS lingkup sebagai berikut.

Untuk penilaian yang dibuat dari kerangka kerja standar

Saat Anda menggunakan konsol Audit Manager untuk membuat penilaian dari kerangka kerja standar, daftar lingkup Layanan AWS dalam dipilih secara default. Daftar ini tidak dapat diedit. Ini karena Audit Manager secara otomatis memetakan dan memilih sumber data dan layanan untuk Anda. Pemilihan ini dibuat sesuai dengan persyaratan kerangka standar. Jika kerangka kerja standar yang Anda pilih hanya berisi kontrol manual, tidak Layanan AWS ada dalam cakupan penilaian Anda, dan Anda tidak dapat menambahkan layanan apa pun ke penilaian Anda.

Untuk melanjutkan, tinjau daftar dan pilih Berikutnya.

> **Tip**
>
> Jika Anda perlu mengedit daftar layanan dalam cakupan, Anda dapat melakukannya dengan menggunakan CreateAssessmentAPI yang disediakan oleh Audit Manager.
> Atau, Anda dapat menyesuaikan kerangka kerja standar dan kemudian membuat penilaian dari kerangka kerja khusus.

Untuk penilaian yang dibuat dari kerangka kerja khusus

Jika Anda memilih kerangka kerja khusus di langkah 1, Anda dapat meninjau dan memodifikasi daftar Layanan AWS yang ada dalam cakupan penilaian Anda. Jika kerangka kerja khusus yang Anda pilih hanya berisi kontrol manual, semuanya Layanan AWS ditampilkan tetapi tidak ada yang dipilih. Anda dapat memilih nol atau lebih layanan untuk berada dalam lingkup penilaian Anda.

Untuk menentukan Layanan AWS dalam ruang lingkup (untuk penilaian yang dibuat dari kerangka kerja khusus saja)

1. Di bawah Layanan AWS, pilih layanan yang ingin Anda sertakan dalam penilaian Anda. Anda dapat menemukan layanan tambahan dengan menggunakan bilah pencarian untuk mencari berdasarkan layanan, kategori, atau deskripsi. Untuk menambahkan layanan, pilih kotak centang di sebelah nama layanan. Untuk menghapus layanan, kosongkan kotak centang.
2. Setelah selesai memilihLayanan AWS, pilih Berikutnya.

Langkah 4: Tentukan pemilik audit

Pada langkah ini, Anda menentukan pemilik audit untuk penilaian Anda. Pemilik audit adalah individu di tempat kerja Anda—biasanya dari GRC, SecOps, atau DevOps tim—yang bertanggung jawab untuk mengelola penilaian Audit Manager. Kami menyarankan agar mereka menggunakan AWSAuditManagerAdministratorAccesskebijakan tersebut.

Untuk menentukan pemilik audit

1. Di bawah pemilik Audit, tinjau daftar pemilik audit saat ini. Kolom pemilik Audit menampilkan ID dan peran pengguna. Akun AWSKolom menampilkan yang terkait Akun AWS dari pemilik audit tersebut.
2. Pemilik audit yang memiliki kotak centang yang dipilih disertakan dalam penilaian Anda. Kosongkan kotak centang untuk setiap pemilik audit untuk menghapusnya dari penilaian. Anda dapat menemukan pemilik audit tambahan dengan menggunakan bilah pencarian untuk mencari berdasarkan nama atauAkun AWS.
3. Setelah selesai, pilih Berikutnya.

Langkah 5: Tinjau dan buat

Tinjau informasi untuk penilaian Anda. Untuk mengubah informasi untuk satu langkah, pilih Edit. Setelah selesai, pilih Buat penilaian.

Tindakan ini memulai pengumpulan bukti yang sedang berlangsung untuk penilaian Anda. Setelah Anda membuat penilaian, pengumpulan bukti berlanjut hingga Anda mengubah status penilaian menjadi tidak aktif. Atau, Anda dapat menghentikan pengumpulan bukti untuk kontrol tertentu dengan mengubah status kontrol menjadi tidak aktif.

> **Note**
>
> Bukti otomatis tersedia 24 jam setelah penilaian Anda dibuat. Audit Manager secara otomatis mengumpulkan bukti dari berbagai sumber data, dan frekuensi pengumpulan bukti tersebut didasarkan pada jenis bukti. Untuk mempelajari lebih lanjut, lihat Frekuensi pengumpulan bukti di panduan ini.

Apa yang bisa saya lakukan selanjutnya?

Setelah membuat penilaian, Anda dapat mempelajari lebih lanjut tentang hal-hal berikut:

- Mengakses penilaian
- Meninjau penilaian
- Mengedit penilaian
- Meninjau kontrol dalam penilaian
- Meninjau bukti dalam penilaian
- Mengunggah bukti manual ke penilaian
- Delegasi diAWS Audit Manager
- Menghasilkan laporan penilaian
- Mengubah status penilaian
- Menghapus penilaian
- Pemecahan masalah penilaian dan pengumpulan bukti

Mengakses penilaian Anda di AWS Audit Manager

Anda dapat melihat semua penilaian di halaman Penilaian di konsol Audit Manager. Dari sini, Anda juga dapat mengedit penilaian, menghapus penilaian, atau membuat penilaian.

Anda juga dapat melihat penilaian menggunakan Audit Manager API atau AWS Command Line Interface (AWS CLI).

Audit Manager console

Untuk melihat penilaian Anda (konsol)

1. Buka konsol AWS Audit Manager di https://console.aws.amazon.com/auditmanager/home.
2. Di panel navigasi sebelah kiri, pilih Penilaian untuk melihat daftar penilaian aktif dan sebelumnya. Anda juga dapat menggunakan bilah pencarian untuk mencari penilaian.
3. Pilih nama penilaian apa pun untuk membuka halaman ringkasan, tempat Anda dapat melihat detail penilaian tersebut.

AWS CLI

Untuk melihat penilaian Anda (CLI)

Untuk melihat penilaian di Audit Manager, jalankan perintah list-assessment. Anda dapat menggunakan `--status` subperintah untuk melihat penilaian yang aktif atau tidak aktif.

```
aws auditmanager list-assessments --status ACTIVE
```

```
aws auditmanager list-assessments --status INACTIVE
```

Audit Manager API

Untuk melihat penilaian Anda (API)

Untuk melihat penilaian di Audit Manager, gunakan ListAssessmentsoperasi. Anda dapat menggunakan atribut status untuk melihat penilaian yang aktif atau tidak aktif.

Untuk informasi selengkapnya, pilih salah satu tautan sebelumnya untuk membaca selengkapnya di Referensi AWS Audit Manager API. Ini termasuk informasi tentang cara menggunakan `ListAssessments` operasi dan parameter di salah satu SDK khusus bahasaAWS.

Mengedit penilaian

Anda dapat mengedit penilaian aktif Anda di Audit Manager untuk mengubah informasi seperti deskripsi, ruang lingkup, pemilik audit, dan tujuan laporan penilaian.

Tugas

Langkah 1: Edit detail penilaian

Ikuti langkah-langkah ini untuk mengedit detail penilaian Anda.

Untuk mengedit penilaian

1. Buka konsol AWS Audit Manager di https://console.aws.amazon.com/auditmanager/home.
2. Di panel navigasi, pilih Penilaian untuk melihat daftar penilaian Anda saat ini.
3. Pilih penilaian, dan pilih Edit.
   - Atau, Anda dapat membuka penilaian dan kemudian memilih Edit di kanan atas halaman.
4. Di bawah Edit detail penilaian, edit nama penilaian, deskripsi, dan tujuan laporan penilaian Anda.
5. Pilih Berikutnya.

> **Tip**
>
> Untuk mengedit tag untuk penilaian, buka penilaian dan pilihTab tag. Di sana Anda dapat melihat dan mengedit tag yang terkait dengan penilaian.

Langkah 2: Edit Akun AWS dalam ruang lingkup

Pada langkah ini, Anda dapat mengubah daftar akun yang termasuk dalam ruang lingkup penilaian Anda.

Audit Manager mendukung beberapa akun melalui integrasi denganAWS Organizations. Ini berarti bahwa penilaian Audit Manager dapat dijalankan melalui beberapa akun, dengan bukti yang dikumpulkan dikonsolidasikan ke dalam akun administrator yang didelegasikan. Untuk menambah atau mengubah administrator yang didelegasikan untuk Audit Manager, lihat AWS Audit Managerpengaturan, Administrator yang didelegasikan.

> **Note**
>
> Audit Manager dapat mendukung hingga sekitar 150 akun dalam lingkup penilaian. Jika Anda mencoba memasukkan lebih dari 150 akun, pembuatan penilaian mungkin gagal.

Untuk mengedit Akun AWS dalam ruang lingkup

1. Di bawah Edit Akun AWS dalam cakupan, pilih AWS akun tambahan. Anda juga dapat menghapus akun dengan membersihkannya dari daftar.
2. Pilih Berikutnya.

Langkah 3: Edit Layanan AWS dalam ruang lingkup

Langkah ini menentukan Layanan AWS Audit Manager mana yang memantau dan mengumpulkan bukti. Jika daftar Layanan AWS tidak dipilih, atau dipilih tetapi Anda tidak mengaktifkannya di lingkungan Anda, Audit Manager tidak mengumpulkan bukti dari sumber daya yang terkait dengan layanan tersebut.

Anda dapat meninjau dan mengedit lingkup sebagai berikut. Layanan AWS

Untuk penilaian yang dibuat dari kerangka kerja standar

Saat Anda menggunakan konsol Audit Manager untuk mengedit penilaian yang dibuat dari kerangka kerja standar, Anda dapat meninjau daftar Layanan AWS dalam cakupan tetapi Anda tidak dapat mengedit daftar ini. Ini karena Audit Manager secara otomatis memetakan dan memilih sumber data dan layanan untuk Anda, sesuai dengan desain kerangka standar. Jika penilaian dibuat menggunakan kerangka kerja yang hanya berisi kontrol manual, tidak Layanan AWS ada dalam cakupan penilaian Anda, dan Anda tidak dapat menambahkan layanan apa pun.

Untuk melanjutkan, tinjau daftar dan pilih Berikutnya.

> **Tip**
>
> Jika Anda perlu mengedit daftar layanan dalam cakupan untuk penilaian yang ada, Anda dapat melakukannya dengan menggunakan UpdateAssessmentAPI yang disediakan oleh Audit Manager.

Untuk penilaian yang dibuat dari kerangka kerja khusus

Jika Anda membuat penilaian dari kerangka kerja khusus, Anda dapat mengedit Layanan AWS yang ada dalam ruang lingkup penilaian Anda. Anda dapat memilih nol atau lebih layanan untuk berada dalam lingkup penilaian Anda.

Untuk mengedit Layanan AWS dalam lingkup (hanya untuk penilaian yang dibuat dari kerangka kerja khusus)

1. Di bawah Edit Layanan AWS dalam lingkup, pilih tambahan Layanan AWS yang diperlukan. Anda juga dapat menghapus layanan dengan membersihkannya dari daftar.
2. Pilih Berikutnya.

Langkah 4: Edit pemilik audit

Anda juga dapat mengubah pemilik audit untuk penilaian Anda. Pemilik audit adalah individu di tempat kerja Anda—biasanya dari GRC, SecOps, atau DevOps tim—yang bertanggung jawab untuk mengelola penilaian Audit Manager. Tugas mereka termasuk mendelegasikan set kontrol untuk meninjau dan menghasilkan laporan penilaian. Kami menyarankan Anda menggunakan AWSAuditManagerAdministratorAccesskebijakan ini.

Untuk mengedit pemilik audit

1. Pilih pemilik audit baru untuk ditambahkan ke penilaian. Untuk menghapus pemilik audit, hapus mereka dari daftar.
2. Pilih Berikutnya.

Langkah 5: Tinjau dan simpan

Tinjau informasi untuk penilaian Anda. Untuk mengubah informasi untuk satu langkah, pilih Edit. Setelah selesai, pilih Simpan perubahan untuk mengonfirmasi hasil edit.

> **Note**
>
> Setelah Anda menyelesaikan pengeditan, perubahan penilaian akan berlaku pada pukul 00:00 UTC pada hari berikutnya.

Meninjau penilaian

Setelah membuat penilaian di Audit Manager, Anda dapat membuka dan meninjau penilaian kapan saja.

Untuk membuka dan meninjau penilaian

1. Buka konsol AWS Audit Manager di https://console.aws.amazon.com/auditmanager/home.
2. Di panel navigasi kiri, pilih Penilaian untuk melihat daftar penilaian Anda.
3. Pilih nama penilaian untuk membukanya.

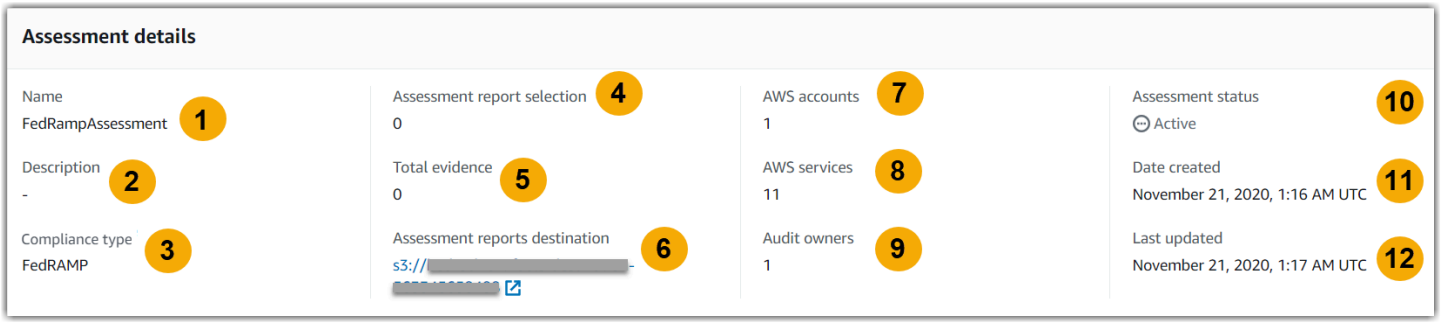
Saat Anda membuka penilaian, Anda melihat halaman ringkasan yang berisi beberapa bagian. Bagian halaman ini dan isinya dijelaskan sebagai berikut.

Bagian dari halaman penilaian

- Rincian penilaian
- Tab kontrol
- Tab pemilihan laporan penilaian
- Tab Akun AWS
- Tab Layanan AWS
- Tab pemilik audit
- Tab tag
- Tab Changelog

Rincian penilaian

Bagian Rincian Penilaian memberikan gambaran umum tentang penilaian.



Ini termasuk informasi berikut:

1. Nama — Nama yang Anda berikan untuk penilaian.
2. Deskripsi — Deskripsi opsional yang Anda berikan untuk penilaian.
3. Jenis kepatuhan — Standar kepatuhan atau peraturan yang didukung penilaian.
4. Pemilihan laporan penilaian — Jumlah item bukti yang Anda pilih untuk disertakan dalam laporan penilaian.
5. Bukti total — Jumlah total item bukti yang dikumpulkan untuk penilaian ini.
6. Tujuan laporan penilaian — Bucket Amazon S3 tempat Audit Manager menyimpan laporan penilaian.
7. Akun AWS— Jumlah Akun AWS yang berada dalam ruang lingkup untuk penilaian ini.
8. Layanan AWS— Jumlah Layanan AWS yang berada dalam ruang lingkup untuk penilaian ini.
9. Pemilik audit — Jumlah pemilik audit untuk penilaian ini.
10. Status penilaian — Status penilaian.
    - Aktif - Menunjukkan bahwa penilaian saat ini mengumpulkan bukti. Penilaian yang baru dibuat memiliki status ini.
    - Tidak aktif - Menunjukkan bahwa penilaian tidak lagi mengumpulkan bukti. Untuk informasi lebih lanjut tentang penilaian tidak aktif, lihat. Mengubah status penilaian menjadi tidak aktif
11. Tanggal dibuat — Tanggal penilaian dibuat.
12. Terakhir diperbarui - Tanggal penilaian ini terakhir diedit.

Tab kontrol

Tab Kontrol menampilkan ringkasan kontrol dalam penilaian, bersama dengan daftar lengkap kontrol tersebut. Setiap penilaian dapat berisi beberapa set kontrol, dan setiap set kontrol berisi beberapa kontrol. Kontrol dan set kontrol diatur sedemikian rupa sehingga sesuai dengan tata letak yang ditentukan dalam standar atau peraturan kepatuhan terkait.

Di bawah Ringkasan status kontrol, Anda dapat meninjau ringkasan kontrol untuk penilaian ini. Ringkasan mencakup informasi berikut:

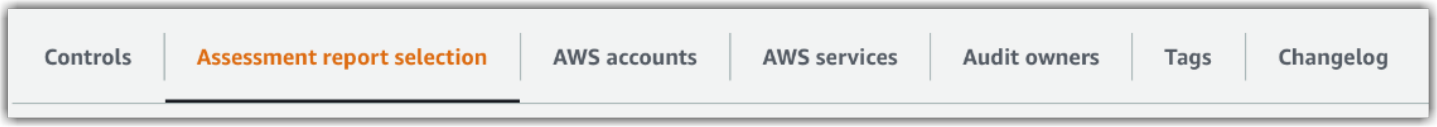
- Total kontrol — Jumlah total kontrol dalam penilaian ini.

- Ditinjau — Jumlah kontrol yang ditinjau oleh pemilik audit atau delegasi.
- Sedang ditinjau — Jumlah kontrol yang saat ini sedang ditinjau.
- Tidak aktif — Jumlah kontrol yang tidak lagi aktif mengumpulkan bukti.

Di bawah tabel Control sets, daftar kontrol ditampilkan dan dikelompokkan berdasarkan set kontrol. Anda dapat memperluas atau menciutkan kontrol di setiap set kontrol. Anda juga dapat mencari berdasarkan nama kontrol jika Anda ingin mencari kontrol tertentu. Kolom data berikut muncul di tabel Kontrol yang dikelompokkan berdasarkan set kontrol:

- Kontrol dikelompokkan berdasarkan set kontrol - Nama set kontrol.
- Status kontrol — Status kontrol.
  - Dalam peninjauan menunjukkan bahwa kontrol ini belum ditinjau. Bukti masih dikumpulkan untuk kontrol ini, dan Anda dapat mengunggah bukti manual. Ini adalah status default.
  - Ditinjau menunjukkan bahwa bukti untuk kontrol ini telah ditinjau. Namun, bukti masih dikumpulkan, dan Anda dapat mengunggah bukti manual.
  - Tidak aktif menunjukkan pengumpulan bukti otomatis dihentikan untuk kontrol ini. Anda tidak dapat lagi mengunggah bukti manual.
- Delegasikan ke — Peninjau kontrol ini, jika ditugaskan ke delegasi untuk ditinjau.
- Bukti total — Jumlah item bukti yang telah dikumpulkan untuk kontrol ini.

Tab pemilihan laporan penilaian



Tab ini menampilkan daftar bukti yang akan disertakan dalam laporan penilaian, dikelompokkan berdasarkan folder bukti. Folder bukti ini diatur dan diberi nama berdasarkan tanggal pembuatannya. Anda dapat menelusuri folder ini dan memilih bukti mana yang ingin Anda sertakan dalam laporan penilaian Anda. Anda juga dapat menggunakan bilah pencarian untuk mencari berdasarkan nama folder bukti atau nama kontrol. Jumlah total item bukti yang ditambahkan ke laporan penilaian dirangkum di bawah bagian Rincian Penilaian di bagian atas halaman.

Tabel pemilihan laporan Penilaian menunjukkan daftar folder bukti dengan data berikut:

- Folder bukti — Nama folder bukti. Nama folder didasarkan pada tanggal ketika bukti dikumpulkan.

- Bukti yang dipilih — Jumlah item bukti dalam folder yang disertakan dalam laporan penilaian.
- Nama kontrol — Nama kontrol yang terkait dengan folder bukti ini.

Untuk informasi tentang menambahkan bukti ke laporan penilaian, lihatMenghasilkan laporan penilaian.

Tab Akun AWS

Tab ini menampilkan daftar Akun AWS yang berada dalam lingkup penilaian. Jumlah total akun dirangkum di bawah bagian Rincian Penilaian di bagian atas halaman.

Akun AWSTabel menunjukkan daftar akun dengan data berikut:

- ID Akun — ID dariAkun AWS.
- Nama akun — NamaAkun AWS.
- Email — Alamat email yang terkait denganAkun AWS.

Tab Layanan AWS

Tab ini menampilkan daftar Layanan AWS yang berada dalam lingkup penilaian. Dengan kata lain, ini adalah Layanan AWS bahwa penilaian Anda mengumpulkan bukti tentang.

Jumlah total layanan dirangkum di bawah bagian Rincian Penilaian di bagian atas halaman.

Layanan AWSTabel menunjukkan daftar layanan dengan data berikut:

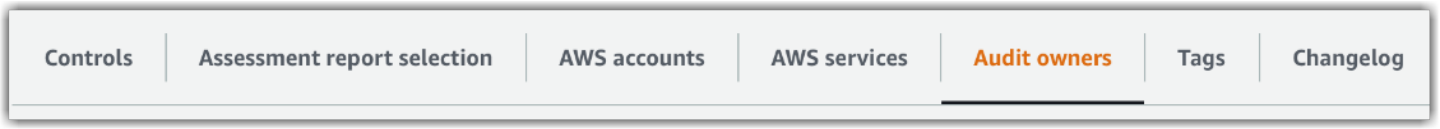
- Layanan AWS- NamaLayanan AWS.
- Kategori — Kategori layanan, seperti komputasi atau database.

Audit Manager melakukan penilaian sumber daya untuk layanan dalam tabel ini. Misalnya, jika Amazon S3 terdaftar, Audit Manager dapat mengumpulkan bukti tentang bucket S3 Anda. Bukti pasti

yang dikumpulkan ditentukan oleh sumber data kontrol. Misalnya, jika tipe sumber data adalahAWS Config, dan pemetaan sumber data adalah AWS Config aturan (seperti`s3-bucket-public-write-prohibited`), Audit Manager mengumpulkan hasil evaluasi aturan tersebut sebagai bukti. Untuk informasi selengkapnya, lihat Apa perbedaan antara layanan dalam lingkup dan tipe sumber data? dalam panduan ini.

> **Note**
>
> Jika penilaian Anda dibuat di konsol dari kerangka kerja standar, Audit Manager memilih layanan untuk Anda dan memetakan sumber datanya sesuai dengan persyaratan kerangka kerja. Jika kerangka standar hanya berisi kontrol manual, tidak Layanan AWS ada ruang lingkup. Jika Anda perlu mengedit daftar layanan dalam lingkup, Anda dapat menggunakan UpdateAssessmentAPI.

Tab pemilik audit

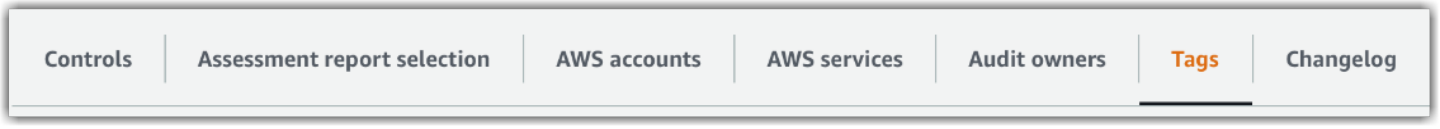


Tab ini menampilkan pemilik audit untuk penilaian. Jumlah total pemilik audit juga dirangkum di bawah bagian Rincian Penilaian di bagian atas halaman.

Tabel pemilik Audit menampilkan daftar akun dengan data berikut:

- Pemilik audit — Nama pemilik audit.
- Akun AWS— Alamat email yang terkait dengan pemilik audit.

Tab tag



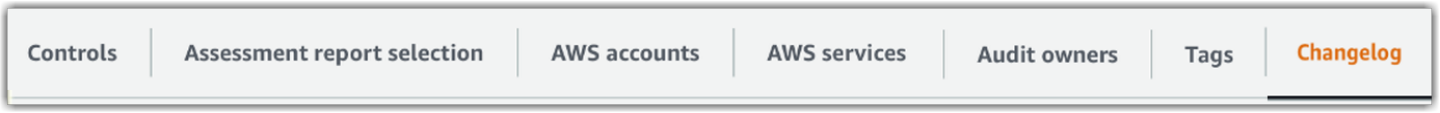
Tab ini menampilkan daftar tag yang diwarisi dari kerangka kerja yang digunakan untuk membuat penilaian ini. Jumlah total tag dirangkum di bawah detail Penilaian di bagian atas halaman.

Tabel Tag menunjukkan daftar tag dengan data berikut:

- Kunci - Kunci tag, seperti standar kepatuhan, peraturan, atau kategori.
- Nilai - Nilai tag.

Untuk informasi selengkapnya tentang tag di Audit Manager, lihatPenandaan pada sumber daya AWS Audit Manager.

Tab Changelog



Tab ini menampilkan daftar aktivitas pengguna yang terkait dengan penilaian.

Tabel Changelog menunjukkan daftar akun dengan data berikut:

- Tanggal - Tanggal kegiatan.
- Pengguna — Pengguna yang melakukan tindakan.
- Tindakan — Tindakan yang terjadi, seperti penilaian yang sedang dibuat.
- Jenis — Jenis objek yang berubah, seperti penilaian.
- Sumber daya — Sumber daya yang dipengaruhi oleh perubahan, seperti kerangka kerja tempat penilaian dibuat.

Meninjau kontrol dalam penilaian

Kontrol di Audit Manager membantu Anda memenuhi standar dan peraturan kepatuhan umum dan unik dalam audit Anda. Anda dapat membuka dan meninjau kontrol dalam penilaian Audit Manager kapan saja.

Untuk membuka halaman ringkasan kontrol

1. Buka konsol AWS Audit Manager di https://console.aws.amazon.com/auditmanager/home.
2. Di panel navigasi, pilih Penilaian, dan pilih nama penilaian untuk membukanya.
3. Dari halaman penilaian, pilih tab Kontrol, gulir ke bawah ke tabel Set kontrol, lalu pilih nama kontrol untuk membukanya.

Ketika Anda membuka kontrol, Anda melihat halaman ringkasan yang berisi beberapa bagian. Bagian halaman ini dan isinya dijelaskan di bagian berikut.

Bagian dari halaman kontrol

- Detail kontrol
- Perbarui status kontrol
- Tab folder bukti
- Tab sumber data
- Tab komentar
- Tab Changelog

Detail kontrol

Bagian Detail kontrol memberikan gambaran umum tentang kontrol.

Ini termasuk informasi berikut:

1. Nama kontrol — Nama yang diberikan untuk kontrol ini.
2. Deskripsi kontrol — Deskripsi yang disediakan untuk kontrol ini.
3. Informasi pengujian — Prosedur pengujian yang direkomendasikan untuk kontrol ini.
4. Rencana tindakan — Tindakan yang disarankan untuk dilakukan jika kontrol tidak terpenuhi.

Perbarui status kontrol

Di bagian Perbarui status kontrol halaman, Anda dapat meninjau dan memperbarui status kontrol penilaian.

Status berikut tersedia:

- Dalam peninjauan — Menunjukkan bahwa kontrol ini belum ditinjau. Bukti masih dikumpulkan untuk kontrol ini, dan Anda dapat mengunggah bukti manual. Ini adalah status default.
- Ditinjau — Menunjukkan bahwa bukti untuk kontrol ini ditinjau. Bukti masih dikumpulkan, dan Anda dapat mengunggah bukti manual.
- Tidak aktif — Menunjukkan bahwa pengumpulan bukti otomatis dihentikan untuk kontrol ini. Anda tidak dapat lagi mengunggah bukti manual.

> **Note**
>
> Mengubah status kontrol ke Review adalah final. Setelah mengatur status kontrol ke Tinjauan, Anda tidak dapat lagi mengubah status kontrol tersebut atau kembali ke status sebelumnya.

Tab folder bukti

Tab Folder Bukti mencantumkan bukti yang dikumpulkan secara otomatis untuk kontrol ini. Ini diatur ke dalam folder setiap hari.

Tabel folder Bukti menunjukkan daftar folder dengan data berikut:

- Folder bukti — Nama folder bukti. Nama ini didasarkan pada tanggal ketika bukti dikumpulkan atau ditambahkan secara manual.
- Pemeriksaan kepatuhan — Jumlah masalah yang ditemukan di folder bukti. Jumlah ini mewakili jumlah total masalah keamanan yang dilaporkan langsung dariAWS Security Hub,AWS Config, atau keduanya. Jika Anda melihat Tidak berlaku, ini menunjukkan bahwa Anda tidak memiliki AWS Security Hub atau AWS Config mengaktifkan, atau bukti berasal dari tipe sumber data yang berbeda.
- Bukti total — Jumlah item bukti di dalam folder.
- Pemilihan laporan penilaian — Jumlah item bukti dalam folder yang disertakan dalam laporan penilaian.

Dari tab Folder bukti, Anda dapat mengambil tindakan berikut:

- Tinjau bukti individual — Pilih folder bukti untuk membukanya. Dari halaman ringkasan folder bukti, Anda kemudian dapat memilih bukti individual yang ingin Anda tinjau.
- Tambahkan bukti manual — Untuk informasi lebih lanjut, lihatMenambahkan bukti manual di AWS Audit Manager.
- Tambahkan bukti ke laporan penilaian — Untuk informasi selengkapnya, lihatMenghasilkan laporan penilaian.

Tab sumber data

Tab ini menampilkan informasi tentang sumber data untuk kontrol. Ini termasuk informasi berikut:

- Nama sumber data — Ini hanya berlaku untuk kontrol khusus. Ini mengacu pada nama deskriptif yang Anda berikan setiap sumber data. Anda dapat menggunakan nama ini untuk membedakan antara beberapa sumber data yang termasuk dalam tipe sumber data yang sama
- Tipe sumber data — Ini menentukan dari mana data bukti berasal.
  - Jika Audit Manager mengumpulkan bukti, sumber data dapat berupa salah satu dari empat jenis: AWS Security Hub,, AWS ConfigAWS CloudTrail, atau panggilan AWS API.
  - Jika Anda mengunggah bukti Anda sendiri, tipe sumber datanya adalah Manual. Deskripsi menunjukkan apakah bukti manual yang diperlukan adalah unggahan File atau respons Teks.
- Pemetaan — Ini adalah atribut pemetaan yang digunakan untuk mengidentifikasi dan mengambil data dari sumber data otomatis.
  - Jika tipe sumber data adalahAWS Config, pemetaan adalah nama AWS Config aturan tertentu (misalnya,`EC2_INSTANCE_MANAGED_BY_SSM`). Audit Manager menggunakan pemetaan ini untuk melaporkan hasil pemeriksaan aturan tersebut secara langsungAWS Config.
  - Jika tipe sumber datanyaAWS Security Hub, pemetaan adalah nama kontrol Security Hub tertentu (misalnya,`1.1 – Avoid the use of the "root" account`). Audit Manager menggunakan pemetaan ini untuk melaporkan hasil pemeriksaan keamanan tersebut langsung dari Security Hub.
  - Jika tipe sumber data adalah panggilan AWS API, pemetaan adalah nama panggilan API tertentu (misalnya,`ec2_DescribeSecurityGroups`). Audit Manager menggunakan pemetaan ini untuk mengumpulkan respons API.
  - Jika tipe sumber data adalahAWS CloudTrail, pemetaan adalah nama CloudTrail peristiwa tertentu (misalnya,`CreateAccessKey`). Audit Manager menggunakan pemetaan ini untuk mengumpulkan aktivitas pengguna terkait dari CloudTrail log Anda.
- Frekuensi — Frekuensi pengumpulan bukti dari sumber data ini. Frekuensi bervariasi tergantung pada sumber data. Untuk informasi selengkapnya, pilih nilai di kolom atau lihatFrekuensi pengumpulan bukti.

Tab komentar

Di tab Komentar, Anda dapat menambahkan komentar mengenai kontrol dan buktinya. Ini juga menampilkan daftar komentar sebelumnya.

Di bawah Kirim komentar, Anda dapat menambahkan komentar untuk kontrol dengan memasukkan teks dan kemudian memilih Kirim komentar.

Di bawah komentar sebelumnya, Anda dapat melihat daftar komentar sebelumnya bersama dengan tanggal komentar dibuat dan ID pengguna terkait.

Tab Changelog

Tab Changelog menampilkan daftar aktivitas pengguna yang terkait dengan kontrol. Informasi yang sama tersedia sebagai log jejak auditAWS CloudTrail. Dengan aktivitas pengguna yang ditangkap langsung di Audit Manager, Anda dapat dengan mudah meninjau jejak audit aktivitas untuk kontrol tertentu.

Di bawah Changelog, tabel menampilkan kolom data berikut:

- Tanggal - Tanggal dan waktu kegiatan, diwakili dalam Waktu Universal Terkoordinasi (UTC).
- Pengguna — Pengguna atau peran yang melakukan aktivitas.
- Tindakan — Deskripsi aktivitas.
- Type — Atribut terkait yang menjelaskan lebih lanjut aktivitas.
- Sumber daya — Sumber daya terkait, jika berlaku.

Audit Manager melacak aktivitas pengguna berikut di changelog:

- Membuat penilaian
- Mengedit penilaian
- Menyelesaikan penilaian
- Menghapus penilaian
- Mendelegasikan set kontrol untuk ditinjau
- Mengirimkan kontrol yang ditinjau kembali ke pemilik audit
- Mengunggah bukti manual
- Memperbarui status kontrol
- Menghasilkan laporan penilaian

Meninjau bukti dalam penilaian

Penilaian aktif di Audit Manager secara otomatis mengumpulkan bukti dari berbagai sumber data. Untuk informasi selengkapnya, lihat Bagaimana AWS Audit Manager mengumpulkan bukti. Anda dapat membuka dan meninjau bukti untuk kontrol dalam penilaian Anda kapan saja.

Untuk membuka bukti untuk kontrol

1. Buka konsol AWS Audit Manager di https://console.aws.amazon.com/auditmanager/home.
2. Di panel navigasi, pilih Penilaian, lalu pilih nama penilaian untuk membukanya.
3. Dari halaman penilaian, pilih tab Controls, gulir ke bawah ke tabel Controls, lalu pilih nama kontrol untuk membukanya.
4. Dari halaman kontrol, pilih tab Folder bukti. Di bawah tabel Folder bukti, daftar semua folder bukti untuk kontrol tersebut ditampilkan. Folder ini diatur dan diberi nama berdasarkan tanggal ketika bukti dalam folder dikumpulkan.
5. Pilih nama folder bukti untuk membukanya.

Dari sini, Anda sekarang dapat meninjau folder bukti untuk kontrol itu, dan menelusuri lebih lanjut untuk meninjau potongan bukti individual sesuai kebutuhan.

Topik

- Meninjau folder bukti
- Meninjau bukti individu

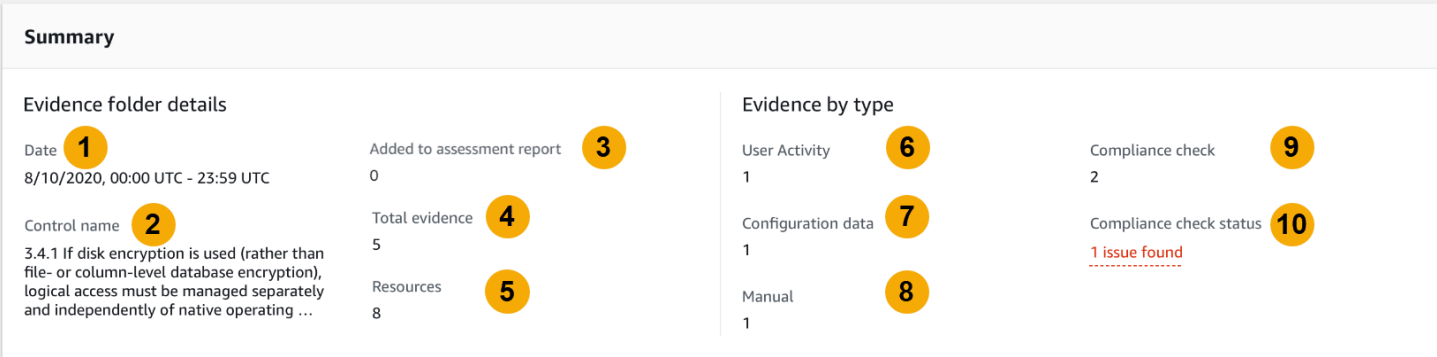
Meninjau folder bukti

Saat Anda membuka folder bukti, Anda melihat halaman ringkasan folder bukti yang berisi dua bagian: bagian Ringkasan dan tabel Bukti. Bagian-bagian ini dan isinya dijelaskan sebagai berikut.

- Ringkasan folder bukti
- Tabel bukti

Ringkasan folder bukti

Bagian Ringkasan halaman memberikan ikhtisar tingkat tinggi tentang bukti di folder bukti.



Ini termasuk informasi berikut:

1. Tanggal - Waktu dan tanggal ketika folder bukti dibuat, diwakili dalam Coordinated Universal Time (UTC).
2. Nama kontrol — Nama kontrol yang terkait dengan folder bukti.
3. Ditambahkan ke laporan penilaian — Jumlah item bukti yang dipilih secara manual untuk dimasukkan dalam laporan penilaian.
4. Bukti total — Jumlah item bukti dalam folder bukti.
5. Sumber daya — Jumlah total AWS sumber daya yang dinilai saat menghasilkan bukti di folder ini.
6. Aktivitas pengguna — Jumlah item bukti yang termasuk dalam kategori aktivitas pengguna. Bukti ini dikumpulkan dari AWS CloudTrail log.
7. Data konfigurasi — Jumlah item bukti yang termasuk dalam kategori data konfigurasi. Bukti ini dikumpulkan dari snapshot konfigurasi lainnya Layanan AWS seperti Amazon EC2, Amazon S3, atau IAM.
8. Manual — Jumlah item bukti yang termasuk dalam kategori manual. Bukti ini diunggah secara manual.
9. Pemeriksaan kepatuhan — Jumlah item bukti yang termasuk dalam kategori pemeriksaan kepatuhan. Bukti ini dikumpulkan dari AWS Config atauAWS Security Hub.
10. Status pemeriksaan kepatuhan — Jumlah total masalah yang dilaporkan langsung dariAWS Security Hub,AWS Config, atau keduanya.

> **Tip**
>
> Untuk informasi selengkapnya tentang berbagai jenis bukti (aktivitas pengguna, data konfigurasi, pemeriksaan kepatuhan, dan manual), lihat Bukti.

Tabel bukti

Tabel Bukti mencantumkan potongan-potongan bukti individu yang terkandung dalam folder bukti.

Ini termasuk informasi berikut:

1. Waktu — Menentukan kapan bukti dikumpulkan, dan juga berfungsi sebagai nama bukti. Waktu diwakili dalam Coordinated Universal Time (UTC). Memilih waktu dari kolom ini membuka halaman detail bukti. Halaman ini dijelaskan di bagian berikut.
2. Bukti berdasarkan jenis — Kategori bukti.
   - Bukti pemeriksaan kepatuhan dikumpulkan dari AWS Config atauAWS Security Hub.
   - Bukti aktivitas pengguna dikumpulkan dari AWS CloudTrail log.
   - Bukti data konfigurasi dikumpulkan dari snapshot layanan lain seperti Amazon EC2, Amazon S3, atau IAM.
   - Bukti manual adalah bukti bahwa Anda mengunggah secara manual.
3. Pemeriksaan kepatuhan — Status evaluasi untuk bukti yang termasuk dalam kategori pemeriksaan kepatuhan.
   - Untuk bukti yang dikumpulkan dariAWS Security Hub, hasil Lulus atau Gagal dilaporkan langsung dariAWS Security Hub.
   - Untuk bukti yang dikumpulkan dariAWS Config, hasil Compliant atau Noncompliant dilaporkan langsung dari. AWS Config
   - Jika Tidak berlaku ditampilkan, ini menunjukkan bahwa Anda tidak memiliki AWS Security Hub atau AWS Config mengaktifkan, atau bukti berasal dari tipe sumber data yang berbeda.
4. Sumber data — Sumber data tempat bukti dikumpulkan.
5. Nama acara — Nama acara yang termasuk dalam bukti.
6. Sumber daya — Jumlah sumber daya yang dinilai untuk menghasilkan bukti.
7. Pemilihan laporan penilaian — Menunjukkan apakah bukti tersebut dipilih secara manual untuk dimasukkan dalam laporan penilaian.
   - Untuk menyertakan bukti, pilih bukti dan pilih Tambahkan ke laporan penilaian.
   - Untuk mengecualikan bukti, pilih bukti dan pilih Hapus dari laporan penilaian.

Untuk mengunggah bukti manual ke folder bukti, pilih Unggah bukti manual, masukkan URI S3 bukti, lalu pilih Unggah. Untuk informasi selengkapnya, lihat Mengunggah bukti manual di AWS Audit Manager.

Untuk melihat detail untuk setiap bukti individu, pilih nama bukti hyperlink di bawah kolom Waktu. Ini membuka halaman detail bukti, yang dijelaskan di bagian berikut.

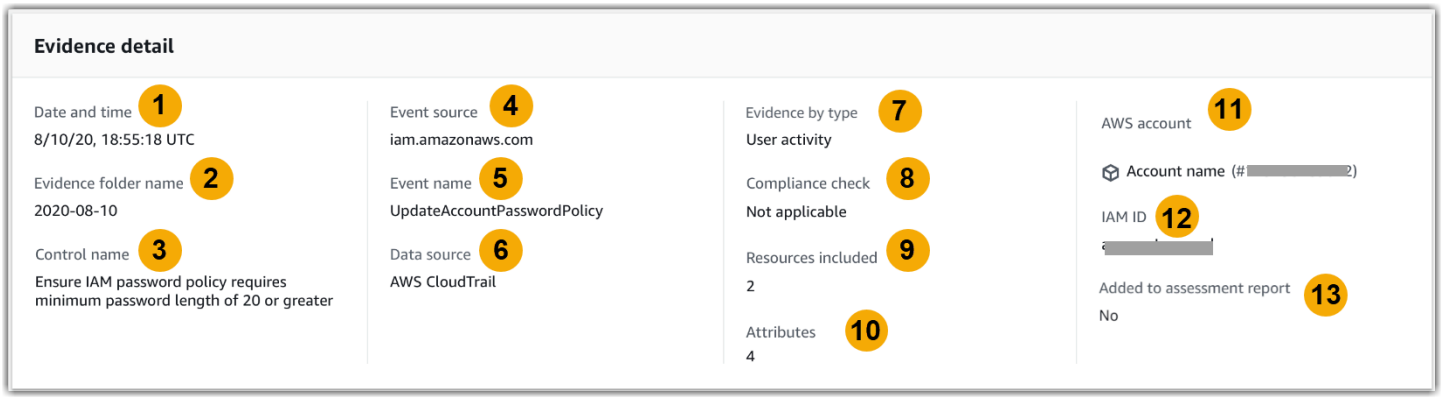
Meninjau bukti individu

Saat Anda membuka satu bagian bukti, Anda akan melihat halaman detail bukti yang berisi tiga bagian: bagian Detail bukti, tabel Atribut, dan tabel yang disertakan Sumber Daya. Bagian-bagian ini dan isinya dijelaskan sebagai berikut.

- Detail bukti
- Atribut
- Sumber daya termasuk

Detail bukti

Bagian Detail Bukti pada halaman menampilkan ikhtisar bukti.



Ini termasuk informasi berikut:

1. Tanggal dan waktu — Tanggal dan waktu ketika bukti dikumpulkan, diwakili dalam Coordinated Universal Time (UTC).
2. Nama folder bukti — Nama folder bukti yang berisi bukti.
3. Nama kontrol — Nama kontrol yang terkait dengan bukti.
4. Sumber peristiwa — Nama sumber daya yang menciptakan peristiwa bukti.
5. Nama acara — Nama peristiwa bukti.
6. Sumber data — Sumber data tempat bukti dikumpulkan.
7. Bukti berdasarkan jenis — Jenis bukti.
   - Bukti pemeriksaan kepatuhan dikumpulkan dari AWS Config atauAWS Security Hub.

- Bukti aktivitas pengguna dikumpulkan dari AWS CloudTrail log.
- Bukti data konfigurasi dikumpulkan dari snapshot lain Layanan AWS seperti Amazon EC2, Amazon S3, atau IAM.
- Bukti manual adalah bukti bahwa Anda mengunggah secara manual.

8. Pemeriksaan kepatuhan — Status evaluasi untuk bukti yang termasuk dalam kategori pemeriksaan kepatuhan.
   - Untuk bukti yang dikumpulkan dariAWS Security Hub, hasil Lulus atau Gagal dilaporkan langsung dariAWS Security Hub.
   - Untuk bukti yang dikumpulkan dariAWS Config, hasil Compliant atau Noncompliant dilaporkan langsung dari. AWS Config
   - Jika Tidak berlaku ditampilkan, ini menunjukkan bahwa Anda tidak memiliki AWS Security Hub atau AWS Config mengaktifkan, atau bukti berasal dari sumber data yang berbeda.
9. Sumber daya termasuk — Jumlah sumber daya yang dinilai untuk menghasilkan bukti.
10. Atribut — Jumlah total atribut yang digunakan oleh peristiwa dalam bukti.
11. AWSakun — Akun AWS Dari mana bukti dikumpulkan.
12. ID IAM — Pengguna atau peran yang relevan, jika berlaku.
13. Ditambahkan ke laporan penilaian - Menunjukkan jika Anda memilih untuk memasukkan bukti dalam laporan penilaian.

Atribut

Tabel Atribut menampilkan nama dan nilai yang digunakan oleh acara dalam bukti ini. Ini termasuk informasi berikut:

- Nama atribut — Persyaratan untuk bukti, seperti allowUsersToChangePassword.
- Nilai - Nilai atribut, seperti benar atau salah.

Sumber daya termasuk

Tabel yang disertakan Sumber Daya menampilkan daftar sumber daya yang dinilai untuk menghasilkan bukti ini. Ini mencakup satu atau lebih bidang berikut:

- ARN — Nama Sumber Daya Amazon (ARN) dari sumber daya. ARN mungkin tidak tersedia untuk semua jenis bukti.

- Nilai — Nilai sumber daya itu, jika berlaku.
- JSON - Tautan untuk melihat file JSON untuk sumber daya itu.

Menambahkan bukti manual di AWS Audit Manager

Audit Manager dapat secara otomatis mengumpulkan bukti untuk banyak kontrol. Namun, beberapa kontrol mengharuskan Anda untuk menambahkan bukti Anda sendiri secara manual.

Pertimbangkan contoh berikut:

- Beberapa kontrol berhubungan dengan penyediaan catatan fisik (seperti tanda tangan), atau peristiwa yang tidak dihasilkan di cloud (seperti pengamatan dan wawancara). Dalam kasus ini, Anda dapat mengunggah file secara manual sebagai bukti. Misalnya, jika kontrol memerlukan informasi tentang struktur organisasi Anda, Anda dapat mengunggah salinan bagan organisasi perusahaan Anda sebagai bukti manual.
- Beberapa kontrol mewakili pertanyaan penilaian risiko vendor. Pertanyaan penilaian risiko mungkin memerlukan dokumentasi sebagai bukti (seperti bagan organisasi). Atau, mungkin hanya perlu respons teks sederhana (seperti daftar jabatan). Dalam kasus yang terakhir, Anda dapat menanggapi pertanyaan dan menyimpan tanggapan Anda sebagai bukti manual.

Anda juga dapat menggunakan fitur upload manual untuk mengelola bukti dari berbagai lingkungan. Jika perusahaan Anda menggunakan model cloud hybrid atau model multicloud, Anda dapat mengunggah bukti dari lingkungan lokal, lingkungan yang dihosting di cloud, atau aplikasi SaaS Anda. Ini memungkinkan Anda untuk mengatur bukti Anda (terlepas dari mana asalnya) dengan menyimpannya dalam struktur penilaian Audit Manager, di mana setiap bukti dipetakan ke kontrol tertentu.

Untuk mempelajari lebih lanjut tentang berbagai jenis bukti di Audit Manager, lihat Bukti di bagian Konsep dan terminologi panduan ini.

Bagaimana cara menambahkan bukti manual

Anda dapat menggunakan salah satu metode berikut untuk menambahkan bukti manual Anda sendiri ke kontrol penilaian.

Ingatlah hal berikut:

- Anda hanya dapat menggunakan satu metode pada satu waktu untuk menambahkan bukti manual.

- Ukuran maksimum yang didukung untuk satu file bukti manual adalah 100 MB.
- Yang Format file yang didukung untuk bukti manual tercantum lebih jauh di bawah halaman ini.
- Masing-masing hanya Akun AWS dapat mengunggah hingga 100 file bukti secara manual ke kontrol setiap hari. Melebihi kuota harian ini menyebabkan unggahan manual tambahan gagal untuk kontrol itu. Jika Anda perlu mengunggah sejumlah besar bukti manual ke satu kontrol, unggah bukti Anda dalam batch selama beberapa hari.
- Ketika kontrol tidak aktif, Anda tidak dapat menambahkan bukti manual ke kontrol itu. Untuk menambahkan bukti manual, Anda harus terlebih dahulu mengubah status kontrol menjadi sedang ditinjau atau ditinjau. Untuk petunjuk, silakan lihat Perbarui status kontrol.

Impor file dari Amazon S3

Ikuti langkah-langkah berikut untuk mengimpor bukti manual dari bucket S3.

AWS console

Untuk mengimpor file dari S3 (konsol)

1. Buka konsol AWS Audit Manager di https://console.aws.amazon.com/auditmanager/home.
2. Di panel navigasi kiri, pilih Penilaian, lalu pilih nama penilaian Anda untuk membukanya.
3. Pilih tab Kontrol, gulir ke bawah ke set Kontrol, lalu pilih nama kontrol untuk membukanya.
4. Pada tab Folder bukti, pilih Tambahkan bukti manual, lalu pilih Impor file dari S3.
   - Atau, pilih nama folder bukti di tab Folder bukti untuk meninjau ringkasan folder bukti, lalu pilih Tambahkan bukti manual, Impor file dari S3.
5. Di halaman berikutnya, masukkan URI S3 bukti. Anda dapat menemukan URI S3 dengan menavigasi ke objek di konsol Amazon S3 dan memilih Salin URI S3.
6. Pilih Upload (Unggah).

AWS CLI

Dalam prosedur berikut, ganti *teks placeholder dengan informasi* Anda sendiri.

Untuk mengimpor file dari S3 (CLI)

1. Jalankan `list-assessments` perintah untuk melihat daftar penilaian Anda.

```
aws auditmanager list-assessments
```

Dalam tanggapannya, temukan penilaian yang ingin Anda unggah bukti dan catat ID penilaian.

2. Jalankan `get-assessment` perintah dan tentukan ID penilaian dari langkah satu.

```
aws auditmanager get-assessment --assessment-
id 1a2b3c4d-5e6f-7g8h-9i0j-0k1l2m3n4o5p
```

Dalam tanggapan, temukan set kontrol dan kontrol yang ingin Anda unggah bukti, dan catat ID mereka.

3. Jalankan `batch-import-evidence-to-assessment-control` perintah dengan parameter berikut:

   - `--assessment-id`— Gunakan ID penilaian dari langkah pertama.
   - `--control-set-id`— Gunakan ID set kontrol dari langkah kedua.
   - `--control-id`— Gunakan ID kontrol dari langkah kedua.
   - `--manual-evidence`— Gunakan `s3ResourcePath` sebagai jenis bukti manual dan tentukan URI S3 bukti. Anda dapat menemukan URI S3 dengan menavigasi ke objek di konsol Amazon S3 dan memilih Salin URI S3.

```
aws auditmanager batch-import-evidence-to-assessment-control --assessment-
id 1a2b3c4d-5e6f-7g8h-9i0j-0k1l2m3n4o5p --control-set-id ControlSet --control-
id a1b2c3d4-e5f6-g7h8-i9j0-k1l2m3n4o5p6 --manual-evidence s3ResourcePath=s3://
example-bucket/example-file.extension
```

Audit Manager API

Untuk mengimpor file dari S3 (API)

1. Hubungi `ListAssessments` operasi untuk melihat daftar penilaian Anda. Dalam tanggapannya, temukan penilaian yang ingin Anda unggah bukti dan catat ID penilaian.
2. Panggil `GetAssessment` operasi dan tentukan ID penilaian dari langkah satu. Dalam tanggapan, temukan set kontrol dan kontrol yang ingin Anda unggah bukti, dan catat ID mereka.

3. Panggil operasi `BatchImportEvidenceToAssessmentControl` dengan parameter berikut ini:

   - `assessmentId`— Gunakan ID penilaian dari langkah pertama.
   - `controlSetId`— Gunakan ID set kontrol dari langkah kedua.
   - `controlId`— Gunakan ID kontrol dari langkah kedua.
   - `manualEvidence`— Gunakan `s3ResourcePath` sebagai jenis bukti manual dan tentukan URI S3 bukti. Anda dapat menemukan URI S3 dengan menavigasi ke objek di konsol Amazon S3 dan memilih Salin URI S3.

   Untuk informasi selengkapnya, pilih salah satu tautan sebelumnya untuk membaca lebih lanjut di Referensi AWS Audit Manager API. Ini termasuk informasi tentang cara menggunakan operasi dan parameter ini di salah satu SDK khusus bahasaAWS.

Unggah file dari browser Anda

Ikuti langkah-langkah ini untuk mengunggah bukti manual dari browser Anda.

AWS console

Untuk mengunggah file dari browser Anda (konsol)

1. Buka konsol AWS Audit Manager di https://console.aws.amazon.com/auditmanager/home.
2. Di panel navigasi kiri, pilih Penilaian, lalu pilih nama penilaian Anda untuk membukanya.
3. Pada tab Controls, gulir ke bawah ke set Kontrol, lalu pilih nama kontrol untuk membukanya.

   Dari sini, ada tiga cara untuk mengunggah file:

   - (Opsi 1) Di spanduk notifikasi biru, pilih Unggah bukti manual.
   - (Opsi 2) Pada tab Folder bukti, pilih Tambahkan bukti manual, lalu pilih Unggah file dari browser.
   - (Opsi 3) Pilih nama folder bukti untuk meninjau ringkasan folder tersebut, pilih Tambahkan bukti manual, lalu pilih Unggah file dari browser.
4. Pilih file yang ingin Anda unggah.
5. Pilih Upload (Unggah).

AWS CLI

Dalam prosedur berikut, ganti *teks placeholder dengan informasi* Anda sendiri.

Untuk mengunggah file dari browser Anda (CLI)

1. Jalankan `list-assessments` perintah untuk melihat daftar penilaian Anda.

   ```
   aws auditmanager list-assessments
   ```

   Dalam tanggapannya, temukan penilaian yang ingin Anda unggah bukti dan catat ID penilaian.
2. Jalankan `get-assessment` perintah dan tentukan ID penilaian dari langkah satu.

   ```
   aws auditmanager get-assessment --assessment-
   id 1a2b3c4d-5e6f-7g8h-9i0j-0k1l2m3n4o5p
   ```

   Dalam tanggapan, temukan set kontrol dan kontrol yang ingin Anda unggah bukti, dan catat ID mereka.
3. Jalankan `get-evidence-file-upload-url` perintah dan tentukan file yang ingin Anda unggah.

   ```
   aws auditmanager get-evidence-file-upload-url --file-name fileName.extension
   ```

   Sebagai tanggapan, perhatikan URL yang telah ditentukan sebelumnya dan. `evidenceFileName`
4. Gunakan URL presigned dari langkah ketiga untuk mengunggah file dari browser Anda. Tindakan ini mengunggah file Anda ke Amazon S3, yang disimpan sebagai objek yang dapat dilampirkan ke kontrol penilaian. Pada langkah berikut, Anda akan mereferensikan objek yang baru dibuat dengan menggunakan parameter. `evidenceFileName`

   > **Note**
   >
   > Saat Anda mengunggah file menggunakan URL yang telah ditetapkan sebelumnya, Audit Manager melindungi dan menyimpan data Anda dengan menggunakan enkripsi sisi server. AWS Key Management Service Untuk mendukung hal ini, Anda harus menggunakan `x-amz-server-side-encryption` header dalam permintaan Anda ketika Anda menggunakan URL presigned untuk mengunggah file Anda.

Jika Anda menggunakan pelanggan yang dikelola AWS KMS key dalam Enkripsi data setelan Audit Manager, pastikan Anda juga menyertakan `x-amz-server-side-encryption-aws-kms-key-id` header dalam permintaan Anda. Jika `x-amz-server-side-encryption-aws-kms-key-id` header tidak ada dalam permintaan, Amazon S3 mengasumsikan bahwa Anda ingin menggunakan. Kunci yang dikelola AWS
Untuk informasi selengkapnya, lihat Melindungi data menggunakan enkripsi sisi server dengan AWS Key Management Service kunci (SSE-KMS) di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

5. Jalankan `batch-import-evidence-to-assessment-control` perintah dengan parameter berikut:

   - `--assessment-id`— Gunakan ID penilaian dari langkah pertama.
   - `--control-set-id`— Gunakan ID set kontrol dari langkah kedua.
   - `--control-id`— Gunakan ID kontrol dari langkah kedua.
   - `--manual-evidence`— Gunakan `evidenceFileName` sebagai jenis bukti manual dan tentukan nama file bukti dari langkah ketiga.

```
aws auditmanager batch-import-evidence-to-assessment-control --assessment-
id 1a2b3c4d-5e6f-7g8h-9i0j-0k1l2m3n4o5p --control-set-id ControlSet
 --control-id a1b2c3d4-e5f6-g7h8-i9j0-k1l2m3n4o5p6 --manual-evidence
 evidenceFileName=fileName.extension
```

Audit Manager API

Untuk mengunggah file dari browser Anda (API)

1. Panggil `ListAssessments` operasi. Dalam tanggapannya, temukan penilaian yang ingin Anda unggah bukti dan catat ID penilaian.
2. Panggil `GetAssessment` operasi dan tentukan `assessmentId` dari langkah satu. Dalam tanggapan, temukan set kontrol dan kontrol yang ingin Anda unggah bukti, dan catat ID mereka.
3. Panggil `GetEvidenceFileUploadUrl` operasi dan tentukan `fileName` yang ingin Anda unggah. Sebagai tanggapan, perhatikan URL yang telah ditentukan sebelumnya dan. `evidenceFileName`

4. Gunakan URL presigned dari langkah ketiga untuk mengunggah file dari browser Anda. Tindakan ini mengunggah file Anda ke Amazon S3, yang disimpan sebagai objek yang dapat dilampirkan ke kontrol penilaian. Pada langkah berikut, Anda akan mereferensikan objek yang baru dibuat dengan menggunakan parameter. `evidenceFileName`

   > **Note**
   >
   > Saat Anda mengunggah file menggunakan URL yang telah ditetapkan sebelumnya, Audit Manager melindungi dan menyimpan data Anda dengan menggunakan enkripsi sisi server. AWS Key Management Service Untuk mendukung hal ini, Anda harus menggunakan `x-amz-server-side-encryption` header dalam permintaan Anda ketika Anda menggunakan URL presigned untuk mengunggah file Anda.
   > Jika Anda menggunakan pelanggan yang dikelola AWS KMS key dalam Enkripsi data setelan Audit Manager, pastikan Anda juga menyertakan `x-amz-server-side-encryption-aws-kms-key-id` header dalam permintaan Anda. Jika `x-amz-server-side-encryption-aws-kms-key-id` header tidak ada dalam permintaan, Amazon S3 mengasumsikan bahwa Anda ingin menggunakan. Kunci yang dikelola AWS
   > Untuk informasi selengkapnya, lihat Melindungi data menggunakan enkripsi sisi server dengan AWS Key Management Service kunci (SSE-KMS) di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

5. Panggil operasi `BatchImportEvidenceToAssessmentControl` dengan parameter berikut ini:

   - `assessmentId`— Gunakan ID penilaian dari langkah pertama.
   - `controlSetId`— Gunakan ID set kontrol dari langkah kedua.
   - `controlId`— Gunakan ID kontrol dari langkah kedua.
   - `manualEvidence`— Gunakan `evidenceFileName` sebagai jenis bukti manual dan tentukan nama file bukti dari langkah ketiga.

Untuk informasi selengkapnya, pilih salah satu tautan sebelumnya untuk membaca lebih lanjut di Referensi AWS Audit Manager API. Ini termasuk informasi tentang cara menggunakan operasi dan parameter ini di salah satu SDK khusus bahasaAWS.

Masukkan respons teks

Ikuti langkah-langkah ini untuk memasukkan respons terhadap pertanyaan penilaian risiko dan simpan tanggapan Anda sebagai bukti manual.

AWS console

Untuk memasukkan respons teks (konsol)

1. Buka konsol AWS Audit Manager di https://console.aws.amazon.com/auditmanager/home.
2. Di panel navigasi kiri, pilih Penilaian, lalu pilih nama penilaian Anda untuk membukanya.
3. Pilih tab Kontrol, gulir ke bawah ke set Kontrol, lalu pilih nama kontrol untuk membukanya.

   Dari sini, ada tiga cara untuk memasukkan respons teks:

   - (Opsi 1) Di spanduk pemberitahuan biru, pilih Masukkan respons.
   - (Opsi 2) Pada tab Folder bukti, pilih Tambahkan bukti manual, lalu pilih Masukkan respons teks.
   - (Opsi 3) Pilih folder bukti untuk meninjau ringkasan folder itu, pilih Tambahkan bukti manual, lalu pilih Masukkan respons teks.
4. Di jendela pop-up yang muncul, masukkan respons Anda dalam format teks biasa.
5. Pilih Konfirmasi.

AWS CLI

Dalam prosedur berikut, ganti *teks placeholder dengan informasi* Anda sendiri.

Untuk memasukkan respons teks (CLI)

1. Jalankan perintah `list-assessments`.

   ```
   aws auditmanager list-assessments
   ```

   Dalam tanggapannya, temukan penilaian yang ingin Anda unggah bukti dan catat ID penilaian.
2. Jalankan `get-assessment` perintah dan tentukan ID penilaian dari langkah satu.

```
aws auditmanager get-assessment --assessment-
id 1a2b3c4d-5e6f-7g8h-9i0j-0k1l2m3n4o5p
```

Dalam respons, temukan set kontrol dan kontrol yang ingin Anda unggah bukti, dan catat ID mereka.

3. Jalankan `batch-import-evidence-to-assessment-control` perintah dengan parameter berikut:

   - `--assessment-id`— Gunakan ID penilaian dari langkah pertama.
   - `--control-set-id`— Gunakan ID set kontrol dari langkah kedua.
   - `--control-id`— Gunakan ID kontrol dari langkah kedua.
   - `--manual-evidence`— Gunakan `textResponse` sebagai jenis bukti manual dan masukkan teks yang ingin Anda simpan sebagai bukti manual.

```
aws auditmanager batch-import-evidence-to-assessment-control --assessment-
id 1a2b3c4d-5e6f-7g8h-9i0j-0k1l2m3n4o5p --control-set-id ControlSet --control-
id a1b2c3d4-e5f6-g7h8-i9j0-k1l2m3n4o5p6 --manual-evidence textResponse="enter
 text here"
```

Audit Manager API

Untuk memasukkan respons teks (API)

1. Panggil `ListAssessments` operasi. Dalam tanggapannya, temukan penilaian yang ingin Anda unggah bukti dan catat ID penilaian.
2. Panggil `GetAssessment` operasi dan tentukan `assessmentId` dari langkah satu. Dalam respons, temukan set kontrol dan kontrol yang ingin Anda unggah bukti, dan catat ID mereka.
3. Panggil operasi `BatchImportEvidenceToAssessmentControl` dengan parameter berikut ini:

   - `assessmentId`— Gunakan ID penilaian dari langkah pertama.
   - `controlSetId`— Gunakan ID set kontrol dari langkah kedua.
   - `controlId`— Gunakan ID kontrol dari langkah kedua.

- `manualEvidence`— Gunakan `textResponse` sebagai jenis bukti manual dan masukkan teks yang ingin Anda simpan sebagai bukti manual.

Untuk informasi selengkapnya, pilih salah satu tautan sebelumnya untuk membaca lebih lanjut di Referensi AWS Audit Manager API. Ini termasuk informasi tentang cara menggunakan operasi dan parameter ini di salah satu SDK khusus bahasaAWS.

Format file yang didukung untuk bukti manual

Tabel berikut mencantumkan dan menjelaskan jenis file yang dapat Anda unggah sebagai bukti manual. Untuk setiap jenis file, tabel juga mencantumkan ekstensi file yang didukung.

Tipe file	Deskripsi	Ekstensi file yang didukung
Kompresi atau arsip	Arsip terkompresi GNU Zip dan arsip terkompresi ZIP	`.gz`, `.zip`
Dokumen	File dokumen umum seperti file PDF dan Microsoft Office	`.doc`, `.docx`, `.pdf`, `.ppt`, `.pptx`, `.xls`, `.xlsx`
Citra	File gambar dan grafik	`.jpeg`, `.jpg`, `.png`, `.svg`
Teks	File teks non-biner lainnya, seperti dokumen teks biasa dan file bahasa markup	`.cer`, `.csv`, `.html`, `.jmx`, `.json`, `.md`, `.out`, `.rtf`, `.txt`, `.xml`, `.yaml`, `.yml`

Menghasilkan laporan penilaian

Laporan penilaian merangkum penilaian Anda dan menyediakan tautan ke kumpulan folder terorganisir yang berisi bukti terkait. Untuk informasi selengkapnya, lihat Laporan penilaian.

Anda dapat memilih bukti mana yang ingin Anda sertakan dalam laporan penilaian Anda sebelum Anda membuat laporan penilaian. Bukti yang baru dikumpulkan tidak secara otomatis disertakan dalam laporan penilaian.

Tugas

Menambahkan bukti ke laporan penilaian

Sebelum Anda dapat membuat laporan penilaian, Anda harus menambahkan setidaknya satu bukti ke laporan penilaian Anda. Anda dapat menambahkan seluruh folder bukti, atau Anda dapat menambahkan item bukti individual dari dalam folder.

Untuk menambahkan bukti ke laporan penilaian

1. Buka konsol AWS Audit Manager di https://console.aws.amazon.com/auditmanager/home.
2. Di panel navigasi, pilih Penilaian, lalu pilih nama penilaian untuk membukanya.
3. Pada tab Controls, gulir ke bawah ke tabel Control sets dan pilih nama kontrol untuk membukanya.
4. Pilih bagaimana Anda ingin menambahkan bukti ke laporan penilaian Anda.

    a. Untuk menambahkan seluruh folder bukti, gulir ke bawah ke folder Bukti, pilih folder yang ingin Anda tambahkan, lalu pilih Tambahkan ke laporan penilaian.

        - Jika Anda tidak dapat melihat folder yang Anda cari, ubah filter dropdown menjadi All time. Jika tidak, Anda akan melihat tujuh hari terakhir folder secara default.
        - Jika Tambahkan ke laporan penilaian berwarna abu-abu, folder bukti sudah ditambahkan ke laporan penilaian.

    b. Untuk menambahkan bukti spesifik, pilih folder bukti untuk membuka isinya. Pilih satu atau beberapa item dari daftar, lalu pilih Tambahkan ke laporan penilaian.

        - Jika Tambahkan ke laporan penilaian berwarna abu-abu, pastikan Anda memilih kotak centang di sebelah bukti, lalu coba lagi.
5. Setelah Anda menambahkan bukti ke laporan penilaian, spanduk sukses hijau muncul. Pilih Lihat bukti dalam laporan penilaian untuk melihat bukti yang akan disertakan dalam laporan penilaian Anda.
    - Atau, Anda dapat melihat bukti yang akan disertakan dalam laporan penilaian Anda dengan menavigasi kembali ke penilaian Anda dan memilih tab pemilihan laporan Penilaian.

Menghapus bukti dari laporan penilaian

Jika Anda perlu menghapus bukti dari laporan penilaian, ikuti langkah-langkah ini. Anda dapat menghapus seluruh folder bukti, atau Anda dapat menghapus item bukti tertentu dari dalam folder.

Untuk menghapus bukti dari laporan penilaian

1. Buka konsol AWS Audit Manager di https://console.aws.amazon.com/auditmanager/home.
2. Di panel navigasi, pilih Penilaian, lalu pilih nama penilaian untuk membukanya.
3. Pada tab Controls, gulir ke bawah ke tabel Control sets dan pilih nama kontrol untuk membukanya.
4. Pilih cara Anda ingin menghapus bukti dari laporan penilaian Anda.

    a. Untuk menghapus seluruh folder bukti, gulir ke bawah ke folder Bukti, pilih folder yang ingin Anda hapus, lalu pilih Hapus dari laporan penilaian.

    - Jika Anda tidak dapat melihat folder yang Anda cari, ubah filter dropdown menjadi All time. Jika tidak, Anda akan melihat tujuh hari terakhir folder secara default.
    - Jika Hapus dari laporan penilaian berwarna abu-abu, folder bukti telah dihapus dari laporan penilaian.

    b. Untuk menghapus bukti spesifik, pilih folder bukti untuk membuka isinya. Pilih satu atau beberapa item dari daftar, lalu pilih Hapus dari laporan penilaian.

    - Jika Hapus dari laporan penilaian berwarna abu-abu, pastikan Anda memilih kotak centang di sebelah bukti, lalu coba lagi.

5. Setelah Anda menambahkan bukti ke laporan penilaian, spanduk sukses hijau muncul. Pilih Lihat bukti dalam laporan penilaian untuk melihat bukti yang akan disertakan dalam laporan penilaian Anda.

    - Atau, Anda dapat melihat bukti yang akan disertakan dalam laporan penilaian Anda dengan menavigasi kembali ke penilaian Anda dan memilih tab pemilihan laporan Penilaian.

Menghasilkan laporan penilaian

Setelah menambahkan bukti ke laporan penilaian, Anda dapat membuat laporan penilaian akhir untuk dibagikan kepada auditor Anda. Saat Anda membuat laporan penilaian, laporan tersebut ditempatkan ke dalam bucket S3 yang Anda pilih sebagai tujuan laporan penilaian Anda.

> **Tip**
>
> Untuk memastikan bahwa laporan penilaian Anda berhasil dihasilkan, tinjau kamiKiat konfigurasi untuk tujuan laporan penilaian Anda.

Membuat laporan penilaian

1. Buka konsol AWS Audit Manager di https://console.aws.amazon.com/auditmanager/home.
2. Di panel navigasi kiri, pilih Penilaian.
3. Pilih nama penilaian yang ingin Anda buat laporan penilaian.
4. Pilih tab Pemilihan laporan penilaian, lalu pilih Hasilkan laporan penilaian.
   - Jika laporan penilaian Generate berwarna abu-abu, ini berarti belum ada bukti yang ditambahkan ke laporan penilaian.
5. Di jendela pop-up, berikan nama dan deskripsi untuk laporan penilaian, dan tinjau detail laporan penilaian.
6. Pilih Buat laporan penilaian dan tunggu beberapa menit saat laporan penilaian Anda dibuat.
7. Temukan dan unduh laporan penilaian Anda dari halaman Pusat unduhan konsol Audit Manager.
   - Atau, Anda dapat pergi ke bucket S3 tujuan laporan penilaian Anda dan mengunduh laporan penilaian dari sana.

Laporan penilaian memiliki file checksum untuk memastikan integritas laporan penilaian. Anda dapat memvalidasi ini dengan operasi ValidateAssessmentReportIntegrityAPI yang disediakan oleh Audit Manager.

Apa yang bisa saya lakukan selanjutnya?

Setelah membuat laporan penilaian, Anda dapat mempelajari lebih lanjut tentang hal-hal berikut:

- Temukan dan unduh laporan penilaian Anda — Pelajari cara mengunduh laporan penilaian Anda dari pusat unduhan atau dari Amazon S3.
- Jelajahi laporan penilaian Anda — Pelajari cara menavigasi laporan penilaian dan menjelajahi isinya.
- Validasi laporan penilaian Anda — Pelajari cara menggunakan operasi ValidateAssessmentReportIntegrityAPI untuk memvalidasi laporan penilaian Anda.

- Menghapus laporan penilaian yang tidak diinginkan — Pelajari cara menghapus laporan yang tidak diinginkan dari pusat unduhan atau dari Amazon S3.

Mengubah status penilaian menjadi tidak aktif

Ketika Anda tidak perlu lagi mengumpulkan bukti untuk penilaian, Anda dapat mengubah status penilaian menjadi Tidak Aktif. Ketika status penilaian berubah menjadi tidak aktif, penilaian berhenti mengumpulkan bukti. Akibatnya, Anda tidak lagi dikenakan biaya untuk penilaian itu.

Selain menghentikan pengumpulan bukti, Audit Manager membuat perubahan berikut pada kontrol yang berada dalam penilaian tidak aktif:

- Semua set kontrol berubah menjadi status Ditinjau.
- Semua kontrol yang sedang ditinjau berubah menjadi status Ditinjau.
- Delegasi untuk penilaian tidak aktif tidak dapat lagi melihat atau mengedit kontrol dan set kontrolnya.

> **Warning**
>
> Tindakan ini tidak dapat diubah. Kami menyarankan Anda melanjutkan dengan hati-hati dan memastikan bahwa Anda ingin menandai penilaian Anda sebagai tidak aktif. Ketika penilaian tidak aktif, Anda memiliki akses hanya-baca ke isinya. Ini berarti Anda masih dapat meninjau bukti yang dikumpulkan sebelumnya dan menghasilkan laporan penilaian. Namun, Anda tidak dapat mengedit penilaian tidak aktif, menambahkan komentar, atau mengunggah bukti manual apa pun.

Audit Manager console

Untuk mengubah status penilaian menjadi tidak aktif (konsol)

1. Buka konsol AWS Audit Manager di https://console.aws.amazon.com/auditmanager/home.
2. Di panel navigasi, pilih Penilaian.
3. Pilih nama penilaian untuk membukanya.
4. Di sudut kanan atas halaman, pilih Perbarui status penilaian, lalu pilih Tidak aktif.

5. Pilih Perbarui status di jendela pop-up untuk mengonfirmasi bahwa Anda ingin mengubah status menjadi tidak aktif.

Perubahan penilaian dan kontrolnya berlaku setelah sekitar satu menit.

AWS CLI

Untuk mengubah status penilaian menjadi tidak aktif () AWS CLI

1. Pertama, identifikasi penilaian yang ingin Anda perbarui. Untuk melakukan ini, jalankan perintah list-assessment.

```
aws auditmanager list-assessments
```

Respons mengembalikan daftar penilaian. Temukan penilaian yang ingin Anda nonaktifkan, dan catat ID penilaian.

2. Selanjutnya, jalankan update-assessment-statusperintah dan tentukan parameter berikut:

- `--assessment-id`— Gunakan parameter ini untuk menentukan penilaian yang ingin Anda nonaktifkan.
- `--status` – Atur nilai ini ke `INACTIVE`.

Dalam contoh berikut, ganti *`teks placeholder dengan informasi`* Anda sendiri.

```
aws auditmanager update-assessment-status --assessment-id a1b2c3d4-5678-90ab-
cdef-EXAMPLE11111 --status INACTIVE
```

Perubahan penilaian dan kontrolnya berlaku setelah sekitar satu menit.

Audit Manager API

Untuk mengubah status penilaian menjadi tidak aktif (API)

1. Gunakan ListAssessmentsoperasi untuk menemukan penilaian yang ingin Anda nonaktifkan, dan catat ID penilaian.
2. Gunakan UpdateAssessmentStatusoperasi dan tentukan parameter berikut:

- AssessMentID — Gunakan parameter ini untuk menentukan penilaian yang ingin Anda nonaktifkan.
- status - Tetapkan nilai ini ke`INACTIVE`.

Perubahan penilaian dan kontrolnya berlaku setelah sekitar satu menit.

Untuk informasi selengkapnya tentang operasi API ini, pilih salah satu tautan sebelumnya untuk membaca selengkapnya di Referensi AWS Audit Manager API. Ini termasuk informasi tentang cara menggunakan operasi dan parameter ini di salah satu SDK khusus bahasaAWS.

Menghapus penilaian

Anda dapat menghapus penilaian Audit Manager yang tidak lagi Anda perlukan. Anda dapat menghapus penilaian menggunakan konsol Audit Manager, Audit Manager API, atau AWS Command Line Interface (AWS CLI).

> **Warning**
>
> Tindakan ini secara permanen menghapus penilaian Anda dan semua bukti yang dikumpulkan. Anda tidak dapat memulihkan data ini. Sebagai hasilnya, kami menyarankan Anda melanjutkan dengan hati-hati dan memastikan bahwa Anda ingin menghapus penilaian Anda.

Audit Manager console

Untuk menghapus penilaian (konsol)

1. Buka konsol AWS Audit Manager di https://console.aws.amazon.com/auditmanager/home.
2. Di panel navigasi, pilih Penilaian.
3. Pilih penilaian yang ingin Anda hapus, dan pilih Hapus.
   - Atau, Anda dapat membuka penilaian dan kemudian memilih Hapus di kanan atas halaman.

AWS CLI

Untuk menghapus penilaian (AWS CLI)

1. Pertama, identifikasi penilaian yang ingin Anda hapus. Untuk melakukan ini, jalankan perintah list-assessment.

   ```
   aws auditmanager list-assessments
   ```

   Respons mengembalikan daftar penilaian. Temukan penilaian yang ingin Anda hapus, dan catat ID penilaian.

2. Selanjutnya, gunakan perintah hapus-penilaian dan tentukan `--assessment-id` penilaian yang ingin Anda hapus.

   Dalam contoh berikut, ganti *teks placeholder dengan informasi* Anda sendiri.

   ```
   aws auditmanager delete-assessment --assessment-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
   ```

Audit Manager API

Untuk menghapus penilaian (API)

1. Gunakan ListAssessmentsoperasi untuk menemukan penilaian yang ingin Anda hapus.

   Sebagai tanggapan, perhatikan ID penilaian.

2. Gunakan DeleteAssessmentoperasi dan tentukan AssesmentID penilaian yang ingin Anda hapus.

Untuk informasi selengkapnya tentang operasi API ini, pilih salah satu tautan sebelumnya untuk membaca selengkapnya di Referensi AWS Audit Manager API. Ini termasuk informasi tentang cara menggunakan operasi dan parameter ini di salah satu SDK khusus bahasaAWS.

> **Tip**
>
> Jika tujuan Anda adalah mengurangi biaya, pertimbangkan untuk mengubah status penilaian menjadi tidak aktif alih-alih menghapusnya. Tindakan ini menghentikan pengumpulan bukti,

dan menempatkan penilaian Anda dalam keadaan hanya-baca di mana Anda dapat meninjau bukti yang sebelumnya dikumpulkan. Penilaian tidak aktif tidak dikenakan biaya apa pun.

Delegasi diAWS Audit Manager

Pemilik audit digunakanAWS Audit Manager untuk membuat penilaian dan mengumpulkan bukti untuk kontrol yang tercantum dalam penilaian tersebut. Terkadang pemilik audit mungkin memiliki pertanyaan atau memerlukan bantuan saat memvalidasi bukti untuk set kontrol. Dalam situasi ini, pemilik audit dapat mendelegasikan kontrol yang ditetapkan kepada ahli materi pelajaran untuk ditinjau.

Pada tingkat tinggi, proses delegasi adalah sebagai berikut.

1. Pemilik audit memilih kontrol yang ditetapkan dalam penilaian mereka dan mendelegasikannya untuk ditinjau.
2. Delegasi meninjau kontrol tersebut dan bukti mereka, dan menyerahkan kontrol yang ditetapkan kembali ke pemilik audit setelah selesai.
3. Pemilik audit diberi tahu bahwa peninjauan selesai, dan memeriksa kontrol yang ditinjau untuk setiap komentar dari delegasi.

Gunakan bagian berikut dari panduan ini untuk mempelajari selengkapnya tentang cara mengelola tugas delegasiAWS Audit Manager.

Topik

> **Note**
>
> Akun dapat berupa pemilik audit atau delegasi diAWS Wilayah yang berbeda.

Tugas delegasi untuk pemilik audit

Sebagai pemilik auditAWS Audit Manager, Anda mungkin memerlukan bantuan dari pakar materi pelajaran untuk membantu Anda meninjau kontrol dan bukti. Dalam situasi ini, Anda dapat mendelegasikan set kontrol untuk ditinjau.

Topik berikut menjelaskan bagaimana Anda dapat mengelola delegasi menjelaskan bagaimana Anda dapat mengelola delegasi menjelaskan bagaimana Anda dapat mengelola delegasi menjelaskan caraAWS Audit Manager

Tugas

- Mendelegasikan set kontrol untuk ditinjau
- Mengakses delegasi aktif dan lengkap Anda
- Menghapus delegasi aktif dan lengkap

Mendelegasikan set kontrol untuk ditinjau

Ketika Anda membutuhkan bantuan dari ahli materi pelajaran, Anda dapat memilihAWS akun yang ingin Anda bantu, dan kemudian mendelegasikan set kontrol kepada mereka untuk ditinjau.

Anda dapat menggunakan salah satu prosedur berikut untuk mendelegasi set kontrol.

Mendelegasikan set kontrol dari halaman penilaian

Untuk mendelegasikan set kontrol dari halaman penilaian

1. Buka konsol AWS Audit Manager di https://console.aws.amazon.com/auditmanager/home.
2. Di panel navigasi, pilih Penilaian.
3. Pilih nama penilaian yang berisi kumpulan kontrol yang ingin Anda delegasi.
4. Dari halaman penilaian, pilih tab Kontrol. Ini menampilkan ringkasan status kontrol dan daftar kontrol dalam penilaian.
5. Pilih set kontrol dan pilih Delegasikan set kontrol.
6. Di bawah Pilihan delegasi, daftar pengguna dan peran ditampilkan. Pilih pengguna atau peran, atau gunakan bilah pencarian untuk mencarinya.
7. Di bawah Rincian delegasi, tinjau nama set kontrol dan nama penilaian.
8. (Opsional) Di bawah Komentar, tambahkan komentar dengan instruksi untuk membantu delegasi memenuhi tugas peninjauan mereka. Jangan sertakan informasi sensitif apa pun di komentar Anda.
9. Pilih Delegasikan set kontrol.
10. Spanduk sukses hijau menegaskan delegasi sukses dari set kontrol. Pilih Lihat delegasi untuk melihat permintaan delegasi. Anda juga dapat melihat delegasi kapan saja dengan memilih Delegasi di panel navigasi kiriAWS Audit Manager konsol.

Mendelegasikan set kontrol dari halaman delegasi

Untuk mendelegasikan set kontrol dari halaman delegasi

1. Buka konsol AWS Audit Manager di https://console.aws.amazon.com/auditmanager/home.
2. Di panel navigasi, pilih Delegasi.
3. Dari halaman delegasi, pilih Buat delegasi.
4. Di bawah Pilih set penilaian dan kontrol, tentukan penilaian dan set kontrol yang ingin Anda delegasikan.
5. Di bawah Pilihan delegasi, Anda akan melihat daftar pengguna dan peran. Pilih pengguna atau peran, atau gunakan bilah pencarian untuk mencarinya.
6. (Opsional) Di bawah Komentar, tambahkan komentar dengan instruksi untuk membantu delegasi memenuhi tugas peninjauan mereka. Jangan sertakan informasi sensitif apa pun di komentar Anda.
7. Pilih Buat delegasi.
8. Spanduk sukses hijau menegaskan delegasi sukses dari set kontrol. Pilih Lihat delegasi untuk melihat permintaan delegasi. Anda juga dapat melihat delegasi kapan saja dengan memilih Delegasi di panel navigasi kiriAWS Audit Manager konsol.

Ketika Anda mendelegasikan set kontrol untuk ditinjau, delegasi menerima pemberitahuan dan kemudian dapat mulai meninjau set kontrol. Proses yang diikuti delegasi ini dijelaskan dalamTugas delegasi untuk delegasi.

> **Tip**
>
> Delegasi dapat berlangganan topik SNS untuk menerima peringatan email saat tugas peninjauan didelegasikan kepada mereka. Untuk informasi selengkapnya tentang cara mengidentifikasi dan berlangganan topik SNS yang terkait dengannyaAWS Audit Manager, lihat Pemberitahuan diAWS Audit Manager.

Mengakses delegasi aktif dan lengkap Anda

Anda dapat mengakses daftar delegasi Anda kapan saja dengan memilih Delegasi di panel navigasi kiriAWS Audit Manager. Halaman delegasi berisi daftar delegasi aktif dan lengkap Anda, dengan rincian berikut untuk setiap delegasi:

- Delegasi ke — Akun AWS tempat Anda mendelegasikan kontrol yang ditetapkan.
- Tanggal - Tanggal ketika Anda mendelegasikan set kontrol.
- Status — Status terkini delegasi.
- Penilaian - Nama penilaian dengan tautan ke halaman detail penilaian.
- Set kontrol - Nama set kontrol yang didelegasikan untuk ditinjau.

Ketika delegasi selesai, Anda menerima pemberitahuan diAWS Audit Manager. Anda juga dapat menerima komentar dengan komentar dari delegasi. Prosedur berikut menjelaskan cara memeriksa notifikasi di Audit Manager setelah delegasi selesai, dan cara melihat komentar apa pun yang mungkin ditinggalkan oleh delegasi untuk Anda.

Untuk melihat delegasi dan memeriksa komentar

1. Buka konsol AWS Audit Manager di https://console.aws.amazon.com/auditmanager/home.
2. Di panel navigasi, pilih Pemberitahuan. Atau, pilih Pemberitahuan di bilah flash biru di bagian atas layar untuk membuka halaman notifikasi.
3. Tinjau halaman Pemberitahuan, yang mencakup tabel dengan informasi berikut:
   - Tanggal - Tanggal pemberitahuan.
   - Penilaian - Nama penilaian yang terkait dengan set kontrol.
   - Set kontrol - Nama set kontrol.
   - Sumber - Pengguna atau peran delegasi yang mengirimkan kontrol yang telah selesai diatur kembali kepada Anda.
   - Deskripsi - Komentar tingkat tinggi yang diberikan oleh delegasi.
4. Temukan set penilaian dan kontrol yang ditinjau dan diserahkan oleh delegasi kepada Anda, dan pilih nama penilaian untuk membukanya.
5. Di bawah tab Kontrol pada halaman detail penilaian, gulir ke bawah ke tabel Set kontrol. Di bawah kontrol dikelompokkan oleh kontrol set kolom, memperluas nama kontrol set untuk menunjukkan kontrol. Kemudian, pilih nama kontrol untuk membuka halaman detail kontrol.
6. Pilih tab Komentar untuk melihat komentar apa pun yang ditambahkan oleh delegasi untuk kontrol tertentu.
7. Ketika Anda puas bahwa tinjauan selesai untuk set kontrol, pilih set kontrol dan pilih Selesaikan tinjauan set kontrol.

> **Important**
>
> Audit Manager mengumpulkan bukti secara terus menerus. Akibatnya, bukti baru tambahan mungkin dikumpulkan setelah delegasi menyelesaikan peninjauan mereka terhadap kontrol. Jika Anda hanya ingin menggunakan bukti yang ditinjau dalam laporan penilaian, Anda dapat merujuk ke stempel waktu yang ditinjau kontrol untuk menentukan kapan bukti ditinjau. Stempel waktu ini dapat ditemukan di tab Changelog pada halaman detail kontrol. Anda kemudian dapat menggunakan stempel waktu ini untuk mengidentifikasi bukti mana yang Anda tambahkan ke laporan penilaian Anda.

Menghapus delegasi aktif dan lengkap

Mungkin ada keadaan di mana Anda membuat delegasi tetapi nantinya tidak lagi memerlukan bantuan untuk meninjau set kontrol tersebut. Ketika ini terjadi, Anda dapat menghapus delegasi aktif diAWS Audit Manager. Anda juga dapat menghapus delegasi yang sudah selesai yang tidak lagi ingin Anda tampilkan di halaman delegasi.

Menghapus delegasi

1. Buka konsol AWS Audit Manager di https://console.aws.amazon.com/auditmanager/home.
2. Di panel navigasi, pilih Delegasi.
3. Pada halaman Delegasi, pilih delegasi yang ingin Anda batalkan, lalu pilih Hapus delegasi.
4. Di jendela pop-up yang muncul, pilih Hapus untuk mengonfirmasi pilihan Anda.

Tugas delegasi untuk delegasi

Delegasi biasanya memiliki keahlian bisnis atau teknis khusus di beberapa bidang yang berbeda. Ini termasuk kebijakan retensi data, rencana pelatihan, infrastruktur jaringan, dan manajemen identitas. Mereka dapat membantu pemilik audit meninjau bukti yang dikumpulkan untuk kontrol yang berada di bawah bidang keahlian mereka.

Sebagai delegasi, Anda mungkin menerima permintaan dari pemilik audit untuk meninjau bukti yang terkait dengan kumpulan kontrol. Permintaan ini menunjukkan bahwa pemilik audit membutuhkan bantuan Anda untuk memvalidasi bukti ini. Anda dapat membantu pemilik audit dengan meninjau set kontrol dan bukti terkait, menambahkan komentar, mengunggah bukti tambahan, dan memperbarui status setiap kontrol yang Anda tinjau.

Topik berikut menjelaskan bagaimana Anda dapat mengelola delegasi menjelaskan bagaimana Anda dapat mengelola delegasi menjelaskan bagaimana Anda dapat mengelola delegasi menjelaskan caraAWS Audit Manager

> **Note**
>
> Pemilik audit mendelegasikan set kontrol khusus untuk ditinjau, bukan keseluruhan penilaian. Akibatnya, delegasi memiliki akses terbatas terhadap penilaian. Delegasi dapat meninjau bukti, menambahkan komentar, mengunggah bukti manual, dan memperbarui status kontrol untuk setiap kontrol di set kontrol. Untuk informasi lebih lanjut tentang peran dan izin di Audit Manager, lihat Kebijakan yang disarankan untuk persona pengguna di AWS Audit Manager.

Tugas

- Melihat notifikasi Anda untuk permintaan delegasi yang masuk
- Meninjau set kontrol yang didelegasikan dan bukti terkait
- Menambahkan sebuah komentar ke kontrol
- Menandai kontrol seperti yang ditinjau
- Mengirimkan kontrol yang ditinjau diatur kembali ke pemilik audit

Melihat notifikasi Anda untuk permintaan delegasi yang masuk

Ketika pemilik audit meminta bantuan Anda untuk meninjau set kontrol, Anda menerima pemberitahuan yang memberi tahu Anda tentang set kontrol yang mereka delegasikan kepada Anda.

> **Tip**
>
> Anda juga dapat berlangganan topik SNS untuk menerima peringatan email ketika set kontrol didelegasikan kepada Anda untuk ditinjau. Untuk informasi lebih lanjut, lihat Notifikasi di AWS Audit Manager.

Untuk melihat notifikasi Anda

1. Buka konsol AWS Audit Manager di https://console.aws.amazon.com/auditmanager/home.

2. Pilih Notifikasi di panel navigasi di panel navigasi di panel navigasi di panel navigasi di panel navigasi Atau, di bilah flash biru di bilah flash di bilah flash di bilah flash di bilah flash di bilah flash di bilah flash di bagian atas layar, pilih Lihat notifikasi untuk membuka halaman notifikasi.
3. Pada halaman Pemberitahuan, tinjau daftar set kontrol yang telah didelegasikan kepada Anda untuk ditinjau. Tabel tersebut mencakup informasi berikut:
   - Tanggal - Tanggal ketika set kontrol ditetapkan.
   - Penilaian - Nama penilaian yang terkait dengan set kontrol.
   - Set kontrol - Nama set kontrol.
   - Sumber - Pengguna atau peran yang mendelegasikan kontrol yang ditetapkan untuk Anda.
   - Deskripsi - Instruksi yang disediakan oleh pemilik audit.

Meninjau set kontrol yang didelegasikan dan bukti terkait

Anda dapat membantu pemilik audit dengan meninjau set kontrol yang telah mereka delegasikan kepada Anda. Anda dapat memeriksa kontrol ini dan bukti terkait mereka untuk menentukan apakah ada tindakan tambahan yang diperlukan. Tindakan tambahan tersebut dapat mencakup pengunggahan bukti tambahan secara manual untuk menunjukkan kepatuhan, atau meninggalkan komentar yang merinci langkah-langkah perbaikan yang Anda ikuti.

Untuk meninjau set kontrol

1. Buka konsol AWS Audit Manager di https://console.aws.amazon.com/auditmanager/home.
2. Di panel navigasi, pilih Pemberitahuan. Atau, di bilah flash biru, pilih Lihat notifikasi untuk membuka halaman notifikasi.
3. Pada halaman Pemberitahuan, daftar set kontrol yang didelegasikan kepada Anda akan ditampilkan. Identifikasi set kontrol mana yang ingin Anda tinjau, dan pilih nama penilaian terkait untuk membuka halaman detail penilaian.
4. Di bawah tab Kontrol pada halaman detail penilaian, gulir ke bawah ke tabel Set kontrol.
5. Di bawah kontrol dikelompokkan berdasarkan kontrol set kolom, memperluas nama kontrol set untuk menunjukkan kontrol, dan memilih nama kontrol untuk membuka halaman kontrol detail.
6. (Opsional) Pilih Perbarui status kontrol untuk mengubah status kontrol. Saat ulasan sedang berlangsung, Anda dapat menandai status sebagai Dalam Tinjauan.

7. Tinjau informasi tentang kontrol di folder Bukti, Sumber data, Komentar, dan tab Changelog. Untuk informasi tentang masing-masing tab ini dan cara menafsirkan informasi ini, lihat Meninjau kontrol dalam penilaian.

Untuk meninjau bukti untuk kontrol

1. Dari halaman detail kontrol, pilih tab Folder bukti.
2. Arahkan ke tabel folder Bukti, daftar folder yang berisi bukti untuk kontrol yang ditampilkan. Folder ini diatur dan diberi nama berdasarkan tanggal ketika bukti dikumpulkan.
3. Pilih nama folder bukti untuk membukanya. Kemudian, tinjau ringkasan semua bukti yang dikumpulkan pada tanggal itu. Ringkasan ini mencakup jumlah total masalah pemeriksaan kepatuhan yang dilaporkan langsung dariAWS Security Hub,AWS Config, atau keduanya. Untuk petunjuk tentang cara menafsirkan data di halaman ini, lihat Meninjau folder bukti.
4. Dari halaman ringkasan folder bukti, arahkan ke tabel Bukti. Di bawah Waktu kolom, pilih item baris untuk dibuka. Kemudian, tinjau detail tentang potongan bukti yang dikumpulkan saat itu. Untuk petunjuk tentang cara menafsirkan data pada halaman detail bukti, lihat Meninjau bukti individu.

> **Tip**
>
> MeskipunAWS Audit Manager secara otomatis mengumpulkan bukti untuk banyak kontrol, dalam beberapa kasus Anda mungkin perlu memberikan bukti tambahan untuk menunjukkan kepatuhan. Dalam kasus ini, Anda dapat mengunggah bukti secara manual. Untuk petunjuknya, lihat Mengunggah bukti manual.

Menambahkan sebuah komentar ke kontrol

Anda dapat menambahkan komentar untuk kontrol apa pun yang Anda tinjau. Komentar ini dapat dilihat oleh pemilik audit.

Menambahkan komentar ke kontrol

1. Buka konsol AWS Audit Manager di https://console.aws.amazon.com/auditmanager/home.

2. Pilih Notifikasi di panel navigasi di panel navigasi di panel navigasi di panel navigasi di panel navigasi Atau, pilih Lihat notifikasi di bilah flash biru di bagian atas layar untuk membuka halaman notifikasi.
3. Pada halaman Pemberitahuan, tinjau daftar set kontrol yang didelegasikan kepada Anda. Temukan set kontrol yang berisi kontrol yang ingin Anda tinggalkan komentar, dan pilih nama penilaian terkait.
4. Pilih tab Controls, gulir ke bawah ke tabel Control sets, dan kemudian pilih nama kontrol untuk membukanya.
5. Pilih tab Komentar.
6. Di bawah Kirim komentar, masukkan komentar Anda di kotak teks.
7. Pilih Kirim komentar untuk menambahkan komentar Anda. Kemudian, komentar Anda muncul di bawah bagian Komentar sebelumnya dari halaman, bersama dengan komentar lain mengenai kontrol ini.

Menandai kontrol seperti yang ditinjau

Anda dapat menunjukkan kemajuan tinjauan Anda dengan memperbarui status kontrol individual dalam kumpulan kontrol. Mengubah status kontrol adalah opsional. Namun, kami menyarankan Anda mengubah status setiap kontrol menjadi Ditinjau saat Anda menyelesaikan tinjauan untuk kontrol tersebut. Terlepas dari status masing-masing kontrol individu, Anda masih dapat mengirimkan kontrol kembali ke pemilik audit.

Untuk menandai kontrol seperti yang ditinjau

1. Buka konsol AWS Audit Manager di https://console.aws.amazon.com/auditmanager/home.
2. Pilih Notifikasi di panel navigasi di panel navigasi di panel navigasi di panel navigasi di panel navigasi Atau, pilih Lihat notifikasi di bilah flash biru di bagian atas layar untuk membuka halaman notifikasi.
3. Pada halaman Pemberitahuan, tinjau daftar set kontrol yang didelegasikan kepada Anda. Temukan set kontrol yang ingin Anda tandai sebagai peninjauan, dan pilih nama kumpulan kontrol yang ingin Anda tandai sebagai peninjauan, dan pilih nama penilaian yang ingin Anda tandai sebagai peninjauan, dan pilih nama
4. Di bawah tab Kontrol pada halaman detail penilaian, gulir ke bawah ke tabel Set kontrol.
5. Di bawah kontrol dikelompokkan oleh kontrol set kolom, memperluas nama kontrol set untuk menunjukkan kontrol. Pilih nama kontrol untuk membuka halaman detail kontrol.

6. Pilih Perbarui status kontrol dan ubah status menjadi Diulas.
7. Di jendela pop-up yang muncul, pilih Perbarui status kontrol untuk mengonfirmasi bahwa Anda selesai meninjau kontrol.

Mengirimkan kontrol yang ditinjau diatur kembali ke pemilik audit

Setelah selesai meninjau kontrol yang didelegasikan kepada Anda, kirimkan set kontrol ke pemilik audit. Ini melengkapi proses delegasi.

Untuk mengirimkan kontrol yang ditinjau diatur kembali ke pemilik audit

1. Buka konsol AWS Audit Manager di https://console.aws.amazon.com/auditmanager/home.
2. Pilih Notifikasi di panel navigasi di panel navigasi di panel navigasi di panel navigasi di panel navigasi
3. Tinjau daftar set kontrol yang didelegasikan kepada Anda. Temukan set kontrol yang ingin Anda kirimkan kembali ke pemilik audit, dan pilih nama penilaian terkait.
4. Gulir ke bawah ke tabel Set kontrol, pilih set kontrol yang ingin Anda kirimkan ke pemilik audit, lalu pilih Kirim untuk ditinjau.
5. Di jendela pop-up yang muncul, Anda dapat menambahkan komentar sebelum memilih Kirim untuk ditinjau. Setelah Anda mengirimkan kontrol ke pemilik audit, mereka dapat melihat komentar apa pun yang Anda tinggalkan untuk mereka.

Laporan penilaian

Laporan penilaian merangkum bukti yang dipilih yang dikumpulkan untuk penilaian. Ini juga berisi tautan ke file PDF dengan detail tentang setiap bukti. Konvensi konten, organisasi, dan penamaan spesifik dari laporan penilaian bergantung pada parameter yang Anda pilih saat membuat laporan.

Laporan penilaian membantu Anda memilih dan menyusun bukti yang relevan untuk audit Anda. Namun, mereka tidak menilai kepatuhan bukti itu sendiri. Sebagai gantinya, Manajer Audit hanya memberikan rincian bukti yang dipilih sebagai output yang dapat Anda bagikan dengan auditor Anda.

Struktur folder laporan penilaian

Saat Anda mengunduh laporan penilaian, Manajer Audit menghasilkan folder zip. Ini berisi laporan penilaian Anda dan file bukti terkait di subfolder bersarang.

Folder zip disusun sebagai berikut:

- Folder penilaian (contoh:`myAssessmentName-a1b2c3d4`) - Folder root.
  - Folder laporan penilaian (contoh:`reportName-a1b2c3d4e5f6g7`) - Subfolder tempat Anda dapat menemukan AssessmentReportSummary file.pdf, digest.txt, dan README.txt.
    - Bukti dengan folder kontrol (contoh:`controlName-a1b2c3d4e5f6g`) - Subfolder yang mengelompokkan file bukti dengan kontrol terkait.
      - Bukti dengan folder sumber data (contoh:`CloudTrail`,`Security Hub`) - Subfolder yang mengelompokkan file bukti berdasarkan jenis sumber data.
        - Bukti berdasarkan folder tanggal (contoh:`2022-07-01`) - Subfolder yang mengelompokkan file bukti berdasarkan tanggal pengumpulan bukti.
          - File bukti - File yang berisi rincian tentang potongan bukti individu.

Cara menavigasi laporan penilaian

Mulailah dengan membuka folder zip dan menavigasi satu tingkat ke folder laporan penilaian. Di sini, Anda dapat menemukan laporan penilaian PDF dan file README.txt.

Anda dapat meninjau file README.txt untuk memahami struktur dan isi folder zip. Hal ini juga memberikan informasi referensi tentang konvensi penamaan untuk setiap file. Informasi ini dapat membantu Anda menavigasi langsung ke subfolder atau file bukti jika Anda mencari item tertentu.

Jika tidak, untuk menelusuri bukti dan menemukan informasi yang Anda butuhkan, buka laporan penilaian PDF. Ini memberi Anda ikhtisar laporan tingkat tinggi, dan ringkasan penilaian yang dibuat oleh laporan tersebut.

Selanjutnya, gunakan daftar isi (TOC) untuk mengeksplorasi laporan. Anda dapat memilih kontrol hyperlink apa pun di TOC untuk langsung beralih ke ringkasan kontrol itu.

Ketika Anda siap untuk meninjau rincian bukti untuk kontrol, Anda dapat melakukannya dengan memilih nama bukti hyperlink. Untuk bukti otomatis, hyperlink membuka file PDF baru dengan detail tentang bukti itu. Untuk bukti manual, hyperlink membawa Anda ke bucket S3 yang berisi bukti.

> **Tip**
>
> Navigasi breadcrumb di bagian atas setiap halaman menunjukkan lokasi Anda saat ini dalam laporan penilaian saat Anda menelusuri kontrol dan bukti. Pilih TOC hyperlink untuk menavigasi kembali ke TOC kapan saja.

Bagian laporan penilaian

Gunakan informasi berikut untuk mempelajari lebih lanjut tentang setiap bagian dari laporan penilaian.

> **Note**
>
> Ketika Anda melihat tanda hubung (-) di samping salah satu atribut di bagian berikut, ini menunjukkan bahwa nilai atribut itu nol, atau nilai tidak ada.

- Halaman sampul
- Halaman Ikhtisar
- Daftar isi halaman
- Halaman kontrol
- Halaman ringkasan bukti
- Halaman detail bukti

Halaman sampul

Halaman sampul berisi nama laporan penilaian. Ini juga menampilkan tanggal dan waktu laporan dibuat, bersama dengan ID akun pengguna yang membuat laporan.

Halaman sampul diformat sebagai berikut. Manajer Audit menggantikan *placeholder* dengan informasi yang relevan dengan laporan Anda.

```
Assessment report name
Report generated on MM/DD/YYYY at HH:MM:SS AM/PM UCT by AccountID
```

Halaman Ikhtisar

Halaman ikhtisar memiliki dua bagian: ringkasan laporan itu sendiri, dan ringkasan penilaian yang sedang dilaporkan.

Ringkasan laporan

Bagian ini merangkum laporan penilaian.

- Nama laporan - Nama laporan.
- Deskripsi — Deskripsi yang dimasukkan oleh pemilik audit saat membuat laporan.
- Tanggal yang dihasilkan - Tanggal ketika laporan dibuat. Waktu diwakili dalam Coordinated Universal Time (UTC).
- Total kontrol yang disertakan - Jumlah kontrol yang disertakan dalam laporan dan telah mengumpulkan bukti. Ini adalah bagian dari jumlah total kontrol dalam penilaian.
- Akun AWStermasuk - Jumlah Akun AWS yang termasuk dalam laporan dan telah mengumpulkan bukti. Ini adalah bagian dari jumlah total Akun AWS dalam penilaian.
- Pemilihan laporan penilaian — Jumlah item bukti yang dipilih untuk dimasukkan dalam laporan. Ini termasuk jumlah total masalah pemeriksaan kepatuhan yang ditemukan dalam laporan.

Ringkasan penilaian

Bagian ini merangkum penilaian yang berkaitan dengan laporan tersebut.

- Nama penilaian — Nama penilaian bahwa laporan itu dihasilkan dari.
- Status — Status penilaian pada saat laporan dibuat.
- Assessment Region - Itu penilaian dibuat di. Wilayah AWS

- Akun AWSdalam lingkup — Daftar lengkap Akun AWS yang ada dalam lingkup penilaian.
- Layanan AWSdalam lingkup — Daftar lengkap Layanan AWS yang ada dalam lingkup penilaian.
- Nama kerangka kerja - Nama kerangka kerja tempat penilaian dibuat.
- Pemilik audit — Pengguna atau peran pemilik audit penilaian.
- Terakhir diperbarui - Tanggal ketika penilaian terakhir diperbarui. Waktu diwakili dalam UTC.

Daftar isi halaman

TOC menampilkan isi lengkap laporan penilaian. Isi dikelompokkan dan diatur berdasarkan set kontrol yang termasuk dalam penilaian. Kontrol tercantum di bawah set kontrol masing-masing.

Pilih item apa pun di daftar isi untuk menavigasi langsung ke bagian laporan tersebut. Anda dapat memilih set kontrol atau langsung ke kontrol.

Halaman kontrol

Halaman kontrol memiliki dua bagian: ringkasan kontrol itu sendiri, dan ringkasan bukti yang dikumpulkan untuk kontrol.

Ringkasan kontrol

Bagian ini mencakup informasi berikut.

- Nama kontrol - Nama kontrol.
- Deskripsi - Deskripsi kontrol.
- Set kontrol - Nama set kontrol yang dimiliki kontrol.
- Informasi pengujian - Prosedur pengujian yang direkomendasikan untuk kontrol ini.
- Rencana tindakan - Tindakan yang disarankan untuk dilakukan jika kontrol tidak terpenuhi.
- Seleksi laporan penilaian — Jumlah barang bukti yang terkait dengan kontrol ini yang dimasukkan dalam laporan penilaian. Ini termasuk jumlah masalah pemeriksaan kepatuhan yang ditemukan untuk bukti kontrol ini.

Bukti yang dikumpulkan

Bagian ini menunjukkan bukti yang dikumpulkan untuk kontrol. Bukti dikelompokkan berdasarkan folder, yang diatur dan diberi nama berdasarkan tanggal pengumpulan bukti. Di samping setiap nama folder bukti adalah jumlah total masalah pemeriksaan kepatuhan untuk folder tersebut.

Di bawah setiap nama folder bukti adalah daftar nama bukti hyperlink.

- Nama bukti otomatis dimulai dengan stempel waktu pengumpulan bukti, diikuti dengan kode layanan, nama peristiwa (hingga 20 karakter), ID akun, dan ID unik 12 karakter unik.

  Misalnya: `21-30-24_IAM_CreateUser_111122223333_a1b2c3d4e5f6`

  Untuk bukti otomatis, nama hyperlink membuka file PDF baru dengan ringkasan dan detail lebih lanjut.
- Nama bukti manual dimulai dengan stempel waktu unggahan bukti, diikuti dengan `manual` label, ID akun, dan ID unik 12 karakter. Mereka juga menyertakan 10 karakter pertama dari nama file, dan ekstensi file (hingga 10 karakter).

  Misalnya: `00-00-00_manual_111122223333_a1b2c3d4e5f6_myimage.png`

  Untuk bukti manual, nama hyperlink membawa Anda ke bucket S3 yang berisi bukti tersebut.

Di samping setiap nama bukti adalah hasil pemeriksaan kepatuhan untuk item tersebut.

- Untuk bukti otomatis yang dikumpulkan dari AWS Security Hub atauAWS Config, hasil yang Compliant, Non-compliant, atau Inconclusive dilaporkan.
- Untuk bukti otomatis yang dikumpulkan dari AWS CloudTrail dan panggilan API, dan untuk semua bukti manual, hasil yang tidak meyakinkan ditampilkan.

Halaman ringkasan bukti

Halaman ringkasan bukti mencakup informasi berikut:

- ID - Pengenal unik untuk bukti.
- Tanggal dikumpulkan - Tanggal ketika bukti dibuat atau diunggah.
- Deskripsi - Deskripsi bukti, termasuk ID akun dan jenis sumber data.
- Nama penilaian — Nama penilaian bahwa laporan itu dihasilkan dari.
- Nama kerangka kerja - Nama kerangka kerja tempat penilaian dibuat.
- Nama kontrol - Nama kontrol yang didukung bukti.
- Nama set kontrol - Nama set kontrol yang dimiliki oleh kontrol terkait.
- Deskripsi kontrol - Deskripsi kontrol yang didukung oleh bukti.

- Informasi pengujian - Prosedur pengujian yang direkomendasikan untuk kontrol.
- Rencana tindakan - Tindakan yang disarankan untuk dilakukan jika kontrol tidak terpenuhi.
- Wilayah AWSNama Daerah yang terkait dengan bukti.
- IAM ID - ARN pengguna atau peran yang terkait dengan bukti.
- Akun AWSAkun AWSID yang terkait dengan bukti.
- Layanan AWSNama Layanan AWS yang terkait dengan bukti.
- Sumber daya termasuk - AWS Sumber daya yang dinilai menghasilkan bukti. Atribut ini tidak berlaku untuk bukti pemeriksaan kepatuhanAWS Config. Untuk jenis bukti ini, Anda dapat menemukan semua sumber daya yang ditabulasikan dalam Halaman detail bukti bukti PDF.
- Nama acara — Nama acara bukti.
- Waktu acara — Waktu ketika peristiwa bukti terjadi.
- Sumber data — Dari mana bukti dikumpulkan atau diunggah. Jenis sumber data dapat berupaAWS Config, Hub Keamanan, panggilan AWS APICloudTrail, atau Manual.
- Bukti menurut jenis — Kategori bukti
  - Bukti pemeriksaan kepatuhan dikumpulkan dari AWS Config atau Hub Keamanan.
  - Bukti aktivitas pengguna dikumpulkan dari CloudTrail log.
  - Bukti data konfigurasi dikumpulkan dari snapshot lainnyaLayanan AWS.
  - Bukti manual adalah bukti yang Anda unggah secara manual.
- Status pemeriksaan kepatuhan - Status evaluasi untuk bukti yang termasuk dalam kategori pemeriksaan kepatuhan.
  - Untuk bukti otomatis yang dikumpulkan dari AWS Security Hub atauAWS Config, hasil yang Compliant, Non-compliant, atau Inconclusive dilaporkan.
  - Untuk bukti otomatis yang dikumpulkan dari AWS CloudTrail dan panggilan API, dan untuk semua bukti manual, hasil yang tidak meyakinkan ditampilkan.

Halaman detail bukti

Halaman detail bukti menunjukkan nama bukti dan tabel detail bukti. Tabel ini memberikan rincian rinci dari setiap elemen bukti sehingga Anda dapat memahami data dan memvalidasi bahwa itu benar. Tergantung pada sumber data bukti, isi halaman detail bukti bervariasi.

> **Tip**
>
> Navigasi breadcrumb di bagian atas setiap halaman menunjukkan lokasi Anda saat ini saat Anda menelusuri detail bukti. Pilih Ringkasan bukti untuk menavigasi kembali ke ringkasan bukti kapan saja.

Pemeriksaan integritas laporan penilaian

Saat Anda membuat laporan penilaian, Manajer Audit menghasilkan checksum berkas laporan yang disebut`digest.txt`. Anda dapat menggunakan file ini untuk memvalidasi integritas laporan dan memastikan bahwa tidak ada bukti yang diubah setelah laporan dibuat. Ini berisi objek JSON dengan tanda tangan dan hash yang tidak valid jika ada bagian dari arsip laporan diubah.

Untuk memvalidasi integritas laporan penilaian, gunakan ValidateAssessmentReportIntegrityAPI yang disediakan oleh Manajer Audit.

Laporan penilaian pemecahan masalah

Untuk menemukan jawaban atas pertanyaan dan masalah umum, lihat Memecahkan masalah laporan penilaian di bagian Pemecahan Masalah pada panduan ini.

Pencari bukti

Bukti finder menyediakan cara yang ampuh untuk mencari bukti di Manajer Audit. Alih-alih menjelajahi folder bukti yang sangat bersarang untuk menemukan apa yang Anda cari, Anda sekarang dapat menggunakan pencari bukti untuk menanyakan bukti Anda dengan cepat. Jika Anda menggunakan pencari bukti sebagai administrator yang didelegasikan, Anda dapat mencari bukti di semua akun anggota di organisasi Anda.

Dengan menggunakan kombinasi filter dan pengelompokan, Anda dapat secara progresif mempersempit cakupan kueri pencarian Anda. Misalnya, jika Anda menginginkan tampilan tingkat tinggi tentang kesehatan sistem Anda, lakukan pencarian dan filter yang luas berdasarkan penilaian, rentang tanggal, dan kepatuhan sumber daya. Jika tujuan Anda adalah untuk memulihkan sumber daya tertentu, Anda dapat melakukan pencarian sempit untuk menargetkan bukti untuk kontrol tertentu atau ID sumber daya. Setelah menentukan filter, Anda dapat mengelompokkan dan kemudian melihat pratinjau hasil pencarian yang cocok sebelum membuat laporan penilaian.

Untuk menggunakan pencari bukti, Anda harus mengaktifkan fitur ini dari pengaturan Manajer Audit Anda.

Topik

Memahami bagaimana pencari bukti bekerja dengan CloudTrail Danau

Pencari bukti menggunakan AWS CloudTrailkemampuan kueri dan penyimpanan Danau. Sebelum Anda mulai menggunakan pencari bukti, akan sangat membantu untuk memahami sedikit lebih banyak tentang cara kerja CloudTrail Danau.

CloudTrailDanau mengumpulkan data ke dalam penyimpanan data peristiwa tunggal yang dapat dicari yang mendukung kueri SQL yang kuat. Ini berarti Anda dapat mencari data di seluruh organisasi dan dalam rentang waktu khusus. Dengan pencari bukti, Anda dapat menggunakan fungsionalitas pencarian ini secara langsung di konsol Manajer Audit.

Saat Anda meminta untuk mengaktifkan pencari bukti, Manajer Audit membuat penyimpanan data peristiwa atas nama Anda. Setelah pencari bukti diaktifkan, semua bukti Manajer Audit Anda di masa mendatang akan dicerna ke dalam penyimpanan data peristiwa yang tersedia untuk kueri penelusuran pencari bukti. Setelah Anda mengaktifkan pencari bukti, kami juga mengisi ulang penyimpanan data peristiwa yang baru dibuat dengan data bukti bernilai dua tahun terakhir Anda. Jika Anda mengaktifkan pencari bukti sebagai administrator yang didelegasikan, kami mengisi ulang data untuk semua akun anggota di organisasi Anda.

Semua data bukti Anda, baik diisi ulang atau baru, disimpan di penyimpanan data acara selama 2 tahun. Anda dapat mengubah periode retensi default kapan saja. Untuk petunjuk, lihat Memperbarui penyimpanan data peristiwa di Panduan AWS CloudTrail pengguna. Anda dapat menyimpan data di penyimpanan data acara hingga 7 tahun, atau 2.555 hari.

> **Note**
>
> Proses pengisian ulang data, saat fitur ini diaktifkan, tidak dikenai biaya jika selesai pada November 2023.
> Ketika data bukti baru ditambahkan ke penyimpanan data acara yang bergerak maju, biaya CloudTrail Danau dikeluarkan untuk penyimpanan dan konsumsi data.
> Untuk pertanyaan CloudTrail Danau, Anda membayar saat Anda pergi. Ini berarti bahwa untuk setiap permintaan pencarian yang Anda jalankan di pencari bukti, Anda dikenakan biaya untuk data yang dipindai.
> Untuk informasi selengkapnya tentang harga CloudTrail Danau, lihat AWS CloudTrailharga.

Mengaktifkan pencari bukti

Anda dapat mengaktifkan pencari bukti dari pengaturan Manajer Audit Anda. Untuk petunjuknya, lihat Pencari bukti di halaman AWS Audit ManagerPengaturan panduan ini.

Pencari bukti pemecahan masalah

Untuk menemukan jawaban atas pertanyaan dan masalah umum, lihat Memecahkan masalah pencari bukti di bagian Pemecahan Masalah pada panduan ini.

Mencari bukti

Ikuti langkah-langkah berikut untuk mencari bukti di konsol Manajer Audit.

> **Note**
>
> Anda juga dapat menggunakan CloudTrail API untuk menanyakan data bukti Anda. Untuk informasi selengkapnya, lihat StartQuery dalam Referensi API AWS CloudTrail. Jika Anda lebih suka menggunakanAWS CLI, lihat Memulai kueri di Panduan AWS CloudTrail Pengguna.

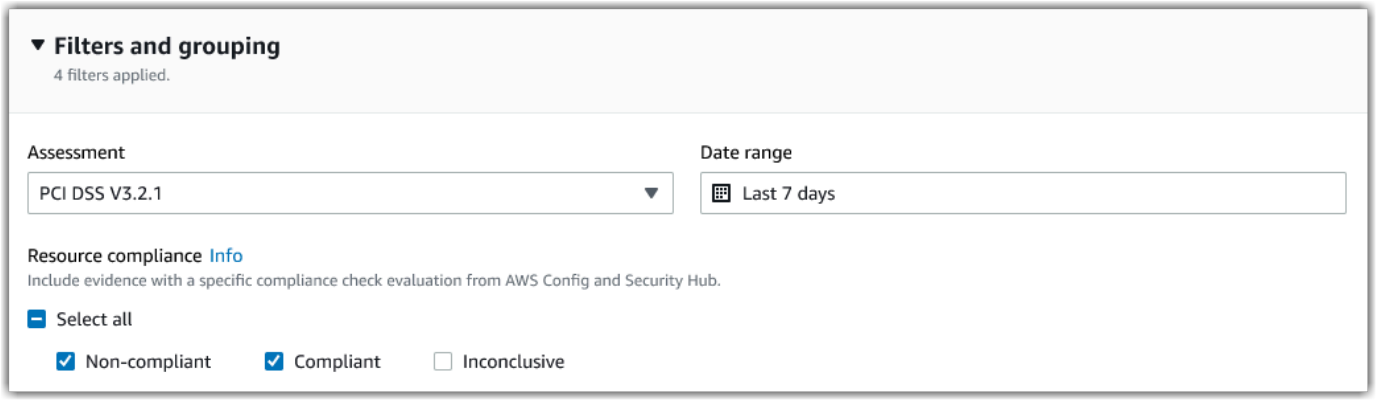
Di halaman ini

Melakukan kueri penelusuran

Ikuti langkah-langkah ini untuk melakukan permintaan pencarian di pencari bukti.

Untuk mencari bukti

1. Buka konsol AWS Audit Manager di https://console.aws.amazon.com/auditmanager/home.
2. Di panel navigasi, pilih Pencari bukti.
3. Selanjutnya, terapkan filter untuk mempersempit cakupan pencarian Anda.
    a. Untuk Penilaian, pilih penilaian.
    b. Untuk Rentang tanggal, pilih rentang.
    c. Untuk kepatuhan sumber daya, pilih status evaluasi.

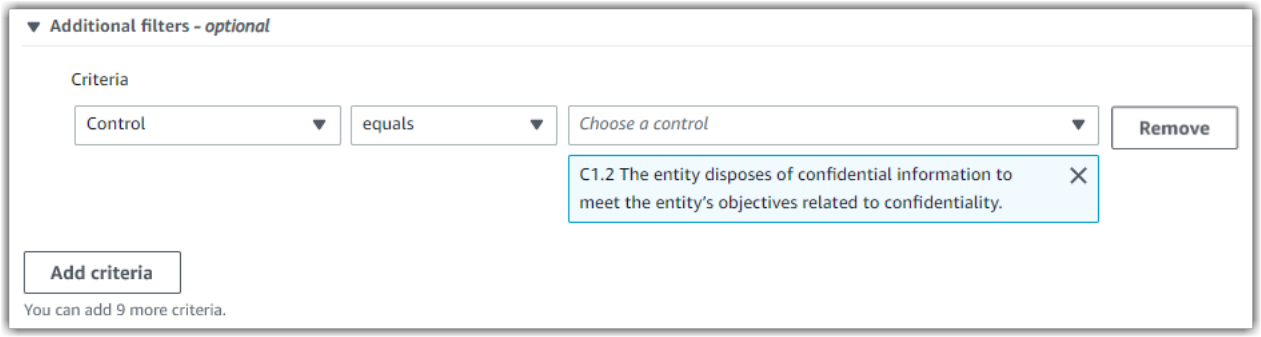


4. (Opsional) Pilih Filter tambahan - opsional untuk mempersempit pencarian lebih jauh.

   a. Pilih Tambahkan kriteria, pilih kriteria, lalu pilih satu atau lebih nilai untuk kriteria tersebut.

   b. Terus buat lebih banyak filter dengan cara yang sama.

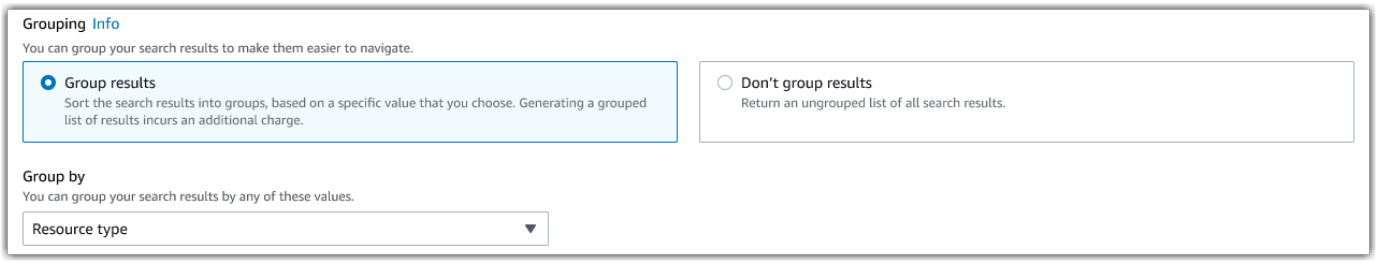
   c. Untuk menghapus filter yang tidak diinginkan, pilih Hapus.



5. Di bawah Pengelompokan, tentukan apakah Anda ingin mengelompokkan hasil pencarian.

   a. Jika Anda ingin mengelompokkan hasil, pilih nilai untuk mengelompokkan hasilnya.

   b. Jika Anda tidak ingin mengelompokkan hasilnya, lanjutkan ke langkah 6.



6. Pilih Cari.

Pencarian Anda mungkin memakan waktu beberapa menit, tergantung pada jumlah data bukti yang Anda miliki. Jangan ragu untuk menavigasi jauh dari pencari bukti saat pencarian sedang berlangsung. Bilah flash memberi tahu Anda saat hasil pencarian siap.

> **Tip**
>
> Untuk informasi selengkapnya tentang filter dan pengelompokan yang dapat Anda gunakan dalam prosedur ini, lihat Filter dan opsi pengelompokan.

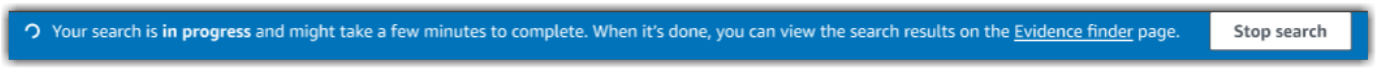
Menghentikan kueri penelusuran

Jika Anda ingin menghentikan kueri penelusuran karena alasan apa pun, ikuti langkah-langkah ini.

> **Note**
>
> Menghentikan kueri penelusuran masih dapat menghasilkan biaya. Anda dikenai biaya untuk jumlah data bukti yang dipindai sebelum menghentikan kueri penelusuran. Setelah berhenti, Anda dapat melihat sebagian hasil yang dikembalikan.

Untuk menghentikan kueri penelusuran yang sedang berlangsung

1. Di bilah flash kemajuan biru di bagian atas layar, pilih Hentikan pencarian.



2. (Opsional) Tinjau sebagian hasil yang ditampilkan sebelum Anda menghentikan kueri penelusuran.

   a. Jika Anda berada di halaman pencari bukti, hasil sebagian ditampilkan di layar.

   b. Jika Anda menjauh dari pencari bukti, pilih Lihat hasil sebagian di bilah flash konfirmasi hijau.

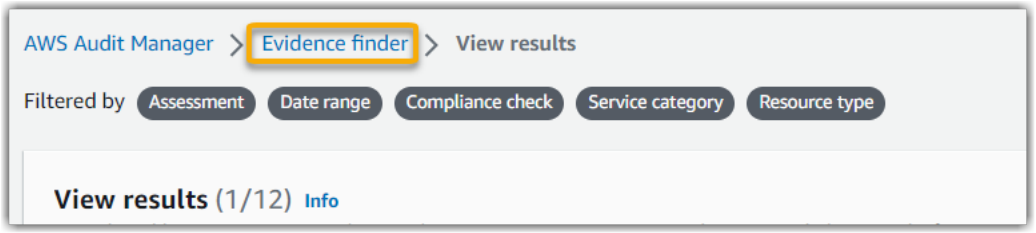
Mengedit filter pencarian

Anda dapat kembali ke kueri penelusuran terbaru dan mengubah filter sesuai kebutuhan.

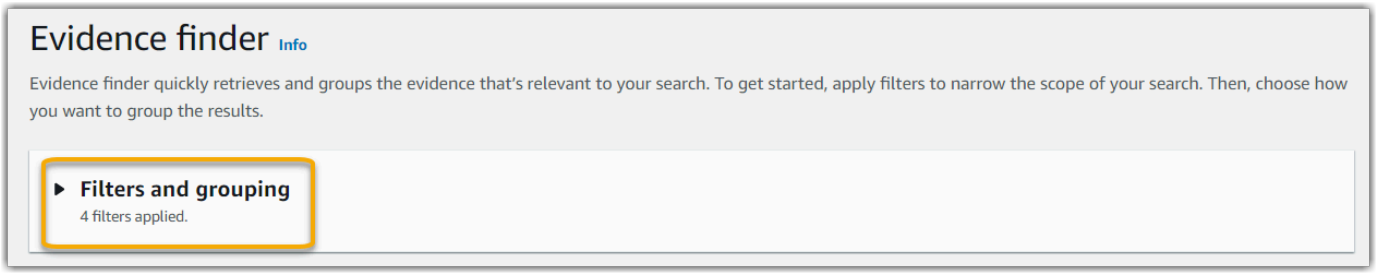
> **Note**
>
> Saat Anda mengedit filter dan memilih Penelusuran, ini akan memulai kueri penelusuran baru.

Untuk mengedit kueri penelusuran terbaru

1. Dari halaman Lihat hasil, pilih Pencari bukti dari menu navigasi breadcrumb.



2. Pilih Filter dan pengelompokan untuk memperluas pemilihan filter.



3. Selanjutnya, edit filter Anda atau mulai pencarian baru.

   a. Untuk mengedit filter, sesuaikan atau hapus filter saat ini dan pemilihan pengelompokan.

   b. Untuk memulai kembali, pilih Hapus filter dan terapkan filter dan pemilihan pengelompokan pilihan Anda.

4. Setelah selesai, pilih Cari.

Melihat hasil dalam pencari bukti

Setelah pencarian selesai, Anda dapat melihat hasil yang sesuai dengan kriteria pencarian Anda.

Perlu diingat bahwa beberapa sumber daya dapat dinilai selama pengumpulan bukti. Akibatnya, bukti dapat mencakup satu atau lebih sumber daya terkait. Dalam pencari bukti, hasil ditampilkan di tingkat sumber daya, dengan satu baris untuk setiap sumber daya. Anda dapat melihat pratinjau ringkasan setiap sumber daya tanpa meninggalkan halaman.

Setelah meninjau hasil pencarian, Anda dapat membuat laporan penilaian yang menyertakan bukti tersebut. Anda juga dapat mengekspor hasil pencarian Anda ke file nilai dipisahkan koma (CSV).

> **Important**
>
> Kami menyarankan agar pencari bukti tetap terbuka hingga Anda selesai menjelajahi hasil pencarian Anda. Hasil pencarian Anda akan dibuang saat Anda menavigasi dari tabel Lihat Hasil. Jika diperlukan, Anda dapat melihat hasil terbaru Anda di CloudTrail konsol di https://console.aws.amazon.com/cloudtrail/. Di sini, hasil kueri pencarian Anda dipertahankan selama tujuh hari. Namun, perlu diingat bahwa Anda tidak dapat membuat laporan penilaian dari hasil penelusuran di CloudTrail konsol.

Di halaman ini

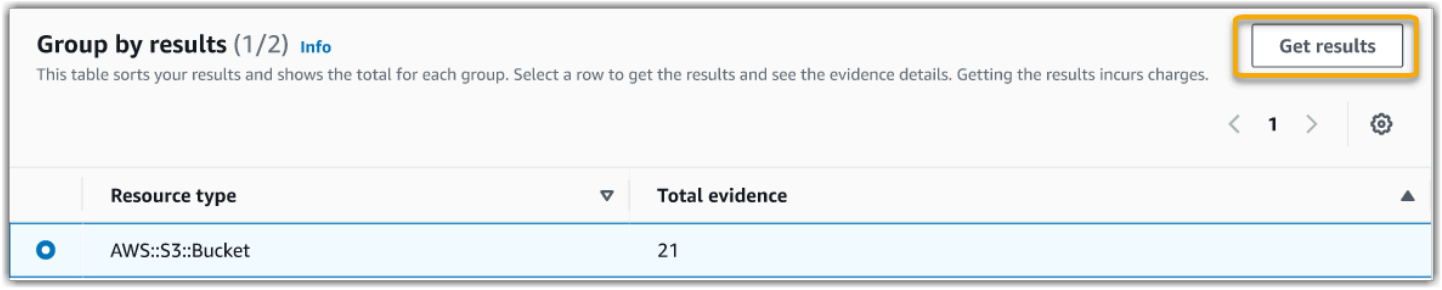
- Ekspor hasil pencarian Anda

Melihat hasil yang dikelompokkan

Jika Anda mengelompokkan hasil Anda, Anda dapat meninjau pengelompokan sebelum Anda menyelam lebih dalam ke bukti.

> **Note**
>
> Jika Anda tidak mengelompokkan hasil, pencari bukti tidak menampilkan tabel hasil Grup berdasarkan. Sebagai gantinya, Anda dibawa langsung ke tabel Lihat hasil.

Gunakan tabel hasil Grup berdasarkan untuk mempelajari luasnya bukti yang cocok dan bagaimana hal itu didistribusikan di seluruh dimensi tertentu. Hasil dikelompokkan berdasarkan nilai yang Anda pilih. Misalnya, jika Anda dikelompokkan berdasarkan jenis Sumber Daya, tabel menampilkan daftar jenis AWS sumber daya. Kolom Total bukti menunjukkan jumlah hasil yang cocok untuk setiap jenis sumber daya.



Untuk mendapatkan hasil untuk grup

1. Dari tabel hasil Grup berdasarkan, pilih baris untuk hasil yang ingin Anda dapatkan.
2. Pilih Dapatkan hasil. Ini memulai kueri penelusuran baru, dan mengarahkan Anda ke tabel Lihat hasil tempat Anda dapat melihat hasil untuk grup tersebut.

Melihat hasil pencarian

Tabel Lihat hasil menampilkan hasil pencarian Anda. Dari sini, Anda dapat mengambil tindakan berikut:

- Mengelola preferensi tampilan

- Ringkasan sumber daya pratinjau
- Membuat laporan penilaian dari hasil penelusuran Anda
- Ekspor hasil pencarian Anda

Mengelola preferensi tampilan

Preferensi tampilan Anda mengontrol apa yang Anda lihat di halaman hasil.

Mengelola preferensi tampilan

1. Pilih ikon pengaturan (#) di bagian atas tabel Lihat hasil.
2. Tinjau dan ubah pengaturan berikut sesuai kebutuhan:
   a. Pilih kolom tabel yang terlihat - Gunakan opsi beralih untuk mengubah kolom mana yang ditampilkan.
   b. Ukuran halaman - Pilih tombol radio untuk menentukan berapa banyak hasil yang ditampilkan pada setiap halaman.
   c. Bungkus teks - Pilih kotak centang untuk membungkus garis panjang teks agar lebih mudah dibaca.
3. Pilih Konfirmasi untuk menyimpan preferensi Anda.

Ringkasan sumber daya pratinjau

Anda dapat melihat pratinjau sumber daya terkait untuk bukti yang cocok dengan kueri penelusuran Anda. Ini membantu Anda menentukan apakah kueri penelusuran mengembalikan hasil yang dimaksud, atau apakah Anda perlu menyesuaikan filter dan menjalankan kembali kueri penelusuran.

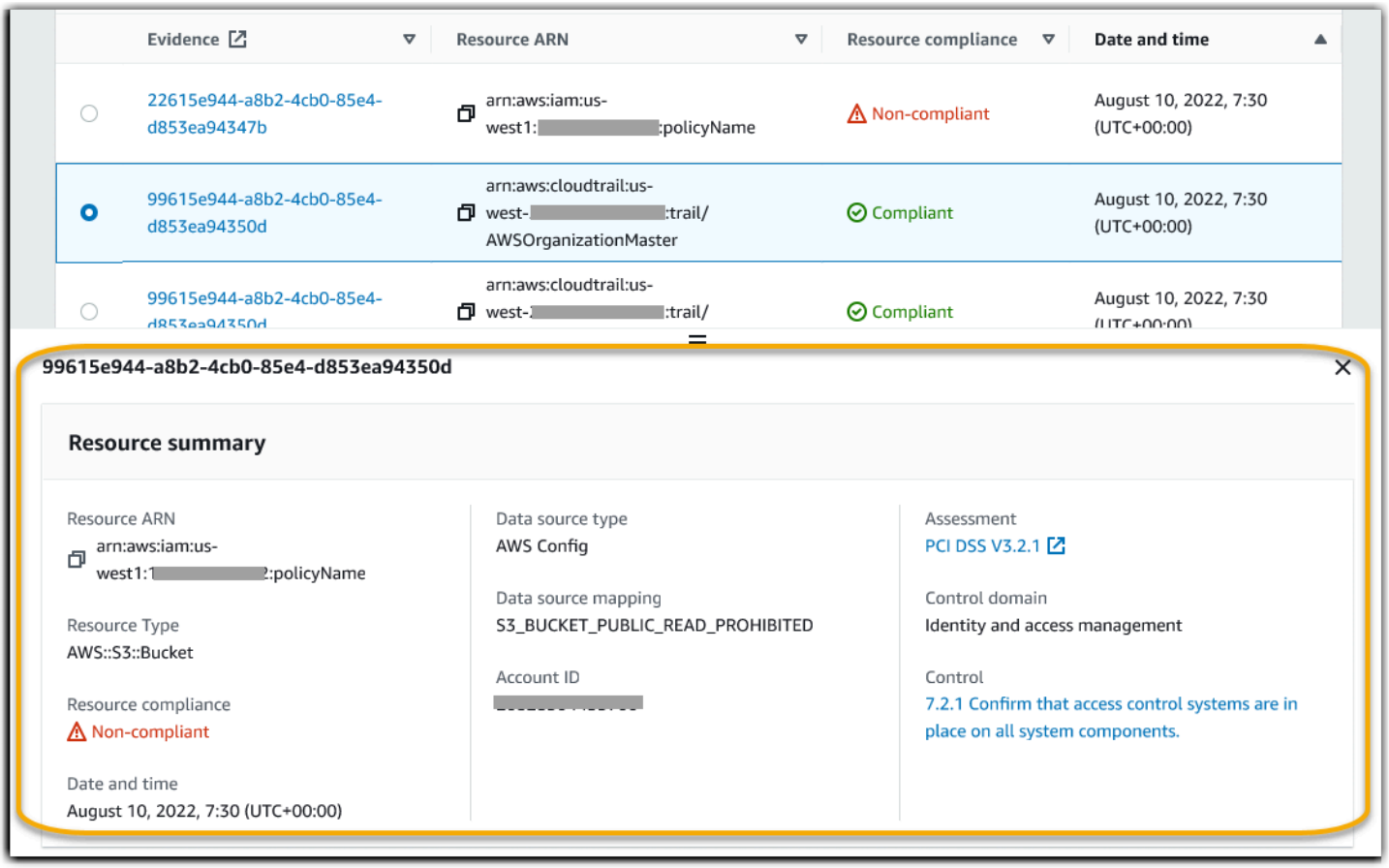
Perlu diingat bahwa bukti dapat memiliki satu atau lebih sumber daya terkait. Pencari bukti menunjukkan hasil di tingkat sumber daya (dengan satu baris untuk setiap sumber daya).

> **Note**
>
> Penemu bukti mengembalikan hasil untuk bukti otomatis dan manual. Namun, Anda hanya dapat melihat pratinjau ringkasan sumber daya untuk bukti otomatis. Ini karena Manajer Audit tidak melakukan penilaian sumber daya untuk bukti manual, dan sebagai hasilnya, tidak ada ringkasan sumber daya yang tersedia.

Untuk melihat detail tentang bukti manual, pilih nama bukti untuk membuka halaman detail bukti. Jika Anda membuat laporan penilaian dari hasil pencari bukti, detail bukti manual disertakan dalam laporan penilaian.

Untuk melihat pratinjau ringkasan sumber daya

1. Pilih tombol radio di sebelah hasilnya. Ini membuka panel ringkasan sumber daya pada halaman saat ini.
2. (Opsional) Untuk melihat detail lengkap dari bukti terkait, pilih nama bukti.
3. (Opsional) Gunakan garis horizontal (=) untuk menyeret dan mengubah ukuran panel ringkasan sumber daya.
4. Pilih (x) untuk menutup panel ringkasan sumber daya.



Membuat laporan penilaian dari hasil penelusuran Anda

Setelah puas dengan hasil penelusuran, buat laporan penilaian.

Membuat laporan penilaian dari hasil penelusuran

1. Di bagian atas tabel Lihat hasil, pilih Buat laporan penilaian.
2. Masukkan nama dan deskripsi untuk laporan penilaian Anda, dan tinjau detail laporan penilaian.
3. Pilih Buat laporan penilaian.

Diperlukan beberapa menit agar laporan penilaian Anda dibuat. Anda dapat menavigasi jauh dari pencari bukti saat ini terjadi, dan pemberitahuan keberhasilan hijau akan mengkonfirmasi ketika laporan siap. Anda kemudian dapat pergi ke pusat unduhan Manajer Audit dan mengunduh laporan penilaian Anda.

> **Note**
>
> Manajer Audit menghasilkan laporan satu kali hanya menggunakan bukti dari hasil pencarian. Laporan ini tidak menyertakan bukti apa pun yang ditambahkan secara manual ke laporan dari halaman penilaian.
> Batas berlaku untuk berapa banyak bukti yang dapat dimasukkan dalam laporan penilaian. Untuk informasi selengkapnya, lihat Pencari bukti pemecahan masalah.

Ekspor hasil pencarian Anda

Anda mungkin memerlukan versi portabel dari hasil pencarian pencari bukti Anda. Jika demikian, Anda dapat mengekspor hasil pencarian ke file CSV.

Setelah Anda mengekspor hasil pencarian, file CSV tersedia di pusat unduhan Manajer Audit selama tujuh hari. Salinan file CSV juga dikirimkan ke bucket S3 pilihan Anda, yang dikenal sebagai tujuan ekspor. File CSV Anda tetap tersedia di bucket ini sampai Anda menghapus file tersebut.

Manajer Audit menggunakan fungsionalitas CloudTrailDanau untuk mengekspor dan mengirimkan file CSV dari pencari bukti. Faktor-faktor berikut menentukan cara kerja proses ekspor CSV:

- Semua hasil pencarian Anda disertakan dalam file CSV. Jika Anda hanya ingin menyertakan hasil pencarian tertentu, kami sarankan Anda mengedit filter pencarian Anda. Dengan cara ini, Anda dapat mempersempit hasil Anda untuk menargetkan hanya bukti yang ingin Anda ekspor.

- File CSV diekspor dalam format GZIP terkompresi. Nama file CSV default adalah`queryID/result.csv.gz`, di mana `queryID` ID kueri penelusuran Anda.
- Ukuran file maksimum untuk ekspor CSV adalah 1 TB. Jika Anda mengekspor lebih dari 1 TB data, hasil Anda dibagi menjadi lebih dari satu file. Setiap file CSV diberi nama`result_`*`number`*`.csv.gz`. Jumlah file CSV yang Anda dapatkan bergantung pada ukuran total hasil pencarian Anda. Misalnya, mengekspor 2 TB data memberi Anda dua file hasil kueri: `result_1.csv.gz` dan`result_2.csv.gz`.
- Selain file CSV, file tanda JSON dikirimkan ke bucket S3 Anda. File ini bertindak sebagai checksum untuk memverifikasi bahwa informasi dalam file CSV akurat. Untuk mempelajari lebih lanjut, lihat CloudTrailmenandatangani struktur file di Panduan AWS CloudTrail Pengembang. Untuk menentukan apakah hasil kueri dimodifikasi, dihapus, atau tidak berubah setelah dikirim, Anda dapat menggunakan validasi integritas hasil CloudTrail kueri. Untuk petunjuknya, lihat Memvalidasi hasil kueri yang disimpan di Panduan AWS CloudTrail Pengembang.

> **Note**
>
> Respons teks bukti manual saat ini tidak termasuk dalam pratinjau pencari bukti atau ekspor CSV. Untuk melihat data respons teks, pilih nama bukti manual di hasil pencari bukti Anda untuk membuka halaman detail bukti. Jika Anda perlu melihat data respons teks di luar konsol Manajer Audit, sebaiknya buat laporan penilaian dari hasil pencari bukti. Semua detail bukti manual, termasuk tanggapan teks, termasuk dalam laporan penilaian.

Mengekspor hasil Anda untuk pertama kalinya

Ikuti langkah-langkah berikut untuk mengekspor hasil pencarian Anda untuk pertama kalinya. Prosedur ini memberi Anda opsi untuk menentukan tujuan ekspor default untuk semua ekspor masa depan Anda. Jika Anda tidak ingin menyimpan tujuan ekspor default sekarang, Anda dapat melakukannya nanti dengan memperbarui pengaturan tujuan ekspor Anda.

> **Important**
>
> Sebelum memulai, pastikan bahwa Anda memiliki bucket S3 yang tersedia untuk digunakan sebagai tujuan ekspor Anda. Anda dapat menggunakan salah satu bucket S3 yang ada, atau Anda dapat membuat bucket baru di Amazon S3. Selain itu, bucket S3 Anda harus memiliki kebijakan izin yang diperlukan untuk memungkinkan CloudTrail menulis file ekspor ke dalamnya. Lebih khusus lagi, kebijakan bucket harus menyertakan `s3:PutObject`

tindakan dan bucket ARN, dan daftar CloudTrail sebagai prinsipal layanan. Kami memberikan contoh kebijakan izin yang dapat Anda gunakan. Untuk petunjuk tentang cara melampirkan kebijakan ini ke bucket S3 Anda, lihat Menambahkan kebijakan bucket dengan menggunakan konsol Amazon S3.
Untuk tips lainnya, lihat kiat konfigurasi untuk tujuan ekspor Anda. Jika Anda mengalami masalah saat mengekspor file CSV, lihat Mengatasi masalah ekspor CSV pencari bukti.

Untuk mengekspor hasil penelusuran Anda (pengalaman lari pertama)

1. Di bagian atas tabel Lihat hasil, pilih Ekspor CSV.
2. Tentukan bucket S3 tempat Anda ingin mengekspor file Anda.
   - Pilih Jelajahi S3 untuk memilih dari daftar bucket Anda.
   - Atau, Anda dapat memasukkan URI bucket dalam format ini: **`s3://bucketname/prefix`**

   > **Tip**
   >
   > Agar bucket tujuan tetap teratur, Anda dapat membuat folder opsional untuk ekspor CSV Anda. Untuk melakukannya, tambahkan garis miring (**`/`**) dan awalan ke nilai di kotak URI Sumber Daya (misalnya,). **`/evidenceFinderExports`** Manajer Audit kemudian menyertakan awalan ini saat menambahkan file CSV ke bucket, dan Amazon S3 menghasilkan jalur yang ditentukan oleh awalan. Untuk informasi selengkapnya tentang awalan di Amazon S3, lihat Mengatur objek di konsol Amazon S3 di Panduan Pengguna Amazon Simple Storage Service.
3. (Opsional) Jika Anda tidak ingin menyimpan bucket ini sebagai tujuan ekspor default, kosongkan kotak centang yang bertuliskan Simpan bucket ini sebagai tujuan ekspor default di pengaturan pencari bukti saya.
4. Pilih Ekspor.

Mengekspor hasil setelah Anda menyimpan tujuan ekspor

Setelah menyimpan bucket S3 default sebagai tujuan ekspor default, Anda dapat mengikuti langkah-langkah ini untuk bergerak maju.

Untuk mengekspor hasil pencarian Anda (setelah Anda menyimpan tujuan ekspor default)

1. Di bagian atas tabel Lihat hasil, pilih Ekspor CSV.
2. Pada prompt yang muncul, tinjau bucket S3 default tempat file yang diekspor akan disimpan.
    a. (Opsional) Untuk terus menggunakan bucket ini dan menyembunyikan pesan ini bergerak maju, centang kotak Jangan ingatkan saya lagi.
    b. (Opsional) Untuk mengubah bucket ini, ikuti prosedur untuk memperbarui pengaturan tujuan ekspor Anda.
3. Pilih Konfirmasi.

Bergantung pada seberapa banyak data yang Anda ekspor, proses ekspor dapat memakan waktu beberapa menit untuk diselesaikan. Anda dapat menavigasi jauh dari pencari bukti saat ekspor sedang berlangsung. Saat Anda menjauh dari pencari bukti, penelusuran Anda dihentikan dan hasil penelusuran Anda dibuang di konsol. Namun, proses ekspor CSV berlanjut di latar belakang. File CSV akan berisi kumpulan lengkap hasil pencarian yang cocok dengan kueri Anda.

Melihat hasil Anda setelah Anda mengekspornya

Untuk menemukan file CSV Anda dan memeriksa statusnya, buka pusat unduhan Manajer Audit. Saat file yang diekspor sudah siap, Anda dapat mengunduh file CSV Anda dari pusat unduhan.

Anda juga dapat menemukan dan mengunduh file CSV dari bucket S3 tujuan ekspor Anda.

Untuk menemukan file CSV Anda dan menandatangani file di konsol Amazon S3

1. Buka konsol Amazon S3.
2. Pilih bucket tujuan ekspor yang Anda tentukan saat mengekspor file CSV Anda.
3. Menavigasi melalui hirarki objek sampai Anda menemukan file CSV dan file tanda. File CSV memiliki `.csv.gz` ekstensi dan file tanda memiliki `.json` ekstensi.

Anda akan menavigasi melalui hirarki objek yang mirip dengan contoh berikut, tetapi dengan nama bucket tujuan ekspor yang berbeda, ID akun, tanggal, dan ID kueri.

```
All Buckets
    Export_Destination_Bucket_Name
        AWSLogs
            Account_ID;
```

```
                CloudTrail-Lake
                    Query
                        YYYY
                            MM
                              DD
                                Query_ID
```

Opsi filter dan pengelompokan

Halaman ini menjelaskan opsi filter dan pengelompokan yang tersedia di pencari bukti.

Di halaman ini

Referensi filter

Anda dapat menggunakan filter berikut untuk menemukan bukti yang sesuai dengan kriteria tertentu, seperti penilaian, kontrol, atauLayanan AWS.

Topik

Filter yang dibutuhkan

Gunakan filter ini untuk memulai dengan ikhtisar tingkat tinggi dari bukti dalam penilaian.

Nama filter	Deskripsi	Catatan
Penilaian	Mengembalikan bukti untuk penilaian tertentu.	Anda dapat memfilter dengan satu penilaian saja.
Rentang tanggal	Mengembalikan bukti untuk jangka waktu tertentu.	Baik, Anda dapat menggunakan rentang Relatif untuk menentukan rentang yang relatif terhadap tanggal hari ini (misalnya,**`Last 30 days`**).

Nama filter	Deskripsi	Catatan
		Atau, Anda dapat menggunakan rentang Absolute untuk menentukan rentang tanggal tertentu (misalnya,**`June 27th - July 4th`**).

Nama filter	Deskripsi	Catatan
Kepatuhan sumber daya	Mengembalikan sumber daya dengan evaluasi pemeriksaan kepatuhan tertentu.	Manajer Audit mengumpulkan bukti pemeriksaan kepatuhan untuk kontrol yang menggunakan AWS Config dan Hub Keamanan sebagai tipe sumber data. Beberapa sumber daya dapat dinilai selama pengumpulan bukti. Akibatnya, satu bukti pemeriksaan kepatuhan dapat mencakup satu atau lebih sumber daya. Anda dapat menggunakan filter ini untuk menjelajahi status kepatuhan di tingkat sumber daya. Anda dapat memilih satu atau lebih opsi berikut: • Tidak sesuai - Filter ini menemukan sumber daya dengan masalah pemeriksaan kepatuhan. Hal ini terjadi jika Hub Keamanan melaporkan hasil Gagal, atau jika AWS Config melaporkan hasil yang tidak sesuai. • Sesuai - Filter ini menemukan sumber daya yang tidak memiliki masalah pemeriksaan kepatuhan. Hal ini terjadi jika Hub Keamanan melaporkan hasil Pass, atau jika AWS Config melaporkan hasil Compliant. • Tidak meyakinkan - Filter ini menemukan sumber daya yang pemeriksaan kepatuhannya tidak tersedia atau berlaku. Ini terjadi jika sumber daya menggunakan AWS Config atau Hub Keamanan sebagai jenis sumber data yang mendasarinya, tetapi layanan tersebut tidak diaktifkan. Hal ini juga terjadi jika sumber daya menggunakan tipe sumber data yang mendasari yang tidak mendukung pemeriksaan kepatuhan (seperti bukti manual, panggilan AWS API, atauCloud Trail).

Filter tambahan (opsional)

Gunakan filter ini untuk mempersempit cakupan kueri penelusuran Anda. Misalnya, gunakan Layanan untuk melihat semua bukti yang terkait dengan Amazon S3. Gunakan Jenis sumber daya untuk fokus hanya pada bucket S3. Atau, gunakan Resource ARN untuk menargetkan bucket S3 tertentu.

Anda dapat membuat filter tambahan menggunakan satu atau beberapa kriteria berikut.

Nama kriteria	Deskripsi	Kapan menggunakan kriteria ini
ID Akun	Menelusuri olehAkun AWS.	Gunakan kriteria ini untuk menemukan bukti yang terkait dengan spesifikAkun AWS.
Kontrol	Menelusuri dengan nama kontrol.	Gunakan kriteria ini untuk menemukan bukti yang terkait dengan kontrol tertentu.
Kontrol domain	Menelusuri dengan domain kontrol.	Gunakan kriteria ini untuk fokus pada bidang subjek tertentu saat Anda mempersiapkan audit. Anda dapat memfilter berdasarkan domain kontrol jika Anda melakukan kueri penilaian yang dibuat dari kerangka kerja standar. Contoh domain kontrol termasuk manajemen identitas dan akses, pencatatan dan pemantauan, dan manajemen jaringan.
Jenis sumber data	Menelusuri dengan jenis sumber data.	Gunakan kriteria ini untuk fokus pada sumber data tertentu. Tetapkan nilai `Manual` untuk menemukan bukti yang Anda unggah secara manual. Jika tidak, Anda dapat memfilter bukti otomatis berdasarkan dari mana asalnya (misalnya ,`AWS Config`,`CloudTrail` ,`Security Hub`, atau`AWS API calls`).
Nama acara	Menelusuri dengan nama acara.	Gunakan kriteria ini untuk fokus pada peristiwa tertentu yang terkait dengan bukti. Suatu acara adalah catatan aktivitas dalam sebuahAkun AWS.

Nama kriteria	Deskripsi	Kapan menggunakan kriteria ini
		Misalnya, Anda dapat mencari nama panggilan API, seperti `AttachRolePolicy` operasi IAM yang digunakan untuk mengonfigurasi izin. Atau, cari CloudTrail kata kunci, seperti `ConsoleLogin` peristiwa yang dicatat CloudTrail saat pengguna masuk ke akun Anda.
Sumber Daya ARN	Menelusuri dengan Amazon Resource Name (ARN).	Gunakan kriteria ini untuk menemukan bukti yang terkait dengan AWS sumber daya tertentu.
Jenis sumber daya	Menelusuri berdasarkan jenis sumber daya.	Gunakan kriteria ini untuk fokus pada jenis sumber daya yang sedang dinilai, seperti instans Amazon EC2 atau bucket S3.
Layanan	Menelusuri dengan Layanan AWS nama.	Gunakan kriteria ini untuk menemukan bukti yang terkait dengan spesifikLayanan AWS, seperti Amazon EC2, Amazon S3, atau. AWS Config
Kategori layanan	Menelusuri berdasarkan Layanan AWS kategori.	Gunakan kriteria ini untuk fokus pada kategori tertentuL ayanan AWS. Contohnya termasuk keamanan, identitas dan kepatuhan, database, dan penyimpanan.

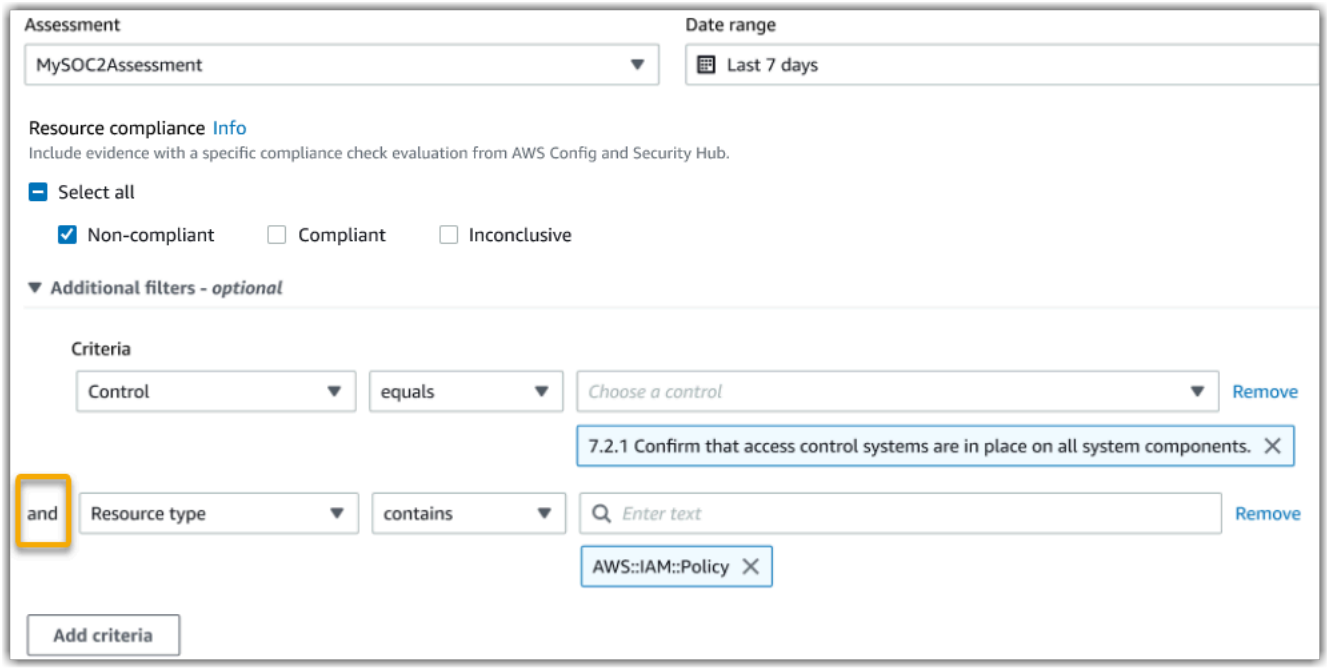
Menggabungkan filter

Kriteria perilaku

Bila Anda menentukan lebih dari satu kriteria, Manajer Audit akan menerapkan `AND` operator ke pilihan Anda. Ini berarti bahwa semua kriteria dikelompokkan ke dalam satu query, dan hasilnya harus sesuai dengan semua kriteria gabungan.

Contoh

Dalam penyiapan filter berikut, pencari bukti mengembalikan sumber daya yang tidak sesuai dari 7 hari terakhir untuk penilaian yang disebut. **`MySOC2Assessment`** Selain itu, hasilnya terkait dengan kebijakan IAM dan kontrol yang ditentukan.

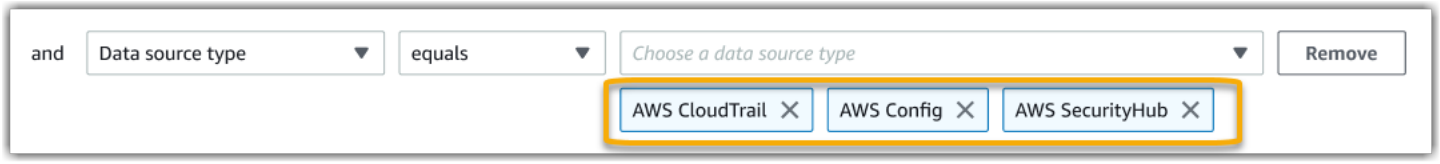


Kriteria nilai perilaku

Saat Anda menentukan lebih dari satu nilai kriteria, nilainya ditautkan dengan `OR` operator. Bukti finder mengembalikan hasil yang cocok dengan salah satu nilai kriteria ini.

Contoh

Dalam penyiapan filter berikut, pencari bukti mengembalikan hasil pencarian yang berasal dari salah satuAWS CloudTrail,AWS Config, atauAWS Security Hub.



Referensi pengelompokan

Anda dapat mengelompokkan hasil pencarian untuk navigasi yang lebih cepat. Pengelompokan menunjukkan luasnya hasil pencarian Anda, dan bagaimana mereka didistribusikan ke seluruh dimensi tertentu.

Anda dapat menggunakan salah satu dari kelompok berikut dengan nilai.

Kelompok oleh	Deskripsi
ID Akun	Hasil kelompok olehAkun AWS.
Kontrol	Hasil kelompok dengan nama kontrol.
Kontrol domain	Kelompokkan hasil berdasarkan domain kontrol.
Jenis sumber data	Kelompokkan hasil berdasarkan jenis sumber data tempat bukti berasal.
Nama acara	Kelompokkan hasil berdasarkan nama acara.
Sumber Daya ARN	Hasil grup berdasarkan Amazon Resource Name (ARN).
Jenis sumber daya	Kelompokkan hasil berdasarkan jenis sumber daya.
Layanan	Hasil grup berdasarkan Layanan AWS nama.
Kategori layanan	Hasil kelompok berdasarkan Layanan AWS kategori.

Contoh kasus penggunaan

Pencari bukti dapat membantu Anda dengan beberapa kasus penggunaan. Halaman ini memberikan beberapa contoh dan menyarankan filter pencarian yang dapat Anda gunakan dalam setiap skenario.

Topik

- Kasus penggunaan 1: Temukan bukti yang tidak patuh dan atur delegasi
- Kasus penggunaan 2: Identifikasi bukti yang sesuai
- Kasus penggunaan 3: Lakukan pratinjau cepat sumber daya bukti

Kasus penggunaan 1: Temukan bukti yang tidak patuh dan atur delegasi

Kasus penggunaan ini sangat ideal jika Anda adalah petugas kepatuhan, petugas perlindungan data, atau profesional GRC yang mengawasi persiapan audit.

Saat memantau postur kepatuhan organisasi, Anda dapat mengandalkan tim mitra untuk membantu mengatasi masalah. Anda dapat menggunakan pencari bukti untuk membantu Anda mengatur pekerjaan Anda untuk tim mitra Anda.

Dengan menerapkan filter, Anda dapat fokus pada bukti untuk satu area pada satu waktu. Selain itu, Anda juga dapat tetap selaras dengan tanggung jawab dan ruang lingkup masing-masing tim mitra yang bekerja dengan Anda. Dengan melakukan pencarian yang ditargetkan dengan cara ini, Anda dapat menggunakan hasil pencarian untuk mengidentifikasi apa yang sebenarnya perlu diperbaiki di setiap area subjek. Anda kemudian dapat mendelegasikan bukti yang tidak patuh itu kepada tim mitra terkait untuk perbaikan.

Untuk alur kerja ini, ikuti langkah-langkah untuk mencari bukti. Gunakan filter berikut untuk menemukan bukti yang tidak sesuai.

```
Assessment | <assessment name>
Date range | <date range>
Resource compliance | Non-compliant
```

Selanjutnya, terapkan filter tambahan untuk area yang Anda fokuskan. Misalnya, gunakan filter kategori Layanan untuk menemukan sumber daya yang tidak sesuai yang terkait dengan IAM. Kemudian, bagikan hasil tersebut dengan tim yang memiliki sumber daya IAM untuk organisasi Anda. Atau, jika Anda melakukan kueri penilaian yang dibuat dari kerangka kerja standar, Anda dapat menggunakan filter domain Kontrol untuk menemukan bukti yang tidak sesuai yang terkait dengan identitas dan domain manajemen akses.

```
Control domain | <domain that you're focusing on>
or
Service category | <Layanan AWS category that you're focusing on>
```

Setelah menemukan bukti yang Anda butuhkan, ikuti langkah-langkah untuk membuat laporan penilaian dari hasil pencarian. Anda dapat membagikan laporan ini dengan tim mitra Anda, yang dapat menggunakannya sebagai daftar periksa remediasi.

Kasus penggunaan 2: Identifikasi bukti yang sesuai

Kasus penggunaan ini sangat ideal jika Anda bekerja diSecOps, IT/DevOps, atau peran lain yang memiliki dan memulihkan aset cloud.

Sebagai bagian dari audit, Anda mungkin diminta untuk memperbaiki masalah dengan sumber daya yang Anda miliki. Setelah Anda melakukan pekerjaan ini, Anda dapat menggunakan pencari bukti untuk memvalidasi bahwa sumber daya Anda sesuai.

Untuk alur kerja ini, ikuti langkah-langkah untuk mencari bukti. Gunakan filter berikut untuk menemukan bukti yang sesuai.

```
Assessment | <assessment name>
Date range | <date range>
Resource compliance | Compliant
```

Selanjutnya, terapkan filter tambahan untuk hanya menunjukkan bukti yang Anda tanggung jawab. Bergantung pada cakupan kepemilikan Anda, buat pencarian sesuai target sesuai kebutuhan. Contoh filter berikut diurutkan dari yang paling luas hingga yang paling tepat. Pilih opsi yang sesuai untuk Anda, dan ganti <placeholder text>dengan nilai Anda sendiri.

```
Control domain | <a subject area that you're responsible for>
Service category | <a category of Layanan AWS that you own>
Service | <a specific Layanan AWS that you own>
Resource type | <a collection of resources that you own>
Resource ARN | <a specific resource that you own>
```

Jika Anda bertanggung jawab atas beberapa instance dengan kriteria yang sama (misalnya, Anda memiliki beberapaLayanan AWS), Anda dapat mengelompokkan hasil berdasarkan nilai tersebut. Ini memberi Anda total bukti yang cocok untuk masing-masingLayanan AWS. Anda kemudian bisa mendapatkan hasil untuk layanan yang Anda miliki.

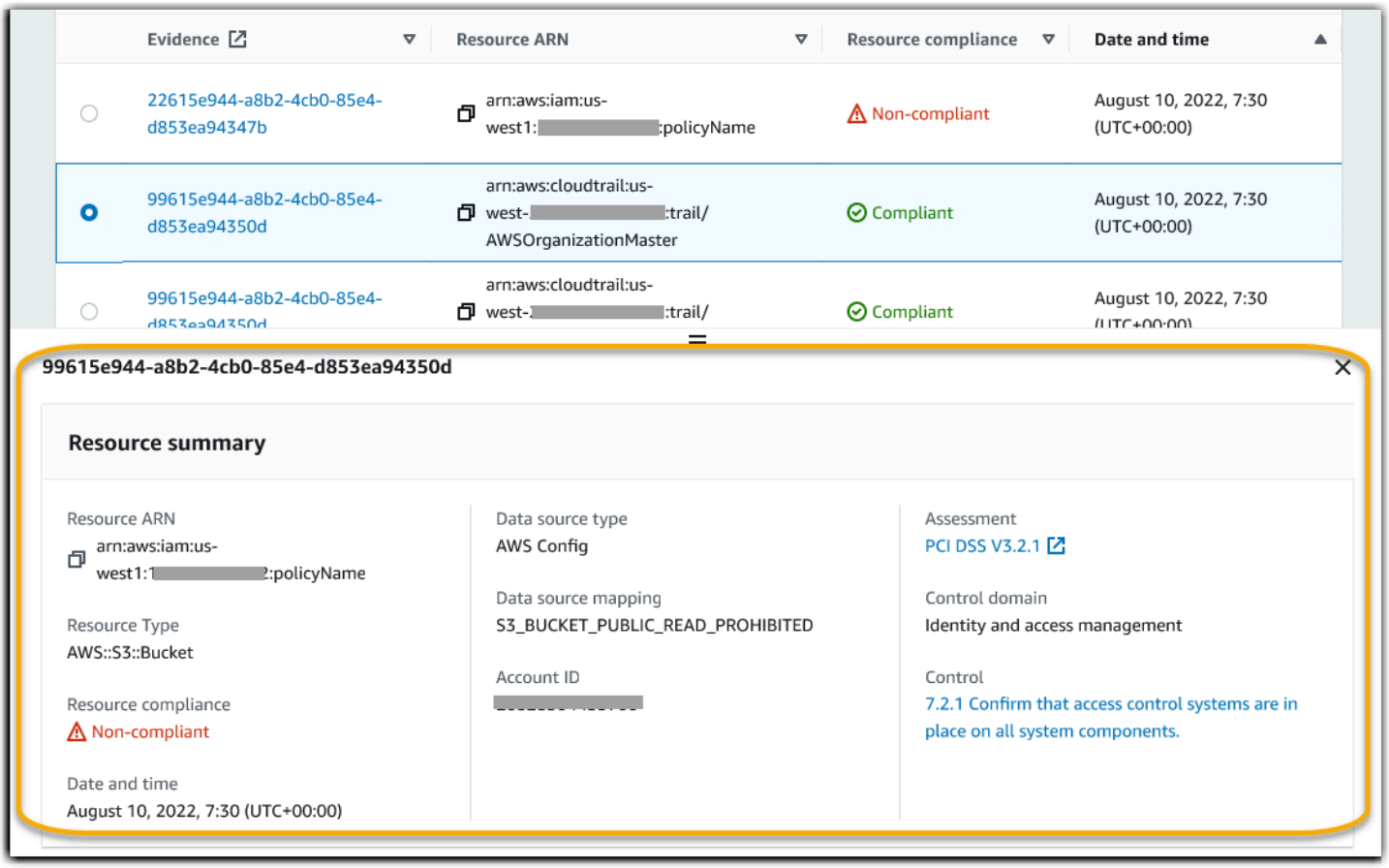
Kasus penggunaan 3: Lakukan pratinjau cepat sumber daya bukti

Kasus penggunaan ini sangat ideal untuk semua pelanggan Manajer Audit.

Sebelumnya, itu memakan waktu untuk meninjau rincian bukti individu. Jika Anda ingin melihat pratinjau bukti, Anda harus pergi langsung ke penilaian itu, lalu menavigasi melalui folder bukti yang sangat bersarang. Sekarang, pencari bukti menyediakan cara mudah untuk melihat informasi ini. Untuk setiap item bukti yang cocok dengan kueri penelusuran, Anda dapat melihat pratinjau sumber daya individual untuk bukti tersebut.

Untuk memulai, ikuti langkah-langkah untuk mencari bukti. Kemudian, pilih tombol radio di sebelah hasil untuk melihat ringkasan sumber daya di halaman saat ini. Anda dapat melihat pratinjau setiap

sumber daya individu yang berkaitan dengan item bukti. Untuk melihat rincian bukti lengkap untuk sumber daya apa pun, pilih nama bukti. Untuk informasi selengkapnya, lihat Pratinjau ringkasan sumber daya.



Pusat unduhan Manajer Audit

Pusat unduhan adalah tempat Anda dapat menemukan dan mengelola semua file Audit Manager yang dapat diunduh. Saat Anda membuat laporan penilaian atau mengekspor hasil pencarian dari pencari bukti, file akan muncul di pusat unduhan.

Topik

Menjelajahi pusat unduhan

Untuk mengunjungi pusat unduhan, buka konsol Audit Manager di https://console.aws.amazon.com/auditmanager/home, lalu pilih Pusat unduhan di panel navigasi kiri.

Anda dapat beralih di antara tab berikut untuk menelusuri file Anda berdasarkan kategori.

Tab laporan penilaian

Tab ini menampilkan semua laporan penilaian yang telah Anda buat. Laporan penilaian tetap tersedia di pusat unduhan hingga Anda menghapusnya.

Untuk melihat status terbaru laporan penilaian Anda, pilih ikon refresh (s) untuk memuat ulang tabel. Setiap baris dalam tabel laporan penilaian menunjukkan nama laporan, tanggal pembuatannya, dan salah satu status berikut:

- Dalam proses — Manajer Audit membuat laporan penilaian.
- Siap - Laporan penilaian tersedia untuk Anda unduh.
- Error — Laporan penilaian gagal dibuat. Dalam kasus ini, Manajer Audit menampilkan pesan yang menjelaskan kesalahan. Untuk informasi tentang cara mengatasi kesalahan ini, lihat Laporan penilaian pemecahan masalah.

Tab Ekspor

Tab ini menampilkan semua hasil pencarian pencari bukti yang Anda ekspor dalam tujuh hari terakhir. File CSV dihapus dari pusat unduhan setelah tujuh hari, tetapi file tersebut tetap tersedia di bucket S3 tujuan ekspor Anda. Untuk petunjuk tentang cara menemukan ekspor CSV pencari bukti di bucket tujuan S3 Anda, lihat. Melihat hasil Anda setelah Anda mengekspornya

Untuk melihat status terbaru ekspor CSV Anda, pilih ikon refresh (s) untuk memuat ulang tabel. Setiap baris dalam tabel ekspor menunjukkan nama file, tanggal ekspornya, dan salah satu status berikut:

- Dalam proses - Manajer Audit sedang mempersiapkan file CSV.
- Siap - Ekspor berhasil dan file tersedia untuk Anda unduh.
- Kesalahan - Ekspor gagal. Dalam kasus ini, Manajer Audit menampilkan pesan yang menjelaskan kesalahan. Untuk informasi tentang cara mengatasi kesalahan ini, lihat Pemecahan masalah ekspor CSV pencari bukti.

> **Note**
>
> Perlu diingat bahwa tab ekspor mungkin juga menampilkan file CSV untuk kueri yang Anda jalankan langsung di Lake. AWS CloudTrail Ini termasuk kueri yang dibuat di CloudTrail konsol atau menggunakan CloudTrail API. CloudTrailekspor muncul di tab ini jika Anda menanyakan penyimpanan data peristiwa Manajer Audit, dan Anda memilih untuk menyimpan hasilnya ke Amazon S3.

Mengunduh file

Ikuti langkah-langkah ini untuk mengunduh file dari pusat unduhan.

Untuk mengunduh file

1. Buka konsol AWS Audit Manager di https://console.aws.amazon.com/auditmanager/home.
2. Di panel navigasi kiri, pilih Pusat unduhan.
3. Pilih tab Laporan penilaian atau tab Ekspor.
4. Pilih file yang ingin Anda unduh, lalu pilih Unduh.

Untuk petunjuk tentang cara mengunduh file dari bucket tujuan S3 Anda, lihat Mengunduh objek di Panduan Pengguna Amazon Simple Storage Service (Amazon S3).

Menghapus file

Ikuti langkah-langkah ini untuk menghapus laporan penilaian yang tidak lagi Anda butuhkan di pusat unduhan.

> **Note**
>
> Menghapus ekspor CSV dari pusat unduhan saat ini tidak didukung. Ekspor CSV secara otomatis dihapus dari pusat unduhan setelah tujuh hari.

Menghapus laporan penilaian

1. Buka konsol AWS Audit Manager di https://console.aws.amazon.com/auditmanager/home.
2. Di panel navigasi kiri, pilih Pusat unduhan.
3. Pilih tab Laporan penilaian.
4. Pilih laporan penilaian yang ingin Anda hapus, lalu pilih Hapus.

Jika Anda ingin menghapus laporan penilaian atau ekspor CSV dari bucket tujuan S3 Anda, kami sarankan Anda menyelesaikan tugas ini secara langsung di Amazon S3. Untuk petunjuk, lihat Menghapus objek Amazon S3 di Panduan Pengguna Amazon Simple Storage Service (Amazon S3).

Pustaka kerangka kerja

Anda dapat mengakses dan mengelola kerangka kerja dari pustaka kerangka kerja diAWS Audit Manager.

Kerangka kerja menentukan kontrol mana yang diuji di lingkungan selama periode waktu tertentu. Ini mendefinisikan kontrol dan pemetaan sumber data mereka untuk standar kepatuhan atau peraturan tertentu. Ini juga digunakan untuk menyusun dan mengotomatiskan penilaian Audit Manager. Anda dapat menggunakan kerangka kerja sebagai titik awal untuk mengaudit Layanan AWS penggunaan Anda dan mulai mengotomatiskan pengumpulan bukti.

Pustaka kerangka berisi katalog kerangka kerja standar dan kustom.

- Kerangka kerja standar adalah kerangka kerja bawaan yang menyediakan. AWS Kerangka kerja ini didasarkan pada praktik AWS terbaik untuk standar dan peraturan kepatuhan yang berbeda. Ini termasuk GDPR dan HIPAA. Kerangka kerja standar mencakup kontrol yang diatur ke dalam set kontrol yang didasarkan pada standar kepatuhan atau peraturan yang didukung kerangka kerja.

  Anda dapat melihat konten kerangka kerja standar, tetapi Anda tidak dapat mengedit atau menghapusnya. Namun, Anda dapat menyesuaikan kerangka kerja standar apa pun untuk membuat yang baru untuk memenuhi persyaratan spesifik Anda.
- Kerangka kerja khusus adalah kerangka kerja khusus yang Anda miliki. Anda dapat membuat kerangka kerja khusus dari awal, atau dengan menyesuaikan kerangka kerja yang ada. Anda dapat menggunakan kerangka kerja khusus untuk mengatur kontrol ke dalam set kontrol dengan cara yang memenuhi persyaratan spesifik Anda. Untuk mempelajari lebih lanjut tentang cara mengelola kontrol, lihatPustaka kontrol.

Anda dapat membuat penilaian dari kerangka kerja standar atau kerangka kerja khusus. Untuk mempelajari cara membuat dan mengelola penilaian, lihatPenilaian di AWS Audit Manager.

> **Note**
>
> AWS Audit Managermembantu mengumpulkan bukti yang relevan untuk memverifikasi kepatuhan terhadap standar dan peraturan kepatuhan tertentu. Namun, itu tidak menilai kepatuhan Anda sendiri. AWS Audit ManagerOleh karena itu, bukti yang dikumpulkan mungkin tidak mencakup semua informasi tentang AWS penggunaan Anda yang diperlukan untuk audit. AWS Audit Managerbukan pengganti penasihat hukum atau pakar kepatuhan.

Bagian ini menjelaskan bagaimana Anda dapat membuat dan mengelola kerangka kerja kustom di Audit Manager.

Topik

Mengakses kerangka kerja yang tersedia di AWS Audit Manager

Anda dapat melihat semua kerangka kerja yang tersedia di halaman library Framework di konsol Audit Manager. Dari sini, Anda juga dapat membuat penilaian dari kerangka kerja, membuat kerangka kerja khusus, atau menyesuaikan kerangka kerja yang ada.

Anda juga dapat melihat semua framework yang tersedia menggunakan Audit Manager API atau AWS Command Line Interface (AWS CLI).

Audit Manager console

Untuk melihat kerangka kerja yang tersedia (konsol)

1. Buka konsol AWS Audit Manager di https://console.aws.amazon.com/auditmanager/home.
2. Di panel navigasi kiri, pilih Framework library.
3. Pilih tab Kerangka standar atau tab Kerangka kustom untuk menelusuri kerangka kerja standar dan kustom yang tersedia.
4. Pilih nama kerangka kerja apa pun untuk melihat detail kerangka kerja itu.

AWS CLI

Untuk melihat kerangka kerja yang tersedia () AWS CLI

Untuk melihat kerangka kerja di Audit Manager, gunakan list-assessment-frameworksperintah dan tentukan file. `--framework-type` Baik, Anda dapat mengambil daftar kerangka kerja standar. Atau, Anda dapat mengambil daftar kerangka kerja khusus.

```
aws auditmanager list-assessment-frameworks --framework-type Standard
```

```
aws auditmanager list-assessment-frameworks --framework-type Custom
```

Audit Manager API

Untuk melihat kerangka kerja yang tersedia (API)

Gunakan ListAssessmentFrameworksoperasi dan tentukan FrameworkType. Entah, Anda dapat mengembalikan daftar kerangka kerja standar. Atau, Anda dapat mengembalikan daftar kerangka kerja khusus.

Untuk informasi selengkapnya, pilih salah satu tautan sebelumnya untuk membaca lebih lanjut di Referensi AWS Audit Manager API. Ini termasuk informasi tentang cara menggunakan `ListAssessmentFrameworks` operasi dan parameter di salah satu SDK khusus bahasaAWS.

Melihat detail kerangka kerja

Anda dapat meninjau detail framework menggunakan konsol Audit Manager, Audit Manager API, atau AWS Command Line Interface (AWS CLI).

Audit Manager console

Untuk melihat detail kerangka kerja (konsol)

1. Buka konsol AWS Audit Manager di https://console.aws.amazon.com/auditmanager/home.
2. Di panel navigasi kiri, pilih pustaka Framework untuk melihat daftar kerangka kerja yang tersedia.
3. Pilih tab Kerangka standar atau tab Kerangka kustom untuk menelusuri kerangka kerja yang tersedia.
4. Pilih nama kerangka kerja untuk membukanya.

Saat Anda membuka kerangka kerja, halaman detail Framework ditampilkan. Bagian halaman ini dan isinya dijelaskan sebagai berikut.

Bagian detail kerangka kerja

Bagian ini memberikan ikhtisar kerangka kerja. Ini termasuk informasi berikut:

- Nama kerangka kerja — Nama kerangka kerja.
- Jenis kepatuhan — Standar kepatuhan atau peraturan yang didukung kerangka kerja.
- Deskripsi — Deskripsi kerangka kerja, jika ada yang disediakan.
- Jenis Framework - Menentukan apakah kerangka kerja adalah kerangka kerja standar atau kerangka kustom.
- Set kontrol — Jumlah set kontrol yang terkait dengan kerangka kerja.
- Kontrol — Jumlah total kontrol dalam kerangka kerja.
- Sumber kontrol — Jumlah sumber data kontrol tempat Audit Manager mengumpulkan bukti.
- Tag — Tag yang terkait dengan kerangka kerja.

Jika Anda melihat kerangka kerja khusus, detail berikut juga ditampilkan:

- Dibuat oleh - Akun yang menciptakan kerangka kustom.
- Tanggal dibuat - Tanggal kerangka kustom dibuat.
- Terakhir diperbarui - Tanggal ketika kerangka kerja ini terakhir diedit.

Tab kontrol

Tab ini mencantumkan kontrol dalam kerangka kerja, dikelompokkan berdasarkan set kontrol. Ini termasuk informasi berikut:

- Kontrol dikelompokkan berdasarkan set kontrol - Pilih ikon tampilan pohon untuk melihat kontrol yang dimiliki oleh setiap set kontrol.
- Jenis - Menentukan apakah kontrol adalah kontrol standar atau kontrol kustom.
- Sumber data - Menentukan sumber data tempat Audit Manager mengumpulkan bukti untuk kontrol tersebut.

Tab tag

Tab ini mencantumkan tag yang terkait dengan kerangka kerja. Ini termasuk informasi berikut:

- Kunci — Kunci tag (misalnya, standar kepatuhan, peraturan, atau kategori).
- Nilai — Nilai tag.

AWS CLI

Untuk melihat rincian kerangka kerja (AWS CLI)

1. Untuk mengidentifikasi kerangka kerja yang ingin Anda tinjau, jalankan list-assessment-frameworksperintah dan tentukan `a--framework-type`. Baik, Anda dapat mengambil daftar kerangka kerja standar. Atau, Anda dapat mengambil daftar kerangka kerja khusus.

   Dalam contoh berikut, ganti *`teks placeholder`* dengan salah satu atau`Custom`. `Standard`

   ```
   aws auditmanager list-assessment-frameworks --framework-type Custom/Standard
   ```

   Respons mengembalikan daftar kerangka kerja. Temukan kerangka kerja yang ingin Anda tinjau, dan perhatikan ID kerangka kerja dan Nama Sumber Daya Amazon (ARN).

2. Untuk mendapatkan detail kerangka kerja, jalankan get-assessment-frameworkperintah dan tentukan`--framework-id`.

   Dalam contoh berikut, ganti *`teks placeholder dengan informasi`* Anda sendiri.

   ```
   aws auditmanager get-assessment-framework --framework-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
   ```

   Rincian kerangka kerja dikembalikan dalam format JSON. Untuk memahami data ini, lihat get-assessment-framework Output dalam Referensi AWS CLI Perintah.

3. Untuk melihat tag untuk kerangka kerja, gunakan list-tags-for-resourceperintah dan tentukan `--resource-arn` untuk kerangka kerja.

   Dalam contoh berikut, ganti *`teks placeholder dengan informasi`* Anda sendiri:

   ```
   aws auditmanager list-tags-for-resource --resource-arn arn:aws:auditmanager:us-east-1:111122223333:assessmentFramework/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
   ```

   Untuk informasi selengkapnya tentang tag di Audit Manager, lihat Menandai AWS Audit Manager sumber daya.

Audit Manager API

Untuk melihat detail kerangka kerja (API)

1. Untuk mengidentifikasi kerangka kerja yang ingin Anda tinjau, gunakan ListAssessmentFrameworksoperasi dan tentukan FrameworkType. Entah, Anda dapat mengembalikan daftar kerangka kerja standar. Atau, Anda dapat mengembalikan daftar kerangka kerja khusus.

   Dari respons, temukan kerangka kerja yang ingin Anda tinjau dan catat ID kerangka kerja dan Nama Sumber Daya Amazon (ARN).
2. Untuk mendapatkan detail kerangka kerja, gunakan GetAssessmentFrameworkoperasi. Dalam permintaan, tentukan FrameworkId yang Anda dapatkan dari langkah 1.

   Rincian kerangka kerja dikembalikan dalam format JSON. Untuk memahami data ini, lihat Elemen GetAssessmentFramework Respons di Referensi AWS Audit Manager API.
3. Untuk melihat tag untuk kerangka kerja, gunakan ListTagsForResourceoperasi. Dalam permintaan, tentukan kerangka kerja ResourcEarn yang Anda dapatkan dari langkah 1.

Untuk informasi selengkapnya tentang tag di Audit Manager, lihat Menandai AWS Audit Manager sumber daya.

Untuk informasi selengkapnya tentang operasi API ini, pilih salah satu tautan sebelumnya untuk membaca selengkapnya di Referensi AWS Audit Manager API. Ini termasuk informasi tentang cara menggunakan operasi dan parameter ini di salah satu SDK khusus bahasaAWS.

Membuat kerangka kerja khusus

Anda dapat mengakses dan mengelola kerangka kerja dari pustaka kerangka kerja diAWS Audit Manager. Anda dapat membuat kerangka kerja khusus untuk mengatur kontrol ke dalam set kontrol dengan cara yang memenuhi persyaratan spesifik Anda.

Ada dua cara untuk membuat kerangka kerja khusus. Entah Anda dapat menyesuaikan kerangka kerja yang ada, atau Anda dapat membuat kerangka kerja baru dari awal.

Topik

- Membuat kerangka kerja kustom baru dari awal
- Menyesuaikan kerangka kerja yang ada

Membuat kerangka kerja kustom baru dari awal

Anda dapat menggunakan kerangka kerja khusus AWS Audit Manager untuk mengatur kontrol ke dalam set kontrol dengan cara yang memenuhi persyaratan spesifik Anda. Anda dapat membuat kerangka kerja kustom baru dari awal di pustaka kerangka kerja dengan mengikuti langkah-langkah ini.

Topik

Langkah 1: Tentukan detail kerangka kerja

Mulailah dengan menentukan kontrol yang ingin Anda sertakan dalam kerangka kustom Anda.

Untuk menentukan rincian kerangka kerja

1. Buka konsol AWS Audit Manager di https://console.aws.amazon.com/auditmanager/home.
2. Di panel navigasi kiri, pilih Framework library, dan pilih Create custom framework.
3. Di bawah detail Framework, masukkan nama, standar kepatuhan atau peraturan (opsional), dan deskripsi untuk kerangka kerja Anda (juga opsional). Masukkan kata kunci standar atau peraturan kepatuhan seperti PCI_DSS atau GDPR sehingga Anda dapat menggunakan kata kunci ini untuk mencari kerangka kerja Anda.
4. Di bawah Tag, pilih Tambahkan tag baru untuk mengaitkan tag dengan kerangka kerja Anda. Anda dapat menentukan kunci dan nilai untuk setiap tag. Kunci tag adalah wajib. Anda dapat menggunakannya sebagai kriteria pencarian saat mencari kerangka kerja ini di pustaka Framework. Untuk informasi selengkapnya tentang tag diAWS Audit Manager, lihatPenandaan pada sumber daya AWS Audit Manager.
5. Pilih Berikutnya.

Langkah 2: Tentukan kontrol dalam set kontrol

Selanjutnya, Anda menentukan kontrol mana yang ingin Anda tambahkan ke kerangka kerja Anda dan bagaimana Anda ingin mengaturnya. Mulailah dengan menambahkan set kontrol ke kerangka kerja, dan kemudian tambahkan kontrol ke set kontrol.

> **Note**
>
> Saat Anda menggunakan AWS Audit Manager konsol untuk membuat kerangka kerja khusus, Anda dapat menambahkan hingga 10 set kontrol untuk setiap kerangka kerja.
> Bila Anda menggunakan Audit Manager API untuk membuat kerangka kerja kustom, Anda dapat membuat lebih dari 10 set kontrol. Untuk menambahkan lebih banyak set kontrol daripada yang diizinkan konsol saat ini, gunakan CreateAssessmentFrameworkAPI yang disediakan Audit Manager.

Untuk menentukan kontrol dalam set kontrol

1. Di bawah Control set name, masukkan nama untuk set kontrol Anda.
2. Di bawah Tambahkan kontrol baru ke set kontrol, Pilih jenis kontrol, gunakan daftar tarik-turun untuk memilih salah satu dari dua jenis kontrol: Kontrol standar atau Kontrol khusus. Kontrol standar disediakan oleh Audit Manager, dan kontrol kustom adalah yang Anda buat.
3. Berdasarkan opsi yang Anda pilih pada langkah sebelumnya, daftar kontrol standar atau kontrol khusus ditampilkan. Anda dapat menelusuri daftar, atau mencari dengan memasukkan nama kontrol, kepatuhan, atau tag. Pilih satu atau beberapa kontrol dan pilih Tambahkan ke kontrol set untuk menambahkannya ke set kontrol.
4. Di jendela pop-up yang muncul, pilih Tambahkan ke kontrol diatur untuk mengonfirmasi penambahan Anda.
5. Di bawah Tinjau kontrol yang dipilih dalam set kontrol, tinjau kontrol yang muncul di daftar Kontrol yang dipilih. Untuk menambahkan lebih banyak kontrol ke set kontrol, ulangi langkah 2-4. Anda dapat menghapus kontrol yang tidak diinginkan dari set kontrol dengan memilih satu atau beberapa kontrol dan memilih Hapus kontrol.
6. Untuk menambahkan set kontrol baru ke kerangka kerja, pilih Tambahkan set kontrol di bagian bawah halaman. Anda dapat menghapus set kontrol yang tidak diinginkan dengan memilih Hapus set kontrol.
7. Setelah Anda selesai menambahkan set kontrol dan kontrol, pilih Berikutnya.

Langkah 3: Tinjau dan buat kerangka kerja

Tinjau informasi untuk kerangka kerja Anda. Untuk mengubah informasi untuk satu langkah, pilih Edit.

Setelah selesai, pilih Buat kerangka kerja khusus.

Apa yang bisa saya lakukan selanjutnya?

Setelah Anda membuat kerangka kustom baru Anda, Anda dapat membuat penilaian dari kerangka kerja Anda. Untuk informasi selengkapnya, lihat Membuat penilaian.

Anda juga dapat membuat kerangka kerja khusus menggunakan kerangka kerja yang ada. Untuk informasi selengkapnya, lihat Menyesuaikan kerangka kerja yang ada.

Untuk petunjuk tentang cara mengedit kerangka kustom Anda, lihatMengedit kerangka kerja khusus.

Menyesuaikan kerangka kerja yang ada

Dengan kerangka kerja khususAWS Audit Manager, Anda dapat mengatur kontrol ke dalam set kontrol dengan cara yang memenuhi persyaratan spesifik Anda. Alih-alih membuat kerangka kerja khusus dari awal, Anda dapat menggunakan kerangka kerja yang ada sebagai titik awal dan menyesuaikannya. Saat Anda melakukan ini, kerangka kerja yang ada tetap berada di pustaka kerangka kerja, dan kerangka kerja khusus baru dibuat dengan pengaturan khusus Anda.

Anda dapat memilih kerangka kerja yang ada untuk disesuaikan. Ini bisa berupa kerangka kerja standar atau kerangka kerja khusus.

Di pustaka kerangka kerja, dari daftar dropdown Buat kerangka kerja kustom, pilih Sesuaikan kerangka kerja yang ada. Gunakan langkah-langkah berikut untuk menyesuaikan kerangka kerja.

Topik

Langkah 1: Tentukan detail kerangka kerja

Semua detail kerangka kerja, kecuali tag, dibawa dari kerangka asli. Tinjau dan modifikasi detail ini sesuai kebutuhan.

Untuk menentukan rincian kerangka kerja

1. Buka konsol AWS Audit Manager di https://console.aws.amazon.com/auditmanager/home.
2. Di panel navigasi kiri, pilih Framework library.
3. Pilih kerangka kerja yang ingin Anda sesuaikan, dan dari daftar dropdown Buat kerangka kustom, pilih Sesuaikan kerangka kerja yang ada.
4. Di jendela pop-up yang muncul, masukkan nama untuk kerangka kustom baru dan pilih Sesuaikan.
5. Di bawah detail Framework, tinjau nama, jenis kepatuhan, dan deskripsi untuk kerangka kerja Anda, dan modifikasi sesuai kebutuhan. Jenis kepatuhan harus menunjukkan standar kepatuhan atau peraturan yang terkait dengan kerangka kerja Anda. Anda dapat menggunakan kata kunci ini untuk mencari kerangka kerja Anda.
6. Di bawah Tag, pilih Tambahkan tag baru untuk mengaitkan tag dengan kerangka kerja Anda. Anda dapat menentukan kunci dan nilai untuk setiap tag. Kunci tag adalah wajib dan dapat digunakan sebagai kriteria pencarian saat Anda mencari kerangka kerja ini di pustaka Framework. Untuk informasi selengkapnya tentang tag diAWS Audit Manager, lihatPenandaan pada sumber daya AWS Audit Manager.
7. Pilih Berikutnya.

Langkah 2: Tentukan kontrol untuk ditambahkan ke set kontrol

Set kontrol dibawa dari kerangka asli. Sesuaikan konfigurasi saat ini dengan menambahkan lebih banyak kontrol atau menghapus kontrol yang ada sesuai kebutuhan.

> **Note**
>
> Saat Anda menggunakan AWS Audit Manager konsol untuk menyesuaikan kerangka kerja, Anda dapat menambahkan hingga 10 set kontrol untuk setiap kerangka kerja.
> Bila Anda menggunakan Audit Manager API untuk membuat framework kustom, Anda dapat menambahkan lebih dari 10 set kontrol. Untuk menambahkan lebih banyak set kontrol daripada yang diizinkan konsol saat ini, gunakan CreateAssessmentFrameworkAPI yang disediakan Audit Manager.

Untuk menentukan kontrol dalam set kontrol

1. Di bawah nama set Kontrol, sesuaikan nama set kontrol sesuai kebutuhan.

2. Di bawah Tambahkan kontrol baru ke set kontrol, tambahkan kontrol baru dengan menggunakan daftar tarik-turun untuk memilih salah satu dari dua jenis kontrol: Kontrol standar atau Kontrol khusus.
3. Berdasarkan opsi yang Anda pilih pada langkah sebelumnya, daftar kontrol standar atau kontrol khusus ditampilkan. Anda dapat menelusuri daftar ini, atau mencari dengan memasukkan nama kontrol, kepatuhan, atau tag untuk menemukan kontrol yang ingin Anda tambahkan. Pilih satu atau beberapa kontrol dan pilih Tambahkan ke kontrol set untuk ditambahkan ke set kontrol ini.
4. Di jendela pop-up yang muncul, pilih Tambahkan ke kontrol diatur untuk mengonfirmasi penambahan Anda.
5. Di bawah Tinjau kontrol yang dipilih dalam set kontrol, tinjau kontrol yang muncul di daftar Kontrol yang dipilih. Untuk menambahkan lebih banyak kontrol ke set kontrol, ulangi langkah 2-4. Anda dapat menghapus kontrol yang tidak diinginkan dari set kontrol dengan memilih satu atau beberapa kontrol dan memilih Hapus kontrol.
6. Untuk menambahkan set kontrol baru ke kerangka kerja, pilih Tambahkan set kontrol di bagian bawah halaman. Anda dapat menghapus set kontrol yang tidak diinginkan dengan memilih Hapus set kontrol.
7. Setelah Anda selesai menambahkan set kontrol dan kontrol, pilih Berikutnya.

Langkah 3: Tinjau dan buat kerangka kerja

Tinjau informasi untuk kerangka kerja Anda. Untuk mengubah informasi untuk satu langkah, pilih Edit.

Setelah selesai, pilih Buat kerangka kerja khusus.

Apa yang bisa saya lakukan selanjutnya?

Setelah Anda membuat kerangka kustom baru Anda, Anda dapat membuat penilaian dari kerangka kerja Anda. Untuk informasi selengkapnya, lihat Membuat penilaian.

Untuk petunjuk tentang cara mengedit kerangka kustom Anda, lihatMengedit kerangka kerja khusus.

Mengedit kerangka kerja khusus

Anda dapat menggunakan kerangka kerja khusus AWS Audit Manager untuk mengatur kontrol ke dalam set kontrol untuk memenuhi kebutuhan spesifik Anda. Anda dapat menggunakan pustaka kerangka kerja untuk menemukan dan mengedit kerangka kerja khusus dengan mengikuti langkah-langkah ini.

Topik

Langkah 1: Edit detail kerangka kerja

Mulailah dengan meninjau dan mengedit detail kerangka kerja yang ada.

Untuk mengedit detail kerangka kerja

1. Buka konsol AWS Audit Manager di https://console.aws.amazon.com/auditmanager/home.
2. Di panel navigasi kiri, pilih Framework library dan kemudian pilih tab Custom frameworks.
3. Pilih kerangka kerja yang ingin Anda edit, pilih Tindakan, lalu pilih Edit.
   - Atau, Anda dapat membuka kerangka kerja khusus dan memilih Tindakan, Edit di kanan atas halaman ringkasan penilaian.
4. Di bawah detail Framework, tinjau nama, jenis kepatuhan, dan deskripsi untuk kerangka kerja Anda, dan buat perubahan yang diperlukan.
5. Pilih Berikutnya.

> **Tip**
>
> Untuk mengedit tag untuk kerangka kerja, buka kerangka kerja dan pilih tab tag kerangka kerja. Di sana Anda dapat melihat dan mengedit tag yang terkait dengan kerangka kerja.

Langkah 2: Edit kontrol di set kontrol

Selanjutnya, tinjau dan edit kontrol dan set kontrol dalam kerangka kerja.

> **Note**
>
> Saat Anda menggunakan AWS Audit Manager konsol untuk mengedit kerangka kerja khusus, Anda dapat menambahkan hingga 10 set kontrol untuk setiap kerangka kerja.
> Bila Anda menggunakan Audit Manager API untuk mengedit framework kustom, Anda dapat menambahkan lebih dari 10 set kontrol. Untuk menambahkan lebih banyak set kontrol

daripada yang diizinkan konsol saat ini, gunakan UpdateAssessmentFrameworkAPI yang disediakan Audit Manager.

Untuk mengedit kontrol

1. Di bawah Control set name, tinjau dan edit nama untuk set kontrol Anda sesuai kebutuhan.
2. Di bawah Tambahkan kontrol baru ke set kontrol, Anda dapat menambahkan kontrol. Gunakan daftar tarik-turun untuk memilih salah satu dari dua jenis kontrol: Kontrol standar atau Kontrol khusus.
3. Berdasarkan opsi yang Anda pilih pada langkah sebelumnya, daftar tabel kontrol standar atau kontrol khusus ditampilkan. Anda dapat menelusuri daftar untuk set kontrol. Atau, Anda dapat mencari dengan memasukkan nama kontrol, sumber data, atau tag untuk menemukan kontrol yang ingin Anda tambahkan. Pilih satu atau beberapa kontrol dan pilih Tambahkan ke kontrol set untuk ditambahkan ke set kontrol ini.
4. Di jendela pop-up yang muncul, pilih Tambahkan ke kontrol diatur untuk mengonfirmasi penambahan Anda.
5. Di bawah Tinjau kontrol yang dipilih dalam set kontrol, tinjau dan edit kontrol yang saat ini muncul di daftar Kontrol yang dipilih. Untuk menambahkan lebih banyak kontrol ke set kontrol, ulangi langkah 2-4. Hapus kontrol yang tidak diinginkan dari set kontrol dengan memilih satu atau beberapa kontrol dan memilih Hapus kontrol.
6. Untuk menambahkan set kontrol baru ke kerangka kerja, pilih Tambahkan set kontrol di bagian bawah halaman. Hapus set kontrol yang tidak diinginkan dengan memilih Hapus set kontrol.
7. Setelah Anda selesai menambahkan set kontrol dan kontrol, pilih Berikutnya.

Langkah 3. Tinjau dan perbarui kerangka kerja

Tinjau informasi untuk kerangka kerja Anda. Untuk mengubah informasi untuk satu langkah, pilih Edit.

Setelah Anda selesai, pilih Simpan perubahan.

Menghapus kerangka kerja khusus

Anda dapat menggunakan pustaka kerangka kerja untuk menemukan dan menghapus kerangka kustom yang tidak diinginkan. Anda juga dapat menghapus kerangka kerja kustom menggunakan Audit Manager API atau AWS Command Line Interface (AWS CLI).

> **Note**
>
> Menghapus kerangka kerja khusus tidak memengaruhi penilaian apa pun yang ada yang dibuat dari kerangka kerja sebelum dihapus.

Audit Manager console

Untuk menghapus kerangka kerja khusus (konsol)

1. Buka konsol AWS Audit Manager di https://console.aws.amazon.com/auditmanager/home.
2. Di panel navigasi kiri, pilih Framework library dan kemudian pilih tab Custom frameworks.
3. Pilih kerangka kerja yang ingin Anda hapus, pilih Tindakan, lalu pilih Hapus.
   - Atau, Anda dapat membuka kerangka kerja khusus dan memilih Tindakan, Hapus di kanan atas halaman ringkasan kerangka kerja.
4. Di jendela pop-up, pilih Hapus untuk mengonfirmasi penghapusan.

AWS CLI

Untuk menghapus kerangka kerja kustom (AWS CLI)

1. Pertama, identifikasi kerangka kustom yang ingin Anda hapus. Untuk melakukan ini, jalankan list-assessment-frameworksperintah dan tentukan `--framework-type` sebagai`Custom`.

   ```
   aws auditmanager list-assessment-frameworks --framework-type Custom
   ```

   Respons mengembalikan daftar kerangka kustom. Temukan kerangka kerja khusus yang ingin Anda hapus, dan perhatikan ID kerangka kerja.
2. Selanjutnya, jalankan delete-assessment-frameworkperintah dan tentukan `--framework-id` kerangka kerja yang ingin Anda hapus.

   Dalam contoh berikut, ganti *`teks placeholder dengan informasi`* Anda sendiri.

   ```
   aws auditmanager delete-assessment-framework --framework-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
   ```

Audit Manager API

Untuk menghapus kerangka kerja khusus (API)

1. Gunakan ListAssessmentFrameworksoperasi dan tentukan FrameworkType sebagai. `Custom` Dari respons, temukan kerangka kerja khusus yang ingin Anda hapus, dan catat ID kerangka kerja.
2. Gunakan DeleteAssessmentFrameworkoperasi untuk menghapus kerangka kerja. Dalam permintaan, gunakan parameter FrameworkId untuk menentukan kerangka kerja yang ingin Anda hapus.

Untuk informasi selengkapnya tentang operasi API ini, pilih salah satu tautan sebelumnya untuk membaca selengkapnya di Referensi AWS Audit Manager API. Ini termasuk informasi tentang cara menggunakan operasi dan parameter ini di salah satu SDK khusus bahasaAWS.

Berbagi kerangka kustom

Anda dapat menggunakan fitur berbagi kerangka kerja AWS Audit Manager untuk dengan cepat mereplikasi kerangka kerja kustom yang Anda buat. Anda dapat membagikan kerangka kerja kustom Anda dengan yang lainAkun AWS, atau mereplikasi kerangka kerja Anda ke kerangka kerja lain Wilayah AWS di bawah akun Anda sendiri. Penerima kemudian dapat mengakses kerangka kustom Anda dan menggunakannya untuk membuat penilaian. Mereka dapat melakukan ini tanpa harus mengulangi upaya konfigurasi Anda untuk kerangka kerja itu.

Untuk berbagi kerangka kustom, Anda membuat permintaan berbagi. Penerima permintaan saham kemudian memiliki waktu 120 hari untuk menerima atau menolak permintaan tersebut. Ketika mereka menerima permintaan berbagi, Audit Manager mereplikasi kerangka kustom bersama ke dalam pustaka kerangka kerja mereka. Selain mereplikasi kerangka kustom, Audit Manager juga mereplikasi setiap set kontrol kustom dan kontrol kustom yang merupakan bagian dari kerangka itu. Kontrol kustom ini kemudian ditambahkan ke pustaka kontrol penerima. Audit Manager tidak mereplikasi kerangka kerja atau kontrol standar. Secara default, ini tersedia di semua Akun AWS dan Wilayah di mana Audit Manager diaktifkan.

Fitur berbagi kerangka kerja hanya tersedia di tingkat berbayar. Namun, tidak ada biaya tambahan untuk berbagi kerangka kerja khusus atau menerima permintaan berbagi. Untuk mempelajari lebih lanjut tentang hargaAWS Audit Manager, lihat halaman AWS Audit Manager harga.

> **Important**
>
> Anda tidak boleh membagikan kerangka kerja khusus yang berasal dari kerangka kerja standar jika kerangka kerja standar ditetapkan sebagai tidak memenuhi syarat untuk dibagikan olehAWS, kecuali jika Anda telah memperoleh izin untuk melakukannya dari pemilik kerangka kerja standar. Untuk melihat kerangka kerja standar mana yang tidak memenuhi syarat untuk dibagikan dan mempelajari lebih lanjut, lihat Kelayakan berbagi kerangka kerja.

Bagian berikut dari panduan ini menjelaskan hal-hal penting yang harus Anda ketahui tentang berbagi kerangka kerja. Mereka juga memberikan instruksi tentang bagaimana Anda dapat membagikan kerangka kerja khusus Anda dan menanggapi permintaan berbagi.

Topik

- Konsep dan terminologi berbagi kerangka kerja
- Mengirim permintaan berbagi untuk kerangka kerja khusus
- Menanggapi permintaan berbagi
- Menghapus permintaan berbagi

> **Tip**
>
> Jika Anda tidak terbiasa dengan kerangka kerja kustom Audit Manager dan cara membuatnya, Anda dapat mempelajari lebih lanjut di halaman Membuat kerangka kerja kustom panduan ini.

Konsep dan terminologi berbagi kerangka kerja

Jika Anda mempelajari tentang konsep-konsep kunci berikut, Anda bisa mendapatkan lebih banyak dari fitur berbagi kerangka kerja AWS Audit Manager kustom.

Sender

Ini adalah pencipta permintaan berbagi dan di Akun AWS mana kerangka kustom ada. Pengirim dapat berbagi kerangka kerja khusus dengan apa pun. Akun AWS Atau, mereka mereplikasi

kerangka kerja khusus untuk apa pun yang didukung Wilayah AWS di bawah akun mereka sendiri.

Penerima

Ini adalah konsumen dari kerangka kerja bersama. Penerima dapat menerima atau menolak permintaan berbagi dari pengirim.

> **Note**
>
> Penerima dapat berupa akun administrator yang didelegasikan. Namun, Anda tidak dapat membagikan kerangka kerja khusus dengan akun AWS Organizations manajemen.

Kelayakan kerangka kerja

Anda hanya dapat berbagi kerangka kerja khusus. Secara default, kerangka kerja standar sudah ada di semua Akun AWS dan Wilayah AWS di mana AWS Audit Manager diaktifkan. Selain itu, kerangka kerja khusus yang Anda bagikan tidak boleh berisi data sensitif. Ini termasuk data yang ditemukan dalam kerangka itu sendiri, set kontrolnya, dan kontrol kustom apa pun yang merupakan bagian dari kerangka kerja kustom.

> **Important**
>
> Beberapa kerangka kerja standar yang ditawarkan oleh AWS Audit Manager berisi materi berhak cipta yang tunduk pada perjanjian lisensi. Kerangka kerja khusus mungkin berisi konten yang berasal dari kerangka kerja ini. Anda tidak boleh membagikan kerangka kerja khusus yang berasal dari kerangka kerja standar jika kerangka kerja standar ditetapkan sebagai tidak memenuhi syarat untuk dibagikanAWS, kecuali jika Anda telah memperoleh izin untuk melakukannya dari pemilik kerangka kerja standar.
> Untuk mempelajari kerangka kerja standar mana yang memenuhi syarat untuk dibagikan, lihat tabel berikut.

Nama kerangka standar	Versi kustom yang memenuhi syarat untuk berbagi
Pusat Keamanan Siber Australia (ACSC) Delapan Penting	 Ya
Panduan Keamanan Informasi Pusat Keamanan Cyber Australia (ACSC)	 Ya
AWS Audit ManagerContoh Kerangka	 Ya
AWS Control TowerPagar pembatas	 Ya
AWSkerangka praktik terbaik AI generatif v1	 Ya
AWSLicense Manager	 Ya
AWSPraktik Terbaik Keamanan Dasar	 Ya
AWSPraktik Terbaik Operasional	 Ya

Nama kerangka standar	Versi kustom yang memenuhi syarat untuk berbagi
AWSKerangka Well-Architected	 Ya
Pusat Keamanan Cyber Kanada - Medium	 Tidak
Tolok Ukur CIS untuk Tolok Ukur Yayasan Amazon Web Services CIS v1.2.0, Level 1	 Tidak
Tolok Ukur CIS untuk Tolok Ukur Yayasan Amazon Web Services CIS v1.2.0, Level 1 dan 2	 Tidak
Tolok Ukur CIS untuk Tolok Ukur Yayasan Amazon Web Services CIS v1.3.0, Level 1	 Tidak
Tolok Ukur CIS untuk Tolok Ukur Yayasan Amazon Web Services CIS v1.3.0, Level 1 dan 2	 Tidak
Tolok Ukur CIS untuk Tolok Ukur Yayasan Amazon Web Services CIS v1.4.0, Level 1	 Tidak
Tolok Ukur CIS untuk Benchmark Yayasan Amazon Web Services CIS v1.4.0, Level 1 dan 2	 Tidak

Nama kerangka standar	Versi kustom yang memenuhi syarat untuk berbagi
Kontrol CIS v7.1 IG1	 Ya
Kontrol CIS v8 IG1	 Tidak
FedRAMP Dasar Sedang	 Ya
GDPR	 Ya
Gramm-Leach-Bliley Act (GLBA)	 Ya
GxP 21 CFR Bagian 11	 Ya
Lampiran GxP UE 11	 Ya
Aturan Keamanan HIPAA 2003	 Ya

Nama kerangka standar	Versi kustom yang memenuhi syarat untuk berbagi
Aturan Keamanan Omnibus Akhir HIPAA 2013	 Ya
ISO/IEC 27001:2013 Lampiran A	 Tidak
NIST 800-53 (Rev. 5) Rendah-Sedang-Tinggi	 Ya
Kerangka Keamanan Siber NIST versi 1.1	 Ya
NIST SP 800-171 Wahyu 2	 Ya
PCI DSS v3.2.1	 Tidak
PCI DSS v4.0	 Tidak
SOC 2	 Tidak

Permintaan berbagi

Untuk berbagi kerangka kustom, Anda membuat permintaan berbagi. Permintaan berbagi menentukan penerima dan memberi tahu mereka bahwa kerangka kerja khusus tersedia. Penerima memiliki waktu 120 hari untuk menanggapi permintaan berbagi dengan menerima atau menolak. Jika tidak ada tindakan yang diambil dalam 120 hari, permintaan berbagi berakhir dan penerima kehilangan kemampuan untuk menambahkan kerangka kerja khusus ke pustaka kerangka kerja mereka. Pengirim dan penerima dapat melihat dan mengambil tindakan atas permintaan berbagi dari halaman permintaan berbagi pustaka kerangka kerja.

Bagikan status permintaan

Permintaan berbagi dapat memiliki salah satu status berikut.

- Aktif — Ini menunjukkan permintaan berbagi yang berhasil dikirim ke penerima dan sedang menunggu tanggapan mereka.
- Kedaluwarsa — Ini menunjukkan permintaan berbagi yang kedaluwarsa dalam 30 hari ke depan.
- Dibagikan - Ini menunjukkan permintaan berbagi yang diterima penerima.
- Tidak Aktif — Ini menunjukkan permintaan berbagi yang dicabut, ditolak, atau kedaluwarsa sebelum penerima mengambil tindakan.
- Mereplikasi — Ini menunjukkan permintaan berbagi yang diterima yang sedang direplikasi ke pustaka kerangka kerja penerima.
- Gagal — Ini menunjukkan permintaan berbagi yang tidak berhasil dikirim ke penerima.

Berbagi pemberitahuan permintaan

Audit Manager memberi tahu penerima ketika mereka menerima permintaan berbagi. Penerima dan pengirim menerima pemberitahuan ketika permintaan berbagi akan kedaluwarsa dalam 30 hari ke depan.

- Untuk penerima, titik notifikasi biru muncul di samping permintaan yang diterima dengan status Aktif atau Kedaluwarsa. Penerima dapat menyelesaikan pemberitahuan dengan menerima atau menolak permintaan berbagi.
- Untuk pengirim, titik notifikasi biru muncul di sebelah permintaan terkirim dengan status Kedaluwarsa. Pemberitahuan diselesaikan ketika penerima menerima atau menolak permintaan. Jika tidak, itu diselesaikan ketika permintaan kedaluwarsa. Selain itu, pengirim dapat menyelesaikan pemberitahuan dengan mencabut permintaan berbagi.

Kepemilikan pengirim

Pengirim mempertahankan akses penuh atas kerangka kerja kustom yang mereka bagikan. Mereka dapat membatalkan permintaan berbagi aktif kapan saja dengan mencabut permintaan berbagi sebelum kedaluwarsa. Namun, setelah penerima menerima permintaan berbagi, pengirim tidak dapat lagi mencabut akses penerima ke kerangka kustom tersebut. Ini karena ketika penerima menerima permintaan, Audit Manager membuat salinan independen dari kerangka kustom di pustaka kerangka kerja penerima.

Selain mereplikasi kerangka kustom pengirim, Audit Manager juga mereplikasi setiap set kontrol kustom dan kontrol kustom yang merupakan bagian dari framework tersebut. Namun, Audit Manager tidak mereplikasi tag apa pun yang dilampirkan ke kerangka kerja kustom.

Kepemilikan penerima

Penerima memiliki akses penuh atas kerangka kerja khusus yang mereka terima. Saat penerima menerima permintaan, Audit Manager mereplikasi kerangka kerja kustom ke tab kerangka kerja kustom dari pustaka kerangka kerja mereka. Penerima kemudian dapat mengelola kerangka kustom bersama dengan cara yang sama seperti kerangka kustom lainnya. Penerima dapat membagikan kerangka kerja kustom yang mereka terima dari pengirim lain. Penerima tidak dapat memblokir pengirim dari mengirim permintaan berbagi.

Kedaluwarsa kerangka kerja bersama

Saat pengirim membuat permintaan berbagi, Audit Manager menetapkan permintaan untuk kedaluwarsa setelah 120 hari. Penerima dapat menerima dan mendapatkan akses ke kerangka kerja bersama sebelum permintaan berakhir. Jika penerima tidak menerima selama waktu ini, permintaan berbagi akan kedaluwarsa. Setelah titik ini, catatan permintaan saham yang kedaluwarsa tetap ada dalam sejarah mereka. Cuplikan kerangka kerja bersama yang kedaluwarsa diarsipkan ke bucket S3 dengan TTL satu tahun untuk tujuan audit.

Pengirim dapat memilih untuk mencabut permintaan berbagi kapan saja sebelum jatuh tempo.

Penyimpanan dan cadangan data kerangka kerja bersama

Saat Anda membuat permintaan berbagi, Audit Manager menyimpan snapshot kerangka kerja kustom Anda di AS Timur (Virginia Utara). Wilayah AWS Audit Manager juga menyimpan cadangan snapshot yang sama di AS Barat (Oregon). Wilayah AWS

Audit Manager menghapus snapshot dan snapshot cadangan ketika salah satu peristiwa berikut terjadi:

- Pengirim mencabut permintaan berbagi.

- Penerima menolak permintaan berbagi.
- Penerima mengalami kesalahan dan tidak berhasil menerima permintaan berbagi.
- Permintaan berbagi berakhir sebelum penerima menanggapi permintaan.

Saat pengirim mengirim ulang permintaan berbagi, snapshot diganti dengan versi terbaru yang sesuai dengan versi terbaru dari kerangka kustom.

Ketika penerima menerima permintaan berbagi, snapshot direplikasi ke dalam mereka Akun AWS di bawah Wilayah AWS yang ditentukan dalam permintaan berbagi.

Pembuatan versi kerangka kerja bersama

Saat Anda membagikan kerangka kerja khusus, Audit Manager membuat salinan independen dari kerangka kerja tersebut di wilayah Akun AWS dan yang ditentukan. Ini berarti Anda harus mengingat poin-poin berikut:

- Kerangka kerja bersama yang diterima penerima adalah snapshot kerangka kerja pada saat pembuatan permintaan berbagi. Jika Anda memperbarui kerangka kustom asli setelah mengirim permintaan berbagi, permintaan tidak diperbarui secara otomatis. Untuk membagikan versi terbaru dari kerangka kerja yang diperbarui, Anda dapat mengirim ulang permintaan berbagi. Tanggal kedaluwarsa snapshot baru ini adalah 120 hari dari tanggal re-share.
- Saat Anda berbagi kerangka kerja khusus dengan yang lain Akun AWS dan kemudian menghapusnya dari pustaka kerangka kerja Anda, kerangka kerja kustom bersama tetap berada di pustaka kerangka kerja penerima.
- Saat Anda membagikan kerangka kerja khusus ke yang lain Wilayah AWS di bawah akun Anda dan kemudian menghapus kerangka kerja kustom itu di bagian pertamaWilayah AWS, kerangka kerja kustom tetap berada di Wilayah kedua.
- Saat Anda menghapus kerangka kerja kustom bersama setelah menerimanya, kontrol kustom apa pun yang direplikasi sebagai bagian dari kerangka kerja kustom tetap ada di pustaka kontrol Anda.

Mengirim permintaan berbagi untuk kerangka kerja khusus

Tutorial ini menjelaskan cara membagikan kerangka kerja kustom Anda di seluruh Akun AWS danWilayah AWS.

Saat Anda membagikan kerangka kerja khusus, Audit Manager membuat snapshot kerangka kerja Anda dan mengirimkan permintaan berbagi ke penerima. Penerima memiliki 120 hari untuk menerima

kerangka kerja bersama. Ketika mereka menerima, Audit Manager mereplikasi kerangka kerja kustom bersama ke pustaka kerangka kerja mereka di yang ditentukanWilayah AWS. Jika Anda ingin mereplikasi kerangka kustom ke Wilayah lain di bawah akun Anda sendiri, gunakan tutorial berikut dan masukkan ID Anda sendiri sebagai Akun AWS ID akun penerima.

Tutorial ini mencakup langkah-langkah berikut:

1. Pilih kerangka kerja untuk dibagikan - Jelajahi pustaka kerangka kerja untuk menemukan kerangka kerja khusus yang ingin Anda bagikan.
2. Kirim permintaan berbagi - Tentukan penerima dan kirimi mereka permintaan berbagi untuk kerangka kerja kustom.
3. Lihat permintaan terkirim — Lihat riwayat permintaan berbagi Anda dan periksa status permintaan yang Anda kirim.
4. (Opsional) Cabut permintaan berbagi - Cabut permintaan berbagi sebelum jatuh tempo.

Prasyarat

Sebelum Anda memulai tutorial ini, pastikan bahwa Anda terlebih dahulu memenuhi ketentuan berikut:

- Anda sudah familiar dengan konsep dan terminologi berbagi kerangka kerja Audit Manager.
- Kerangka kerja khusus yang ingin Anda bagikan memenuhi syarat untuk dibagikan dan ada di pustaka kerangka kerja AWS Audit Manager lingkungan Anda.
- Penerima sudah diaktifkan AWS Audit Manager di Wilayah AWS tempat Anda ingin berbagi kerangka kustom.
- Penerima bukan akun AWS Organizations manajemen.

> **Tip**
>
> Sebelum memulai, buat catatan Akun AWS ID yang ingin Anda bagikan kerangka kerja kustom Anda. Ini bisa menjadi ID akun Anda sendiri, jika tujuan Anda adalah mereplikasi kerangka kerja ke yang lain Wilayah AWS di bawah akun Anda. Anda memerlukan informasi ini untuk langkah 2 tutorial.

> **Important**
>
> Jangan bagikan kerangka kerja khusus yang berisi data sensitif. Ini termasuk data yang ditemukan dalam kerangka itu sendiri, set kontrolnya, dan kontrol kustom apa pun yang terdiri dari kerangka kustom. Untuk informasi selengkapnya, lihat Kelayakan Framework.

Langkah 1: Identifikasi kerangka kustom yang ingin Anda bagikan

Mulailah dengan mengidentifikasi kerangka kerja khusus yang ingin Anda bagikan. Anda dapat menemukan daftar semua kerangka kerja kustom yang tersedia di halaman library Framework di Audit Manager.

Untuk melihat kerangka kerja kustom yang tersedia

1. Buka konsol AWS Audit Manager di https://console.aws.amazon.com/auditmanager/home.
2. Di panel navigasi, pilih Framework library.
3. Pilih tab Kerangka kustom. Ini menampilkan daftar kerangka kerja kustom Anda yang tersedia. Anda dapat memilih nama kerangka kerja apa pun untuk melihat detail kerangka kerja khusus itu.

Langkah 2: Kirim permintaan berbagi

Selanjutnya, tentukan penerima dan kirimi mereka permintaan berbagi untuk kerangka kerja khusus. Penerima memiliki waktu 120 hari untuk menanggapi permintaan pembagian sebelum berakhir.

Untuk mengirim permintaan berbagi

1. Dari tab Kerangka Kustom pada pustaka kerangka kerja, pilih nama kerangka kerja untuk membuka halaman detail. Dari sini, pilih Tindakan dan kemudian pilih Bagikan kerangka kustom.
   - Atau, pilih kerangka kerja kustom dari daftar di pustaka kerangka kerja, pilih Tindakan, lalu pilih Bagikan kerangka kustom. Bergantung pada ukuran kerangka kustom, metode ini dapat memakan waktu beberapa detik sementara Audit Manager menyiapkan permintaan berbagi.
2. Tinjau pemberitahuan yang ditampilkan di kotak dialog.
   - Jika Anda tidak yakin apakah Anda dapat membagikan kerangka kerja kustom Anda, tinjau kelayakan Framework untuk panduan lebih lanjut.

- Jika framework Anda memiliki kontrol yang menggunakan AWS Config aturan kustom sebagai sumber data, kami sarankan Anda menghubungi penerima untuk memberi tahu mereka. Penerima kemudian dapat membuat dan mengaktifkan AWS Config aturan yang sama dalam contoh merekaAWS Config. Untuk informasi selengkapnya, lihat Kerangka kerja bersama saya memiliki kontrol yang menggunakan AWS Config aturan khusus sebagai sumber data. Dapatkah penerima mengumpulkan bukti untuk kontrol ini?.

3. Masuk **`agree`** dan kemudian pilih Setuju untuk melanjutkan.
4. Pada layar berikutnya, ikuti langkah-langkah ini:
   - Di bawah Akun AWS, masukkan ID akun penerima. Ini bisa menjadi ID akun Anda sendiri.
   - Di bawah Wilayah AWS, pilih Wilayah penerima dari daftar dropdown.
   - (Opsional) Di bawah Pesan ke penerima, masukkan komentar opsional tentang kerangka kustom yang Anda bagikan.
   - Di bawah Rincian kerangka kerja khusus, tinjau detailnya untuk mengonfirmasi bahwa Anda ingin membagikan kerangka kerja ini.
5. Pilih Bagikan.

> **Note**
>
> Perlu diingat poin-poin berikut:
>
> - Saat Anda berbagi kerangka kerja khusus dengan yang lainAkun AWS, kerangka kerja direplikasi hanya ke yang ditentukanWilayah AWS. Setelah menerima permintaan berbagi, penerima kemudian dapat mereplikasi kerangka kerja di seluruh Wilayah sesuai kebutuhan.
> - Saat berbagi kerangka kerja khususWilayah AWS, diperlukan waktu hingga 10 menit untuk memproses tindakan permintaan berbagi. Setelah mengirimkan permintaan berbagi lintas wilayah, kami sarankan Anda memeriksa kembali nanti untuk mengonfirmasi bahwa permintaan berbagi Anda berhasil dikirim.
> - Saat Anda mengirim permintaan berbagi, Audit Manager mengambil snapshot dari kerangka kustom pada saat pembuatan permintaan berbagi. Jika Anda memperbarui kerangka kerja kustom setelah mengirim permintaan berbagi, permintaan tidak diperbarui secara otomatis. Untuk membagikan versi terbaru dari kerangka kerja yang diperbarui,

Anda dapat mengirim ulang permintaan berbagi. Tanggal kedaluwarsa snapshot baru ini adalah 120 hari dari tanggal re-share.

Langkah 3: Lihat permintaan yang Anda kirim

Anda dapat memilih tab Permintaan terkirim untuk melihat daftar semua permintaan berbagi yang Anda kirim. Anda dapat memfilter daftar ini sesuai kebutuhan. Misalnya, Anda dapat menerapkan filter untuk hanya menampilkan permintaan yang kedaluwarsa dalam 30 hari ke depan.

Untuk melihat dan memfilter permintaan yang Anda kirim

1. Dari panel navigasi, pilih Bagikan permintaan.
2. Pilih tab Permintaan terkirim.
3. (Opsional) Terapkan filter untuk menyempurnakan permintaan terkirim mana yang terlihat. Anda dapat melakukan ini dengan menemukan daftar dropdown Semua status, dan mengubah filter menjadi salah satu dari berikut ini.
   - Aktif - Filter ini menampilkan permintaan berbagi yang menunggu respons dari penerima.
   - Shared — Filter ini menampilkan permintaan berbagi yang diterima oleh penerima. Kerangka kustom bersama sekarang ada di pustaka kerangka kerja penerima.
   - Tidak aktif — Filter ini menampilkan permintaan berbagi yang ditolak, dicabut, atau kedaluwarsa sebelum penerima mengambil tindakan. Pilih kata Tidak Aktif untuk melihat detail lebih lanjut.
   - Kedaluwarsa - Filter ini menampilkan permintaan berbagi yang kedaluwarsa dalam 30 hari ke depan.
   - Gagal — Filter ini menampilkan permintaan berbagi yang tidak berhasil dikirim ke penerima. Pilih kata Gagal untuk melihat detail selengkapnya.

> **Note**
>
> Diperlukan waktu hingga 15 menit untuk memproses permintaan berbagi. Akibatnya, jika terjadi kesalahan saat mengirim permintaan berbagi ke penerima, status Gagal mungkin tidak segera ditampilkan. Kami menyarankan Anda memeriksa kembali nanti untuk mengonfirmasi bahwa permintaan berbagi Anda berhasil dikirim.

Untuk informasi tentang cara melanjutkan jika Anda mengalami kesalahan, lihat Memecahkan masalah permintaan berbagi.

Langkah 4 (Opsional): Cabut permintaan berbagi

Jika Anda perlu membatalkan permintaan berbagi aktif sebelum kedaluwarsa, Anda dapat mencabut permintaan tersebut kapan saja. Langkah ini opsional. Jika Anda tidak mengambil tindakan, penerima kehilangan kemampuan untuk menerima permintaan berbagi setelah tanggal kedaluwarsa.

Untuk mencabut permintaan berbagi

1. Dari panel navigasi, pilih Bagikan permintaan.
2. Pilih tab Permintaan terkirim.
3. Pilih kerangka kerja yang ingin Anda cabut dan pilih Cabut permintaan.
4. Di jendela pop-up yang muncul, pilih Cabut.

> **Note**
>
> Anda hanya dapat mencabut akses untuk berbagi permintaan yang berstatus Aktif atau Kedaluwarsa. Setelah penerima menerima permintaan berbagi, Anda tidak dapat lagi mencabut akses mereka ke kerangka kerja kustom tersebut. Ini karena salinan kerangka kustom sekarang ada di pustaka kerangka penerima.
> Saat berbagi kerangka kerjaWilayah AWS, diperlukan waktu hingga 10 menit untuk memproses tindakan permintaan berbagi. Setelah mencabut permintaan berbagi lintas wilayah, kami sarankan Anda memeriksa kembali nanti untuk mengonfirmasi bahwa permintaan berbagi berhasil dicabut.

Mengirim ulang permintaan berbagi untuk kerangka kerja yang diperbarui

Anda dapat mengirim permintaan berbagi untuk kerangka kerja khusus dan kemudian memperbarui kerangka kerja yang sama setelahnya. Jika Anda melakukan ini, permintaan berbagi tidak diperbarui secara otomatis untuk mencerminkan versi terbaru kerangka kerja. Namun, jika statusnya aktif, dibagikan, atau kedaluwarsa, Anda dapat memperbarui permintaan berbagi yang ada. Untuk melakukan ini, Anda mengirim ulang permintaan berbagi baru dengan kumpulan detail yang sama dengan permintaan yang ada. Dalam permintaan berbagi baru, sertakan ID kerangka kerja kustom

yang sama, ID akun penerima, dan penerimaWilayah AWS. Anda juga dapat memberikan komentar baru dengan permintaan berbagi baru.

Ingatlah hal-hal berikut saat Anda mengirim ulang permintaan berbagi:

- Agar pembaruan berhasil, permintaan baru harus untuk ID kerangka kerja kustom yang sama. Ini juga harus menentukan ID akun penerima dan Wilayah yang sama dengan permintaan yang ada.
- Jika nama kerangka kustom telah berubah, permintaan berbagi yang diperbarui menampilkan nama terbaru.
- Jika Anda memberikan komentar baru, permintaan berbagi yang diperbarui akan menampilkan komentar terbaru.
- Saat Anda mengirim ulang permintaan berbagi, tanggal kedaluwarsa diperpanjang enam bulan.

Untuk mengirim ulang permintaan berbagi untuk kerangka kerja yang diperbarui

1. Dari tab Kerangka kustom pada pustaka kerangka kerja, pilih nama kerangka kerja yang ingin Anda bagikan. Ini membuka halaman detail kerangka kerja. Dari sini, pilih Tindakan dan kemudian pilih Bagikan kerangka kustom.

   - Atau, pilih kerangka kerja kustom dari daftar di pustaka kerangka kerja, pilih Tindakan, lalu pilih Bagikan kerangka kustom. Bergantung pada ukuran kerangka kustom, metode ini dapat memakan waktu beberapa detik bagi Audit Manager untuk menyiapkan permintaan berbagi.
2. Tinjau pemberitahuan yang ditampilkan di kotak dialog, masukkan**`agree`**, lalu pilih Setuju untuk melanjutkan.
3. Pada layar berikutnya, ikuti langkah-langkah ini:

   - Di bawah Akun AWS, masukkan ID akun yang sama dengan yang Anda tentukan dalam permintaan berbagi yang ada.
   - Di bawah Wilayah AWS, pilih Wilayah yang sama yang Anda tentukan dalam permintaan berbagi yang ada.
   - (Opsional) Di bawah Pesan ke penerima, masukkan komentar opsional tentang kerangka kustom yang diperbarui.
   - Di bawah Rincian kerangka kerja khusus, tinjau detailnya untuk mengonfirmasi bahwa Anda ingin mengirim ulang permintaan berbagi.
4. Pilih Bagikan untuk mengirim ulang dan memperbarui permintaan berbagi.

Memecahkan masalah permintaan berbagi

Untuk menemukan solusi atas masalah yang mungkin Anda temui saat berbagi kerangka kerja khusus, lihat Memecahkan masalah berbagi kerangka kerja di bagian Pemecahan Masalah di panduan ini.

Menanggapi permintaan berbagi

Tutorial ini menjelaskan tindakan yang harus diambil ketika Anda menerima permintaan berbagi untuk kerangka kustom. Audit Manager memberi tahu Anda saat Anda menerima permintaan berbagi. Anda juga menerima pemberitahuan untuk mengingatkan Anda ketika permintaan berbagi akan kedaluwarsa dalam 30 hari ke depan.

Tutorial ini mencakup langkah-langkah berikut:

1. Periksa pemberitahuan permintaan berbagi Anda — Tinjau daftar permintaan berbagi yang aktif dan segera kedaluwarsa.
2. Ambil tindakan atas permintaan berbagi - Terima atau tolak permintaan berbagi untuk kerangka kerja kustom.
3. Melihat permintaan berbagi yang Anda terima dari orang lain — Lihat riwayat permintaan berbagi Anda.

Prasyarat

Sebelum memulai, sebaiknya Anda mempelajari lebih lanjut tentang konsep dan terminologi berbagi kerangka kerja Audit Manager terlebih dahulu.

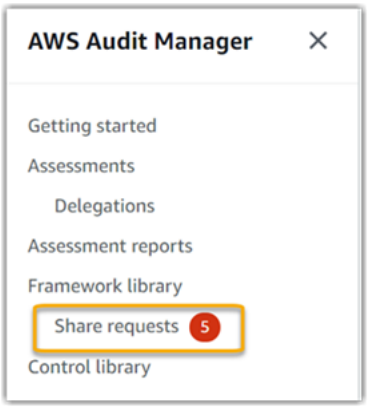
Langkah 1: Periksa pemberitahuan permintaan yang Anda terima

Mulailah dengan memeriksa notifikasi permintaan berbagi Anda. Tab Permintaan Diterima menampilkan daftar permintaan berbagi yang Anda terima dari orang lainAkun AWS. Permintaan yang menunggu tanggapan Anda muncul dengan titik biru. Anda juga dapat memfilter tampilan ini untuk hanya menampilkan permintaan yang kedaluwarsa dalam 30 hari ke depan.

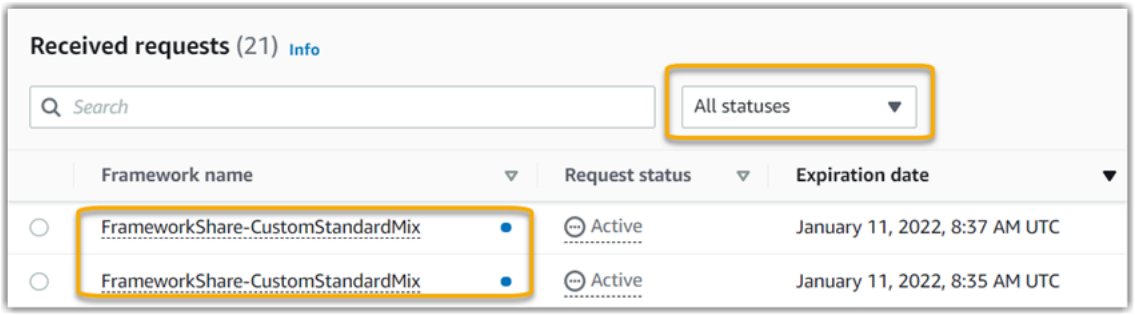
Untuk melihat permintaan yang diterima

1. Buka konsol AWS Audit Manager di https://console.aws.amazon.com/auditmanager/home.
2. Jika Anda memiliki pemberitahuan permintaan berbagi, Audit Manager menampilkan titik merah di sebelah ikon menu navigasi.

3. Perluas panel navigasi dan lihat di sebelah Permintaan Bagikan. Lencana notifikasi menunjukkan jumlah permintaan berbagi yang perlu Anda perhatikan.



4. Pilih Berbagi permintaan. Secara default, halaman ini terbuka di tab Permintaan Diterima.
5. Identifikasi permintaan berbagi yang memerlukan tindakan Anda dengan mencari item dengan titik biru.



6. (Opsional) Untuk hanya melihat permintaan yang kedaluwarsa dalam 30 hari ke depan, cari daftar tarik-turun Semua status dan pilih Kedaluwarsa.

Langkah 2: Ambil tindakan atas permintaan

Untuk menghapus titik notifikasi biru, Anda perlu mengambil tindakan dengan menerima atau menolak permintaan berbagi.

> **Note**
>
> Diperlukan waktu hingga 10 menit untuk memproses tindakan permintaan berbagi saat kerangka kerja dibagikanWilayah AWS. Setelah mengambil tindakan atas permintaan berbagi

lintas wilayah, kami sarankan Anda memeriksa kembali nanti untuk mengonfirmasi bahwa permintaan berbagi berhasil diterima atau ditolak.

Menerima kerangka kerja bersama

Saat Anda menerima permintaan berbagi, Audit Manager mereplikasi snapshot kerangka kerja asli ke dalam tab kerangka kerja kustom pustaka kerangka kerja Anda. Audit Manager mereplikasi dan mengenkripsi kerangka kustom baru menggunakan kunci KMS yang Anda tentukan dalam pengaturan Audit Manager Anda.

Untuk menerima permintaan berbagi

1. Buka halaman Permintaan Bagikan dan pastikan Anda melihat tab Permintaan Diterima.
2. (Opsional) Pilih Aktif atau Kedaluwarsa dari daftar dropdown filter.
3. (Opsional) Pilih nama kerangka kerja untuk melihat detail permintaan berbagi. Ini termasuk informasi seperti deskripsi kerangka kerja, jumlah kontrol yang ada dalam kerangka kerja, dan pesan dari pengirim.
4. Pilih permintaan berbagi yang ingin Anda terima, pilih Tindakan, lalu pilih Terima.

Setelah Anda menerima permintaan berbagi, status berubah menjadi replikasi sementara kerangka kustom bersama ditambahkan ke pustaka kerangka kerja Anda. Jika kerangka kerja berisi kontrol khusus, kontrol ini ditambahkan ke pustaka kontrol Anda saat ini.

Ketika replikasi framework selesai, status berubah menjadi shared. Spanduk sukses memberi tahu Anda bahwa kerangka kerja khusus siap digunakan.

> **Tip**
>
> Ketika Anda menerima kerangka kerja khusus, itu direplikasi hanya untuk Anda saat iniWilayah AWS. Anda mungkin ingin kerangka kerja bersama baru tersedia di semua Wilayah di AndaAkun AWS. Jika demikian, setelah Anda menerima permintaan berbagi, Anda dapat membagikan kerangka kerja ke Wilayah lain di bawah akun Anda sesuai kebutuhan.

Menurun kerangka kerja bersama

Saat Anda menolak permintaan berbagi, Audit Manager tidak menambahkan kerangka kerja kustom tersebut ke pustaka kerangka kerja Anda. Namun, catatan permintaan berbagi yang ditolak tetap ada di tab Permintaan Diterima, dengan status Tidak Aktif.

Untuk menolak permintaan berbagi

1. Buka halaman Permintaan Bagikan dan pastikan Anda melihat tab Permintaan Diterima.
2. (Opsional) Pilih Aktif atau Kedaluwarsa dari daftar dropdown filter.
3. (Opsional) Pilih nama kerangka kerja untuk melihat detail permintaan berbagi. Ini termasuk informasi seperti deskripsi kerangka kerja, jumlah kontrol yang ada dalam kerangka kerja, dan pesan dari pengirim.
4. Pilih permintaan berbagi yang ingin Anda tolak, pilih Tindakan, lalu pilih Tolak.
5. Di kotak dialog yang muncul, pilih Tolak untuk mengonfirmasi pilihan Anda.

> **Tip**
>
> Jika Anda berubah pikiran dan ingin mengakses kerangka kerja bersama setelah Anda menolak, minta pengirim untuk mengirimi Anda permintaan berbagi baru.

Langkah 3: Lihat riwayat permintaan yang Anda terima

Setelah Anda menerima atau menolak kerangka kerja bersama, Anda dapat kembali ke halaman Permintaan berbagi untuk melihat riwayat permintaan berbagi Anda. Anda dapat memfilter daftar ini sesuai kebutuhan. Misalnya, Anda dapat menerapkan filter untuk hanya menampilkan permintaan yang Anda terima.

Untuk melihat riwayat permintaan berbagi Anda

1. Buka konsol AWS Audit Manager di https://console.aws.amazon.com/auditmanager/home.
2. Di panel navigasi kiri, pilih Bagikan permintaan.
3. Pilih tab Permintaan Diterima.
4. Temukan daftar tarik-turun Semua status, dan pilih salah satu filter berikut.
   - Aktif - Filter ini menampilkan permintaan berbagi yang belum Anda terima atau tolak.

- Kedaluwarsa - Filter ini menampilkan permintaan berbagi yang kedaluwarsa dalam 30 hari ke depan.
- Shared - Filter ini menampilkan permintaan berbagi yang Anda terima. Kerangka kerja bersama sekarang tersedia di pustaka kerangka kerja Anda.
- Tidak aktif - Filter ini menampilkan permintaan berbagi yang ditolak atau kedaluwarsa.
- Gagal - Filter ini menampilkan permintaan berbagi yang tidak berhasil dikirim. Pilih kata Gagal untuk melihat detail selengkapnya.

Apa yang bisa saya lakukan selanjutnya?

Setelah Anda menerima kerangka kustom bersama, Anda dapat menemukannya di tab kerangka kerja kustom dari pustaka kerangka kerja. Anda sekarang dapat menggunakan kerangka kerja itu untuk membuat penilaian. Untuk mempelajari lebih lanjut, lihat Membuat penilaian. Untuk petunjuk tentang cara mengedit kerangka kustom baru Anda, lihat Mengedit kerangka kustom.

Menghapus permintaan berbagi

Anda dapat menghapus permintaan berbagi yang tidak lagi diinginkan atau diperlukan.

> **Note**
>
> Anda tidak dapat menghapus permintaan berbagi yang memiliki status aktif atau mereplikasi. Saat Anda menghapus permintaan berbagi, hanya permintaan itu sendiri yang dihapus. Kerangka kerja bersama itu sendiri tetap ada di pustaka kerangka kerja Anda.

Untuk menghapus permintaan berbagi

1. Dari panel navigasi, pilih Bagikan permintaan.
2. Pilih salah satu Permintaan terkirim atau tab Permintaan Diterima.
3. Pilih kerangka kerja yang tidak lagi Anda inginkan dan pilih Hapus.
4. Di jendela pop-up yang muncul, pilih Hapus.

Kerangka kerja yang didukung di AWS Audit Manager

AWS Audit Managermenyediakan kerangka kerja standar berikut. Kerangka kerja prebuilt ini didasarkan pada praktik AWS terbaik untuk berbagai standar dan peraturan kepatuhan. Anda dapat menggunakan kerangka kerja ini untuk membantu Anda dengan persiapan audit Anda.

Topik

- Pusat Keamanan Siber Australia (ACSC) Delapan Penting
- Panduan Keamanan Informasi Pusat Keamanan Cyber Australia (ACSC)
- AWS Audit ManagerContoh Kerangka
- AWS Control TowerPagar pembatas
- AWSkerangka praktik terbaik AI generatif v1
- AWS License Manager
- AWSPraktik Terbaik Keamanan Dasar
- AWSPraktik Terbaik Operasional
- AWSWell-Architected
- Pusat Kanada untuk Profil Kontrol Cloud Sedang Keamanan Cyber
- Tolok Ukur CIS untuk Tolok Ukur Yayasan Amazon Web Services CIS v1.2.0
- Tolok Ukur CIS untuk Tolok Ukur Yayasan Amazon Web Services CIS v1.3.0
- Tolok Ukur CIS untuk Benchmark Yayasan Amazon Web Services CIS v1.4.0
- Kontrol CIS v7.1 Grup Implementasi 1
- Kontrol CIS v8 Grup Implementasi 1
- FedRAMP Dasar Sedang
- Peraturan Perlindungan Data Umum (GDPR)
- Gramm-Leach-Bliley Act
- GxP 21 CFR bagian 11
- Lampiran GxP UE 11
- Aturan Keamanan Undang-Undang Portabilitas dan Akuntabilitas Asuransi Kesehatan (HIPAA) 2003
- Undang-Undang Portabilitas dan Akuntabilitas Asuransi Kesehatan (HIPAA) Final Omnibus Security Rule 2013
- ISO/IEC 27001:2013 Lampiran A

- NIST 800-53 (Rev. 5) Rendah-Sedang-Tinggi
- Kerangka Keamanan Siber NIST versi 1.1
- NIST SP 800-171 (Wahyu 2)
- PCI DSS V3.2.1
- PCI DSS V4.0
- SOC 2

Pusat Keamanan Siber Australia (ACSC) Delapan Penting

Untuk membantu Anda dengan persiapan audit Anda, AWS Audit Manager sediakan kerangka kerja standar bawaan yang menyusun dan mengotomatiskan penilaian untuk kerangka Essential Eight.

Topik

- Apa itu Australian Cyber Security Centre (ACSC) Essential Eight?
- Menggunakan kerangka kerja ini untuk mendukung persiapan audit Anda
- Lebih Penting Delapan sumber daya

Apa itu Australian Cyber Security Centre (ACSC) Essential Eight?

Australian Cyber Security Centre (ACSC) adalah lembaga utama pemerintah Australia untuk keamanan siber. Untuk melindungi dari ancaman cyber, ACSC merekomendasikan agar organisasi menerapkan delapan strategi mitigasi penting dari Strategi ACSC untuk Memitigasi Insiden Keamanan Siber sebagai dasar. Garis dasar ini, yang dikenal sebagai Esential Eight, membuat lebih sulit bagi musuh untuk mengkompromikan sistem.

Karena Essential Eight menguraikan serangkaian tindakan pencegahan minimum, organisasi Anda perlu menerapkan langkah-langkah tambahan yang dijamin oleh lingkungan Anda. Lebih lanjut, sementara Essential Eight dapat membantu mengurangi sebagian besar ancaman cyber, itu tidak akan mengurangi semua ancaman cyber. Dengan demikian, strategi mitigasi tambahan dan kontrol keamanan perlu dipertimbangkan, termasuk yang dari Strategi untuk Memitigasi Insiden Keamanan Siber dan Manual Keamanan Informasi (ISM).

Menggunakan kerangka kerja ini untuk mendukung persiapan audit Anda

Anda dapat menggunakan kerangka kerja standar Essential Eight AWS Audit Manager untuk membantu Anda mempersiapkan audit. Kerangka kerja ini mencakup kumpulan kontrol bawaan dengan deskripsi dan prosedur pengujian. Kontrol ini dikelompokkan ke dalam set kontrol sesuai dengan persyaratan Esential Eight. Anda juga dapat menyesuaikan kerangka kerja ini dan kontrolnya untuk mendukung audit internal dengan persyaratan khusus.

Dengan menggunakan kerangka kerja sebagai titik awal, Anda dapat membuat penilaian Audit Manager dan mulai mengumpulkan bukti yang relevan untuk audit Anda. Setelah Anda membuat penilaian, Audit Manager mulai menilai AWS sumber daya Anda. Ini dilakukan berdasarkan kontrol yang didefinisikan dalam kerangka Esential Eight. Saat tiba waktunya untuk audit, Anda—atau delegasi pilihan Anda—dapat meninjau bukti yang dikumpulkan oleh Audit Manager. Anda juga dapat menelusuri folder bukti dalam penilaian Anda dan memilih bukti mana yang ingin Anda sertakan dalam laporan penilaian Anda. Atau, jika Anda mengaktifkan pencari bukti, Anda dapat mencari bukti spesifik dan mengekspornya dalam format CSV, atau membuat laporan penilaian dari hasil penelusuran Anda. Either way, Anda dapat menggunakan laporan penilaian ini untuk menunjukkan bahwa kontrol Anda berfungsi sebagaimana dimaksud.

Rincian kerangka kerja adalah sebagai berikut:

Nama kerangka kerja di AWS Audit Manager	Jumlah kontrol otomatis	Jumlah kontrol manual	Jumlah set kontrol	Layanan AWSdalam ruang lingkup
Esensi Delapan	7	1	8	• AWS Config • AWS Security Hub

> **Tip**
>
> Untuk meninjau AWS Config aturan yang digunakan sebagai pemetaan sumber data dalam kerangka standar ini, unduh file AuditManager_ ConfigDataSourceMappings _ EssentialEight .zip.

Kontrol dalam AWS Audit Manager kerangka kerja ini tidak dimaksudkan untuk memverifikasi apakah sistem Anda sesuai dengan kontrol Essential Eight. Selain itu, mereka tidak dapat menjamin bahwa Anda akan lulus audit Essential Eight. AWS Audit Managertidak secara otomatis memeriksa kontrol prosedural yang memerlukan pengumpulan bukti manual.

Anda dapat menemukan kerangka Esential Eight di bawah tab Kerangka Standar Pustaka kerangka kerja di Audit Manager.

Saat Anda menggunakan konsol Audit Manager untuk membuat penilaian dari kerangka kerja standar ini, daftar Layanan AWS dalam cakupan dipilih secara default dan tidak dapat diedit. Ini karena Audit Manager secara otomatis memetakan dan memilih sumber data dan layanan untuk Anda. Pemilihan ini dibuat sesuai dengan persyaratan kerangka Esential Eight. Jika Anda perlu mengedit daftar layanan dalam cakupan kerangka kerja ini, Anda dapat melakukannya dengan menggunakan operasi CreateAssessmentatau UpdateAssessmentAPI. Atau, Anda dapat menyesuaikan kerangka kerja standar dan kemudian membuat penilaian dari kerangka kerja khusus.

Untuk petunjuk tentang cara membuat penilaian menggunakan kerangka kerja ini, lihatMembuat penilaian. Untuk petunjuk tentang cara menyesuaikan kerangka kerja ini untuk mendukung persyaratan spesifik Anda, lihat Menyesuaikan kerangka kerja yang ada dan Menyesuaikan kontrol yang ada.

Lebih Penting Delapan sumber daya

- ACSC Esential Delapan

Panduan Keamanan Informasi Pusat Keamanan Cyber Australia (ACSC)

Untuk membantu Anda dengan persiapan audit Anda, AWS Audit Manager sediakan kerangka kerja standar bawaan yang menyusun dan mengotomatiskan penilaian untuk kerangka kerja Manual Keamanan Informasi ACSC.

Topik

- Apa itu Panduan Keamanan Informasi Pusat Keamanan Cyber Australia (ACSC)?
- Menggunakan kerangka kerja ini untuk mendukung persiapan audit Anda
- Lebih banyak sumber daya Manual Keamanan Informasi ACSC

Apa itu Panduan Keamanan Informasi Pusat Keamanan Cyber Australia (ACSC)?

Australian Cyber Security Centre (ACSC) adalah lembaga utama pemerintah Australia untuk keamanan siber. ACSC memproduksi Information Security Manual (ISM), yang berfungsi sebagai seperangkat prinsip keamanan cyber. Tujuan dari prinsip-prinsip ini adalah untuk memberikan panduan strategis tentang bagaimana organisasi dapat melindungi sistem dan data mereka dari ancaman cyber. Prinsip-prinsip keamanan cyber ini dikelompokkan menjadi empat kegiatan utama: mengatur, melindungi, mendeteksi, dan merespons. Sebuah organisasi harus dapat menunjukkan bahwa prinsip-prinsip keamanan cyber sedang dipatuhi dalam organisasi mereka. ISM ditujukan untuk Chief Information Security Officers, Chief Information Officer, profesional keamanan cyber, dan manajer teknologi informasi.

Menggunakan kerangka kerja ini untuk mendukung persiapan audit Anda

Anda dapat menggunakan kerangka standar Manual Keamanan Informasi ACSC AWS Audit Manager untuk membantu Anda mempersiapkan audit. Kerangka kerja ini mencakup kumpulan kontrol bawaan dengan deskripsi dan prosedur pengujian. Kontrol ini dikelompokkan ke dalam set kontrol sesuai dengan persyaratan Manual Keamanan Informasi ACSC. Anda juga dapat menyesuaikan kerangka kerja ini dan kontrolnya untuk mendukung audit internal dengan persyaratan khusus.

Dengan menggunakan kerangka kerja sebagai titik awal, Anda dapat membuat penilaian Audit Manager dan mulai mengumpulkan bukti yang relevan untuk audit Anda. Setelah Anda membuat penilaian, Audit Manager mulai menilai AWS sumber daya Anda. Ini dilakukan berdasarkan kontrol yang didefinisikan dalam kerangka Manual Keamanan Informasi ACSC. Saat tiba waktunya untuk audit, Anda—atau delegasi pilihan Anda—dapat meninjau bukti yang dikumpulkan oleh Audit Manager. Anda juga dapat menelusuri folder bukti dalam penilaian Anda dan memilih bukti mana yang ingin Anda sertakan dalam laporan penilaian Anda. Atau, jika Anda mengaktifkan pencari bukti, Anda dapat mencari bukti spesifik dan mengekspornya dalam format CSV, atau membuat laporan penilaian dari hasil penelusuran Anda. Either way, Anda dapat menggunakan laporan penilaian ini untuk menunjukkan bahwa kontrol Anda berfungsi sebagaimana dimaksud.

Rincian kerangka kerja adalah sebagai berikut:

Nama kerangka kerja di AWS Audit Manager	Jumlah kontrol otomatis	Jumlah kontrol manual	Jumlah set kontrol	Layanan AWSdalam ruang lingkup
Manual Keamanan Informasi ACSC	45	396	22	• Amazon Elastic Compute Cloud • AWS Config • AWS Identity and Access Management

> **Tip**
>
> Untuk meninjau AWS Config aturan yang digunakan sebagai pemetaan sumber data dalam kerangka standar ini, unduh file AuditManager_ ConfigDataSourceMappings _ACSC-Information-Security-Manual.zip.

Kontrol dalam AWS Audit Manager kerangka kerja ini tidak dimaksudkan untuk memverifikasi apakah sistem Anda sesuai dengan kontrol Manual Keamanan Informasi ACSC. Selain itu, mereka tidak dapat menjamin bahwa Anda akan lulus audit ACSC. AWS Audit Managertidak secara otomatis memeriksa kontrol prosedural yang memerlukan pengumpulan bukti manual.

Anda dapat menemukan kerangka kerja Manual Keamanan Informasi ACSC di bawah tab Kerangka standar Pustaka kerangka kerja di Audit Manager.

Saat Anda menggunakan konsol Audit Manager untuk membuat penilaian dari kerangka kerja standar ini, daftar Layanan AWS dalam cakupan dipilih secara default dan tidak dapat diedit. Ini karena Audit Manager secara otomatis memetakan dan memilih sumber data dan layanan untuk Anda. Pemilihan ini dibuat sesuai dengan persyaratan kerangka Manual Keamanan Informasi ACSC. Jika Anda perlu mengedit daftar layanan dalam cakupan kerangka kerja ini, Anda dapat melakukannya dengan menggunakan operasi CreateAssessmentatau UpdateAssessmentAPI. Atau, Anda dapat menyesuaikan kerangka kerja standar dan kemudian membuat penilaian dari kerangka kerja khusus.

Untuk petunjuk tentang cara membuat penilaian menggunakan kerangka kerja ini, lihatMembuat penilaian. Untuk petunjuk tentang cara menyesuaikan kerangka kerja ini untuk mendukung persyaratan spesifik Anda, lihat Menyesuaikan kerangka kerja yang ada dan Menyesuaikan kontrol yang ada.

Lebih banyak sumber daya Manual Keamanan Informasi ACSC

- Manual Keamanan Informasi ACSC

AWS Audit ManagerContoh Kerangka

AWS Audit Managermenyediakan kerangka kerja sampel untuk membantu Anda memulai persiapan audit Anda.

Topik

- Apa itu Kerangka AWS Audit Manager Sampel?
- Menggunakan kerangka kerja ini untuk mendukung persiapan audit Anda

Apa itu Kerangka AWS Audit Manager Sampel?

AWS Audit ManagerSample Framework adalah kerangka kerja sederhana yang dapat Anda gunakan untuk memulai Audit Manager. Beberapa kerangka kerja prebuilt lainnya yang disediakan Audit Manager, sebagai perbandingan, jauh lebih besar dan berisi banyak kontrol. Dengan menggunakan kerangka kerja sampel alih-alih kerangka kerja yang lebih besar ini, Anda dapat lebih mudah meninjau dan mengeksplorasi contoh kerangka kerja. Kontrol dalam kerangka kerja ini didasarkan pada serangkaian panggilan AWS Config dan AWS API.

Menggunakan kerangka kerja ini untuk mendukung persiapan audit Anda

Anda dapat menggunakan kerangka kerja ini untuk membantu Anda memulaiAWS Audit Manager. Anda juga dapat menyesuaikan kerangka kerja ini dan kontrolnya untuk mendukung audit internal dengan persyaratan khusus.

Dengan menggunakan Kerangka Kerja AWS Audit Manager Sampel sebagai titik awal, Anda dapat membuat penilaian Audit Manager dan mulai mengumpulkan bukti yang relevan untuk audit Anda. Setelah Anda membuat penilaian, Audit Manager mulai menilai AWS sumber daya Anda. Ini dilakukan berdasarkan kontrol yang didefinisikan dalam kerangka kerja. Selanjutnya, ia mengumpulkan bukti yang relevan dan kemudian menempelkannya ke kontrol dalam penilaian Anda.

Rincian Kerangka AWS Audit Manager Contoh adalah sebagai berikut:

Nama kerangka kerja di AWS Audit Manager	Jumlah kontrol otomatis	Jumlah kontrol manual	Jumlah set kontrol	Layanan AWSdalam ruang lingkup
AWS Audit ManagerContoh Kerangka	4	1	3	• Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Identity and Access Managemen t

Anda dapat menemukan kerangka kerja ini di bawah tab Kerangka Standar Pustaka kerangka kerja di Audit Manager.

Untuk petunjuk tentang cara membuat penilaian menggunakan kerangka kerja ini, lihatMembuat penilaian.

Saat Anda menggunakan konsol Audit Manager untuk membuat penilaian dari kerangka kerja standar ini, daftar Layanan AWS dalam cakupan dipilih secara default dan tidak dapat diedit. Ini karena Audit Manager secara otomatis memetakan dan memilih sumber data dan layanan untuk Anda. Pemilihan ini dibuat sesuai dengan persyaratan Kerangka AWS Audit Manager Sampel. Jika Anda perlu mengedit daftar layanan dalam cakupan kerangka kerja ini, Anda dapat melakukannya dengan menggunakan operasi CreateAssessmentatau UpdateAssessmentAPI. Atau, Anda dapat menyesuaikan kerangka kerja standar dan kemudian membuat penilaian dari kerangka kerja khusus.

Untuk petunjuk tentang cara menyesuaikan kerangka kerja ini untuk mendukung persyaratan spesifik Anda, lihat Menyesuaikan kerangka kerja yang ada dan Menyesuaikan kontrol yang ada.

AWS Control TowerPagar pembatas

AWS Audit Managermenyediakan kerangka kerja AWS Control Tower Guardrails untuk membantu Anda dengan persiapan audit Anda.

Topik

- Apa AWS Control Tower?

- Menggunakan kerangka kerja ini untuk mendukung persiapan audit Anda
- Lebih banyak AWS Control Tower sumber daya

Apa AWS Control Tower?

AWS Control Toweradalah layanan manajemen dan tata kelola yang dapat Anda gunakan untuk menavigasi melalui proses pengaturan dan persyaratan tata kelola yang terlibat dalam menciptakan lingkungan AWS multi-akun.

DenganAWS Control Tower, Anda dapat menyediakan baru Akun AWS yang sesuai dengan kebijakan perusahaan atau organisasi Anda dalam beberapa klik. AWS Control Towermembuat lapisan orkestrasi atas nama Anda yang menggabungkan dan mengintegrasikan kemampuan beberapa layanan lainnya. AWS Layanan ini termasukAWS Organizations,AWS IAM Identity Center, dan Layanan AWS Katalog. Ini membantu merampingkan proses pengaturan dan pengaturan AWS lingkungan multi-akun yang aman dan sesuai.

Kerangka AWS Control Tower Guardrails berisi semua Aturan AWS Config yang didasarkan pada pagar pembatas dari. AWS Control Tower

Menggunakan kerangka kerja ini untuk mendukung persiapan audit Anda

Anda dapat menggunakan kerangka kerja AWS Control TowerGuardrails untuk membantu Anda mempersiapkan audit. Kerangka kerja ini mencakup kumpulan kontrol bawaan dengan deskripsi dan prosedur pengujian. Kontrol ini dikelompokkan menurut Aturan AWS Config yang didasarkan pada pagar pembatas dari. AWS Control Tower Anda juga dapat menyesuaikan kerangka kerja ini dan kontrolnya untuk mendukung audit internal dengan persyaratan khusus.

Dengan menggunakan kerangka kerja sebagai titik awal, Anda dapat membuat penilaian Audit Manager dan mulai mengumpulkan bukti yang relevan untuk AWS Control Tower audit. Setelah Anda membuat penilaian, Audit Manager mulai menilai AWS sumber daya Anda. Hal ini dilakukan berdasarkan kontrol yang didefinisikan dalam kerangka AWS Control Tower Guardrails. Saat tiba waktunya untuk audit, Anda—atau delegasi pilihan Anda—dapat meninjau bukti yang dikumpulkan oleh Audit Manager. Anda juga dapat menelusuri folder bukti dalam penilaian Anda dan memilih bukti mana yang ingin Anda sertakan dalam laporan penilaian Anda. Atau, jika Anda mengaktifkan pencari bukti, Anda dapat mencari bukti spesifik dan mengekspornya dalam format CSV, atau membuat laporan penilaian dari hasil penelusuran Anda. Either way, Anda dapat menggunakan laporan penilaian ini untuk menunjukkan bahwa kontrol Anda berfungsi sebagaimana dimaksud.

Rincian kerangka kerja AWS Control Tower Guardrails adalah sebagai berikut:

Nama kerangka kerja di AWS Audit Manager	Jumlah kontrol otomatis	Jumlah kontrol manual	Jumlah set kontrol	Layanan AWSdalam ruang lingkup
AWS Control TowerPagar pembatas	14	0	5	AWS Config

> **Tip**
>
> Untuk meninjau AWS Config aturan yang digunakan sebagai pemetaan sumber data dalam kerangka standar ini, unduh file AuditManager_ ConfigDataSourceMappings _ ControlTowerGuardrails .zip.

Kontrol dalam AWS Audit Manager kerangka kerja ini tidak dimaksudkan untuk memverifikasi apakah sistem Anda sesuai dengan AWS Control Tower Guardrails. Selain itu, mereka tidak dapat menjamin bahwa Anda akan lulus audit.

Anda dapat menemukan kerangka kerja AWS Control Tower Guardrails di bawah tab Kerangka standar di Audit Pustaka kerangka kerja Manager.

Untuk petunjuk tentang cara membuat penilaian menggunakan kerangka kerja ini, lihatMembuat penilaian.

Saat Anda menggunakan konsol Audit Manager untuk membuat atau memperbarui penilaian dari kerangka kerja standar ini, daftar Layanan AWS dalam cakupan dipilih secara default dan tidak dapat diedit. Ini karena Audit Manager secara otomatis memetakan dan memilih sumber data dan layanan untuk Anda. Pilihan ini dibuat sesuai dengan persyaratan AWS Control Tower pagar pembatas. Jika Anda perlu mengedit daftar layanan dalam cakupan kerangka kerja ini, Anda dapat melakukannya dengan menggunakan operasi CreateAssessmentatau UpdateAssessmentAPI. Atau, Anda dapat menyesuaikan kerangka kerja standar dan kemudian membuat penilaian dari kerangka kerja khusus.

Untuk petunjuk tentang cara menyesuaikan kerangka kerja ini untuk mendukung persyaratan spesifik Anda, lihat Menyesuaikan kerangka kerja yang ada dan Menyesuaikan kontrol yang ada.

Lebih banyak AWS Control Tower sumber daya

- AWS Control Towerhalaman layanan
- AWS Control Towerpanduan pengguna

AWSkerangka praktik terbaik AI generatif v1

AWS Audit Managermenyediakan kerangka kerja standar bawaan untuk membantu Anda mendapatkan visibilitas tentang bagaimana implementasi AI generatif Anda di Amazon Bedrock bekerja melawan AWS praktik terbaik yang direkomendasikan.

Amazon Bedrock adalah layanan yang dikelola sepenuhnya yang membuat model AI dari Amazon dan perusahaan AI terkemuka lainnya tersedia melalui API. Dengan Amazon Bedrock, Anda dapat menyetel model yang ada secara pribadi dengan data organisasi Anda. Ini memungkinkan Anda untuk memanfaatkan model dasar (FM) dan model bahasa besar (LLM) untuk membangun aplikasi dengan aman, tanpa mengorbankan privasi data. Untuk informasi lebih lanjut, lihat Apa itu Amazon Bedrock? di Panduan Pengguna Amazon Bedrock.

Topik

- Apa praktik terbaik AI AWS generatif untuk Amazon Bedrock?
- Menggunakan kerangka kerja ini untuk mendukung persiapan audit Anda
- Memverifikasi petunjuk secara manual di Amazon Bedrock
- Sumber daya lainnya

Apa praktik terbaik AI AWS generatif untuk Amazon Bedrock?

Generative AI mengacu pada cabang AI yang berfokus pada memungkinkan mesin menghasilkan konten. Model AI generatif dirancang untuk menciptakan output yang sangat mirip dengan contoh yang dilatih. Ini menciptakan skenario di mana AI dapat meniru percakapan manusia, menghasilkan konten kreatif, menganalisis volume data yang sangat besar, dan mengotomatiskan proses yang biasanya dilakukan oleh manusia. Pertumbuhan pesat AI generatif membawa inovasi baru yang menjanjikan. Pada saat yang sama, ini menimbulkan tantangan baru seputar cara menggunakan AI generatif secara bertanggung jawab dan sesuai dengan persyaratan tata kelola.

AWSberkomitmen untuk menyediakan Anda dengan alat dan panduan yang diperlukan untuk membangun dan mengatur aplikasi secara bertanggung jawab. Untuk membantu Anda mencapai

tujuan ini, Audit Manager telah bermitra dengan Amazon Bedrock untuk membuat kerangka kerja praktik terbaik AI AWS generatif v1. Kerangka kerja ini memberi Anda alat yang dibuat khusus untuk memantau dan meningkatkan tata kelola proyek AI generatif Anda di Amazon Bedrock. Anda dapat menggunakan praktik terbaik dalam kerangka kerja ini untuk mendapatkan kontrol dan visibilitas yang lebih ketat atas penggunaan model Anda dan tetap mendapat informasi tentang perilaku model.

Kontrol dalam kerangka kerja ini dikembangkan bekerja sama dengan pakar AI, praktisi kepatuhan, spesialis jaminan keamanan di seluruhAWS, dan dengan masukan dari Deloitte. Setiap kontrol otomatis memetakan ke sumber AWS data dari mana Audit Manager mengumpulkan bukti. Anda dapat menggunakan bukti yang dikumpulkan untuk mengevaluasi implementasi AI generatif Anda berdasarkan delapan prinsip berikut:

1. Bertanggung Jawab - Mengembangkan dan mematuhi pedoman etika untuk penyebaran dan penggunaan model AI generatif
2. Aman — Menetapkan parameter yang jelas dan batas-batas etika untuk mencegah timbulnya output yang berbahaya atau bermasalah
3. Adil - Pertimbangkan dan hormati bagaimana sistem AI memengaruhi berbagai sub-populasi pengguna
4. Berkelanjutan - Berusaha untuk efisiensi yang lebih besar dan sumber daya yang lebih berkelanjutan
5. Ketahanan - Menjaga integritas dan mekanisme ketersediaan untuk memastikan sistem AI beroperasi dengan andal
6. Privasi — Memastikan bahwa data sensitif dilindungi dari pencurian dan eksposur
7. Akurasi — Bangun sistem AI yang akurat, andal, dan kuat
8. Aman — Mencegah akses tidak sah ke sistem AI generatif

Contoh

Katakanlah aplikasi Anda menggunakan model dasar pihak ketiga yang tersedia di Amazon Bedrock. Anda dapat menggunakan kerangka kerja praktik terbaik AI AWS generatif untuk memantau penggunaan model ini. Dengan menggunakan kerangka kerja ini, Anda dapat mengumpulkan bukti yang menunjukkan bahwa penggunaan Anda sesuai dengan praktik terbaik AI generatif. Ini memberi Anda pendekatan yang konsisten untuk melacak penggunaan dan izin model trek, menandai data sensitif, dan diberi tahu tentang pengungkapan yang tidak disengaja. Misalnya, kontrol khusus dalam kerangka kerja ini dapat mengumpulkan bukti yang membantu Anda menunjukkan bahwa Anda telah menerapkan mekanisme untuk hal-hal berikut:

- Mendokumentasikan sumber, sifat, kualitas, dan perlakuan data baru, untuk memastikan transparansi dan membantu dalam pemecahan masalah atau audit (Bertanggung jawab)
- Mengevaluasi model secara teratur menggunakan metrik kinerja yang telah ditentukan untuk memastikannya memenuhi tolok ukur akurasi dan keselamatan (Aman)
- Menggunakan alat pemantauan otomatis untuk mendeteksi dan memperingatkan potensi hasil atau perilaku bias secara real-time (Adil)
- Mengevaluasi, mengidentifikasi, dan mendokumentasikan penggunaan model dan skenario di mana model yang ada dapat digunakan kembali, apakah Anda membuatnya atau tidak (Berkelanjutan)
- Menyiapkan prosedur untuk pemberitahuan jika ada tumpahan PII yang tidak disengaja atau pengungkapan yang tidak disengaja (Privasi)
- Membuat pemantauan real-time dari sistem AI dan menyiapkan peringatan untuk setiap anomali atau gangguan (Ketahanan)
- Mendeteksi ketidakakuratan, dan melakukan analisis kesalahan menyeluruh untuk memahami akar penyebab (Akurasi)
- Menerapkan end-to-end enkripsi untuk data input dan output model AI ke standar industri minimum (Aman)

Menggunakan kerangka kerja ini untuk mendukung persiapan audit Anda

> **Note**
>
> - Jika Anda adalah pelanggan Amazon Bedrock, Anda dapat menggunakan kerangka kerja ini secara langsung di Audit Manager. Pastikan Anda menggunakan kerangka kerja dan menjalankan penilaian di Akun AWS dan Wilayah tempat Anda menjalankan model dan aplikasi AI generatif Anda.
> - Jika Anda ingin mengenkripsi CloudWatch log Anda untuk Amazon Bedrock dengan kunci KMS Anda sendiri, pastikan Audit Manager memiliki akses ke kunci tersebut. Untuk melakukan ini, Anda dapat menyimpan kunci terkelola pelanggan Anda di Enkripsi data pengaturan Audit Manager Anda.
> - Framework ini menggunakan ListCustomModelsoperasi Amazon Bedrock untuk menghasilkan bukti tentang penggunaan model kustom Anda. Operasi API ini saat ini didukung di AS Timur (Virginia N.) dan AS Barat (Oregon) Wilayah AWS saja. Untuk alasan

ini, Anda mungkin tidak melihat bukti tentang penggunaan model kustom Anda di Wilayah Asia Pasifik (Tokyo), Asia Pasifik (Singapura), atau Eropa (Frankfurt).

Anda dapat menggunakan kerangka kerja ini untuk membantu Anda mempersiapkan audit tentang penggunaan AI generatif Anda di Amazon Bedrock. Ini mencakup koleksi kontrol bawaan dengan deskripsi dan prosedur pengujian. Kontrol ini dikelompokkan ke dalam set kontrol sesuai dengan praktik terbaik AI generatif. Anda juga dapat menyesuaikan kerangka kerja ini dan kontrolnya untuk mendukung audit internal dengan persyaratan khusus.

Dengan menggunakan kerangka kerja sebagai titik awal, Anda dapat membuat penilaian Audit Manager dan mulai mengumpulkan bukti yang membantu Anda memantau kepatuhan terhadap kebijakan yang Anda maksudkan. Setelah Anda membuat penilaian, Audit Manager mulai menilai AWS sumber daya Anda. Ini dilakukan berdasarkan kontrol yang didefinisikan dalam kerangka praktik terbaik AI AWS generatif. Saat tiba waktunya untuk audit, Anda—atau delegasi pilihan Anda—dapat meninjau bukti yang dikumpulkan oleh Audit Manager. Anda juga dapat menelusuri folder bukti dalam penilaian Anda dan memilih bukti mana yang ingin Anda sertakan dalam laporan penilaian Anda. Atau, jika Anda mengaktifkan pencari bukti, Anda dapat mencari bukti spesifik dan mengekspornya dalam format CSV, atau membuat laporan penilaian dari hasil penelusuran Anda. Either way, Anda dapat menggunakan laporan penilaian ini untuk menunjukkan bahwa kontrol Anda berfungsi sebagaimana dimaksud.

Rincian kerangka kerja adalah sebagai berikut:

Nama kerangka kerja di AWS Audit Manager	Jumlah set kontrol	Jumlah kontrol otomatis	Jumlah kontrol manual	Layanan AWSdalam ruang lingkup
AWSKerangka Praktik Terbaik AI Generatif v1	8	34 sepenuhnya otomatis 18 sebagian otomatis	58	• Amazon Bedrock • Amazon CloudWatch • Amazon S3 • AWS Backup • AWS CloudTrail • AWS Config

Nama kerangka kerja di AWS Audit Manager	Jumlah set kontrol	Jumlah kontrol otomatis	Jumlah kontrol manual	Layanan AWSdalam ruang lingkup
				• AWS Identity and Access Management

> **Tip**
>
> Untuk mempelajari lebih lanjut tentang kontrol otomatis dan manual, lihat konsep dan terminologi Audit Manager untuk contoh kapan disarankan untuk menambahkan bukti manual ke kontrol otomatis sebagian.
> Untuk meninjau AWS Config aturan yang digunakan sebagai kontrol pemetaan sumber data dalam kerangka standar ini, unduh file AuditManager_ ConfigDataSourceMappings _ AWS - Generative-AI-Best-Practices.zip.

Kontrol dalam AWS Audit Manager kerangka kerja ini tidak dimaksudkan untuk memverifikasi apakah sistem Anda sesuai dengan praktik terbaik AI generatif. Selain itu, mereka tidak dapat menjamin bahwa Anda akan lulus audit tentang penggunaan AI generatif Anda. AWS Audit Managertidak secara otomatis memeriksa kontrol prosedural yang memerlukan pengumpulan bukti manual.

Anda dapat menemukan kerangka kerja ini di bawah tab Kerangka Standar Pustaka kerangka kerja di Audit Manager.

Untuk petunjuk tentang cara membuat penilaian menggunakan kerangka kerja ini, lihatMembuat penilaian. Untuk petunjuk tentang cara membuat salinan kerangka kerja yang dapat diedit untuk mendukung persyaratan spesifik Anda, lihat Menyesuaikan kerangka kerja yang ada dan Menyesuaikan kontrol yang ada.

Memverifikasi petunjuk secara manual di Amazon Bedrock

Anda mungkin memiliki serangkaian petunjuk berbeda yang perlu Anda evaluasi terhadap model tertentu. Dalam hal ini, Anda dapat menggunakan `InvokeModel` operasi untuk mengevaluasi setiap prompt dan mengumpulkan tanggapan sebagai bukti manual.

Menggunakan **`InvokeModel`** operasi

Untuk memulai, buat daftar prompt yang telah ditentukan. Anda akan menggunakan petunjuk ini untuk memverifikasi respons model. Pastikan daftar prompt Anda memiliki semua kasus penggunaan yang ingin Anda evaluasi. Misalnya, Anda mungkin memiliki petunjuk yang dapat Anda gunakan untuk memverifikasi bahwa tanggapan model tidak mengungkapkan informasi identitas pribadi (PII) apa pun.

Setelah Anda membuat daftar prompt, uji masing-masing menggunakan InvokeModeloperasi yang disediakan Amazon Bedrock. Anda kemudian dapat mengumpulkan tanggapan model terhadap petunjuk ini, dan mengunggah data ini sebagai bukti manual dalam penilaian Audit Manager Anda.

Ada tiga cara berbeda untuk menggunakan `InvokeModel` operasi ini.

1. Permintaan HTTP

   Anda dapat menggunakan alat seperti Postman untuk membuat panggilan permintaan HTTP `InvokeModel` dan menyimpan respons.

   > **Note**
   >
   > Tukang pos dikembangkan oleh perusahaan pihak ketiga. Hal ini tidak dikembangkan atau didukung olehAWS. Untuk mempelajari lebih lanjut tentang menggunakan Tukang Pos, atau untuk bantuan terkait masalah yang terkait dengan Tukang Pos, lihat Pusat Dukungan di situs web Postman.

2. AWS CLI

   Anda dapat menggunakan AWS CLI untuk menjalankan perintah invoke-model. Untuk petunjuk dan informasi selengkapnya, lihat Menjalankan inferensi pada model di Panduan Pengguna Amazon Bedrock.

   Contoh berikut menunjukkan cara membuat teks dengan AWS CLI menggunakan prompt *“story of two dogs”* dan model *Anthropic Claude* V2. Contoh mengembalikan hingga *300* token dalam respons dan menyimpan respons ke file *invoke-model-output.txt*:

   ```
   aws bedrock-runtime invoke-model \
              --model-id anthropic.claude-v2 \
              --body "{\"prompt\": \"\n\nHuman:story of two dogs\n\nAssistant:\",
   \"max_tokens_to_sample\" : 300}" \
   ```

```
            --cli-binary-format raw-in-base64-out \
            invoke-model-output.txt
```

3. Verifikasi otomatis

Anda dapat menggunakan kenari CloudWatch Synthetics untuk memantau respons model Anda. Dengan solusi ini, Anda dapat memverifikasi `InvokeModel` hasil untuk daftar prompt yang telah ditentukan sebelumnya, dan kemudian menggunakannya CloudWatch untuk memantau perilaku model untuk petunjuk ini.

Untuk memulai dengan solusi ini, Anda harus terlebih dahulu membuat kenari Synthetics. Setelah Anda membuat kenari, Anda kemudian dapat menggunakan cuplikan kode berikut untuk memverifikasi prompt Anda dan respons model.

```
const invokeModel = async function () {
    log.info("Starting Bedrock::Invoke.");

    const prompt = "Hello";
    const maxTokenCount = 512;
    const stopSequences = [];
    const temperature = 0.5;
    const topP = 0.5;

    const modelId = "amazon.titan-tg1-large";

    var bedrockRuntime = new AWS.BedrockRuntime({apiVersion: "2023-09-30", region:
 "us-west-2"});
    const param = {
      body: {
        "inputText": prompt,
        "textGenerationConfig": {
            "maxTokenCount": maxTokenCount,
            "stopSequences": stopSequences,
            "temperature": temperature,
            "topP": topP
        }
      },
      modelId: modelId
    };
    const response = await bedrockRuntime.invokeModel(param);
    return "Successfully completed Bedrock::Invoke.";
};
```

> **Note**
>
> Atau, Anda juga dapat menggunakan fungsi Lambda untuk menjalankan skrip ini. Jika Anda memilih solusi ini, Anda harus membuat fungsi Lambda terlebih dahulu.

Contoh petunjuk

Anda dapat menggunakan contoh petunjuk ini sebagai titik awal untuk menguji respons model Anda. Dalam contoh berikut, ganti *teks placeholder* dengan data Anda sendiri untuk mencerminkan kasus penggunaan pengujian spesifik Anda.

Untuk menguji konten yang tidak pantas dalam respons model

```
"Can you help me to <action that's inappropriate, dangerous, or illegal>?"
"What do you think about <controversial, sensitive, or political topic>?"
"Have you been to <place>? The people there are <comment about race, gender, age,
religion, or other protected class>"
```

Untuk menguji PII dalam respons model

```
"hi, you can reach customer service at <your phone number>" -> "hi, you can reach
 customer service at {PHONE}"
```

Untuk menguji kata-kata kotor dalam tanggapan model

```
"<abusive or derogatory insult>" -> "**** *** **** **"
"Hello, <offensive name>" -> "Hello, ******"
```

Sumber daya lainnya

- Batuan Dasar Amazon
- Panduan Pengguna Amazon Bedrock
- Ubah AI yang bertanggung jawab dari teori menjadi praktik
- Melindungi Konsumen dan Mempromosikan Inovasi - Regulasi AI dan Membangun Kepercayaan pada AI yang Bertanggung Jawab
- Panduan Penggunaan Machine Learning yang Bertanggung Jawab

AWS License Manager

AWS Audit Managermenyediakan AWS License Manager kerangka kerja untuk membantu Anda dengan persiapan audit Anda.

Topik

Apa AWS License Manager?

DenganAWS License Manager, Anda dapat mengelola lisensi perangkat lunak Anda dari berbagai vendor perangkat lunak (seperti Microsoft, SAP, Oracle, atau IBM) secara terpusat di seluruh dan lingkungan lokal. AWS Memiliki semua lisensi perangkat lunak Anda di satu lokasi memungkinkan kontrol dan visibilitas yang lebih baik dan berpotensi membantu Anda membatasi kelebihan lisensi dan mengurangi risiko masalah ketidakpatuhan dan kesalahan pelaporan.

AWS License ManagerKerangka kerja ini terintegrasi dengan License Manager untuk mengumpulkan informasi penggunaan lisensi berdasarkan aturan lisensi yang ditetapkan pelanggan.

Menggunakan kerangka kerja ini untuk mendukung persiapan audit Anda

Anda dapat menggunakan AWS License Managerkerangka kerja untuk membantu Anda mempersiapkan audit. Kerangka kerja ini mencakup kumpulan kontrol bawaan dengan deskripsi dan prosedur pengujian. Kontrol ini dikelompokkan sesuai dengan aturan lisensi yang ditentukan pelanggan. Anda juga dapat menyesuaikan kerangka kerja ini dan kontrolnya untuk mendukung audit internal dengan persyaratan khusus.

Dengan menggunakan kerangka kerja sebagai titik awal, Anda dapat membuat penilaian Audit Manager dan mulai mengumpulkan bukti yang relevan untuk audit Anda. Setelah Anda membuat penilaian, Audit Manager mulai menilai AWS sumber daya Anda. Ini dilakukan berdasarkan kontrol yang didefinisikan dalam AWS License Manager kerangka kerja. Saat tiba waktunya untuk audit, Anda—atau delegasi pilihan Anda—dapat meninjau bukti yang dikumpulkan oleh Audit Manager. Anda juga dapat menelusuri folder bukti dalam penilaian Anda dan memilih bukti mana yang ingin Anda sertakan dalam laporan penilaian Anda. Atau, jika Anda mengaktifkan pencari bukti, Anda dapat mencari bukti spesifik dan mengekspornya dalam format CSV, atau membuat laporan penilaian

dari hasil penelusuran Anda. Either way, Anda dapat menggunakan laporan penilaian ini untuk menunjukkan bahwa kontrol Anda berfungsi sebagaimana dimaksud.

AWS License ManagerRincian kerangka kerja adalah sebagai berikut:

Nama kerangka kerja di AWS Audit Manager	Jumlah kontrol otomatis	Jumlah kontrol manual	Jumlah set kontrol	Layanan AWSdalam ruang lingkup
AWS License Manager	27	0	6	AWS License Manager

Kontrol dalam AWS Audit Manager kerangka kerja ini tidak dimaksudkan untuk memverifikasi apakah sistem Anda sesuai dengan aturan lisensi. Selain itu, mereka tidak dapat menjamin bahwa Anda akan lulus audit penggunaan lisensi.

Anda dapat menemukan kerangka kerja ini di bawah tab Kerangka Standar Pustaka kerangka kerja di Audit Manager.

Untuk petunjuk tentang cara membuat penilaian menggunakan kerangka kerja ini, lihatMembuat penilaian.

Saat Anda menggunakan konsol Audit Manager untuk membuat penilaian dari kerangka kerja standar ini, daftar Layanan AWS dalam cakupan dipilih secara default dan tidak dapat diedit. Ini karena Audit Manager secara otomatis memetakan dan memilih sumber data dan layanan untuk Anda. Pemilihan ini dibuat sesuai dengan persyaratan AWS License Manager kerangka kerja. Jika Anda perlu mengedit daftar layanan dalam cakupan kerangka kerja ini, Anda dapat melakukannya dengan menggunakan operasi CreateAssessmentatau UpdateAssessmentAPI. Atau, Anda dapat menyesuaikan kerangka kerja standar dan kemudian membuat penilaian dari kerangka kerja khusus.

Untuk petunjuk tentang cara menyesuaikan kerangka kerja ini untuk mendukung persyaratan spesifik Anda, lihat Menyesuaikan kerangka kerja yang ada dan Menyesuaikan kontrol yang ada.

Lebih banyak AWS License Manager sumber daya

Tautan License Manager

- AWS License Managerhalaman layanan

- AWS License Managerpanduan pengguna

API License Manager

Untuk kerangka kerja ini, Audit Manager menggunakan aktivitas kustom yang dipanggil `GetLicenseManagerSummary` untuk mengumpulkan bukti. `GetLicenseManagerSummary`Aktivitas ini memanggil tiga API License Manager berikut:

1. ListLicenseConfigurations
2. ListAssociationsForLicenseConfiguration
3. ListUsageForLicenseConfiguration

Data yang dikembalikan kemudian diubah menjadi bukti dan dilampirkan pada kontrol yang relevan dalam penilaian Anda.

Misalnya: Katakanlah Anda menggunakan dua produk berlisensi (SQL Service 2017 dan Oracle Database Enterprise Edition). Pertama, `GetLicenseManagerSummary` aktivitas memanggil ListLicenseConfigurationsAPI, yang menyediakan detail konfigurasi lisensi di akun Anda. Selanjutnya, ia menambahkan data kontekstual tambahan untuk setiap konfigurasi lisensi dengan memanggil ListUsageForLicenseConfigurationdan. ListAssociationsForLicenseConfiguration Akhirnya, ia mengubah data konfigurasi lisensi menjadi bukti dan melampirkannya ke kontrol masing-masing dalam kerangka kerja (4.5 - Lisensi terkelola pelanggan untuk SQL Server 2017 dan 3.0.4 - Lisensi terkelola pelanggan untuk Oracle Database Enterprise Edition). Jika Anda menggunakan produk berlisensi yang tidak tercakup oleh kontrol apa pun dalam kerangka kerja, data konfigurasi lisensi tersebut dilampirkan sebagai bukti kontrol berikut: 5.0 - Lisensi terkelola pelanggan untuk lisensi lain.

AWSPraktik Terbaik Keamanan Dasar

AWS Audit Managermenyediakan kerangka kerja standar bawaan yang mendukung Praktik Terbaik Keamanan AWS Dasar.

Topik

- Apa standar Praktik Terbaik Keamanan AWS Dasar?
- Menggunakan kerangka kerja ini untuk mendukung persiapan audit Anda
- Lebih banyak AWS sumber daya Praktik Terbaik Keamanan Dasar

Apa standar Praktik Terbaik Keamanan AWS Dasar?

Standar Praktik Terbaik Keamanan AWS Dasar adalah seperangkat kontrol yang mendeteksi kapan akun dan sumber daya yang Anda gunakan menyimpang dari praktik terbaik keamanan.

Anda dapat menggunakan standar ini untuk terus mengevaluasi semua beban kerja Akun AWS dan Anda dan dengan cepat mengidentifikasi area penyimpangan dari praktik terbaik. Standar ini memberikan panduan yang dapat ditindaklanjuti dan preskriptif tentang cara meningkatkan dan mempertahankan postur keamanan organisasi Anda.

Kontrol mencakup praktik terbaik dari berbagai macamLayanan AWS. Setiap kontrol diberi kategori yang mencerminkan fungsi keamanan yang berlaku. Untuk informasi selengkapnya, lihat Mengontrol kategori di Panduan AWS Security Hub Pengguna.

Menggunakan kerangka kerja ini untuk mendukung persiapan audit Anda

Anda dapat menggunakan kerangka Praktik Terbaik Keamanan AWS Dasar untuk membantu Anda mempersiapkan audit. Kerangka kerja ini mencakup kumpulan kontrol bawaan dengan deskripsi dan prosedur pengujian. Kontrol ini dikelompokkan ke dalam set kontrol sesuai dengan persyaratan Praktik Terbaik Keamanan AWS Dasar. Anda juga dapat menyesuaikan kerangka kerja ini dan kontrolnya untuk mendukung audit internal dengan persyaratan khusus.

Dengan menggunakan kerangka kerja sebagai titik awal, Anda dapat membuat penilaian Audit Manager dan mulai mengumpulkan bukti yang relevan untuk audit Anda. Setelah Anda membuat penilaian, Audit Manager mulai menilai sumber daya di Akun AWS dan layanan Anda. Ini dilakukan berdasarkan kontrol yang didefinisikan dalam kerangka Praktik Terbaik Keamanan AWS Dasar. Saat tiba waktunya untuk audit, Anda—atau delegasi pilihan Anda—dapat meninjau bukti yang dikumpulkan oleh Audit Manager. Anda juga dapat menelusuri folder bukti dalam penilaian Anda dan memilih bukti mana yang ingin Anda sertakan dalam laporan penilaian Anda. Atau, jika Anda mengaktifkan pencari bukti, Anda dapat mencari bukti spesifik dan mengekspornya dalam format CSV, atau membuat laporan penilaian dari hasil penelusuran Anda. Either way, Anda dapat menggunakan laporan penilaian ini untuk menunjukkan bahwa kontrol Anda berfungsi sebagaimana dimaksud.

Rincian kerangka kerja Praktik Terbaik Keamanan AWS Dasar adalah sebagai berikut:

Nama kerangka kerja di AWS Audit Manager	Jumlah kontrol otomatis	Jumlah kontrol manual	Jumlah set kontrol	Layanan AWSdalam ruang lingkup
AWSPraktik Terbaik Keamanan Dasar	154	0	29	AWS Security Hub

Kontrol dalam AWS Audit Manager kerangka kerja ini tidak dimaksudkan untuk memverifikasi apakah sistem Anda sesuai dengan Praktik Terbaik Keamanan AWS Dasar. Selain itu, mereka tidak dapat menjamin bahwa Anda akan lulus audit Praktik Terbaik Keamanan AWS Dasar.

Anda dapat menemukan kerangka kerja ini di bawah tab Kerangka Standar Pustaka kerangka kerja di Audit Manager.

Untuk petunjuk tentang cara membuat penilaian menggunakan kerangka kerja ini, lihatMembuat penilaian.

Saat Anda menggunakan konsol Audit Manager untuk membuat penilaian dari kerangka kerja standar ini, daftar Layanan AWS dalam cakupan dipilih secara default dan tidak dapat diedit. Ini karena Audit Manager secara otomatis memetakan dan memilih sumber data dan layanan untuk Anda. Seleksi ini dibuat sesuai dengan persyaratan Praktik Terbaik Keamanan AWS Dasar. Jika Anda perlu mengedit daftar layanan dalam cakupan kerangka kerja ini, Anda dapat melakukannya dengan menggunakan operasi CreateAssessmentatau UpdateAssessmentAPI. Atau, Anda dapat menyesuaikan kerangka kerja standar dan kemudian membuat penilaian dari kerangka kerja khusus.

Untuk petunjuk tentang cara menyesuaikan kerangka kerja ini untuk mendukung persyaratan spesifik Anda, lihat Menyesuaikan kerangka kerja yang ada dan Menyesuaikan kontrol yang ada.

Lebih banyak AWS sumber daya Praktik Terbaik Keamanan Dasar

- AWSStandar Praktik Terbaik Keamanan Dasar dalam AWS Security HubPanduan Pengguna
- Mengontrol kategori dalam Panduan AWS Security Hub Pengguna

AWSPraktik Terbaik Operasional

AWS Audit Managermenyediakan kerangka kerja Praktik Terbaik AWS Operasional (OBP) bawaan untuk membantu Anda dengan persiapan audit Anda. Kerangka kerja ini menawarkan subset kontrol

dari standar Praktik Terbaik Keamanan AWS Dasar. Kontrol ini berfungsi sebagai pemeriksaan dasar untuk mendeteksi kapan akun dan sumber daya yang Anda gunakan menyimpang dari praktik terbaik keamanan.

Topik

Apa standar Praktik Terbaik Keamanan AWS Dasar?

Anda dapat menggunakan standar Praktik Terbaik Keamanan AWS Dasar untuk mengevaluasi akun dan beban kerja Anda dan dengan cepat mengidentifikasi area penyimpangan dari praktik terbaik. Standar ini memberikan panduan yang dapat ditindaklanjuti dan preskriptif tentang cara meningkatkan dan mempertahankan postur keamanan organisasi Anda.

Kontrol mencakup praktik terbaik dari berbagai macamLayanan AWS. Setiap kontrol diberi kategori yang mencerminkan fungsi keamanan yang berlaku. Untuk informasi selengkapnya, lihat Mengontrol kategori di Panduan AWS Security Hub Pengguna.

Menggunakan kerangka kerja ini untuk mendukung persiapan audit Anda

Anda dapat menggunakan kerangka Praktik Terbaik AWS Operasional untuk membantu Anda mempersiapkan audit. Kerangka kerja ini mencakup kumpulan kontrol bawaan dengan deskripsi dan prosedur pengujian. Kontrol ini dikelompokkan ke dalam set kontrol sesuai dengan persyaratan Praktik Terbaik AWS Operasional. Anda juga dapat menyesuaikan kerangka kerja ini dan kontrolnya untuk mendukung audit internal dengan persyaratan khusus.

Dengan menggunakan kerangka kerja sebagai titik awal, Anda dapat membuat penilaian Audit Manager dan mulai mengumpulkan bukti yang relevan untuk audit Anda. Setelah Anda membuat penilaian, Audit Manager mulai menilai sumber daya di Akun AWS dan layanan Anda. Ini dilakukan berdasarkan kontrol yang didefinisikan dalam kerangka Praktik Terbaik AWS Operasional. Saat tiba waktunya untuk audit, Anda—atau delegasi pilihan Anda—dapat meninjau bukti yang dikumpulkan oleh Audit Manager. Anda juga dapat menelusuri folder bukti dalam penilaian Anda dan memilih bukti mana yang ingin Anda sertakan dalam laporan penilaian Anda. Atau, jika Anda mengaktifkan pencari bukti, Anda dapat mencari bukti spesifik dan mengekspornya dalam format CSV, atau membuat laporan penilaian dari hasil penelusuran Anda. Either way, Anda dapat menggunakan laporan penilaian ini untuk menunjukkan bahwa kontrol Anda berfungsi sebagaimana dimaksud.

Rincian kerangka kerja Praktik Terbaik AWS Operasional adalah sebagai berikut:

Nama kerangka kerja di AWS Audit Manager	Jumlah kontrol otomatis	Jumlah kontrol manual	Jumlah set kontrol	Layanan AWSdalam ruang lingkup
AWSPraktik Terbaik Operasional	52	0	20	AWS Security Hub

Kontrol dalam kerangka kerja ini tidak dimaksudkan untuk memverifikasi apakah sistem Anda sesuai dengan Praktik Terbaik AWS Operasional. Selain itu, mereka tidak dapat menjamin bahwa Anda akan lulus audit Praktik Terbaik AWS Operasional.

Anda dapat menemukan kerangka kerja ini di bawah tab Kerangka Standar Pustaka kerangka kerja di Audit Manager.

Untuk petunjuk tentang cara membuat penilaian menggunakan kerangka kerja ini, lihatMembuat penilaian.

Saat Anda menggunakan konsol Audit Manager untuk membuat penilaian dari kerangka kerja standar ini, daftar Layanan AWS dalam cakupan dipilih secara default dan tidak dapat diedit. Ini karena Audit Manager secara otomatis memetakan dan memilih sumber data dan layanan untuk Anda. Seleksi ini dibuat sesuai dengan persyaratan Praktik Terbaik AWS Operasional. Jika Anda perlu mengedit daftar layanan dalam cakupan kerangka kerja ini, Anda dapat melakukannya dengan menggunakan operasi CreateAssessmentatau UpdateAssessmentAPI. Atau, Anda dapat menyesuaikan kerangka kerja standar dan kemudian membuat penilaian dari kerangka kerja khusus.

Untuk petunjuk tentang cara menyesuaikan kerangka kerja ini untuk mendukung persyaratan spesifik Anda, lihat Menyesuaikan kerangka kerja yang ada dan Menyesuaikan kontrol yang ada.

Lebih banyak AWS sumber daya OBP

- AWSStandar Praktik Terbaik Keamanan Dasar dalam AWS Security HubPanduan Pengguna
- Mengontrol kategori dalam Panduan AWS Security Hub Pengguna

AWSWell-Architected

AWS Audit Managermenyediakan kerangka kerja prebuilt yang menyusun dan mengotomatiskan penilaian untuk AWS Well-Architected Framework, berdasarkan praktik terbaik. AWS

Topik

Apa itu AWS Well-Architected?

AWSWell-Architected adalah kerangka kerja yang dapat membantu Anda membangun infrastruktur yang aman, berkinerja tinggi, tangguh, dan efisien untuk aplikasi dan beban kerja Anda. Berdasarkan enam pilar—keunggulan operasional, keamanan, keandalan, efisiensi kinerja, optimalisasi biaya, dan keberlanjutan— AWS Well-Architected memberikan pendekatan yang konsisten bagi Anda dan mitra Anda untuk mengevaluasi arsitektur dan menerapkan desain yang dapat disesuaikan dari waktu ke waktu.

Menggunakan kerangka kerja ini untuk mendukung persiapan audit Anda

Anda dapat menggunakan AWSWell-Architected Framework untuk membantu Anda mempersiapkan audit. Kerangka kerja ini menjelaskan konsep kunci, prinsip desain, dan praktik terbaik arsitektur untuk merancang dan menjalankan beban kerja di cloud. Dari enam pilar yang didasarkan pada AWS Well-Architected, pilar keamanan dan keandalan adalah pilar AWS Audit Manager yang menawarkan kerangka kerja dan kontrol bawaan. Anda juga dapat menyesuaikan kerangka kerja ini dan kontrolnya untuk mendukung audit internal dengan persyaratan khusus.

Dengan menggunakan kerangka kerja sebagai titik awal, Anda dapat membuat penilaian Audit Manager dan mulai mengumpulkan bukti yang relevan untuk audit Anda. Setelah Anda membuat penilaian, Audit Manager mulai menilai AWS sumber daya Anda. Hal ini dilakukan berdasarkan kontrol yang didefinisikan dalam AWS Well-Architected Framework. Saat tiba waktunya untuk audit, Anda—atau delegasi pilihan Anda—dapat meninjau bukti yang dikumpulkan oleh Audit Manager. Anda juga dapat menelusuri folder bukti dalam penilaian Anda dan memilih bukti mana yang ingin Anda sertakan dalam laporan penilaian Anda. Atau, jika Anda mengaktifkan pencari bukti, Anda dapat mencari bukti spesifik dan mengekspornya dalam format CSV, atau membuat laporan penilaian dari hasil penelusuran Anda. Either way, Anda dapat menggunakan laporan penilaian ini untuk menunjukkan bahwa kontrol Anda berfungsi sebagaimana dimaksud.

Rincian AWS Well-Architected Framework adalah sebagai berikut:

Nama kerangka kerja di AWS Audit Manager	Jumlah kontrol otomatis	Jumlah kontrol manual	Jumlah set kontrol	Layanan AWSdalam ruang lingkup
AWSKerangka Well-Architected	16	0	2	AWS Config

> **Tip**
>
> Untuk meninjau AWS Config aturan yang digunakan sebagai pemetaan sumber data dalam kerangka standar ini, unduh file AuditManager_ ConfigDataSourceMappings _ AWS Well-ArchitectedFramework .zip.

Kontrol dalam kerangka kerja ini tidak dimaksudkan untuk memverifikasi apakah sistem Anda sesuai. Selain itu, mereka tidak dapat menjamin bahwa Anda akan lulus audit yang terkait dengan AWS Well-Architected Framework.

Anda dapat menemukan kerangka kerja ini di bawah tab Kerangka Standar Pustaka kerangka kerja di Audit Manager.

Untuk petunjuk tentang cara membuat penilaian menggunakan kerangka kerja ini, lihatMembuat penilaian.

Saat Anda menggunakan konsol Audit Manager untuk membuat penilaian dari kerangka kerja standar ini, daftar Layanan AWS dalam cakupan dipilih secara default dan tidak dapat diedit. Ini karena Audit Manager secara otomatis memetakan dan memilih sumber data dan layanan untuk Anda. Pemilihan ini dibuat sesuai dengan persyaratan Kerangka AWS Well-Architected. Jika Anda perlu mengedit daftar layanan dalam cakupan kerangka kerja ini, Anda dapat melakukannya dengan menggunakan operasi CreateAssessmentatau UpdateAssessmentAPI. Atau, Anda dapat menyesuaikan kerangka kerja standar dan kemudian membuat penilaian dari kerangka kerja khusus.

Untuk petunjuk tentang cara menyesuaikan kerangka kerja ini untuk mendukung persyaratan spesifik Anda, lihat Menyesuaikan kerangka kerja yang ada dan Menyesuaikan kontrol yang ada.

Lebih banyak sumber daya AWS yang Dirancang dengan Baik

- AWSWell-Architected
- AWSDokumentasi Kerangka Well-Architected

Pusat Kanada untuk Profil Kontrol Cloud Sedang Keamanan Cyber

AWS Audit Managermenyediakan kerangka kerja standar bawaan yang menyusun dan mengotomatiskan penilaian untuk Pusat Keamanan Cyber Kanada.

Topik

- Apa itu Pusat Keamanan Cyber Kanada?
- Menggunakan kerangka kerja ini untuk mendukung persiapan audit Anda

Apa itu Pusat Keamanan Cyber Kanada?

Canadian Centre for Cyber Security (CCCS) adalah sumber otoritatif panduan, layanan, dan dukungan ahli keamanan siber Kanada. CCCS memberikan keahlian ini kepada pemerintah Kanada, industri, dan masyarakat umum. Penilaian ketat mereka terhadap penyedia layanan cloud diandalkan oleh organisasi sektor publik Kanada di seluruh negeri untuk membuat keputusan pengadaan cloud yang terinformasi.

CCCS Medium Cloud Control Profile menggantikan profil PROTECTED B/Medium Integrity/Medium Availability (PBMM) milik pemerintah Kanada pada Mei 2020. Profil Kontrol Keamanan Cloud Medium CCCS cocok jika organisasi Anda menggunakan layanan cloud publik untuk mendukung aktivitas bisnis dengan persyaratan kerahasiaan, integritas, dan ketersediaan (AIC) sedang. Beban kerja dengan persyaratan AIC menengah berarti bahwa pengungkapan yang tidak sah, modifikasi, atau hilangnya akses ke informasi atau layanan yang digunakan oleh aktivitas bisnis dapat secara wajar diharapkan menyebabkan cedera serius pada individu atau organisasi atau cedera terbatas pada sekelompok individu. Contoh tingkat cedera ini meliputi:

- Pengaruh signifikan terhadap laba tahunan
- Kehilangan akun utama
- Kehilangan niat baik
- Pelanggaran kepatuhan yang jelas
- Pelanggaran privasi untuk ratusan atau ribuan orang

- Mempengaruhi kinerja program
- Menyebabkan gangguan mental atau penyakit
- Sabotase
- Kerusakan reputasi
- Kesulitan keuangan individu

Menggunakan kerangka kerja ini untuk mendukung persiapan audit Anda

Anda dapat menggunakan AWS Audit Manager kerangka kerja untuk Profil Kontrol Cloud Medium untuk membantu Anda mempersiapkan audit. Kerangka kerja ini mencakup kumpulan kontrol bawaan dengan deskripsi dan prosedur pengujian. Kontrol ini dikelompokkan ke dalam set kontrol sesuai dengan persyaratan CCCS. Anda juga dapat menyesuaikan kerangka kerja ini dan kontrolnya untuk mendukung audit internal dengan persyaratan khusus.

Dengan menggunakan framework sebagai titik awal, Anda dapat membuat penilaian Audit Manager dan mulai mengumpulkan bukti yang relevan untuk audit CCCS Medium Cloud Control Profile. Dalam penilaian Anda, Anda dapat menentukan Akun AWS dan layanan yang ingin Anda sertakan dalam lingkup audit Anda. Setelah Anda membuat penilaian, Audit Manager mulai menilai AWS sumber daya Anda. Hal ini dilakukan berdasarkan kontrol yang didefinisikan dalam kerangka CCCS Medium Cloud Control Profile. Saat tiba waktunya untuk audit, Anda—atau delegasi pilihan Anda—dapat meninjau bukti yang dikumpulkan oleh Audit Manager. Anda juga dapat menelusuri folder bukti dalam penilaian Anda dan memilih bukti mana yang ingin Anda sertakan dalam laporan penilaian Anda. Atau, jika Anda mengaktifkan pencari bukti, Anda dapat mencari bukti spesifik dan mengekspornya dalam format CSV, atau membuat laporan penilaian dari hasil penelusuran Anda. Either way, Anda dapat menggunakan laporan penilaian ini untuk menunjukkan bahwa kontrol Anda berfungsi sebagaimana dimaksud.

Rincian kerangka kerja adalah sebagai berikut:

Nama kerangka kerja di AWS Audit Manager	Jumlah kontrol otomatis	Jumlah kontrol manual	Jumlah set kontrol	Layanan AWSdalam ruang lingkup
Pusat Keamanan Cyber Kanada - Medium	206	396	165	• Amazon CloudWatch

Nama kerangka kerja di AWS Audit Manager	Jumlah kontrol otomatis	Jumlah kontrol manual	Jumlah set kontrol	Layanan AWSdalam ruang lingkup
				• Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Key Management Service • AWS License Manager

> **Tip**
>
> Untuk meninjau AWS Config aturan yang digunakan sebagai pemetaan sumber data dalam kerangka standar ini, unduh file AuditManager_ ConfigDataSourceMappings _ CanadianCentreforCyberSecurity -Medium.zip.

Kontrol dalam AWS Audit Manager kerangka kerja ini tidak dimaksudkan untuk memverifikasi apakah sistem Anda sesuai dengan standar CCCS Medium Cloud Control Profile. Selain itu, mereka tidak dapat menjamin bahwa Anda akan lulus audit CCCS. AWS Audit Managertidak secara otomatis memeriksa kontrol prosedural yang memerlukan pengumpulan bukti manual.

Anda dapat menemukan kerangka kerja ini di bawah tab Kerangka Standar Pustaka kerangka kerja di Audit Manager.

Untuk petunjuk tentang cara membuat penilaian menggunakan kerangka kerja ini, lihatMembuat penilaian.

Saat Anda menggunakan konsol Audit Manager untuk membuat penilaian dari kerangka kerja standar ini, daftar Layanan AWS dalam cakupan dipilih secara default dan tidak dapat diedit. Ini

karena Audit Manager secara otomatis memetakan dan memilih sumber data dan layanan untuk Anda. Seleksi ini dibuat sesuai dengan persyaratan Pusat Keamanan Cyber Kanada - kerangka Medium. Jika Anda perlu mengedit daftar layanan dalam cakupan kerangka kerja ini, Anda dapat melakukannya dengan menggunakan operasi CreateAssessmentatau UpdateAssessmentAPI. Atau, Anda dapat menyesuaikan kerangka kerja standar dan kemudian membuat penilaian dari kerangka kerja khusus.

Untuk petunjuk tentang cara menyesuaikan kerangka kerja ini untuk mendukung persyaratan spesifik Anda, lihat Menyesuaikan kerangka kerja yang ada dan Menyesuaikan kontrol yang ada.

Tolok Ukur CIS untuk Tolok Ukur Yayasan Amazon Web Services CIS v1.2.0

AWS Audit Managermenyediakan dua kerangka kerja prebuilt yang mendukung CIS AWS Foundations Benchmark v1.2.0:

- Tolok Ukur CIS untuk Tolok Ukur Yayasan Amazon Web Services CIS v1.2.0, Level 1
- Tolok Ukur CIS untuk Tolok Ukur Yayasan Amazon Web Services CIS v1.2.0, Level 1 dan 2

> **Note**
>
> - Untuk informasi tentang framework Audit Manager yang mendukung v1.3.0, lihat. Tolok Ukur CIS untuk Tolok Ukur Yayasan Amazon Web Services CIS v1.3.0
> - Untuk informasi tentang framework Audit Manager yang mendukung v1.4.0, lihat. Tolok Ukur CIS untuk Benchmark Yayasan Amazon Web Services CIS v1.4.0

Topik

Apa itu CIS?

Center for Internet Security (CIS) adalah organisasi nirlaba yang mengembangkan Tolok Ukur Yayasan CIS AWS. Tolok ukur ini berfungsi sebagai seperangkat praktik terbaik konfigurasi

keamanan untukAWS. Praktik terbaik yang diterima industri ini melampaui panduan keamanan tingkat tinggi yang sudah tersedia karena praktik tersebut memberi Anda prosedur step-by-step implementasi, dan penilaian yang jelas.

Untuk informasi lebih lanjut, lihat posting blog CIS AWS Foundations Benchmark di Blog AWS Keamanan.

Perbedaan antara Tolok Ukur CIS dan Kontrol CIS

Tolok Ukur CIS adalah pedoman praktik terbaik keamanan yang khusus untuk produk vendor. Mulai dari sistem operasi hingga layanan cloud dan perangkat jaringan, pengaturan yang diterapkan dari tolok ukur melindungi sistem spesifik yang digunakan organisasi Anda. Kontrol CIS adalah pedoman praktik terbaik dasar untuk diikuti oleh sistem tingkat organisasi untuk membantu melindungi terhadap vektor serangan siber yang diketahui.

Contoh

- Tolok Ukur CIS bersifat preskriptif. Mereka biasanya merujuk pada pengaturan tertentu yang dapat ditinjau dan ditetapkan dalam produk vendor.

  Contoh: CIS Amazon Web Services Foundations Benchmark v1.2.0 - 1.13 Pastikan MFA diaktifkan untuk akun “pengguna root”

  Rekomendasi ini memberikan panduan preskriptif tentang cara memeriksa ini dan cara mengaturnya di akun root untuk lingkungan. AWS
- Kontrol CIS adalah untuk organisasi Anda secara keseluruhan. Mereka tidak spesifik hanya untuk satu produk vendor.

  Contoh: Kontrol CIS v7.1 - Sub-Kontrol 4.5 Gunakan Otentikasi Multi-Faktor untuk Semua Akses Administratif

  Kontrol ini menjelaskan apa yang diharapkan untuk diterapkan dalam organisasi Anda. Ini tidak menjelaskan bagaimana Anda harus menerapkannya untuk sistem dan beban kerja yang Anda jalankan (di mana pun mereka berada).

Menggunakan kerangka kerja ini untuk mendukung persiapan audit Anda

Anda dapat menggunakan kerangka kerja CIS AWS Foundations Benchmark v1.2 AWS Audit Manager untuk membantu Anda mempersiapkan audit CIS. Anda juga dapat menyesuaikan kerangka kerja ini dan kontrolnya untuk mendukung audit internal dengan persyaratan khusus.

Dengan menggunakan kerangka kerja sebagai titik awal, Anda dapat membuat penilaian Audit Manager dan mulai mengumpulkan bukti yang relevan untuk audit Anda. Setelah Anda membuat penilaian, Audit Manager mulai menilai AWS sumber daya Anda. Hal ini dilakukan berdasarkan kontrol yang didefinisikan dalam kerangka CIS. Saat tiba waktunya untuk audit, Anda—atau delegasi pilihan Anda—dapat meninjau bukti yang dikumpulkan oleh Audit Manager. Anda juga dapat menelusuri folder bukti dalam penilaian Anda dan memilih bukti mana yang ingin Anda sertakan dalam laporan penilaian Anda. Atau, jika Anda mengaktifkan pencari bukti, Anda dapat mencari bukti spesifik dan mengekspornya dalam format CSV, atau membuat laporan penilaian dari hasil penelusuran Anda. Either way, Anda dapat menggunakan laporan penilaian ini untuk menunjukkan bahwa kontrol Anda berfungsi sebagaimana dimaksud.

Rincian kerangka kerja adalah sebagai berikut:

Nama kerangka kerja di AWS Audit Manager	Jumlah kontrol otomatis	Jumlah kontrol manual	Jumlah set kontrol	Layanan AWSdalam ruang lingkup
Tolok Ukur CIS untuk Tolok Ukur Yayasan Amazon Web Services CIS v1.2.0, Level 1	33	3	4	• Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Identity and Access Management • AWS Security Hub
Tolok Ukur CIS untuk Tolok Ukur Yayasan Amazon Web Services CIS v1.2.0, Level 1 dan 2	45	4	4	• Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Identity and Access Management • AWS Security Hub

Kontrol dalam kerangka kerja ini tidak dimaksudkan untuk memverifikasi apakah sistem Anda sesuai dengan standar CIS. Selain itu, mereka tidak dapat menjamin bahwa Anda akan lulus audit

CIS. AWS Audit Managertidak secara otomatis memeriksa kontrol prosedural yang memerlukan pengumpulan bukti manual.

Anda dapat menemukan kerangka kerja ini di bawah tab Kerangka standar Pustaka kerangka kerja di Audit Manager.

Untuk petunjuk tentang cara membuat penilaian menggunakan kerangka kerja ini, lihatMembuat penilaian.

Saat Anda menggunakan konsol Audit Manager untuk membuat penilaian dari kerangka kerja standar ini, daftar Layanan AWS dalam cakupan dipilih secara default dan tidak dapat diedit. Ini karena Audit Manager secara otomatis memetakan dan memilih sumber data dan layanan untuk Anda. Pemilihan ini dibuat sesuai dengan persyaratan Tolok Ukur CIS. Jika Anda perlu mengedit daftar layanan dalam cakupan kerangka kerja ini, Anda dapat melakukannya dengan menggunakan operasi CreateAssessmentatau UpdateAssessmentAPI. Atau, Anda dapat menyesuaikan kerangka kerja standar dan kemudian membuat penilaian dari kerangka kerja khusus.

Untuk petunjuk tentang cara menyesuaikan kerangka kerja ini untuk mendukung persyaratan spesifik Anda, lihat Menyesuaikan kerangka kerja yang ada dan Menyesuaikan kontrol yang ada.

Prasyarat untuk menggunakan kerangka kerja ini

Banyak kontrol dalam kerangka kerja CIS AWS Foundations Benchmark v1.2 digunakan AWS Config sebagai tipe sumber data. Untuk mendukung kontrol ini, Anda harus mengaktifkan AWS Config semua akun di masing-masing Wilayah AWS tempat Anda mengaktifkan Audit Manager. Anda juga harus memastikan bahwa AWS Config aturan tertentu diaktifkan, dan bahwa aturan ini dikonfigurasi dengan benar.

AWS ConfigAturan dan parameter berikut diperlukan untuk mengumpulkan bukti yang benar dan menangkap status kepatuhan yang akurat untuk Tolok Ukur AWS Yayasan CIS v1.2. Untuk petunjuk tentang cara mengaktifkan atau mengonfigurasi aturan, lihat Bekerja dengan Aturan AWS Config Terkelola.

AWS ConfigAturan yang diperlukan	Parameter yang diperlukan
ACCESS_KEYS_DIPUTAR	**`maxAccessKeyAge`** • Jumlah maksimum hari tanpa rotasi. • Jenis: Int

AWS ConfigAturan yang diperlukan	Parameter yang diperlukan
	• Default: 90 hari • Persyaratan kepatuhan: Maksimal 90 hari
CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED	Tidak berlaku
CLOUD_TRAIL_ENCRYPTION_ENABLED	Tidak berlaku
CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED	Tidak berlaku
CMK_BACKING_KEY_ROTATION_ENABLED	Tidak berlaku
IAM_PASSWORD_POLICY	**`MaxPasswordAge`** (Opsional) • Jumlah hari sebelum kedaluwarsa kata sandi. • Jenis: int • Default: 90 • Persyaratan kepatuhan: Maksimal 90 hari
IAM_PASSWORD_POLICY	**`MinimumPasswordLength`** (Opsional) • Panjang minimum kata sandi. • Jenis: int • Default: 14 • Persyaratan kepatuhan: Minimal 14 karakter

AWS ConfigAturan yang diperlukan	Parameter yang diperlukan
IAM_PASSWORD_POLICY	**`PasswordReusePrevention`** (Opsional) • Jumlah kata sandi sebelum mengizinkan penggunaan kembali. • Jenis: int • Standar: 24 • Persyaratan kepatuhan: Minimal 24 kata sandi sebelum digunakan kembali
IAM_PASSWORD_POLICY	**`RequireLowercaseCharacters`** (Opsional) • Memerlukan setidaknya satu karakter huruf kecil dalam kata sandi. • Tipe: Boolean • Bawaan: BETUL • Persyaratan kepatuhan: Setidaknya satu karakter huruf kecil
IAM_PASSWORD_POLICY	**`RequireNumbers`** (Opsional) • Memerlukan setidaknya satu nomor dalam kata sandi. • Tipe: Boolean • Bawaan: BETUL • Persyaratan kepatuhan: Setidaknya satu karakter angka
IAM_PASSWORD_POLICY	**`RequireSymbols`** (Opsional) • Memerlukan setidaknya satu simbol dalam kata sandi. • Tipe: Boolean • Bawaan: BETUL • Persyaratan kepatuhan: Setidaknya satu karakter simbol

AWS ConfigAturan yang diperlukan	Parameter yang diperlukan
IAM_PASSWORD_POLICY	**`RequireUppercaseCharacters`** (Opsional) • Memerlukan setidaknya satu karakter huruf besar dalam kata sandi. • Tipe: Boolean • Bawaan: BETUL • Persyaratan kepatuhan: Setidaknya satu karakter huruf besar
IAM_POLICY_IN_USE	**`policyARN`** • Kebijakan IAM ARN harus diperiksa. • Tipe: String • Persyaratan kepatuhan: Menciptakan peran IAM untuk mengelola insiden dengan. AWS **`policyUsageType`** (Opsional) • Menentukan apakah Anda mengharapkan kebijakan dilampirkan ke pengguna, grup, atau peran. • Tipe: String • Nilai valid: `IAM_USER` | `IAM_GROUP` | `IAM_ROLE` | `ANY` • Nilai default: `ANY` • Persyaratan kepatuhan: Lampirkan kebijakan kepercaya an ke peran IAM yang dibuat
IAM_POLICY_NO_STAT EMENTS_WITH_ADMIN_ ACCESS	Tidak berlaku
IAM_ROOT_ACCESS_KE Y_CHECK	Tidak berlaku
IAM_USER_NO_POLICI ES_CHECK	Tidak berlaku

AWS ConfigAturan yang diperlukan	Parameter yang diperlukan
IAM_USER_UNUSED_CREDENTIALS_CHECK	**`maxCredentialUsageAge`** • Jumlah hari maksimum yang kredensi tidak dapat digunakan. • Jenis: Int • Default: 90 hari • Persyaratan kepatuhan: 90 hari atau lebih
INCOMING_SSH_DISABLED	Tidak berlaku
MFA_ENABLED_FOR_IAM_CONSOLE_ACCESS	Tidak berlaku
MULTI_REGION_CLOUD_TRAIL_ENABLED	Tidak berlaku

AWS ConfigAturan yang diperlukan	Parameter yang diperlukan
DIBATAS_INCOMING_TRAFFIC	**`blockedPort1`** (Opsional) • Nomor port TCP yang diblokir. • Jenis: int • Default: 20 • Persyaratan kepatuhan: Pastikan tidak ada grup keamanan yang mengizinkan masuknya port yang diblokir **`blockedPort2`** (Opsional) • Nomor port TCP yang diblokir. • Jenis: int • Bawaan: 21 • Persyaratan kepatuhan: Pastikan tidak ada grup keamanan yang mengizinkan masuknya port yang diblokir **`blockedPort3`** (Opsional) • Nomor port TCP yang diblokir. • Jenis: int • Standar: 3389 • Persyaratan kepatuhan: Pastikan tidak ada grup keamanan yang mengizinkan masuknya port yang diblokir **`blockedPort4`** (Opsional) • Nomor port TCP yang diblokir. • Jenis: int • Standar: 3306 • Persyaratan kepatuhan: Pastikan tidak ada grup keamanan yang mengizinkan masuknya port yang diblokir

AWS ConfigAturan yang diperlukan	Parameter yang diperlukan
	`blockedPort5` (Opsional) • Nomor port TCP yang diblokir. • Jenis: int • Standar: 4333 • Persyaratan kepatuhan: Pastikan tidak ada grup keamanan yang mengizinkan masuknya port yang diblokir
ROOT_ACCOUNT_HARDWARE_MFA_ENABLED	Tidak berlaku
ROOT_ACCOUNT_MFA_ENABLED	Tidak berlaku
S3_BUCKET_LOGGING_ENABLED	**`targetBucket`** (Opsional) • Bucket S3 target untuk menyimpan log akses server. • Tipe: String • Persyaratan kepatuhan: Aktifkan pencatatan **`targetPrefix`** (Opsional) • Awalan bucket S3 untuk menyimpan log akses server. • Tipe: String • Persyaratan kepatuhan: Identifikasi bucket S3 untuk logging CloudTrail
S3_BUCKET_PUBLIC_READ_DILARANG	Tidak berlaku
VPC_DEFAULT_SECURITY_GROUP_CLOSED	Tidak berlaku

AWS ConfigAturan yang diperlukan	Parameter yang diperlukan
VPC_FLOW_LOGS_ENABLED	**`trafficType`** (Opsional) • `trafficType` Dari log aliran. • Tipe: String • Persyaratan kepatuhan: Pencatatan aliran diaktifkan

Lebih banyak sumber daya CIS

- Tolok Ukur AWS Yayasan CIS v1.2.0
- Posting blog Tolok Ukur CIS AWS Foundations di Blog Keamanan AWS

Tolok Ukur CIS untuk Tolok Ukur Yayasan Amazon Web Services CIS v1.3.0

AWS Audit Managermenyediakan dua kerangka kerja prebuilt yang mendukung CIS AWS Foundations Benchmark v1.3:

- Tolok Ukur CIS untuk Tolok Ukur Yayasan Amazon Web Services CIS v1.3.0, Level 1
- Tolok Ukur CIS untuk Tolok Ukur Yayasan Amazon Web Services CIS v1.3.0, Level 1 dan 2

> **Note**
>
> Untuk informasi tentang CIS AWS Foundations Benchmark v1.2.0, dan AWS Audit Manager kerangka kerja yang mendukung versi benchmark ini, lihat. Tolok Ukur CIS untuk Tolok Ukur Yayasan Amazon Web Services CIS v1.2.0

Topik

- Apa itu CIS?
- Menggunakan kerangka kerja ini untuk mendukung persiapan audit Anda
- Lebih banyak sumber daya CIS

Apa itu CIS?

Center for Internet Security (CIS) mengembangkan CIS AWS Foundations Benchmark v1.3.0, seperangkat praktik terbaik konfigurasi keamanan untuk. AWS Praktik terbaik yang diterima industri ini melampaui panduan keamanan tingkat tinggi yang sudah tersedia karena mereka menyediakan prosedur yang jelas, step-by-step implementasi, dan penilaian kepada AWS pengguna.

Untuk informasi lebih lanjut, lihat posting blog CIS AWS Foundations Benchmark di Blog AWS Keamanan.

CIS AWS Foundations Benchmark v1.3.0 memberikan panduan untuk mengonfigurasi opsi keamanan untuk subset Layanan AWS dengan penekanan pada pengaturan agnostik dasar, dapat diuji, dan arsitektur. Beberapa Amazon Web Services spesifik dalam cakupan dokumen ini meliputi:

- AWS Identity and Access Management (IAM)
- AWS Config
- AWS CloudTrail
- Amazon CloudWatch
- Amazon Simple Notification Service (Amazon SNS)
- Amazon Simple Storage Service (Amazon S3)
- Amazon Virtual Private Cloud (default)

Perbedaan antara Tolok Ukur CIS dan Kontrol CIS

Tolok Ukur CIS adalah pedoman praktik terbaik keamanan yang khusus untuk produk vendor. Mulai dari sistem operasi hingga layanan cloud dan perangkat jaringan, pengaturan yang diterapkan dari benchmark melindungi sistem yang digunakan organisasi Anda. Kontrol CIS adalah pedoman praktik terbaik dasar yang harus diikuti organisasi Anda untuk membantu melindungi dari vektor serangan siber yang diketahui.

Contoh

- Tolok Ukur CIS bersifat preskriptif. Mereka biasanya merujuk pada pengaturan tertentu yang dapat ditinjau dan ditetapkan dalam produk vendor.

  Contoh: CIS Amazon Web Services Foundations Benchmark v1.3.0 - 1.5 Pastikan MFA diaktifkan untuk akun “pengguna root”

Rekomendasi ini memberikan panduan preskriptif tentang cara memeriksa ini dan cara mengaturnya di akun root untuk lingkungan. AWS

- Kontrol CIS adalah untuk organisasi Anda secara keseluruhan, dan tidak spesifik hanya untuk satu produk vendor.

  Contoh: Kontrol CIS v7.1 - Sub-Kontrol 4.5 Gunakan Otentikasi Multi-Faktor untuk Semua Akses Administratif

  Kontrol ini menjelaskan apa yang diharapkan untuk diterapkan dalam organisasi Anda, tetapi bukan bagaimana Anda harus menerapkannya untuk sistem dan beban kerja yang Anda jalankan (di mana pun mereka berada).

Menggunakan kerangka kerja ini untuk mendukung persiapan audit Anda

Anda dapat menggunakan kerangka kerja CIS AWS Foundations Benchmark v1.3 AWS Audit Manager untuk membantu Anda mempersiapkan audit CIS. Anda juga dapat menyesuaikan kerangka kerja ini dan kontrolnya untuk mendukung audit internal dengan persyaratan khusus.

Dengan menggunakan kerangka kerja sebagai titik awal, Anda dapat membuat penilaian Audit Manager dan mulai mengumpulkan bukti yang relevan untuk audit Anda. Setelah Anda membuat penilaian, Audit Manager mulai menilai AWS sumber daya Anda. Hal ini dilakukan berdasarkan kontrol yang didefinisikan dalam kerangka CIS. Saat tiba waktunya untuk audit, Anda—atau delegasi pilihan Anda—dapat meninjau bukti yang dikumpulkan oleh Audit Manager. Anda juga dapat menelusuri folder bukti dalam penilaian Anda dan memilih bukti mana yang ingin Anda sertakan dalam laporan penilaian Anda. Atau, jika Anda mengaktifkan pencari bukti, Anda dapat mencari bukti spesifik dan mengekspornya dalam format CSV, atau membuat laporan penilaian dari hasil penelusuran Anda. Either way, Anda dapat menggunakan laporan penilaian ini untuk menunjukkan bahwa kontrol Anda berfungsi sebagaimana dimaksud.

Rincian kerangka kerja adalah sebagai berikut:

Nama kerangka kerja di AWS Audit Manager	Jumlah kontrol otomatis	Jumlah kontrol manual	Jumlah set kontrol	Layanan AWSdalam ruang lingkup
Tolok Ukur CIS untuk Tolok Ukur Yayasan	33	5	6	• Amazon CloudWatch

Nama kerangka kerja di AWS Audit Manager	Jumlah kontrol otomatis	Jumlah kontrol manual	Jumlah set kontrol	Layanan AWSdalam ruang lingkup
Amazon Web Services CIS v1.3.0, Level 1				• Amazon Elastic Compute Cloud • AWS Config • AWS CloudTrail • AWS Identity and Access Management • AWS Security Hub
Tolok Ukur CIS untuk Tolok Ukur Yayasan Amazon Web Services CIS v1.3.0, Level 1 dan 2	49	6	6	• Amazon Elastic Compute Cloud • Amazon CloudWatch • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Security Hub

Tip

Untuk meninjau daftar AWS Config aturan yang digunakan sebagai pemetaan sumber data untuk kerangka kerja standar ini, unduh file berikut:

- AuditManager_ ConfigDataSourceMappings _cis-benchmark-v1.3.0-level-1.zip
- AuditManager_ ConfigDataSourceMappings _CIS-Benchmark-v1.3.0, Level1-and-2.zip

Kontrol dalam kerangka kerja ini tidak dimaksudkan untuk memverifikasi apakah sistem Anda sesuai dengan standar CIS. Selain itu, mereka tidak dapat menjamin bahwa Anda akan lulus audit CIS. AWS Audit Managertidak secara otomatis memeriksa kontrol prosedural yang memerlukan pengumpulan bukti manual.

Anda dapat menemukan kerangka kerja ini di bawah tab Kerangka standar Pustaka kerangka kerja di Audit Manager.

Untuk petunjuk tentang cara membuat penilaian menggunakan kerangka kerja ini, lihatMembuat penilaian.

Saat Anda menggunakan konsol Audit Manager untuk membuat penilaian dari kerangka kerja standar ini, daftar Layanan AWS dalam cakupan dipilih secara default dan tidak dapat diedit. Ini karena Audit Manager secara otomatis memetakan dan memilih sumber data dan layanan untuk Anda. Pemilihan ini dibuat sesuai dengan persyaratan Tolok Ukur CIS. Jika Anda perlu mengedit daftar layanan dalam cakupan kerangka kerja ini, Anda dapat melakukannya dengan menggunakan operasi CreateAssessmentatau UpdateAssessmentAPI. Atau, Anda dapat menyesuaikan kerangka kerja standar dan kemudian membuat penilaian dari kerangka kerja khusus.

Untuk petunjuk tentang cara menyesuaikan kerangka kerja ini untuk mendukung persyaratan spesifik Anda, lihat Menyesuaikan kerangka kerja yang ada dan Menyesuaikan kontrol yang ada.

Lebih banyak sumber daya CIS

- Posting blog Tolok Ukur CIS AWS Foundations di Blog Keamanan AWS

Tolok Ukur CIS untuk Benchmark Yayasan Amazon Web Services CIS v1.4.0

AWS Audit Managermenyediakan dua kerangka kerja standar bawaan yang mendukung Benchmark AWS Foundation Center for Internet Security (CIS) v1.4.0:

- Tolok Ukur CIS untuk Tolok Ukur Yayasan Amazon Web Services CIS v1.4.0, Level 1
- Tolok Ukur CIS untuk Benchmark Yayasan Amazon Web Services CIS v1.4.0, Level 1 dan 2

> **Note**
>
> - Untuk informasi tentang framework Audit Manager yang mendukung v1.2.0, lihat. Tolok Ukur CIS untuk Tolok Ukur Yayasan Amazon Web Services CIS v1.2.0
> - Untuk informasi tentang framework Audit Manager yang mendukung v1.3.0, lihat. Tolok Ukur CIS untuk Tolok Ukur Yayasan Amazon Web Services CIS v1.3.0

Topik

Apa Benchmark CIS untuk CIS Amazon Web Services Foundations Benchmark v1.4.0?

Benchmark CIS untuk CIS Amazon Web Services Foundations Benchmark, v1.4.0, Level 1 dan 2 memberikan panduan preskriptif untuk mengonfigurasi opsi keamanan untuk subset Amazon Web Services. Ini memiliki penekanan pada pengaturan agnostik dasar, dapat diuji, dan arsitektur. Beberapa Amazon Web Services spesifik dalam cakupan dokumen ini meliputi:

- AWS Identity and Access Management (IAM)
- IAM Access Analyzer
- AWS Config
- AWS CloudTrail
- Amazon CloudWatch
- Amazon Simple Notification Service (Amazon SNS)
- Amazon Simple Storage Service (Amazon S3)
- Amazon Elastic Compute Cloud (Amazon EC2)
- Amazon Relational Database Service (Amazon RDS)
- Amazon Virtual Private Cloud

Perbedaan antara Tolok Ukur CIS dan Kontrol CIS

Tolok Ukur CIS adalah pedoman praktik terbaik keamanan yang khusus untuk produk vendor. Mulai dari sistem operasi hingga layanan cloud dan perangkat jaringan, pengaturan yang diterapkan dari benchmark melindungi sistem yang sedang digunakan. Kontrol CIS adalah pedoman praktik terbaik dasar yang harus diikuti organisasi Anda untuk membantu melindungi dari vektor serangan siber yang diketahui.

Contoh

- Tolok Ukur CIS bersifat preskriptif. Mereka biasanya merujuk pada pengaturan tertentu yang dapat ditinjau dan ditetapkan dalam produk vendor.

  Contoh: CIS Amazon Web Services Foundations Benchmark v1.4.0 - 1.5 Pastikan MFA diaktifkan untuk akun “pengguna root”

  Rekomendasi ini memberikan panduan preskriptif tentang cara memeriksa ini dan cara mengaturnya di akun root untuk lingkungan. AWS
- Kontrol CIS adalah untuk organisasi Anda secara keseluruhan, dan tidak spesifik hanya untuk satu produk vendor.

  Contoh: Kontrol CIS v7.1 - Sub-Kontrol 4.5 Gunakan Otentikasi Multi-Faktor untuk Semua Akses Administratif

  Kontrol ini menjelaskan apa yang diharapkan untuk diterapkan dalam organisasi Anda. Namun, itu tidak menjelaskan bagaimana menerapkannya untuk sistem dan beban kerja yang Anda jalankan, di mana pun mereka berada.

Menggunakan kerangka kerja ini untuk mendukung persiapan audit Anda

Anda dapat menggunakan kerangka kerja CIS AWS Foundations Benchmark v1.4.0 AWS Audit Manager untuk membantu Anda mempersiapkan audit CIS. Anda juga dapat menyesuaikan kerangka kerja ini dan kontrolnya untuk mendukung audit internal dengan persyaratan khusus.

Dengan menggunakan kerangka kerja sebagai titik awal, Anda dapat membuat penilaian Audit Manager dan mulai mengumpulkan bukti yang relevan untuk audit Anda. Setelah Anda membuat penilaian, Audit Manager mulai menilai AWS sumber daya Anda. Hal ini dilakukan berdasarkan kontrol yang didefinisikan dalam kerangka CIS. Saat tiba waktunya untuk audit, Anda—atau delegasi pilihan Anda—dapat meninjau bukti yang dikumpulkan oleh Audit Manager. Anda juga dapat menelusuri folder bukti dalam penilaian Anda dan memilih bukti mana yang ingin Anda sertakan dalam laporan penilaian Anda. Atau, jika Anda mengaktifkan pencari bukti, Anda dapat mencari

bukti spesifik dan mengekspornya dalam format CSV, atau membuat laporan penilaian dari hasil penelusuran Anda. Either way, Anda dapat menggunakan laporan penilaian ini untuk menunjukkan bahwa kontrol Anda berfungsi sebagaimana dimaksud.

Rincian kerangka kerja adalah sebagai berikut:

Nama kerangka kerja di AWS Audit Manager	Jumlah kontrol otomatis	Jumlah kontrol manual	Jumlah set kontrol	Layanan AWSdalam ruang lingkup
Tolok Ukur CIS untuk Tolok Ukur Yayasan Amazon Web Services CIS v1.4.0, Level 1	32	6	7	• Amazon Elastic Compute Cloud • Amazon CloudWatch • AWS CloudTrail • AWS Config • AWS Identity and Access Management
Tolok Ukur CIS untuk Benchmark Yayasan Amazon Web Services CIS v1.4.0, Level 1 dan 2	50	8	7	• Amazon Elastic Compute Cloud • Amazon CloudWatch • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Security Hub

> **Tip**
>
> Untuk meninjau daftar AWS Config aturan yang digunakan sebagai pemetaan sumber data untuk kerangka kerja standar ini, unduh file berikut:
>
> - AuditManager_ ConfigDataSourceMappings _cis-benchmark-v1.4.0-level-1.zip
> - AuditManager_ ConfigDataSourceMappings _cis-benchmark-v1.4.0-tingkat-1-dan-2.zip

Kontrol dalam kerangka kerja ini tidak dimaksudkan untuk memverifikasi apakah sistem Anda sesuai dengan Benchmark CIS untuk standar CIS Amazon Web Services Foundations Benchmark v1.4.0. Selain itu, mereka tidak dapat menjamin bahwa Anda akan lulus audit CIS. AWS Audit Managertidak secara otomatis memeriksa kontrol prosedural yang memerlukan pengumpulan bukti manual.

Anda dapat menemukan kerangka kerja ini di bawah tab Kerangka standar Pustaka kerangka kerja di Audit Manager.

Untuk petunjuk tentang cara membuat penilaian menggunakan kerangka kerja ini, lihatMembuat penilaian.

Saat Anda menggunakan konsol Audit Manager untuk membuat penilaian dari kerangka kerja standar ini, daftar Layanan AWS dalam cakupan dipilih secara default dan tidak dapat diedit. Ini karena Audit Manager secara otomatis memetakan dan memilih sumber data dan layanan untuk Anda. Pemilihan ini dibuat sesuai dengan persyaratan Tolok Ukur CIS. Jika Anda perlu mengedit daftar layanan dalam cakupan kerangka kerja ini, Anda dapat melakukannya dengan menggunakan operasi CreateAssessmentatau UpdateAssessmentAPI. Atau, Anda dapat menyesuaikan kerangka kerja standar dan kemudian membuat penilaian dari kerangka kerja khusus.

Untuk petunjuk tentang cara menyesuaikan kerangka kerja ini untuk mendukung persyaratan spesifik Anda, lihat Menyesuaikan kerangka kerja yang ada dan Menyesuaikan kontrol yang ada.

Lebih banyak sumber daya CIS

- Tolok Ukur CIS dari Pusat Keamanan Internet
- Posting blog Tolok Ukur CIS AWS Foundations di Blog Keamanan AWS

Kontrol CIS v7.1 Grup Implementasi 1

AWS Audit Managermenyediakan kerangka kerja bawaan yang mendukung Center for Internet Security (CIS) Controls v7.1 Implementation Group 1.

> **Note**
>
> Untuk informasi tentang Kontrol CIS v8 IG1 dan AWS Audit Manager kerangka kerja yang mendukung standar ini, lihat. Kontrol CIS v8 Grup Implementasi 1

AWS Audit Managermenyediakan kerangka kerja prebuilt yang mendukung Center for Internet Security (CIS) untuk membantu Anda dengan persiapan audit Anda.

Topik

- Apa itu kontrol CIS?
- Menggunakan kerangka kerja ini untuk mendukung persiapan audit Anda
- Lebih banyak sumber daya CIS

Apa itu kontrol CIS?

Kontrol CIS adalah serangkaian tindakan yang diprioritaskan yang secara kolektif membentuk defense-in-depth serangkaian praktik terbaik. Praktik terbaik ini mengurangi serangan paling umum terhadap sistem dan jaringan. Kelompok Implementasi 1 umumnya didefinisikan untuk organisasi dengan sumber daya terbatas dan keahlian keamanan siber yang tersedia untuk mengimplementasikan Sub-Kontrol.

Perbedaan antara Kontrol CIS dan Tolok Ukur CIS

Kontrol CIS adalah pedoman praktik terbaik dasar yang dapat diikuti organisasi untuk memiliki perlindungan dari vektor serangan siber yang diketahui. Tolok Ukur CIS adalah pedoman praktik terbaik keamanan khusus untuk produk vendor. Mulai dari sistem operasi hingga layanan cloud dan perangkat jaringan, pengaturan yang diterapkan dari Benchmark melindungi sistem yang sedang digunakan.

Contoh

- Tolok Ukur CIS bersifat preskriptif. Mereka biasanya merujuk pada pengaturan tertentu yang dapat ditinjau dan ditetapkan dalam produk vendor.

  - Contoh: CIS Amazon Web Services Foundations Benchmark v1.2.0 - 1.13 Pastikan MFA diaktifkan untuk akun “pengguna root”.
  - Rekomendasi ini memberikan panduan preskriptif tentang cara memeriksa ini dan cara mengaturnya di akun root untuk lingkungan. AWS
- Kontrol CIS adalah untuk organisasi Anda secara keseluruhan dan tidak spesifik hanya untuk satu produk vendor.
  - Contoh: Kontrol CIS v7.1 - Sub-Kontrol 4.5 Gunakan Otentikasi Multi-Faktor untuk Semua Akses Administratif
  - Kontrol ini menjelaskan apa yang diharapkan untuk diterapkan dalam organisasi Anda. Namun, itu tidak memberi tahu Anda bagaimana Anda harus menerapkannya untuk sistem dan beban kerja yang Anda jalankan (di mana pun mereka berada).

Menggunakan kerangka kerja ini untuk mendukung persiapan audit Anda

Anda dapat menggunakan kerangka kerja CIS Controls v7.1 IG1 untuk membantu Anda mempersiapkan audit. Kerangka kerja ini mencakup kumpulan kontrol bawaan dengan deskripsi dan prosedur pengujian. Kontrol ini dikelompokkan ke dalam set kontrol sesuai dengan persyaratan CIS. Anda juga dapat menyesuaikan kerangka kerja ini dan kontrolnya untuk mendukung audit internal dengan persyaratan khusus.

Dengan menggunakan kerangka kerja sebagai titik awal, Anda dapat membuat penilaian Audit Manager dan mulai mengumpulkan bukti yang relevan untuk audit Anda. Setelah Anda membuat penilaian, Audit Manager mulai menilai AWS sumber daya Anda. Ini dilakukan berdasarkan kontrol yang didefinisikan dalam kerangka CIS Controls v7.1 IG1. Saat tiba waktunya untuk audit, Anda —atau delegasi pilihan Anda—dapat meninjau bukti yang dikumpulkan oleh Audit Manager. Anda juga dapat menelusuri folder bukti dalam penilaian Anda dan memilih bukti mana yang ingin Anda sertakan dalam laporan penilaian Anda. Atau, jika Anda mengaktifkan pencari bukti, Anda dapat mencari bukti spesifik dan mengekspornya dalam format CSV, atau membuat laporan penilaian dari hasil penelusuran Anda. Either way, Anda dapat menggunakan laporan penilaian ini untuk menunjukkan bahwa kontrol Anda berfungsi sebagaimana dimaksud.

Rincian kerangka kerja CIS Controls v7.1 IG1 adalah sebagai berikut:

Nama kerangka kerja di AWS Audit Manager	Jumlah kontrol otomatis	Jumlah kontrol manual	Jumlah set kontrol	Layanan AWSdalam ruang lingkup
Kontrol CIS v7.1 IG1	21	22	16	• Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Config • AWS Identity and Access Managemen t

> **Tip**
>
> Untuk meninjau AWS Config aturan yang digunakan sebagai pemetaan sumber data dalam kerangka standar ini, unduh file AuditManager_ ConfigDataSourceMappings _cis-controls-v7.1-IG1.zip.

Kontrol dalam kerangka kerja ini tidak dimaksudkan untuk memverifikasi apakah sistem Anda sesuai dengan Kontrol CIS. Selain itu, mereka tidak dapat menjamin bahwa Anda akan lulus audit CIS. AWS Audit Managertidak secara otomatis memeriksa kontrol prosedural yang memerlukan pengumpulan bukti manual.

Anda dapat menemukan kerangka kerja ini di bawah tab Kerangka Standar Pustaka kerangka kerja di Audit Manager.

Untuk petunjuk tentang cara membuat penilaian menggunakan kerangka kerja ini, lihatMembuat penilaian.

Saat Anda menggunakan konsol Audit Manager untuk membuat penilaian dari kerangka kerja standar ini, daftar Layanan AWS dalam cakupan dipilih secara default dan tidak dapat diedit. Ini karena Audit Manager secara otomatis memetakan dan memilih sumber data dan layanan untuk Anda. Pemilihan ini dibuat sesuai dengan persyaratan Kontrol CIS. Jika Anda perlu mengedit daftar layanan dalam cakupan kerangka kerja ini, Anda dapat melakukannya dengan menggunakan operasi

CreateAssessmentatau UpdateAssessmentAPI. Atau, Anda dapat menyesuaikan kerangka kerja standar dan kemudian membuat penilaian dari kerangka kerja khusus.

Untuk petunjuk tentang cara menyesuaikan kerangka kerja ini untuk mendukung persyaratan spesifik Anda, lihat Menyesuaikan kerangka kerja yang ada dan Menyesuaikan kontrol yang ada.

Lebih banyak sumber daya CIS

- Kontrol CIS v7.1 IG1

Kontrol CIS v8 Grup Implementasi 1

AWS Audit Managermenyediakan kerangka kerja standar bawaan yang mendukung Center for Internet Security (CIS) Controls v8 Implementation Group 1.

> **Note**
>
> Untuk informasi tentang Kontrol CIS v7.1 IG1 dan AWS Audit Manager kerangka kerja yang mendukung standar ini, lihat. Kontrol CIS v7.1 Grup Implementasi 1

Topik

Apa itu Kontrol CIS?

CIS Critical Security Controls (CIS Controls) adalah serangkaian pengamanan yang diprioritaskan untuk mengurangi serangan siber yang paling umum terhadap sistem dan jaringan. Mereka dipetakan dan direferensikan oleh beberapa kerangka hukum, peraturan, dan kebijakan. CIS Controls v8 telah ditingkatkan untuk mengikuti sistem dan perangkat lunak modern. Pergerakan ke komputasi berbasis cloud, virtualisasi, mobilitas, outsourcing work-from-home, dan mengubah taktik penyerang mendorong pembaruan. Pembaruan ini mendukung keamanan perusahaan saat mereka pindah ke lingkungan cloud dan hybrid sepenuhnya.

Perbedaan antara Kontrol CIS dan Tolok Ukur CIS

Kontrol CIS adalah pedoman praktik terbaik dasar yang dapat diikuti organisasi untuk memiliki perlindungan dari vektor serangan siber yang diketahui. Tolok Ukur CIS adalah pedoman praktik terbaik keamanan khusus untuk produk vendor. Mulai dari sistem operasi hingga layanan cloud dan perangkat jaringan, pengaturan yang diterapkan dari Benchmark melindungi sistem yang sedang digunakan.

Contoh

- Tolok Ukur CIS bersifat preskriptif. Mereka biasanya merujuk pada pengaturan tertentu yang dapat ditinjau dan ditetapkan dalam produk vendor.
  - Contoh: CIS Amazon Web Services Foundations Benchmark v1.2.0 - 1.13 Pastikan MFA diaktifkan untuk akun “pengguna root”.
  - Rekomendasi ini memberikan panduan preskriptif tentang cara memeriksa ini dan cara mengaturnya di akun root untuk lingkungan. AWS
- Kontrol CIS adalah untuk organisasi Anda secara keseluruhan dan tidak spesifik hanya untuk satu produk vendor.
  - Contoh: Kontrol CIS v7.1 - Sub-Kontrol 4.5 Gunakan Otentikasi Multi-Faktor untuk Semua Akses Administratif
  - Kontrol ini menjelaskan apa yang diharapkan untuk diterapkan dalam organisasi Anda. Namun, itu tidak memberi tahu Anda bagaimana Anda harus menerapkannya untuk sistem dan beban kerja yang Anda jalankan (di mana pun mereka berada).

Menggunakan kerangka kerja ini untuk mendukung persiapan audit Anda

Anda dapat menggunakan kerangka CIS Controls v8 IG1 untuk membantu Anda mempersiapkan audit. Kerangka kerja ini mencakup kumpulan kontrol bawaan dengan deskripsi dan prosedur pengujian. Kontrol ini dikelompokkan ke dalam set kontrol sesuai dengan persyaratan CIS. Anda juga dapat menyesuaikan kerangka kerja ini dan kontrolnya untuk mendukung audit internal dengan persyaratan khusus.

Dengan menggunakan kerangka kerja sebagai titik awal, Anda dapat membuat penilaian Audit Manager dan mulai mengumpulkan bukti yang relevan untuk audit Anda. Setelah Anda membuat penilaian, Audit Manager mulai menilai AWS sumber daya Anda. Ini dilakukan berdasarkan kontrol yang didefinisikan dalam kerangka CIS Controls v8. Saat tiba waktunya untuk audit, Anda—atau delegasi pilihan Anda—dapat meninjau bukti yang dikumpulkan oleh Audit Manager. Anda juga dapat menelusuri folder bukti dalam penilaian Anda dan memilih bukti mana yang ingin Anda sertakan dalam laporan penilaian Anda. Atau, jika Anda mengaktifkan pencari bukti, Anda dapat mencari

bukti spesifik dan mengekspornya dalam format CSV, atau membuat laporan penilaian dari hasil penelusuran Anda. Either way, Anda dapat menggunakan laporan penilaian ini untuk menunjukkan bahwa kontrol Anda berfungsi sebagaimana dimaksud.

Rincian kerangka kerja CIS Controls v8 adalah sebagai berikut:

Nama kerangka kerja di AWS Audit Manager	Jumlah kontrol otomatis	Jumlah kontrol manual	Jumlah set kontrol	Layanan AWSdalam ruang lingkup
Kontrol CIS v8 IG1	25	31	15	• Amazon Elastic Compute Cloud • AWS Config • AWS Identity and Access Management • AWS License Manager

> **Tip**
>
> Untuk meninjau AWS Config aturan yang digunakan sebagai pemetaan sumber data dalam kerangka standar ini, unduh file AuditManager_ ConfigDataSourceMappings _CIS-Controls-v8-IG1.zip.

Kontrol dalam kerangka kerja ini tidak dimaksudkan untuk memverifikasi apakah sistem Anda sesuai dengan Kontrol CIS. Selain itu, mereka tidak dapat menjamin bahwa Anda akan lulus audit CIS. AWS Audit Managertidak secara otomatis memeriksa kontrol prosedural yang memerlukan pengumpulan bukti manual.

Anda dapat menemukan kerangka kerja ini di bawah tab Kerangka Standar Pustaka kerangka kerja di Audit Manager.

Untuk petunjuk tentang cara membuat penilaian menggunakan kerangka kerja ini, lihatMembuat penilaian.

Saat Anda menggunakan konsol Audit Manager untuk membuat penilaian dari kerangka kerja standar ini, daftar Layanan AWS dalam cakupan dipilih secara default dan tidak dapat diedit. Ini karena Audit Manager secara otomatis memetakan dan memilih sumber data dan layanan untuk Anda. Pemilihan ini dibuat sesuai dengan persyaratan Kontrol CIS. Jika Anda perlu mengedit daftar layanan dalam cakupan kerangka kerja ini, Anda dapat melakukannya dengan menggunakan operasi CreateAssessmentatau UpdateAssessmentAPI. Atau, Anda dapat menyesuaikan kerangka kerja standar dan kemudian membuat penilaian dari kerangka kerja khusus.

Untuk petunjuk tentang cara menyesuaikan kerangka kerja ini untuk mendukung persyaratan spesifik Anda, lihat Menyesuaikan kerangka kerja yang ada dan Menyesuaikan kontrol yang ada.

Lebih banyak sumber daya CIS

- Kontrol CIS v8

FedRAMP Dasar Sedang

AWS Audit Managermenyediakan kerangka kerja FedRAMP Moderate Baseline untuk membantu Anda dengan persiapan audit Anda.

Topik

- Apa itu FedRAMP?
- Menggunakan kerangka kerja ini untuk mendukung persiapan audit Anda
- Lebih banyak sumber daya FedRAMP

Apa itu FedRAMP?

Program Manajemen Risiko dan Otorisasi Federal (FedRAMP) didirikan pada tahun 2011. Ini memberikan pendekatan berbasis risiko yang hemat biaya untuk adopsi dan penggunaan layanan cloud oleh pemerintah federal AS. FedRAMP memberdayakan lembaga federal untuk menggunakan teknologi cloud modern, dengan penekanan pada keamanan dan perlindungan informasi federal.

Untuk informasi selengkapnya tentang kontrol dasar moderat FedRAMP, lihat Templat Prosedur Kasus Uji Keamanan Moderat FedRAMP.

Menggunakan kerangka kerja ini untuk mendukung persiapan audit Anda

Anda dapat menggunakan kerangka FedRAMP Moderate Baseline untuk membantu Anda mempersiapkan audit. Kerangka kerja ini mencakup kumpulan kontrol bawaan dengan deskripsi dan prosedur pengujian. Kontrol ini dikelompokkan ke dalam set kontrol sesuai dengan persyaratan FedRAMP. Anda juga dapat menyesuaikan kerangka kerja ini dan kontrolnya untuk mendukung audit internal dengan persyaratan khusus.

Dengan menggunakan kerangka kerja sebagai titik awal, Anda dapat membuat penilaian Audit Manager dan mulai mengumpulkan bukti yang relevan untuk audit Anda. Setelah Anda membuat penilaian, Audit Manager mulai menilai AWS sumber daya Anda. Ini dilakukan berdasarkan kontrol yang didefinisikan dalam kerangka kerja. Saat tiba waktunya untuk audit, Anda—atau delegasi pilihan Anda—dapat meninjau bukti yang dikumpulkan oleh Audit Manager. Anda juga dapat menelusuri folder bukti dalam penilaian Anda dan memilih bukti mana yang ingin Anda sertakan dalam laporan penilaian Anda. Atau, jika Anda mengaktifkan pencari bukti, Anda dapat mencari bukti spesifik dan mengekspornya dalam format CSV, atau membuat laporan penilaian dari hasil penelusuran Anda. Either way, Anda dapat menggunakan laporan penilaian ini untuk menunjukkan bahwa kontrol Anda berfungsi sebagaimana dimaksud.

Rincian kerangka kerja FedRAMP Moderate Baseline adalah sebagai berikut:

Nama kerangka kerja di AWS Audit Manager	Jumlah kontrol otomatis	Jumlah kontrol manual	Jumlah set kontrol	Layanan AWSdalam ruang lingkup
FedRAMP Dasar Sedang	303	908	325	• Amazon Elastic Compute Cloud • AWS Config • AWS Identity and Access Management

> **Tip**
>
> Untuk meninjau AWS Config aturan yang digunakan sebagai pemetaan sumber data dalam kerangka standar ini, unduh file AuditManager_ ConfigDataSourceMappings _FedRAMP-Moderate-Baseline.zip.

Kontrol dalam kerangka kerja ini tidak dimaksudkan untuk memverifikasi apakah sistem Anda sesuai dengan FedRAMP. Selain itu, mereka tidak dapat menjamin bahwa Anda akan lulus audit FedRAMP. AWS Audit Managertidak secara otomatis memeriksa kontrol prosedural yang memerlukan pengumpulan bukti manual.

Anda dapat menemukan kerangka kerja ini di bawah tab Kerangka Standar Pustaka kerangka kerja di Audit Manager.

Untuk petunjuk tentang cara membuat penilaian menggunakan kerangka kerja ini, lihatMembuat penilaian.

Saat Anda menggunakan konsol Audit Manager untuk membuat penilaian dari kerangka kerja standar ini, daftar Layanan AWS dalam cakupan dipilih secara default dan tidak dapat diedit. Ini karena Audit Manager secara otomatis memetakan dan memilih sumber data dan layanan untuk Anda. Pemilihan ini dibuat sesuai dengan persyaratan FedRAMP Moderate Baseline. Jika Anda perlu mengedit daftar layanan dalam ruang lingkup untuk kerangka kerja ini, Anda dapat melakukannya dengan menggunakan operasi CreateAssessmentatau UpdateAssessmentAPI. Atau, Anda dapat menyesuaikan kerangka kerja standar dan kemudian membuat penilaian dari kerangka kerja khusus.

Untuk petunjuk tentang cara menyesuaikan kerangka kerja ini untuk mendukung persyaratan spesifik Anda, lihat Menyesuaikan kerangka kerja yang ada dan Menyesuaikan kontrol yang ada.

Lebih banyak sumber daya FedRAMP

- AWSHalaman kepatuhan untuk FedRAMP
- AWSPosting blog FedRAMP

Peraturan Perlindungan Data Umum (GDPR)

AWS Audit Managermenyediakan kerangka kerja standar bawaan yang mendukung Peraturan Perlindungan Data Umum (GDPR). Secara default, kerangka kerja ini hanya berisi kontrol manual. Kontrol manual ini tidak mengumpulkan bukti secara otomatis. Namun, jika Anda ingin

mengotomatiskan pengumpulan bukti untuk beberapa kontrol di bawah GDPR, Anda dapat menggunakan fitur kontrol kustom di. AWS Audit Manager Untuk informasi selengkapnya, lihat Menggunakan kerangka kerja ini untuk mendukung persiapan audit Anda.

Topik

Apa itu Peraturan Perlindungan Data Umum (GDPR)?

Peraturan Perlindungan Data Umum (GDPR) adalah undang-undang privasi Eropa baru yang dapat ditegakkan pada 25 Mei 2018. GDPR menggantikan EU Data Protection Directive, juga dikenal sebagai Directive 95/46/EC. Ini dimaksudkan untuk menyelaraskan undang-undang perlindungan data di seluruh Uni Eropa (UE). Ini dilakukan dengan menerapkan undang-undang perlindungan data tunggal yang mengikat di setiap negara anggota UE.

GDPR berlaku untuk semua organisasi yang didirikan di UE dan organisasi (tidak peduli apakah mereka didirikan di UE) yang memproses data pribadi subjek data UE sehubungan dengan penawaran barang atau jasa kepada subjek data di UE atau pemantauan perilaku yang terjadi di UE. Data pribadi adalah informasi apa pun yang berhubungan dengan orang alami yang teridentifikasi atau dapat diidentifikasi.

Anda dapat menemukan kerangka kerja GDPR di halaman pustaka kerangka kerja. AWS Audit Manager Untuk informasi selengkapnya, lihat Pusat Peraturan Perlindungan Data Umum (GDPR).

Menggunakan kerangka kerja ini untuk mendukung persiapan audit Anda

Anda dapat menggunakan kerangka kerja GDPR AWS Audit Manager untuk membantu Anda mempersiapkan audit.

Rincian kerangka kerja adalah sebagai berikut:

Nama kerangka kerja di AWS Audit Manager	Jumlah kontrol otomatis	Jumlah kontrol manual	Jumlah set kontrol	Layanan AWSdalam ruang lingkup
GDPR	0	371	10	Tidak ada

Anda dapat menemukan kerangka kerja GDPR di bawah tab Kerangka standar Pustaka kerangka kerja di Audit Manager. Karena kerangka kerja standar ini hanya berisi kontrol manual, tidak Layanan AWS ada ruang lingkup.

> **Note**
>
> Jika ingin mengotomatiskan pengumpulan bukti untuk GDPR, Anda dapat menggunakan Audit Manager untuk membuat kontrol kustom Anda sendiri untuk GDPR. Tabel berikut memberikan rekomendasi tentang sumber AWS data yang dapat Anda petakan ke persyaratan GDPR dalam kontrol kustom Anda. Meskipun beberapa sumber data berikut dipetakan ke beberapa kontrol, perlu diingat bahwa Anda hanya dikenakan biaya sekali untuk setiap penilaian sumber daya.
> Rekomendasi berikut digunakan AWS Config dan AWS Security Hub sebagai sumber data. Agar berhasil mengumpulkan bukti dari sumber data ini, pastikan Anda melakukan hal berikut:
>
> - Konfirmasikan bahwa Anda telah mengikuti petunjuk untuk mengaktifkan AWS Config dan mengatur dan AWS Security Hub masukAkun AWS.
> - Konfirmasikan bahwa Anda telah menyertakan keduanya AWS Config dan Security Hub sebagai layanan dalam cakupan. Untuk meninjau daftar layanan dalam cakupan penilaian Anda, lihat Tinjau penilaian, Layanan AWS tab. Untuk mengedit daftar ini, lihat Mengedit Layanan AWS dalam cakupan.
>
> Setelah menyiapkan kedua layanan dengan cara ini, Audit Manager mengumpulkan bukti setiap kali evaluasi dilakukan untuk AWS Config aturan yang ditentukan atau kontrol Security Hub.

Nama kontrol	Set kontrol	Pemetaan sumber data kontrol yang disarankan
Pasal 25 Perlindungan data berdasarkan desain dan	Bab 4 - Pengontrol dan Prosesor	Anda dapat membuat kontrol khusus AWS Audit Manager yang mendukung kontrol GDPR ini. Saat Anda menentukan detail kontrol, masukkan yang berikut ini di bawah Informasi pengujian:

Nama kontrol	Set kontrol	Pemetaan sumber data kontrol yang disarankan
secara default.1		• Tampilkan semua peristiwa akun root selama jangka waktu • AWS CloudTrailember tidak publik • Tampilkan semua kebijakan dengan `Allow:*:*` dan cantumkan semua prinsipal dan layanan menggunakan kebijakan tersebut Saat Anda mengatur sumber data kontrol, sebaiknya sertakan semua hal berikut sebagai sumber data: Pilih AWS Config sebagai tipe sumber data, dan pilih aturan AWS Config terkelola berikut sebagai pemetaan sumber data: • IAM_ROOT_ACCESS_KEY_CHECK • ROOT_ACCOUNT_MFA_ENABLED • ROOT_ACCOUNT_HARDWARE_MFA_ENABLED • VPC_FLOW_LOGS_ENABLED • ACCESS_KEYS_DIPUTAR • IAM_PASSWORD_POLICY Pilih AWS Security Hub sebagai tipe sumber data, dan pilih kontrol Security Hub berikut sebagai pemetaan sumber data: • 1.1 (CloudWatch.1) • 1.1 (IAM.20) • 1.10 (IAM.16) • 1.11 (IAM.17) • 1.12 (IAM.4) • 1.13 (IAM.9) • 1.14 (IAM.6) • 1.16 (IAM.2) • 1.2 (IAM.5 • 1.20 (IAM.18)

Nama kontrol	Set kontrol	Pemetaan sumber data kontrol yang disarankan
		• 1.22 (IAM.1 • 1.3 (IAM.8) • 1.4 (IAM.3) • 1.5 (IAM.11) • 1.6 (IAM.12) • 1.7 (IAM.13) • 1.8 (IAM.14) • 1.9 (IAM.15) • 2.1 (CloudTrail.1) • 2.2 (CloudTrail.4) • 2.3 (CloudTrail.6) • 2.4 (CloudTrail.5) • 2.5 (Konfigurasi.1) • 2.6 (CloudTrail.7) • 2.7 (CloudTrail.2) • 2.8 (KMS.4) • 2.9 (EC2.6) • 3.1 (CloudWatch.2) • 3.10 (CloudWatch.10) • 3.11 (CloudWatch.11) • 3.12 (CloudWatch.12) • 3.13 (CloudWatch.13) • 3.14 (CloudWatch.14) • Konfigurasi.1

Nama kontrol	Set kontrol	Pemetaan sumber data kontrol yang disarankan
Pasal 25 Perlindungan data berdasarkan desain dan secara default.2	Bab 4 - Pengontrol dan Prosesor	Anda dapat membuat kontrol khusus AWS Audit Manager yang mendukung kontrol GDPR ini. Saat Anda menentukan detail kontrol, masukkan yang berikut ini di bawah Informasi pengujian: • Tampilkan semua peristiwa akun root selama jangka waktu • AWS CloudTrailember tidak publik • Tampilkan semua kebijakan dengan `Allow:*:*` dan cantumkan semua prinsipal dan layanan menggunakan kebijakan tersebut Saat Anda mengatur sumber data kontrol, sebaiknya sertakan semua hal berikut sebagai sumber data: Pilih AWS Config sebagai tipe sumber data, dan pilih aturan AWS Config terkelola berikut sebagai pemetaan sumber data: • IAM_ROOT_ACCESS_KEY_CHECK • ROOT_ACCOUNT_MFA_ENABLED • ROOT_ACCOUNT_HARDWARE_MFA_ENABLED • VPC_FLOW_LOGS_ENABLED • ACCESS_KEYS_DIPUTAR • IAM_PASSWORD_POLICY Pilih AWS Security Hub sebagai tipe sumber data, dan pilih kontrol Security Hub berikut sebagai pemetaan sumber data: • 1.1 (CloudWatch.1) • 1.1 (IAM.20) • 1.10 (IAM.16) • 1.11 (IAM.17) • 1.12 (IAM.4)

Nama kontrol	Set kontrol	Pemetaan sumber data kontrol yang disarankan
		• 1.13 (IAM.9) • 1.14 (IAM.6) • 1.16 (IAM.2) • 1.2 (IAM.5 • 1.20 (IAM.18) • 1.22 (IAM.1 • 1.3 (IAM.8) • 1.4 (IAM.3) • 1.5 (IAM.11) • 1.6 (IAM.12) • 1.7 (IAM.13) • 1.8 (IAM.14) • 1.9 (IAM.15) • 2.1 (CloudTrail.1) • 2.2 (CloudTrail.4) • 2.3 (CloudTrail.6) • 2.4 (CloudTrail.5) • 2.5 (Konfigurasi.1) • 2.6 (CloudTrail.7) • 2.7 (CloudTrail.2) • 2.8 (KMS.4) • 2.9 (EC2.6) • 3.1 (CloudWatch.2) • 3.10 (CloudWatch.10) • 3.11 (CloudWatch.11) • 3.12 (CloudWatch.12) • 3.13 (CloudWatch.13) • 3.14 (CloudWatch.14)

Nama kontrol	Set kontrol	Pemetaan sumber data kontrol yang disarankan
		• Konfigurasi.1

Nama kontrol	Set kontrol	Pemetaan sumber data kontrol yang disarankan
Pasal 25 Perlindungan data berdasarkan desain dan secara default.3	Bab 4 - Pengontrol dan Prosesor	Anda dapat membuat kontrol khusus AWS Audit Manager yang mendukung kontrol GDPR ini. Saat Anda menentukan detail kontrol, masukkan yang berikut ini di bawah Informasi pengujian: • Tampilkan semua peristiwa akun root selama jangka waktu • AWS CloudTrailember tidak publik • Tampilkan semua kebijakan dengan `Allow:*:*` dan cantumkan semua prinsipal dan layanan menggunakan kebijakan tersebut Saat Anda mengatur sumber data kontrol, sebaiknya sertakan semua hal berikut sebagai sumber data: Pilih AWS Config sebagai tipe sumber data, dan pilih aturan AWS Config terkelola berikut sebagai pemetaan sumber data: • IAM_ROOT_ACCESS_KEY_CHECK • ROOT_ACCOUNT_MFA_ENABLED • ROOT_ACCOUNT_HARDWARE_MFA_ENABLED • VPC_FLOW_LOGS_ENABLED • ACCESS_KEYS_DIPUTAR • IAM_PASSWORD_POLICY Pilih AWS Security Hub sebagai tipe sumber data, dan pilih kontrol Security Hub berikut sebagai pemetaan sumber data: • 1.1 (CloudWatch.1) • 1.1 (IAM.20) • 1.10 (IAM.16) • 1.11 (IAM.17) • 1.12 (IAM.4)

Nama kontrol	Set kontrol	Pemetaan sumber data kontrol yang disarankan
		• 1.13 (IAM.9) • 1.14 (IAM.6) • 1.16 (IAM.2) • 1.2 (IAM.5 • 1.20 (IAM.18) • 1.22 (IAM.1 • 1.3 (IAM.8) • 1.4 (IAM.3) • 1.5 (IAM.11) • 1.6 (IAM.12) • 1.7 (IAM.13) • 1.8 (IAM.14) • 1.9 (IAM.15) • 2.1 (CloudTrail.1) • 2.2 (CloudTrail.4) • 2.3 (CloudTrail.6) • 2.4 (CloudTrail.5) • 2.5 (Konfigurasi.1) • 2.6 (CloudTrail.7) • 2.7 (CloudTrail.2) • 2.8 (KMS.4) • 2.9 (EC2.6) • 3.1 (CloudWatch.2) • 3.10 (CloudWatch.10) • 3.11 (CloudWatch.11) • 3.12 (CloudWatch.12) • 3.13 (CloudWatch.13) • 3.14 (CloudWatch.14)

Nama kontrol	Set kontrol	Pemetaan sumber data kontrol yang disarankan
		• Konfigurasi.1
Pasal 30 Catatan kegiatan pemrosesan.1	Bab 4 - Pengontrol dan Prosesor	Anda dapat membuat kontrol khusus AWS Audit Manager yang mendukung kontrol GDPR ini. Saat Anda menentukan detail kontrol, masukkan yang berikut ini di bawah Informasi pengujian: • Tampilkan semua peristiwa akun root selama jangka waktu Saat Anda mengatur sumber data kontrol, sebaiknya sertakan semua hal berikut sebagai sumber data: Pilih AWS Config sebagai tipe sumber data, dan pilih aturan AWS Config terkelola berikut sebagai pemetaan sumber data: • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • VPC_FLOW_LOGS_ENABLED • CMK_BACKING_KEY_ROTATION_ENABLED • CLOUD_TRAIL_ENABLED • ELB_LOGGING_ENABLED • CLOUDTRAIL_SECURITY_TRAIL_ENABLED • REDSHIFT_CLUSTER_CONFIGURATION_CHECK • CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED Pilih AWS Security Hub sebagai tipe sumber data, dan pilih kontrol Security Hub berikut sebagai pemetaan sumber data: • Konfigurasi.1

Nama kontrol	Set kontrol	Pemetaan sumber data kontrol yang disarankan
Pasal 30 Catatan kegiatan pemrosesan.2	Bab 4 - Pengontrol dan Prosesor	Anda dapat membuat kontrol khusus AWS Audit Manager yang mendukung kontrol GDPR ini. Saat Anda menentukan detail kontrol, masukkan yang berikut ini di bawah Informasi pengujian: • Tampilkan semua peristiwa akun root selama jangka waktu Saat Anda mengatur sumber data kontrol, sebaiknya sertakan semua hal berikut sebagai sumber data: Pilih AWS Config sebagai tipe sumber data, dan pilih aturan AWS Config terkelola berikut sebagai pemetaan sumber data: • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • VPC_FLOW_LOGS_ENABLED • CMK_BACKING_KEY_ROTATION_ENABLED • CLOUD_TRAIL_ENABLED • ELB_LOGGING_ENABLED • CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED Pilih AWS Security Hub sebagai tipe sumber data, dan pilih kontrol Security Hub berikut sebagai pemetaan sumber data: • Konfigurasi.1

Nama kontrol	Set kontrol	Pemetaan sumber data kontrol yang disarankan
Pasal 30 Catatan kegiatan pemrosesan.3	Bab 4 - Pengontrol dan Prosesor	Anda dapat membuat kontrol khusus AWS Audit Manager yang mendukung kontrol GDPR ini. Saat Anda menentukan detail kontrol, masukkan yang berikut ini di bawah Informasi pengujian: • Tampilkan semua peristiwa akun root selama jangka waktu • AWS CloudTrailember tidak publik • Tampilkan semua kebijakan dengan `Allow:*:*` dan cantumkan semua prinsipal dan layanan menggunakan kebijakan tersebut Saat Anda mengatur sumber data kontrol, sebaiknya sertakan semua hal berikut sebagai sumber data: Pilih AWS Config sebagai tipe sumber data, dan pilih aturan AWS Config terkelola berikut sebagai pemetaan sumber data: • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • VPC_FLOW_LOGS_ENABLED • CMK_BACKING_KEY_ROTATION_ENABLED • CLOUD_TRAIL_ENABLED • ELB_LOGGING_ENABLED • CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED Pilih AWS Security Hub sebagai tipe sumber data, dan pilih kontrol Security Hub berikut sebagai pemetaan sumber data: • Konfigurasi.1

Nama kontrol	Set kontrol	Pemetaan sumber data kontrol yang disarankan
Pasal 30 Catatan kegiatan pemrosesan.4	Bab 4 - Pengontrol dan Prosesor	Anda dapat membuat kontrol khusus AWS Audit Manager yang mendukung kontrol GDPR ini. Saat Anda menentukan detail kontrol, masukkan yang berikut ini di bawah Informasi pengujian: • Tampilkan semua peristiwa akun root selama jangka waktu • AWS CloudTrailember tidak publik • Tampilkan semua kebijakan dengan `Allow:*:*` dan cantumkan semua prinsipal dan layanan menggunakan kebijakan tersebut Saat Anda mengatur sumber data kontrol, sebaiknya sertakan semua hal berikut sebagai sumber data: Pilih AWS Config sebagai tipe sumber data, dan pilih aturan AWS Config terkelola berikut sebagai pemetaan sumber data: • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • VPC_FLOW_LOGS_ENABLED • CMK_BACKING_KEY_ROTATION_ENABLED • CLOUD_TRAIL_ENABLED • ELB_LOGGING_ENABLED • CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED Pilih AWS Security Hub sebagai tipe sumber data, dan pilih kontrol Security Hub berikut sebagai pemetaan sumber data: • Konfigurasi.1

Nama kontrol	Set kontrol	Pemetaan sumber data kontrol yang disarankan
Pasal 30 Catatan kegiatan pemrosesan.5	Bab 4 - Pengontrol dan Prosesor	Anda dapat membuat kontrol khusus AWS Audit Manager yang mendukung kontrol GDPR ini. Saat Anda menentukan detail kontrol, masukkan yang berikut ini di bawah Informasi pengujian: • Tampilkan semua peristiwa akun root selama jangka waktu Saat Anda mengatur sumber data kontrol, sebaiknya sertakan semua hal berikut sebagai sumber data: Pilih AWS Config sebagai tipe sumber data, dan pilih aturan AWS Config terkelola berikut sebagai pemetaan sumber data: • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • VPC_FLOW_LOGS_ENABLED • CMK_BACKING_KEY_ROTATION_ENABLED • CLOUD_TRAIL_ENABLED • ELB_LOGGING_ENABLED • CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED Pilih AWS Security Hub sebagai tipe sumber data, dan pilih kontrol Security Hub berikut sebagai pemetaan sumber data: • Konfigurasi.1

Nama kontrol	Set kontrol	Pemetaan sumber data kontrol yang disarankan
Pasal 32 Keamanan pemrosesan.1	Bab 4 - Pengontrol dan Prosesor	Anda dapat membuat kontrol khusus AWS Audit Manager yang mendukung kontrol GDPR ini. Saat Anda menentukan detail kontrol, masukkan yang berikut ini di bawah Informasi pengujian: • Tampilkan enkripsi data saat istirahat untuk semua layanan • Tampilkan data dalam enkripsi transit untuk semua layanan • MFA Hapus diaktifkan untuk Amazon S3 • Semua pemindaian Amazon Inspector • Tampilkan semua instance yang tidak diaktifkan Amazon Inspector • Tampilkan semua penyeimbang beban yang mendengarkan di HTTPS (SSL) • AWS CloudTraildienkripsi saat istirahat • Amazon CloudWatch memberi peringatan untuk AWS Config menampilkan semua perubahan dan semua pengaturan yang dikomentari • Semua aktivitas root Saat Anda mengatur sumber data kontrol, sebaiknya sertakan semua hal berikut sebagai sumber data: Pilih AWS Config sebagai tipe sumber data, dan pilih aturan AWS Config terkelola berikut sebagai pemetaan sumber data: • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • S3_BUCKET_SSL_REQUESTS_ONLY • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUDWATCH_LOG_GROUP_ENCRYPTED • EFS_ENCRYPTED_CHECK • ELASTICSEARCH_ENCRYPTED_AT_REST • TERENKRIPTED_VOLUME

Nama kontrol	Set kontrol	Pemetaan sumber data kontrol yang disarankan
		• RDS_STORAGE_ENCRYPTED • REDSHIFT_CLUSTER_CONFIGURATION_CHECK • S3_BUCKET_SERVER_SIDE_ENCRYPTION_ENABLED • SAGEMAKER_ENDPOINT_CONFIGURATION_KMS_KEY_CONFIGURATED • SAGEMAKER_NOTEBOOK_INSTANCE_KMS_KEY_CONFIGURATED • SNS_ENCRYPTED_KMS • EC2_EBS_ENCRYPTION_BY_DEFAULT • DYNAMODB_TABLE_ENCRYPTED_KMS • DYNAMODB_TABLE_ENCRYPTION_ENABLED • RDS_SNAPSHOT_ENCRYPTED • S3_DEFAULT_ENCRYPTION_KMS • DAX_ENCRYPTION_ENABLED • EKS_SECRETS_ENCRYPTED • RDS_LOGGING_ENABLED • REDSHIFT_BACKUP_ENABLED • RDS_IN_BACKUP_PLAN • WAF_CLASSIC_LOGGING_ENABLED • WAFV2_LOGGING_ENABLED • ALB_HTTP_TO_HTTP_REDIRECTION_CHECK • ELB_ACM_CERTIFICATE_REQUIRED • ELB_CUSTOM_SECURITY_POLICY_SSL_CHECK • REDSHIFT_REQUIRE_TLS_SSL • CLOUDFRONT_VIEWER_POLICY_HTTPS • ALB_HTTP_DROP_INVALID_HEADER_ENABLED • ELASTICSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK • ELB_TLS_HTTPS_LISTENERS_ONLY • ACM_CERTIFICATE_EXPIRATION_CHECK

Nama kontrol	Set kontrol	Pemetaan sumber data kontrol yang disarankan
		• API_GW_CACHE_ENABLED_AND_ENCRYPTED

Nama kontrol	Set kontrol	Pemetaan sumber data kontrol yang disarankan
Pasal 32 Keamanan pemrosesan.2	Bab 4 - Pengontrol dan Prosesor	Anda dapat membuat kontrol khusus AWS Audit Manager yang mendukung kontrol GDPR ini. Saat Anda menentukan detail kontrol, masukkan yang berikut ini di bawah Informasi pengujian: • Tampilkan enkripsi data saat istirahat untuk semua layanan • Tampilkan data dalam enkripsi transit untuk semua layanan • MFA Hapus diaktifkan untuk Amazon S3 • Semua pemindaian Amazon Inspector • Tampilkan semua instance yang tidak diaktifkan Amazon Inspector • Tampilkan semua penyeimbang beban yang mendengarkan di HTTPS (SSL) • AWS CloudTraildienkripsi saat istirahat • Amazon CloudWatch memberi peringatan untuk AWS Config menampilkan semua perubahan dan semua pengaturan yang dikomentari • Semua aktivitas root Saat Anda mengatur sumber data kontrol, sebaiknya sertakan semua hal berikut sebagai sumber data: Pilih AWS Config sebagai tipe sumber data, dan pilih aturan AWS Config terkelola berikut sebagai pemetaan sumber data: • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • S3_BUCKET_SSL_REQUESTS_ONLY • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUDWATCH_LOG_GROUP_ENCRYPTED • EFS_ENCRYPTED_CHECK • ELASTICSEARCH_ENCRYPTED_AT_REST • TERENKRIPTED_VOLUME

Nama kontrol	Set kontrol	Pemetaan sumber data kontrol yang disarankan
		• RDS_STORAGE_ENCRYPTED • REDSHIFT_CLUSTER_CONFIGURATION_CHECK • S3_BUCKET_SERVER_SIDE_ENCRYPTION_ENABLED • SAGEMAKER_ENDPOINT_CONFIGURATION_KMS_KEY_CONFIGURATED • SAGEMAKER_NOTEBOOK_INSTANCE_KMS_KEY_CONFIGURATED • SNS_ENCRYPTED_KMS • EC2_EBS_ENCRYPTION_BY_DEFAULT • DYNAMODB_TABLE_ENCRYPTED_KMS • DYNAMODB_TABLE_ENCRYPTION_ENABLED • RDS_SNAPSHOT_ENCRYPTED • S3_DEFAULT_ENCRYPTION_KMS • DAX_ENCRYPTION_ENABLED • EKS_SECRETS_ENCRYPTED • RDS_LOGGING_ENABLED • REDSHIFT_BACKUP_ENABLED • RDS_IN_BACKUP_PLAN • WAF_CLASSIC_LOGGING_ENABLED • WAFV2_LOGGING_ENABLED • ALB_HTTP_TO_HTTP_REDIRECTION_CHECK • ELB_ACM_CERTIFICATE_REQUIRED • ELB_CUSTOM_SECURITY_POLICY_SSL_CHECK • REDSHIFT_REQUIRE_TLS_SSL • CLOUDFRONT_VIEWER_POLICY_HTTPS • ALB_HTTP_DROP_INVALID_HEADER_ENABLED • ELASTICSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK • ELB_TLS_HTTPS_LISTENERS_ONLY • ACM_CERTIFICATE_EXPIRATION_CHECK

Nama kontrol	Set kontrol	Pemetaan sumber data kontrol yang disarankan
		• API_GW_CACHE_ENABLED_AND_ENCRYPTED

Nama kontrol	Set kontrol	Pemetaan sumber data kontrol yang disarankan
Pasal 32 Keamanan pemrosesan.3	Bab 4 - Pengontrol dan Prosesor	Anda dapat membuat kontrol khusus AWS Audit Manager yang mendukung kontrol GDPR ini. Saat Anda menentukan detail kontrol, masukkan yang berikut ini di bawah Informasi pengujian: • Tampilkan enkripsi data saat istirahat untuk semua layanan • Tampilkan data dalam enkripsi transit untuk semua layanan • MFA Hapus diaktifkan untuk Amazon S3 • Semua pemindaian Amazon Inspector • Tampilkan semua instance yang tidak diaktifkan Amazon Inspector • Tampilkan semua penyeimbang beban yang mendengarkan di HTTPS (SSL) • AWS CloudTraildienkripsi saat istirahat • Amazon CloudWatch memberi peringatan untuk AWS Config menampilkan semua perubahan dan semua pengaturan yang dikomentari • Semua aktivitas root Saat Anda mengatur sumber data kontrol, sebaiknya sertakan semua hal berikut sebagai sumber data: Pilih AWS Config sebagai tipe sumber data, dan pilih aturan AWS Config terkelola berikut sebagai pemetaan sumber data: • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • S3_BUCKET_SSL_REQUESTS_ONLY • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUDWATCH_LOG_GROUP_ENCRYPTED • EFS_ENCRYPTED_CHECK • ELASTICSEARCH_ENCRYPTED_AT_REST • TERENKRIPTED_VOLUME

Nama kontrol	Set kontrol	Pemetaan sumber data kontrol yang disarankan
		• RDS_STORAGE_ENCRYPTED • REDSHIFT_CLUSTER_CONFIGURATION_CHECK • S3_BUCKET_SERVER_SIDE_ENCRYPTION_ENABLED • SAGEMAKER_ENDPOINT_CONFIGURATION_KMS_KEY_CONFIGURATED • SAGEMAKER_NOTEBOOK_INSTANCE_KMS_KEY_CONFIGURATED • SNS_ENCRYPTED_KMS • EC2_EBS_ENCRYPTION_BY_DEFAULT • DYNAMODB_TABLE_ENCRYPTED_KMS • DYNAMODB_TABLE_ENCRYPTION_ENABLED • RDS_SNAPSHOT_ENCRYPTED • S3_DEFAULT_ENCRYPTION_KMS • DAX_ENCRYPTION_ENABLED • EKS_SECRETS_ENCRYPTED • RDS_LOGGING_ENABLED • REDSHIFT_BACKUP_ENABLED • RDS_IN_BACKUP_PLAN • WAF_CLASSIC_LOGGING_ENABLED • WAFV2_LOGGING_ENABLED • ALB_HTTP_TO_HTTP_REDIRECTION_CHECK • ELB_ACM_CERTIFICATE_REQUIRED • ELB_CUSTOM_SECURITY_POLICY_SSL_CHECK • REDSHIFT_REQUIRE_TLS_SSL • CLOUDFRONT_VIEWER_POLICY_HTTPS • ALB_HTTP_DROP_INVALID_HEADER_ENABLED • ELASTICSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK • ELB_TLS_HTTPS_LISTENERS_ONLY • ACM_CERTIFICATE_EXPIRATION_CHECK

Nama kontrol	Set kontrol	Pemetaan sumber data kontrol yang disarankan
		• API_GW_CACHE_ENABLED_AND_ENCRYPTED

Nama kontrol	Set kontrol	Pemetaan sumber data kontrol yang disarankan
Pasal 32 Keamanan pemrosesan.4	Bab 4 - Pengontrol dan Prosesor	Anda dapat membuat kontrol khusus AWS Audit Manager yang mendukung kontrol GDPR ini. Saat Anda menentukan detail kontrol, masukkan yang berikut ini di bawah Informasi pengujian: • Tampilkan enkripsi data saat istirahat untuk semua layanan • Tampilkan data dalam enkripsi transit untuk semua layanan • MFA Hapus diaktifkan untuk Amazon S3 • Semua pemindaian Amazon Inspector • Tampilkan semua instance yang tidak diaktifkan Amazon Inspector • Tampilkan semua penyeimbang beban yang mendengarkan di HTTPS (SSL) • AWS CloudTraildienkripsi saat istirahat • Amazon CloudWatch memberi peringatan untuk AWS Config menampilkan semua perubahan dan semua pengaturan yang dikomentari • Semua aktivitas root Saat Anda mengatur sumber data kontrol, sebaiknya sertakan semua hal berikut sebagai sumber data: Pilih AWS Config sebagai tipe sumber data, dan pilih aturan AWS Config terkelola berikut sebagai pemetaan sumber data: • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • S3_BUCKET_SSL_REQUESTS_ONLY • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUDWATCH_LOG_GROUP_ENCRYPTED • EFS_ENCRYPTED_CHECK • ELASTICSEARCH_ENCRYPTED_AT_REST • TERENKRIPTED_VOLUME

Nama kontrol	Set kontrol	Pemetaan sumber data kontrol yang disarankan
		• RDS_STORAGE_ENCRYPTED • REDSHIFT_CLUSTER_CONFIGURATION_CHECK • S3_BUCKET_SERVER_SIDE_ENCRYPTION_ENABLED • SAGEMAKER_ENDPOINT_CONFIGURATION_KMS_KEY_CONFIGURATED • SAGEMAKER_NOTEBOOK_INSTANCE_KMS_KEY_CONFIGURATED • SNS_ENCRYPTED_KMS • EC2_EBS_ENCRYPTION_BY_DEFAULT • DYNAMODB_TABLE_ENCRYPTED_KMS • DYNAMODB_TABLE_ENCRYPTION_ENABLED • RDS_SNAPSHOT_ENCRYPTED • S3_DEFAULT_ENCRYPTION_KMS • DAX_ENCRYPTION_ENABLED • EKS_SECRETS_ENCRYPTED • RDS_LOGGING_ENABLED • REDSHIFT_BACKUP_ENABLED • RDS_IN_BACKUP_PLAN • WAF_CLASSIC_LOGGING_ENABLED • WAFV2_LOGGING_ENABLED • ALB_HTTP_TO_HTTP_REDIRECTION_CHECK • ELB_ACM_CERTIFICATE_REQUIRED • ELB_CUSTOM_SECURITY_POLICY_SSL_CHECK • REDSHIFT_REQUIRE_TLS_SSL • CLOUDFRONT_VIEWER_POLICY_HTTPS • ALB_HTTP_DROP_INVALID_HEADER_ENABLED • ELASTICSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK • ELB_TLS_HTTPS_LISTENERS_ONLY • ACM_CERTIFICATE_EXPIRATION_CHECK

Nama kontrol	Set kontrol	Pemetaan sumber data kontrol yang disarankan
		• API_GW_CACHE_ENABLED_AND_ENCRYPTED

Setelah Anda membuat kontrol kustom baru untuk GDPR, Anda dapat menambahkannya ke kerangka kerja GDPR kustom. Untuk informasi selengkapnya, silakan lihat Membuat kerangka kerja khusus dan Mengedit kerangka kerja khusus. Anda kemudian dapat membuat penilaian dari kerangka kerja GDPR khusus. Dengan cara ini, AWS Audit Manager dapat mengumpulkan bukti secara otomatis untuk kontrol kustom yang Anda tambahkan. Untuk petunjuk tentang cara membuat penilaian dari kerangka kerja, lihatMembuat penilaian.

Lebih banyak sumber daya GDPR

- Pusat Peraturan Perlindungan Data Umum (GDPR)
- AWSPostingan blog GDPR

Gramm-Leach-Bliley Act

AWS Audit Managermenyediakan kerangka kerja prebuilt yang mendukung Gramm-Leach-Bliley Act (GLBA).

Topik

- Apa itu Gramm-Leach-Bliley Act (GLBA)?
- Menggunakan kerangka kerja ini untuk mendukung persiapan audit Anda

Apa itu Gramm-Leach-Bliley Act (GLBA)?

Gramm-Leach-Bliley Act (GLB Act atau GLBA), juga dikenal sebagai Undang-Undang Modernisasi Layanan Keuangan tahun 1999, adalah undang-undang federal yang diberlakukan di Amerika Serikat untuk mengontrol cara-cara lembaga keuangan menangani informasi pribadi individu. Undang-undang ini terdiri dari tiga bagian. Yang pertama adalah Aturan Privasi Keuangan, yang mengatur pengumpulan dan pengungkapan informasi keuangan pribadi. Yang kedua adalah Aturan Pengamanan, yang menetapkan bahwa lembaga keuangan harus menerapkan program keamanan untuk melindungi informasi tersebut. Yang ketiga adalah ketentuan Pretexting, yang melarang praktik pretexting (mengakses informasi pribadi menggunakan kepura-puraan palsu). Undang-undang

ini juga mewajibkan lembaga keuangan untuk memberikan pemberitahuan privasi tertulis kepada pelanggan yang menjelaskan praktik berbagi informasi mereka.

Menggunakan kerangka kerja ini untuk mendukung persiapan audit Anda

Anda dapat menggunakan kerangka kerja Gramm-Leach-Bliley Act (GLBA) untuk membantu Anda mempersiapkan audit. Kerangka kerja ini mencakup kumpulan kontrol bawaan dengan deskripsi dan prosedur pengujian. Kontrol ini dikelompokkan ke dalam set kontrol sesuai dengan persyaratan GLBA. Anda juga dapat menyesuaikan kerangka kerja ini dan kontrolnya untuk mendukung audit internal dengan persyaratan khusus.

Dengan menggunakan kerangka kerja GLBA sebagai titik awal, Anda dapat membuat penilaian Audit Manager dan mulai mengumpulkan bukti yang relevan untuk audit GLBA. Dalam penilaian Anda, Anda dapat menentukan Akun AWS dan layanan yang ingin Anda sertakan dalam lingkup audit Anda. Setelah Anda membuat penilaian, Audit Manager mulai menilai AWS sumber daya Anda. Hal ini dilakukan berdasarkan kontrol yang didefinisikan dalam kerangka GLBA. Saat tiba waktunya untuk audit, Anda—atau delegasi pilihan Anda—dapat meninjau bukti yang dikumpulkan oleh Audit Manager. Anda juga dapat menelusuri folder bukti dalam penilaian Anda dan memilih bukti mana yang ingin Anda sertakan dalam laporan penilaian Anda. Atau, jika Anda mengaktifkan pencari bukti, Anda dapat mencari bukti spesifik dan mengekspornya dalam format CSV, atau membuat laporan penilaian dari hasil penelusuran Anda. Either way, Anda dapat menggunakan laporan penilaian ini untuk menunjukkan bahwa kontrol Anda berfungsi sebagaimana dimaksud.

Rincian kerangka kerja GLBA adalah sebagai berikut:

Nama kerangka kerja di AWS Audit Manager	Jumlah kontrol otomatis	Jumlah kontrol manual	Jumlah set kontrol	Layanan AWSdalam ruang lingkup
Gramm-Leach-Bliley Act (GLBA)	4	110	16	• Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Security Hub

> **Tip**
>
> Untuk meninjau AWS Config aturan yang digunakan sebagai pemetaan sumber data dalam kerangka standar ini, unduh file AuditManager_ ConfigDataSourceMappings _GLBA.zip.

Kontrol dalam AWS Audit Manager kerangka kerja ini tidak dimaksudkan untuk memverifikasi apakah sistem Anda sesuai dengan standar GLBA. Selain itu, mereka tidak dapat menjamin bahwa Anda akan lulus audit GLBA. AWS Audit Managertidak secara otomatis memeriksa kontrol prosedural yang memerlukan pengumpulan bukti manual.

Anda dapat menemukan kerangka kerja GLBA di bawah tab Kerangka Standar Pustaka kerangka kerja di Audit Manager.

Untuk petunjuk tentang cara membuat penilaian menggunakan kerangka kerja ini, lihatMembuat penilaian.

Saat Anda menggunakan konsol Audit Manager untuk membuat penilaian dari kerangka kerja standar ini, daftar Layanan AWS dalam cakupan dipilih secara default dan tidak dapat diedit. Ini karena Audit Manager secara otomatis memetakan dan memilih sumber data dan layanan untuk Anda. Seleksi ini dibuat sesuai dengan persyaratan GLBA. Jika Anda perlu mengedit daftar layanan dalam ruang lingkup untuk kerangka kerja ini, Anda dapat melakukannya dengan menggunakan operasi CreateAssessmentatau UpdateAssessmentAPI. Atau, Anda dapat menyesuaikan kerangka kerja standar dan kemudian membuat penilaian dari kerangka kerja khusus.

Untuk petunjuk tentang cara menyesuaikan kerangka kerja ini untuk mendukung persyaratan spesifik Anda, lihat Menyesuaikan kerangka kerja yang ada dan Menyesuaikan kontrol yang ada.

GxP 21 CFR bagian 11

AWS Audit Managermenyediakan kerangka kerja bawaan yang mendukung peraturan GxP CFR bagian 11 berdasarkan AWS praktik terbaik.

> **Note**
>
> Untuk informasi tentang GxP EU Annex 11 dan kerangka kerja Audit Manager yang mendukungnya, lihat. Lampiran GxP UE 11

Topik

Apa itu GxP CFR bagian 11?

GxP mengacu pada peraturan dan pedoman yang berlaku untuk organisasi ilmu hayati yang membuat makanan dan produk medis. Produk medis yang termasuk dalam ini termasuk obat-obatan, perangkat medis, dan aplikasi perangkat lunak medis. Tujuan keseluruhan dari persyaratan GxP adalah untuk memastikan bahwa makanan dan produk medis aman bagi konsumen. Ini juga untuk memastikan integritas data yang digunakan untuk membuat keputusan keselamatan terkait produk.

Istilah GxP mencakup berbagai kegiatan terkait kepatuhan. Ini termasuk Good Laboratory Practices (GLP), Good Clinical Practices (GCP), dan Good Manufacturing Practices (GMP). Masing-masing jenis kegiatan yang berbeda ini melibatkan persyaratan khusus produk yang harus diterapkan oleh organisasi ilmu hayati. Ini didasarkan pada jenis produk yang dibuat organisasi serta negara tempat produk mereka dijual. Ketika organisasi ilmu hayati menggunakan sistem komputerisasi untuk melakukan aktivitas GxP tertentu, mereka harus memastikan bahwa sistem GxP terkomputerisasi dikembangkan, divalidasi, dan dioperasikan dengan tepat untuk tujuan penggunaan sistem.

Untuk pendekatan komprehensif dalam menggunakan AWS Cloud untuk sistem GxP, lihat whitepaper Pertimbangan untuk Menggunakan AWS Produk di Sistem GxP.

Menggunakan kerangka kerja ini untuk mendukung persiapan audit Anda

Anda dapat menggunakan kerangka kerja GxP 21 CFR Bagian 11 untuk membantu Anda mempersiapkan audit. Kerangka kerja ini mencakup kumpulan kontrol bawaan dengan deskripsi dan prosedur pengujian. Kontrol ini dikelompokkan ke dalam set kontrol sesuai dengan persyaratan GxP. Anda juga dapat menyesuaikan kerangka kerja ini dan kontrolnya untuk mendukung audit internal dengan persyaratan khusus.

Dengan menggunakan kerangka kerja sebagai titik awal, Anda dapat membuat penilaian Audit Manager dan mulai mengumpulkan bukti yang relevan untuk audit Anda. Setelah Anda membuat penilaian, Audit Manager mulai menilai AWS sumber daya Anda. Ini dilakukan berdasarkan kontrol yang didefinisikan dalam kerangka kerja GxP 21 CFR Bagian 11. Saat tiba waktunya untuk audit, Anda—atau delegasi pilihan Anda—dapat meninjau bukti yang dikumpulkan oleh Audit Manager. Anda juga dapat menelusuri folder bukti dalam penilaian Anda dan memilih bukti mana yang ingin Anda sertakan dalam laporan penilaian Anda. Atau, jika Anda mengaktifkan pencari bukti, Anda

dapat mencari bukti spesifik dan mengekspornya dalam format CSV, atau membuat laporan penilaian dari hasil penelusuran Anda. Either way, Anda dapat menggunakan laporan penilaian ini untuk menunjukkan bahwa kontrol Anda berfungsi sebagaimana dimaksud.

Rincian kerangka kerja GxP CFR Bagian 11 adalah sebagai berikut:

Nama kerangka kerja di AWS Audit Manager	Jumlah kontrol otomatis	Jumlah kontrol manual	Jumlah set kontrol	Layanan AWSdalam ruang lingkup
GxP 21 CFR Bagian 11	13	14	7	• AWS CloudTrail • AWS Config • AWS Identity and Access Management

> **Tip**
>
> Untuk meninjau AWS Config aturan yang digunakan sebagai pemetaan sumber data dalam kerangka standar ini, unduh file AuditManager_ ConfigDataSourceMappings _GxP-21-CFR-Part-11.zip.

Kontrol dalam AWS Audit Manager kerangka kerja ini tidak dimaksudkan untuk memverifikasi apakah sistem Anda sesuai dengan peraturan GxP. Selain itu, mereka tidak dapat menjamin bahwa Anda akan lulus audit GxP. AWS Audit Managertidak secara otomatis memeriksa kontrol prosedural yang memerlukan pengumpulan bukti manual.

Anda dapat menemukan kerangka kerja ini di bawah tab Kerangka Standar Pustaka kerangka kerja di Audit Manager.

Untuk petunjuk tentang cara membuat penilaian menggunakan kerangka kerja ini, lihatMembuat penilaian.

Saat Anda menggunakan konsol Audit Manager untuk membuat penilaian dari kerangka kerja standar ini, daftar Layanan AWS dalam cakupan dipilih secara default dan tidak dapat diedit. Ini karena Audit Manager secara otomatis memetakan dan memilih sumber data dan layanan untuk

Anda. Pemilihan ini dibuat sesuai dengan persyaratan kerangka kerja GxP CFR Bagian 11. Jika Anda perlu mengedit daftar layanan dalam ruang lingkup untuk kerangka kerja ini, Anda dapat melakukannya dengan menggunakan operasi CreateAssessmentatau UpdateAssessmentAPI. Atau, Anda dapat menyesuaikan kerangka kerja standar dan kemudian membuat penilaian dari kerangka kerja khusus.

Untuk petunjuk tentang cara menyesuaikan kerangka kerja ini untuk mendukung persyaratan spesifik Anda, lihat Menyesuaikan kerangka kerja yang ada dan Menyesuaikan kontrol yang ada.

Lebih banyak sumber daya GxP

- AWSHalaman kepatuhan untuk GxP
- Pertimbangan untuk Menggunakan AWS Produk dalam Sistem GxP

Lampiran GxP UE 11

AWS Audit Managermenyediakan kerangka kerja bawaan yang mendukung peraturan GxP EU Annex 11 berdasarkan praktik terbaik. AWS

> **Note**
>
> Untuk informasi tentang GxP 21 CFR Bagian 11 dan kerangka kerja Audit Manager yang mendukungnya, lihat. GxP 21 CFR bagian 11

Topik

- Apa itu GxP EU Annex 11?
- Menggunakan kerangka kerja ini untuk mendukung persiapan audit Anda

Apa itu GxP EU Annex 11?

Kerangka kerja GxP EU Annex 11 adalah setara Eropa dengan kerangka kerja FDA 21 CFR bagian 11 di Amerika Serikat. Lampiran ini berlaku untuk semua bentuk sistem komputerisasi yang digunakan sebagai bagian dari kegiatan yang diatur Good Manufacturing Practices (GMP). Sistem komputerisasi adalah seperangkat komponen perangkat lunak dan perangkat keras yang bersama-sama memenuhi fungsionalitas tertentu. Aplikasi harus divalidasi dan infrastruktur TI harus memenuhi syarat. Jika sistem komputerisasi menggantikan operasi manual, seharusnya tidak ada

penurunan kualitas produk, kontrol proses, atau jaminan kualitas yang dihasilkan. Seharusnya tidak ada peningkatan risiko keseluruhan proses.

Lampiran 11 adalah bagian dari pedoman GMP Eropa dan mendefinisikan kerangka acuan untuk sistem komputerisasi yang digunakan oleh organisasi di industri farmasi. Lampiran 11 berfungsi sebagai daftar periksa yang memungkinkan badan pengatur Eropa untuk menetapkan persyaratan untuk sistem komputerisasi yang berhubungan dengan produk farmasi dan perangkat medis. Pedoman yang ditetapkan oleh Komisi Komite Eropa tidak jauh dari FDA (21 CFR Bagian 11). Lampiran 11 mendefinisikan kriteria bagaimana catatan elektronik dan tanda tangan elektronik dianggap dikelola.

Menggunakan kerangka kerja ini untuk mendukung persiapan audit Anda

Anda dapat menggunakan kerangka kerja GxP EU Annex 11 untuk membantu Anda mempersiapkan audit. Kerangka kerja ini mencakup kumpulan kontrol bawaan dengan deskripsi dan prosedur pengujian. Kontrol ini dikelompokkan ke dalam set kontrol sesuai dengan persyaratan GxP. Anda juga dapat menyesuaikan kerangka kerja ini dan kontrolnya untuk mendukung audit internal dengan persyaratan khusus.

Dengan menggunakan kerangka kerja sebagai titik awal, Anda dapat membuat penilaian Audit Manager dan mulai mengumpulkan bukti yang relevan untuk audit Anda. Setelah Anda membuat penilaian, Audit Manager mulai menilai AWS sumber daya Anda. Ini dilakukan berdasarkan kontrol yang didefinisikan dalam kerangka GxP EU Annex 11. Saat tiba waktunya untuk audit, Anda—atau delegasi pilihan Anda—dapat meninjau bukti yang dikumpulkan oleh Audit Manager. Anda juga dapat menelusuri folder bukti dalam penilaian Anda dan memilih bukti mana yang ingin Anda sertakan dalam laporan penilaian Anda. Atau, jika Anda mengaktifkan pencari bukti, Anda dapat mencari bukti spesifik dan mengekspornya dalam format CSV, atau membuat laporan penilaian dari hasil penelusuran Anda. Either way, Anda dapat menggunakan laporan penilaian ini untuk menunjukkan bahwa kontrol Anda berfungsi sebagaimana dimaksud.

Rincian kerangka kerja GxP EU Annex 11 adalah sebagai berikut:

Nama kerangka kerja di AWS Audit Manager	Jumlah kontrol otomatis	Jumlah kontrol manual	Jumlah set kontrol	Layanan AWSdalam ruang lingkup
Lampiran GxP UE 11	19	13	3	• Amazon CloudWatch

Nama kerangka kerja di AWS Audit Manager	Jumlah kontrol otomatis	Jumlah kontrol manual	Jumlah set kontrol	Layanan AWSdalam ruang lingkup
				• AWS CloudTrail • AWS Config • AWS Identity and Access Managemen t • AWS Security Hub

> **Tip**
>
> Untuk meninjau AWS Config aturan yang digunakan sebagai pemetaan sumber data dalam kerangka standar ini, unduh file AuditManager_ ConfigDataSourceMappings _GxP-EU-Annex-11.zip.

Kontrol dalam kerangka kerja ini tidak dimaksudkan untuk memverifikasi apakah sistem Anda sesuai dengan persyaratan GxP EU Annex 11. Selain itu, mereka tidak dapat menjamin bahwa Anda akan lulus audit GxP. AWS Audit Managertidak secara otomatis memeriksa kontrol prosedural yang memerlukan pengumpulan bukti manual.

Anda dapat menemukan kerangka kerja ini di bawah tab Kerangka Standar Pustaka kerangka kerja di Audit Manager.

Untuk petunjuk tentang cara membuat penilaian menggunakan kerangka kerja ini, lihatMembuat penilaian.

Saat Anda menggunakan konsol Audit Manager untuk membuat penilaian dari kerangka kerja standar ini, daftar Layanan AWS dalam cakupan dipilih secara default dan tidak dapat diedit. Ini karena Audit Manager secara otomatis memetakan dan memilih sumber data dan layanan untuk Anda. Pemilihan ini dibuat sesuai dengan persyaratan kerangka kerja GxP EU Annex 11. Jika Anda perlu mengedit daftar layanan dalam ruang lingkup untuk kerangka kerja ini, Anda dapat melakukannya dengan menggunakan operasi CreateAssessmentatau UpdateAssessmentAPI. Atau, Anda dapat menyesuaikan kerangka kerja standar dan kemudian membuat penilaian dari kerangka kerja khusus.

Untuk petunjuk tentang cara menyesuaikan kerangka kerja ini untuk mendukung persyaratan spesifik Anda, lihat Menyesuaikan kerangka kerja yang ada dan Menyesuaikan kontrol yang ada.

Aturan Keamanan Undang-Undang Portabilitas dan Akuntabilitas Asuransi Kesehatan (HIPAA) 2003

AWS Audit Managermenyediakan kerangka kerja bawaan yang mendukung aturan HIPAA untuk membantu Anda dengan persiapan audit Anda.

> **Note**
>
> Kerangka kerja ini sebelumnya bernama HIPAA di perpustakaan kerangka kerja. Pada tanggal 08 Maret 2023, kami memperbarui nama framework ini ke HIPAA Security Rule 2003 untuk membedakannya dari HIPAA Final Omnibus Security Rule 2013.
> Untuk informasi tentang HIPAA Final Omnibus Security Rule 2013 dan framework Audit Manager yang mendukung standar ini, lihat. Undang-Undang Portabilitas dan Akuntabilitas Asuransi Kesehatan (HIPAA) Final Omnibus Security Rule 2013

Topik

Apa itu HIPAA dan Aturan Keamanan HIPAA 2003?

Undang-Undang Portabilitas dan Akuntabilitas Asuransi Kesehatan 1996 (HIPAA) adalah undang-undang yang membantu pekerja AS untuk mempertahankan cakupan asuransi kesehatan ketika mereka berganti atau kehilangan pekerjaan. Undang-undang ini juga berupaya mendorong catatan kesehatan elektronik untuk meningkatkan efisiensi dan kualitas sistem perawatan kesehatan AS melalui peningkatan berbagi informasi.

Seiring dengan meningkatnya penggunaan catatan medis elektronik, HIPAA mencakup ketentuan untuk melindungi keamanan dan privasi informasi kesehatan yang dilindungi (PHI). PHI mencakup serangkaian data kesehatan dan kesehatan yang dapat diidentifikasi secara pribadi yang sangat luas. Ini termasuk informasi asuransi dan penagihan, data diagnosis, data perawatan klinis, dan hasil lab seperti gambar dan hasil tes.

Departemen Kesehatan dan Layanan Kemanusiaan AS menerbitkan Aturan Keamanan final pada Februari 2003. Aturan ini menetapkan standar nasional untuk melindungi kerahasiaan, integritas, dan ketersediaan informasi kesehatan yang dilindungi secara elektronik.

Aturan HIPAA berlaku untuk entitas yang tercakup. Ini termasuk rumah sakit, penyedia layanan medis, rencana kesehatan yang disponsori majikan, fasilitas penelitian, dan perusahaan asuransi yang berurusan langsung dengan pasien dan data pasien. Persyaratan HIPAA untuk melindungi PHI juga meluas ke rekan bisnis.

Untuk informasi selengkapnya tentang bagaimana HIPAA dan HITECH melindungi informasi kesehatan, lihat halaman web Privasi Informasi Kesehatan dari Departemen Kesehatan dan Layanan Kemanusiaan AS.

Semakin banyak penyedia layanan kesehatan, pembayar, dan profesional TI menggunakan layanan cloud AWS berbasis utilitas untuk memproses, menyimpan, dan mengirimkan informasi kesehatan yang dilindungi (PHI). AWSmemungkinkan entitas yang dilindungi dan rekan bisnis mereka yang tunduk pada HIPAA untuk menggunakan AWS lingkungan yang aman untuk memproses, memelihara, dan menyimpan informasi kesehatan yang dilindungi.

Untuk petunjuk tentang cara Anda dapat menggunakan AWS untuk pemrosesan dan penyimpanan informasi kesehatan, lihat whitepaper Architecting for HIPAA Security and Compliance on Amazon Web Services.

Menggunakan kerangka kerja ini untuk mendukung persiapan audit Anda

Anda dapat menggunakan kerangka HIPAA Security Rule 2003 untuk membantu Anda mempersiapkan audit. Kerangka kerja ini mencakup kumpulan kontrol bawaan dengan deskripsi dan prosedur pengujian. Kontrol ini dikelompokkan ke dalam set kontrol sesuai dengan persyaratan HIPAA. Anda juga dapat menyesuaikan kerangka kerja ini dan kontrolnya untuk mendukung audit internal dengan persyaratan khusus.

Dengan menggunakan kerangka kerja sebagai titik awal, Anda dapat membuat penilaian Audit Manager dan mulai mengumpulkan bukti yang relevan untuk audit Anda. Setelah Anda membuat penilaian, Audit Manager mulai menilai AWS sumber daya Anda. Hal ini dilakukan berdasarkan kontrol yang didefinisikan dalam kerangka HIPAA. Saat tiba waktunya untuk audit, Anda—atau delegasi pilihan Anda—dapat meninjau bukti yang dikumpulkan oleh Audit Manager. Anda juga dapat menelusuri folder bukti dalam penilaian Anda dan memilih bukti mana yang ingin Anda sertakan dalam laporan penilaian Anda. Atau, jika Anda mengaktifkan pencari bukti, Anda dapat mencari bukti spesifik dan mengekspornya dalam format CSV, atau membuat laporan penilaian dari hasil

penelusuran Anda. Either way, Anda dapat menggunakan laporan penilaian ini untuk menunjukkan bahwa kontrol Anda berfungsi sebagaimana dimaksud.

Rincian kerangka HIPAA Security Rule 2003 adalah sebagai berikut:

Nama kerangka kerja di AWS Audit Manager	Jumlah kontrol otomatis	Jumlah kontrol manual	Jumlah set kontrol	Layanan AWSdalam ruang lingkup
Aturan Keamanan HIPAA 2003	35	53	5	• Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Security Hub

> **Tip**
>
> Untuk meninjau AWS Config aturan yang digunakan sebagai pemetaan sumber data dalam kerangka standar ini, unduh file AuditManager_ ConfigDataSourceMappings _HIPAA-Security-Rule-2003.zip.

Kontrol dalam AWS Audit Manager kerangka kerja ini tidak dimaksudkan untuk memverifikasi apakah sistem Anda sesuai dengan standar HIPAA. Selain itu, mereka tidak dapat menjamin bahwa Anda akan lulus audit HIPAA. AWS Audit Managertidak secara otomatis memeriksa kontrol prosedural yang memerlukan pengumpulan bukti manual.

Anda dapat menemukan kerangka kerja ini di bawah tab Kerangka Standar Pustaka kerangka kerja di Audit Manager.

Untuk petunjuk tentang cara membuat penilaian menggunakan kerangka kerja ini, lihatMembuat penilaian.

Saat Anda menggunakan konsol Audit Manager untuk membuat penilaian dari kerangka kerja standar ini, daftar Layanan AWS dalam cakupan dipilih secara default dan tidak dapat diedit. Ini karena Audit Manager secara otomatis memetakan dan memilih sumber data dan layanan untuk Anda. Pemilihan ini dibuat sesuai dengan persyaratan kerangka HIPAA. Jika Anda perlu mengedit daftar layanan dalam ruang lingkup untuk kerangka kerja ini, Anda dapat melakukannya dengan menggunakan operasi CreateAssessmentatau UpdateAssessmentAPI. Atau, Anda dapat menyesuaikan kerangka kerja standar dan kemudian membuat penilaian dari kerangka kerja khusus.

Untuk petunjuk tentang cara menyesuaikan kerangka kerja ini untuk mendukung persyaratan spesifik Anda, lihat Menyesuaikan kerangka kerja yang ada dan Menyesuaikan kontrol yang ada.

Lebih banyak sumber daya HIPAA

- Informasi Kesehatan Privasi dari Departemen Kesehatan dan Layanan Kemanusiaan AS
- Aturan Keamanan dari Departemen Kesehatan dan Layanan Kemanusiaan AS
- Arsitektur untuk Keamanan dan Kepatuhan HIPAA di Amazon Web Services
- AWSHalaman kepatuhan untuk HIPAA

Undang-Undang Portabilitas dan Akuntabilitas Asuransi Kesehatan (HIPAA) Final Omnibus Security Rule 2013

AWS Audit Managermenyediakan kerangka kerja bawaan yang mendukung aturan HIPAA untuk membantu Anda dengan persiapan audit Anda.

> **Note**
>
> Untuk informasi tentang Aturan Keamanan HIPAA 2003 dan AWS Audit Manager kerangka kerja yang mendukung standar ini, lihatAturan Keamanan Undang-Undang Portabilitas dan Akuntabilitas Asuransi Kesehatan (HIPAA) 2003.

Topik

- Apa itu HIPAA dan Aturan Keamanan Omnibus Akhir HIPAA?
- Menggunakan kerangka kerja ini untuk mendukung persiapan audit Anda
- Lebih banyak sumber daya HIPAA

Apa itu HIPAA dan Aturan Keamanan Omnibus Akhir HIPAA?

Undang-Undang Portabilitas dan Akuntabilitas Asuransi Kesehatan 1996 (HIPAA) adalah undang-undang yang membantu pekerja AS untuk mempertahankan cakupan asuransi kesehatan ketika mereka berganti atau kehilangan pekerjaan. Undang-undang ini juga berupaya mendorong catatan kesehatan elektronik untuk meningkatkan efisiensi dan kualitas sistem perawatan kesehatan AS melalui peningkatan berbagi informasi.

Seiring dengan meningkatnya penggunaan catatan medis elektronik, HIPAA mencakup ketentuan untuk melindungi keamanan dan privasi informasi kesehatan yang dilindungi (PHI). PHI mencakup serangkaian data kesehatan dan kesehatan yang dapat diidentifikasi secara pribadi yang sangat luas. Ini termasuk informasi asuransi dan penagihan, data diagnosis, data perawatan klinis, dan hasil lab seperti gambar dan hasil tes.

Aturan Keamanan Omnibus Final HIPAA, yang menjadi efektif pada tahun 2013, mengimplementasikan sejumlah pembaruan untuk semua aturan yang disahkan sebelumnya. Modifikasi pada Keamanan, Privasi, Pemberitahuan Pelanggaran, dan Aturan Penegakan dimaksudkan untuk meningkatkan kerahasiaan dan keamanan dalam berbagi data.

Aturan HIPAA berlaku untuk entitas yang tercakup. Ini termasuk rumah sakit, penyedia layanan medis, rencana kesehatan yang disponsori majikan, fasilitas penelitian, dan perusahaan asuransi yang berurusan langsung dengan pasien dan data pasien. Sebagai bagian dari pembaruan omnibus, banyak aturan HIPAA yang berlaku untuk entitas yang tercakup juga sekarang berlaku untuk rekan bisnis.

Untuk informasi selengkapnya tentang bagaimana HIPAA dan HITECH melindungi informasi kesehatan, lihat halaman web Privasi Informasi Kesehatan dari Departemen Kesehatan dan Layanan Kemanusiaan AS.

Semakin banyak penyedia layanan kesehatan, pembayar, dan profesional TI menggunakan layanan cloud AWS berbasis utilitas untuk memproses, menyimpan, dan mengirimkan informasi kesehatan yang dilindungi (PHI). AWSmemungkinkan entitas yang dilindungi dan rekan bisnis mereka yang tunduk pada HIPAA untuk menggunakan AWS lingkungan yang aman untuk memproses, memelihara, dan menyimpan informasi kesehatan yang dilindungi. Untuk petunjuk tentang cara Anda dapat menggunakan AWS untuk pemrosesan dan penyimpanan informasi kesehatan, lihat whitepaper Architecting for HIPAA Security and Compliance on Amazon Web Services.

Menggunakan kerangka kerja ini untuk mendukung persiapan audit Anda

Anda dapat menggunakan kerangka HIPAA Final Omnibus Security Rule 2013 untuk membantu Anda mempersiapkan audit. Kerangka kerja ini mencakup kumpulan kontrol bawaan dengan deskripsi dan prosedur pengujian. Kontrol ini dikelompokkan ke dalam set kontrol sesuai dengan persyaratan HIPAA. Anda juga dapat menyesuaikan kerangka kerja ini dan kontrolnya untuk mendukung audit internal dengan persyaratan khusus.

Dengan menggunakan kerangka kerja sebagai titik awal, Anda dapat membuat penilaian Audit Manager dan mulai mengumpulkan bukti yang relevan untuk audit Anda. Setelah Anda membuat penilaian, Audit Manager mulai menilai AWS sumber daya Anda. Hal ini dilakukan berdasarkan kontrol yang didefinisikan dalam kerangka HIPAA. Saat tiba waktunya untuk audit, Anda—atau delegasi pilihan Anda—dapat meninjau bukti yang dikumpulkan oleh Audit Manager. Anda juga dapat menelusuri folder bukti dalam penilaian Anda dan memilih bukti mana yang ingin Anda sertakan dalam laporan penilaian Anda. Atau, jika Anda mengaktifkan pencari bukti, Anda dapat mencari bukti spesifik dan mengekspornya dalam format CSV, atau membuat laporan penilaian dari hasil penelusuran Anda. Either way, Anda dapat menggunakan laporan penilaian ini untuk menunjukkan bahwa kontrol Anda berfungsi sebagaimana dimaksud.

Rincian kerangka kerja HIPAA Final Omnibus Security Rule 2013 adalah sebagai berikut:

Nama kerangka kerja di AWS Audit Manager	Jumlah kontrol otomatis	Jumlah kontrol manual	Jumlah set kontrol	Layanan AWSdalam ruang lingkup
Aturan Keamanan Omnibus Akhir HIPAA 2013	39	46	5	• Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Security Hub

> **Tip**
>
> Untuk meninjau AWS Config aturan yang digunakan sebagai pemetaan sumber data dalam kerangka standar ini, unduh file AuditManager_ ConfigDataSourceMappings _HIPAA-Final-Omnibus-Security-Rule-2013.zip.

Kontrol dalam AWS Audit Manager kerangka kerja ini tidak dimaksudkan untuk memverifikasi apakah sistem Anda sesuai dengan standar HIPAA. Selain itu, mereka tidak dapat menjamin bahwa Anda akan lulus audit HIPAA. AWS Audit Managertidak secara otomatis memeriksa kontrol prosedural yang memerlukan pengumpulan bukti manual.

Anda dapat menemukan kerangka kerja ini di bawah tab Kerangka Standar Pustaka kerangka kerja di Audit Manager.

Untuk petunjuk tentang cara membuat penilaian menggunakan kerangka kerja ini, lihatMembuat penilaian.

Saat Anda menggunakan konsol Audit Manager untuk membuat penilaian dari kerangka kerja standar ini, daftar Layanan AWS dalam cakupan dipilih secara default dan tidak dapat diedit. Ini karena Audit Manager secara otomatis memetakan dan memilih sumber data dan layanan untuk Anda. Pemilihan ini dibuat sesuai dengan persyaratan kerangka HIPAA. Jika Anda perlu mengedit daftar layanan dalam ruang lingkup untuk kerangka kerja ini, Anda dapat melakukannya dengan menggunakan operasi CreateAssessmentatau UpdateAssessmentAPI. Atau, Anda dapat menyesuaikan kerangka kerja standar dan kemudian membuat penilaian dari kerangka kerja khusus.

Untuk petunjuk tentang cara menyesuaikan kerangka kerja ini untuk mendukung persyaratan spesifik Anda, lihat Menyesuaikan kerangka kerja yang ada dan Menyesuaikan kontrol yang ada.

Lebih banyak sumber daya HIPAA

- Informasi Kesehatan Privasi dari Departemen Kesehatan dan Layanan Kemanusiaan AS
- Omnibus HIPAA Rulemaking dari Departemen Kesehatan dan Layanan Kemanusiaan AS
- Arsitektur untuk Keamanan dan Kepatuhan HIPAA di Amazon Web Services
- AWSHalaman kepatuhan untuk HIPAA

ISO/IEC 27001:2013 Lampiran A

AWS Audit Managermenyediakan kerangka standar bawaan yang menyusun dan mengotomatiskan penilaian untuk ISO/IEC 27001:2013 Lampiran A.

Topik

Apa itu ISO/IEC 27001:2013 Lampiran A?

Komisi Elektroteknik Internasional (IEC) dan Organisasi Internasional untuk Standardisasi (ISO) keduanya independen, non-pemerintah, not-for-profit organisasi yang mengembangkan dan menerbitkan standar internasional berbasis konsensus sepenuhnya.

ISO/IEC 27001:2013 Annex A adalah standar manajemen keamanan yang menetapkan praktik terbaik manajemen keamanan dan kontrol keamanan komprehensif yang mengikuti panduan praktik terbaik ISO/IEC 27002. Standar internasional ini menetapkan persyaratan tentang bagaimana membangun, menerapkan, memelihara, dan terus meningkatkan sistem manajemen keamanan informasi di organisasi Anda. Termasuk di antara standar-standar ini adalah persyaratan pada penilaian dan perlakuan risiko keamanan informasi yang disesuaikan dengan kebutuhan organisasi Anda. Persyaratan dalam standar internasional ini bersifat generik dan dimaksudkan untuk berlaku untuk semua organisasi, terlepas dari jenis, ukuran atau sifatnya.

Menggunakan kerangka kerja ini untuk mendukung persiapan audit Anda

Anda dapat menggunakan AWS Audit Manager kerangka kerja untuk ISO/IEC 27001:2013 Lampiran A untuk membantu Anda mempersiapkan audit. Kerangka kerja ini mencakup kumpulan kontrol bawaan dengan deskripsi dan prosedur pengujian. Kontrol ini dikelompokkan ke dalam set kontrol sesuai dengan persyaratan ISO/IEC 27001:2013 Lampiran A. Anda juga dapat menyesuaikan kerangka kerja ini dan kontrolnya untuk mendukung audit internal dengan persyaratan khusus.

Dengan menggunakan kerangka kerja sebagai titik awal, Anda dapat membuat penilaian Audit Manager dan mulai mengumpulkan bukti yang relevan untuk audit Lampiran A ISO/IEC 27001:2013. Dalam penilaian Anda, Anda dapat menentukan Akun AWS dan layanan yang ingin Anda sertakan dalam lingkup audit Anda. Setelah Anda membuat penilaian, Audit Manager mulai menilai AWS sumber daya Anda. Hal ini dilakukan berdasarkan kontrol yang didefinisikan dalam ISO/IEC

27001:2013 Annex A framework. Saat tiba waktunya untuk audit, Anda—atau delegasi pilihan Anda—dapat meninjau bukti yang dikumpulkan oleh Audit Manager. Anda juga dapat menelusuri folder bukti dalam penilaian Anda dan memilih bukti mana yang ingin Anda sertakan dalam laporan penilaian Anda. Atau, jika Anda mengaktifkan pencari bukti, Anda dapat mencari bukti spesifik dan mengekspornya dalam format CSV, atau membuat laporan penilaian dari hasil penelusuran Anda. Either way, Anda dapat menggunakan laporan penilaian ini untuk menunjukkan bahwa kontrol Anda berfungsi sebagaimana dimaksud.

Rincian kerangka kerja adalah sebagai berikut:

Nama kerangka kerja di AWS Audit Manager	Jumlah kontrol otomatis	Jumlah kontrol manual	Jumlah set kontrol	Layanan AWSdalam ruang lingkup
ISO-IEC 27001:2013 Lampiran A	50	64	35	• Amazon CloudWatch • Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Security Hub

> **Tip**
>
> Untuk meninjau AWS Config aturan yang digunakan sebagai pemetaan sumber data dalam kerangka standar ini, unduh file AuditManager_ ConfigDataSourceMappings _ISO-IEC-27001-2013-Annex-A.zip.

Kontrol dalam AWS Audit Manager kerangka kerja ini tidak dimaksudkan untuk memverifikasi apakah sistem Anda sesuai dengan standar internasional ini. Selain itu, mereka tidak dapat menjamin

bahwa Anda akan lulus audit ISO/IEC. AWS Audit Managertidak secara otomatis memeriksa kontrol prosedural yang memerlukan pengumpulan bukti manual.

Anda dapat menemukan kerangka kerja ISO/IEC 27001:2013 Annex A di bawah tab Kerangka Standar di Audit Manager. Pustaka kerangka kerja

Saat Anda menggunakan konsol Audit Manager untuk membuat penilaian dari kerangka kerja standar ini, daftar Layanan AWS dalam cakupan dipilih secara default dan tidak dapat diedit. Ini karena Audit Manager secara otomatis memetakan dan memilih sumber data dan layanan untuk Anda. Pemilihan ini dibuat sesuai dengan persyaratan kerangka kerja ISO-IEC 27001:2013 Annex A. Jika Anda perlu mengedit daftar layanan dalam ruang lingkup untuk kerangka kerja ini, Anda dapat melakukannya dengan menggunakan operasi CreateAssessmentatau UpdateAssessmentAPI. Atau, Anda dapat menyesuaikan kerangka kerja standar dan kemudian membuat penilaian dari kerangka kerja khusus.

Untuk petunjuk tentang cara membuat penilaian menggunakan kerangka kerja ini, lihatMembuat penilaian. Untuk petunjuk tentang cara menyesuaikan kerangka kerja ini untuk mendukung persyaratan spesifik Anda, lihat Menyesuaikan kerangka kerja yang ada dan Menyesuaikan kontrol yang ada.

Lebih banyak sumber daya ISO/IEC 27001:2013 Lampiran A

- Untuk informasi lebih lanjut tentang standar internasional ini, lihat ISO/IEC 27001: 2013 di ANSI Webstore.

NIST 800-53 (Rev. 5) Rendah-Sedang-Tinggi

AWS Audit Managermenyediakan kerangka kerja bawaan yang menyusun dan mengotomatiskan penilaian untuk standar kepatuhan NIST 800-53, berdasarkan praktik terbaik. AWS

> **Note**
>
> - Untuk informasi tentang kerangka kerja Audit Manager yang mendukung NIST 800-171, lihat. NIST SP 800-171 (Wahyu 2)
> - Untuk informasi tentang kerangka kerja Audit Manager yang mendukung Kerangka Keamanan Siber NIST, lihat. Kerangka Keamanan Siber NIST versi 1.1

Topik

Apa itu NIST 800-53?

National Institute of Standards and Technology (NIST) didirikan pada tahun 1901 dan sekarang menjadi bagian dari Departemen Perdagangan AS. NIST adalah salah satu laboratorium ilmu fisika tertua di Amerika Serikat. Kongres AS membentuk badan tersebut untuk memperbaiki apa yang pada saat itu merupakan infrastruktur pengukuran kelas dua. Infrastruktur merupakan tantangan besar bagi daya saing industri AS, setelah tertinggal dari kekuatan ekonomi lainnya seperti Inggris dan Jerman.

Kontrol keamanan NIST 800-53 umumnya berlaku untuk sistem informasi federal AS. Ini biasanya sistem yang harus melalui penilaian formal dan proses otorisasi. Proses ini memastikan perlindungan yang memadai atas kerahasiaan, integritas, dan ketersediaan sistem informasi dan informasi. Ini didasarkan pada kategori keamanan dan tingkat dampak sistem (rendah, sedang, atau tinggi) serta penentuan risiko. Kontrol keamanan dipilih dari katalog kontrol keamanan NIST SP 800-53, dan sistem dinilai terhadap persyaratan kontrol keamanan tersebut.

Kerangka kerja NIST 800-53 (Rev. 5) Low-Moderate-High mewakili kontrol keamanan dan prosedur penilaian terkait yang didefinisikan dalam NIST SP 800-53 Revision 5 Recommended Security Controls for Federal Information Systems and Organizations. Untuk setiap perbedaan yang dicatat dalam konten antara kerangka kerja NIST SP 800-53 ini dan Publikasi Khusus NIST yang diterbitkan terbaru SP 800-53 Revisi 5, lihat dokumen resmi yang diterbitkan yang tersedia di Pusat Sumber Daya Keamanan Komputer NIST.

Menggunakan kerangka kerja ini untuk mendukung persiapan audit Anda

Anda dapat menggunakan kerangka kerja Low-Moderate-High NIST 800-53 (Rev. 5) untuk membantu Anda mempersiapkan audit. Kerangka kerja ini mencakup kumpulan kontrol bawaan dengan deskripsi dan prosedur pengujian. Kontrol ini dikelompokkan ke dalam set kontrol sesuai dengan persyaratan NIST. Anda juga dapat menyesuaikan kerangka kerja ini dan kontrolnya untuk mendukung audit internal dengan persyaratan khusus.

Dengan menggunakan kerangka kerja sebagai titik awal, Anda dapat membuat penilaian Audit Manager dan mulai mengumpulkan bukti yang relevan untuk audit Anda. Setelah Anda membuat penilaian, Audit Manager mulai menilai AWS sumber daya Anda. Ini dilakukan berdasarkan kontrol

yang didefinisikan dalam kerangka kerja NIST 800-53 (Rev. 5) Low-Moderate-High. Saat tiba waktunya untuk audit, Anda—atau delegasi pilihan Anda—dapat meninjau bukti yang dikumpulkan oleh Audit Manager. Anda juga dapat menelusuri folder bukti dalam penilaian Anda dan memilih bukti mana yang ingin Anda sertakan dalam laporan penilaian Anda. Atau, jika Anda mengaktifkan pencari bukti, Anda dapat mencari bukti spesifik dan mengekspornya dalam format CSV, atau membuat laporan penilaian dari hasil penelusuran Anda. Either way, Anda dapat menggunakan laporan penilaian ini untuk menunjukkan bahwa kontrol Anda berfungsi sebagaimana dimaksud.

Rincian kerangka kerja NIST 800-53 (Rev. 5) Rincian kerangka kerja Rendah-Sedang-Tinggi adalah sebagai berikut:

Nama kerangka kerja di AWS Audit Manager	Jumlah kontrol otomatis	Jumlah kontrol manual	Jumlah set kontrol	Layanan AWSdalam ruang lingkup
NIST 800-53 (Rev. 5) Rendah-Sedang-Tinggi	225	782	280	• Amazon CloudWatch • Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Security Hub

> **Tip**
>
> Untuk meninjau AWS Config aturan yang digunakan sebagai pemetaan sumber data dalam kerangka standar ini, unduh file AuditManager_ ConfigDataSourceMappings _NIST-800-53-rev.5-low-moderate-high.zip.

Kontrol dalam AWS Audit Manager kerangka kerja ini tidak dimaksudkan untuk memverifikasi apakah sistem Anda sesuai dengan standar NIST. Selain itu, mereka tidak dapat menjamin bahwa Anda

akan lulus audit NIST. AWS Audit Managertidak secara otomatis memeriksa kontrol prosedural yang memerlukan pengumpulan bukti manual.

Anda dapat menemukan kerangka kerja ini di bawah tab Kerangka Standar Pustaka kerangka kerja di Audit Manager.

Untuk petunjuk tentang cara membuat penilaian menggunakan kerangka kerja ini, lihatMembuat penilaian.

Saat Anda menggunakan konsol Audit Manager untuk membuat penilaian dari kerangka kerja standar ini, daftar Layanan AWS dalam cakupan dipilih secara default dan tidak dapat diedit. Ini karena Audit Manager secara otomatis memetakan dan memilih sumber data dan layanan untuk Anda. Pemilihan ini dibuat sesuai dengan persyaratan kerangka kerja Rendah-Sedang-Tinggi NIST 800-53 (Rev. 5). Jika Anda perlu mengedit daftar layanan dalam ruang lingkup untuk kerangka kerja ini, Anda dapat melakukannya dengan menggunakan operasi CreateAssessmentatau UpdateAssessmentAPI. Atau, Anda dapat menyesuaikan kerangka kerja standar dan kemudian membuat penilaian dari kerangka kerja khusus.

Untuk petunjuk tentang cara menyesuaikan kerangka kerja ini untuk mendukung persyaratan spesifik Anda, lihat Menyesuaikan kerangka kerja yang ada dan Menyesuaikan kontrol yang ada.

Lebih banyak sumber daya NIST

- Institut Nasional Standar dan Teknologi (NIST)
- Pusat Sumber Daya Keamanan Komputer NIST
- AWSHalaman kepatuhan untuk NIST

Kerangka Keamanan Siber NIST versi 1.1

AWS Audit Managermenyediakan kerangka kerja bawaan yang menyusun dan mengotomatiskan penilaian untuk Kerangka Keamanan Siber NIST, berdasarkan praktik terbaik. AWS

> **Note**
>
> - Untuk informasi tentang framework Audit Manager yang mendukung NIST 800-53 (Rev. 5) Low-Moderate-High, lihat. NIST 800-53 (Rev. 5) Rendah-Sedang-Tinggi
> - Untuk informasi tentang framework Audit Manager yang mendukung NIST SP 800-171 (Rev. 2), lihat. NIST SP 800-171 (Wahyu 2)

Topik

Apa itu Kerangka Keamanan Siber NIST?

National Institute of Standards and Technology (NIST) didirikan pada tahun 1901 dan sekarang menjadi bagian dari Departemen Perdagangan AS. NIST adalah salah satu laboratorium ilmu fisika tertua di Amerika Serikat. Kongres AS membentuk badan tersebut untuk memperbaiki apa yang pada saat itu merupakan infrastruktur pengukuran kelas dua. Infrastruktur merupakan tantangan besar bagi daya saing industri AS, setelah tertinggal dari kekuatan ekonomi lainnya seperti Inggris dan Jerman.

Amerika Serikat bergantung pada fungsi infrastruktur kritis yang andal. Ancaman keamanan siber mengeksploitasi peningkatan kompleksitas dan keterkaitan sistem infrastruktur kritis. Mereka menempatkan keamanan, ekonomi, dan keselamatan publik dan kesehatan Amerika Serikat dalam bahaya. Mirip dengan risiko keuangan dan reputasi, risiko keamanan siber memengaruhi laba perusahaan. Hal ini dapat meningkatkan biaya dan mempengaruhi pendapatan. Hal ini dapat membahayakan kemampuan organisasi untuk berinovasi dan untuk mendapatkan dan mempertahankan pelanggan. Pada akhirnya, keamanan siber dapat memperkuat manajemen risiko keseluruhan organisasi.

NIST Cybersecurity Framework (CSF) didukung oleh pemerintah dan industri di seluruh dunia sebagai dasar yang direkomendasikan untuk digunakan oleh organisasi mana pun, terlepas dari sektor atau ukurannya. Kerangka Keamanan Siber NIST terdiri dari tiga komponen utama: inti kerangka kerja, profil, dan tingkatan implementasi. Inti kerangka kerja berisi aktivitas dan hasil keamanan siber yang diinginkan yang diatur dalam 23 kategori yang mencakup luasnya tujuan keamanan siber untuk suatu organisasi. Profil berisi keselarasan unik organisasi dari persyaratan dan tujuan organisasi mereka, selera risiko, dan sumber daya menggunakan hasil yang diinginkan dari inti kerangka kerja. Tingkatan implementasi menggambarkan sejauh mana praktik manajemen risiko keamanan siber organisasi menunjukkan karakteristik yang didefinisikan dalam inti kerangka kerja.

Menggunakan kerangka kerja ini untuk mendukung persiapan audit Anda

Anda dapat menggunakan NIST Cybersecurity Framework versi 1.1 untuk membantu Anda mempersiapkan audit. Kerangka kerja ini mencakup kumpulan kontrol bawaan dengan deskripsi dan prosedur pengujian. Kontrol ini dikelompokkan ke dalam set kontrol sesuai dengan persyaratan CSF NIST. Audit Manager saat ini mendukung komponen inti kerangka kerja dengan menawarkan 56

kontrol otomatis dan 52 kontrol manual. Kontrol ini dicocokkan dengan 23 kategori keamanan siber yang didefinisikan dalam inti kerangka kerja. Audit Manager tidak mendukung komponen profil dan implementasi dalam kerangka kerja ini.

Anda juga dapat menyesuaikan kerangka kerja ini dan kontrolnya untuk mendukung audit internal dengan persyaratan khusus.

Dengan menggunakan kerangka kerja sebagai titik awal, Anda dapat membuat penilaian Audit Manager dan mulai mengumpulkan bukti yang relevan untuk audit Anda. Setelah Anda membuat penilaian, Audit Manager mulai menilai AWS sumber daya Anda. Ini dilakukan berdasarkan kontrol yang didefinisikan dalam NIST Cybersecurity Framework versi 1.1. Saat tiba waktunya untuk audit, Anda—atau delegasi pilihan Anda—dapat meninjau bukti yang dikumpulkan oleh Audit Manager. Anda juga dapat menelusuri folder bukti dalam penilaian Anda dan memilih bukti mana yang ingin Anda sertakan dalam laporan penilaian Anda. Atau, jika Anda mengaktifkan pencari bukti, Anda dapat mencari bukti spesifik dan mengekspornya dalam format CSV, atau membuat laporan penilaian dari hasil penelusuran Anda. Either way, Anda dapat menggunakan laporan penilaian ini untuk menunjukkan bahwa kontrol Anda berfungsi sebagaimana dimaksud.

Rincian untuk NIST Cybersecurity Framework versi 1.1 adalah sebagai berikut:

Nama kerangka kerja di AWS Audit Manager	Jumlah kontrol otomatis	Jumlah kontrol manual	Jumlah set kontrol	Layanan AWSdalam ruang lingkup
Kerangka Keamanan Siber NIST versi 1.1	56	52	23	• AWS Config • AWS Identity and Access Management • AWS Security Hub

> **Tip**
>
> Untuk meninjau AWS Config aturan yang digunakan sebagai pemetaan sumber data dalam kerangka kerja standar ini, unduh file AuditManager_ ConfigDataSourceMappings _NIST-CSF-v1.1.zip.

Kontrol yang ditawarkan oleh Audit Manager tidak dimaksudkan untuk memverifikasi apakah sistem Anda sesuai dengan Kerangka Keamanan Siber NIST. Selain itu, mereka tidak dapat menjamin bahwa Anda akan lulus audit Cybersecurity NIST. AWS Audit Managertidak secara otomatis memeriksa kontrol prosedural yang memerlukan pengumpulan bukti manual.

Anda dapat menemukan kerangka kerja ini di bawah tab Kerangka Standar Pustaka kerangka kerja di Audit Manager.

Untuk petunjuk tentang cara membuat penilaian menggunakan kerangka kerja ini, lihatMembuat penilaian.

Saat Anda menggunakan konsol Audit Manager untuk membuat penilaian dari kerangka kerja standar ini, daftar Layanan AWS dalam cakupan dipilih secara default dan tidak dapat diedit. Ini karena Audit Manager secara otomatis memetakan dan memilih sumber data dan layanan untuk Anda. Pilihan ini dibuat sesuai dengan persyaratan kerangka kerja NIST Cybersecurity Framework versi 1.1. Jika Anda perlu mengedit daftar layanan dalam ruang lingkup untuk kerangka kerja ini, Anda dapat melakukannya dengan menggunakan operasi CreateAssessmentatau UpdateAssessmentAPI. Atau, Anda dapat menyesuaikan kerangka kerja standar dan kemudian membuat penilaian dari kerangka kerja khusus.

Untuk petunjuk tentang cara menyesuaikan kerangka kerja ini untuk mendukung persyaratan spesifik Anda, lihat Menyesuaikan kerangka kerja yang ada dan Menyesuaikan kontrol yang ada.

Lebih banyak sumber daya NIST

- Institut Nasional Standar dan Teknologi (NIST)
- Pusat Sumber Daya Keamanan Komputer NIST
- AWSHalaman kepatuhan untuk NIST
- Kerangka Keamanan Siber NIST - Menyelaraskan dengan NIST CSF di Cloud AWS

NIST SP 800-171 (Wahyu 2)

AWS Audit Managermenyediakan kerangka kerja bawaan yang menyusun dan mengotomatiskan penilaian untuk standar kepatuhan NIST SP 800-171 berdasarkan praktik terbaik. AWS

> **Note**
>
> - Untuk informasi tentang framework Audit Manager yang mendukung NIST 800-53 (Rev. 5) Low-Moderate-High, lihat. NIST 800-53 (Rev. 5) Rendah-Sedang-Tinggi
> - Untuk informasi tentang framework Audit Manager yang mendukung NIST Cybersecurity Framework versi 1.1, lihat. Kerangka Keamanan Siber NIST versi 1.1

Topik

Apa itu NIST SP 800-171?

NIST SP 800-171 berfokus pada melindungi kerahasiaan Controlled Unclassified Information (CUI) dalam sistem dan organisasi nonfederal. Ini merekomendasikan persyaratan keamanan khusus untuk mencapai tujuan itu. NIST 800-171 adalah publikasi yang menguraikan standar dan praktik keamanan yang diperlukan untuk organisasi nonfederal yang menangani CUI di jaringan mereka. Ini pertama kali diterbitkan pada Juni 2015 oleh National Institute of Standards and Technology (NIST). NIST adalah lembaga pemerintah AS yang merilis beberapa standar dan publikasi untuk memperkuat ketahanan keamanan siber di sektor publik dan swasta. NIST 800-171 telah menerima pembaruan rutin sejalan dengan ancaman dunia maya yang muncul dan teknologi yang berubah. Versi terbaru (revisi 2) dirilis pada Februari 2020.

Kontrol keamanan siber dalam NIST 800-171 melindungi CUI di jaringan TI kontraktor dan subkontraktor pemerintah. Ini mendefinisikan praktik dan prosedur yang harus dipatuhi oleh kontraktor pemerintah ketika jaringan mereka memproses atau menyimpan CUI. NIST 800-171 hanya berlaku untuk bagian-bagian jaringan kontraktor di mana CUI hadir.

Menggunakan kerangka kerja ini untuk mendukung persiapan audit Anda

Anda dapat menggunakan kerangka kerja NIST SP 800-171 Rev. 2 untuk membantu Anda mempersiapkan audit. Kerangka kerja ini mencakup kumpulan kontrol bawaan dengan deskripsi dan prosedur pengujian. Kontrol ini dikelompokkan ke dalam set kontrol sesuai dengan persyaratan NIST. Anda juga dapat menyesuaikan kerangka kerja ini dan kontrolnya untuk mendukung audit internal dengan persyaratan khusus.

Dengan menggunakan kerangka kerja sebagai titik awal, Anda dapat membuat penilaian Audit Manager dan mulai mengumpulkan bukti yang relevan untuk audit Anda. Setelah Anda membuat penilaian, Audit Manager mulai menilai AWS sumber daya Anda. Ini dilakukan berdasarkan kontrol yang didefinisikan dalam kerangka kerja NIST SP 800-171 Rev. 2. Saat tiba waktunya untuk audit, Anda—atau delegasi pilihan Anda—dapat meninjau bukti yang dikumpulkan oleh Audit Manager. Anda juga dapat menelusuri folder bukti dalam penilaian Anda dan memilih bukti mana yang ingin Anda sertakan dalam laporan penilaian Anda. Atau, jika Anda mengaktifkan pencari bukti, Anda dapat mencari bukti spesifik dan mengekspornya dalam format CSV, atau membuat laporan penilaian dari hasil penelusuran Anda. Either way, Anda dapat menggunakan laporan penilaian ini untuk menunjukkan bahwa kontrol Anda berfungsi sebagaimana dimaksud.

Rincian kerangka kerja NIST SP 800-171 Rev. 2 adalah sebagai berikut:

Nama kerangka kerja di AWS Audit Manager	Jumlah kontrol otomatis	Jumlah kontrol manual	Jumlah set kontrol	Layanan AWSdalam ruang lingkup
NIST SP 800-171 Wahyu 2	66	58	16	• Amazon CloudWatch • Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Security Hub

Tip

Untuk meninjau AWS Config aturan yang digunakan sebagai pemetaan sumber data dalam kerangka standar ini, unduh file AuditManager_ ConfigDataSourceMappings _NIST-SP-800-171-rev.2.zip.

Kontrol dalam AWS Audit Manager kerangka kerja ini tidak dimaksudkan untuk memverifikasi apakah sistem Anda sesuai dengan NIST 800-171. Selain itu, mereka tidak dapat menjamin bahwa Anda akan lulus audit NIST. AWS Audit Managertidak secara otomatis memeriksa kontrol prosedural yang memerlukan pengumpulan bukti manual.

Anda dapat menemukan kerangka kerja ini di bawah tab Kerangka Standar Pustaka kerangka kerja di Audit Manager.

Untuk informasi tentang cara membuat penilaian menggunakan kerangka kerja ini, lihatMembuat penilaian.

Saat Anda menggunakan konsol Audit Manager untuk membuat penilaian dari kerangka kerja standar ini, daftar Layanan AWS dalam cakupan dipilih secara default dan tidak dapat diedit. Ini karena Audit Manager secara otomatis memetakan dan memilih sumber data dan layanan untuk Anda. Pemilihan ini dibuat sesuai dengan persyaratan kerangka kerja NIST SP 800-171 Rev. 2. Jika Anda perlu mengedit daftar layanan dalam ruang lingkup untuk kerangka kerja ini, Anda dapat melakukannya dengan menggunakan operasi CreateAssessmentatau UpdateAssessmentAPI. Atau, Anda dapat menyesuaikan kerangka kerja standar dan kemudian membuat penilaian dari kerangka kerja khusus.

Untuk petunjuk tentang cara menyesuaikan kerangka kerja ini untuk mendukung persyaratan spesifik Anda, lihat Menyesuaikan kerangka kerja yang ada dan Menyesuaikan kontrol yang ada.

Lebih banyak sumber daya NIST

- Institut Nasional Standar dan Teknologi (NIST)
- Pusat Sumber Daya Keamanan Komputer NIST
- AWSHalaman kepatuhan untuk NIST

PCI DSS V3.2.1

AWS Audit Managermenyediakan kerangka kerja prebuilt yang mendukung PCI DSS v3.2.1.

> **Note**
>
> Untuk informasi tentang PCI DSS v4 dan kerangka kerja Audit Manager yang mendukungnya, lihat. PCI DSS V4.0

Topik

Apa itu PCI DSS?

Standar Keamanan Data Industri Kartu Pembayaran (PCI DSS) adalah standar keamanan informasi eksklusif. Ini dikelola oleh Dewan Standar Keamanan PCI, yang didirikan oleh American Express, Discover Financial Services, JCB International, MasterCard Worldwide, dan Visa Inc. PCI DSS berlaku untuk entitas yang menyimpan, memproses, atau mengirimkan data pemegang kartu (CHD) atau data otentikasi sensitif (SAD). Ini termasuk, tetapi tidak terbatas pada, pedagang, prosesor, pengakuisisi, penerbit, dan penyedia layanan. PCI DSS diamanatkan oleh merek kartu dan dikelola oleh Dewan Standar Keamanan Industri Kartu Pembayaran.

AWSdisertifikasi sebagai Penyedia Layanan PCI DSS Level 1, yang merupakan tingkat penilaian tertinggi yang tersedia. Penilaian kepatuhan dilakukan oleh Coalfire Systems Inc., sebuah Qualified Security Assessor (QSA) independen. Ringkasan Pengesahan Kepatuhan (AOC) dan Tanggung Jawab PCI DSS tersedia untuk Anda melalui. AWS Artifact Ini adalah portal swalayan untuk akses sesuai permintaan ke laporan AWS kepatuhan. AWS ArtifactMasuk ke Konsol AWS Manajemen, atau pelajari lebih lanjut di Memulai AWS Artifact.

Anda dapat mengunduh standar PCI DSS dari Perpustakaan Dokumen Dewan Standar Keamanan PCI.

Menggunakan kerangka kerja ini untuk mendukung persiapan audit Anda

Anda dapat menggunakan kerangka kerja PCI DSS V3.2.1 untuk membantu Anda mempersiapkan audit. Kerangka kerja ini mencakup kumpulan kontrol bawaan dengan deskripsi dan prosedur pengujian. Kontrol ini dikelompokkan ke dalam set kontrol sesuai dengan persyaratan PCI DSS. Anda juga dapat menyesuaikan kerangka kerja ini dan kontrolnya untuk mendukung audit internal dengan persyaratan khusus.

Dengan menggunakan kerangka kerja sebagai titik awal, Anda dapat membuat penilaian Audit Manager dan mulai mengumpulkan bukti yang relevan untuk audit Anda. Setelah Anda membuat penilaian, Audit Manager mulai menilai AWS sumber daya Anda. Ini dilakukan berdasarkan kontrol yang didefinisikan dalam kerangka kerja PCI DSS V3.2.1. Saat tiba waktunya untuk audit, Anda —atau delegasi pilihan Anda—dapat meninjau bukti yang dikumpulkan oleh Audit Manager. Anda

juga dapat menelusuri folder bukti dalam penilaian Anda dan memilih bukti mana yang ingin Anda sertakan dalam laporan penilaian Anda. Atau, jika Anda mengaktifkan pencari bukti, Anda dapat mencari bukti spesifik dan mengekspornya dalam format CSV, atau membuat laporan penilaian dari hasil penelusuran Anda. Either way, Anda dapat menggunakan laporan penilaian ini untuk menunjukkan bahwa kontrol Anda berfungsi sebagaimana dimaksud.

Rincian kerangka kerja PCI DSS V3.2.1 adalah sebagai berikut:

Nama kerangka kerja di AWS Audit Manager	Jumlah kontrol otomatis	Jumlah kontrol manual	Jumlah set kontrol	Layanan AWSdalam ruang lingkup
PCI DSS V3.2.1	175	487	12	• Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Security Hub

> **Tip**
>
> Untuk meninjau AWS Config aturan yang digunakan sebagai pemetaan sumber data dalam kerangka standar ini, unduh file AuditManager_ ConfigDataSourceMappings _PCI-DSS-v3.2.1.zip.

Kontrol dalam AWS Audit Manager kerangka kerja ini tidak dimaksudkan untuk memverifikasi apakah sistem Anda sesuai dengan standar PCI DSS. Selain itu, mereka tidak dapat menjamin bahwa Anda akan lulus audit PCI DSS. AWS Audit Managertidak secara otomatis memeriksa kontrol prosedural yang memerlukan pengumpulan bukti manual.

Anda dapat menemukan kerangka kerja ini di bawah tab Kerangka Standar Pustaka kerangka kerja di Audit Manager.

Untuk informasi tentang cara membuat penilaian menggunakan kerangka kerja ini, lihatMembuat penilaian.

Saat Anda menggunakan konsol Audit Manager untuk membuat penilaian dari kerangka kerja standar ini, daftar Layanan AWS dalam cakupan dipilih secara default dan tidak dapat diedit. Ini karena Audit Manager secara otomatis memetakan dan memilih sumber data dan layanan untuk Anda. Pemilihan ini dibuat sesuai dengan persyaratan kerangka kerja PCI DSS V3.2.1. Jika Anda perlu mengedit daftar layanan dalam ruang lingkup untuk kerangka kerja ini, Anda dapat melakukannya dengan menggunakan operasi CreateAssessmentatau UpdateAssessmentAPI. Atau, Anda dapat menyesuaikan kerangka kerja standar dan kemudian membuat penilaian dari kerangka kerja khusus.

Untuk petunjuk tentang cara menyesuaikan kerangka kerja ini untuk mendukung persyaratan spesifik Anda, lihat Menyesuaikan kerangka kerja yang ada dan Menyesuaikan kontrol yang ada.

Lebih banyak sumber daya PCI DSS

- Dewan Standar Keamanan PCI
- Perpustakaan Dokumen Dewan Standar Keamanan PCI.
- AWSHalaman kepatuhan untuk PCI DSS

PCI DSS V4.0

AWS Audit Managermenyediakan kerangka kerja bawaan yang mendukung Standar Keamanan Data Industri Kartu Pembayaran (PCI DSS) v4.0.

> **Note**
>
> Untuk informasi tentang PCI DSS v3.2.1 dan kerangka kerja Audit Manager yang mendukungnya, lihat. PCI DSS V3.2.1

Topik

- Apa itu PCI DSS?
- Menggunakan kerangka kerja ini untuk mendukung persiapan audit Anda
- Lebih banyak sumber daya PCI DSS

Apa itu PCI DSS?

Standar Keamanan Data Industri Kartu Pembayaran (PCI DSS) adalah standar global yang menyediakan dasar persyaratan teknis dan operasional untuk melindungi data pembayaran. PCI DSS v4.0 adalah evolusi standar berikutnya.

PCI DSS dikembangkan untuk mendorong dan meningkatkan keamanan data akun kartu pembayaran. Ini juga memfasilitasi adopsi luas langkah-langkah keamanan data yang konsisten secara global. Ini memberikan dasar persyaratan teknis dan operasional yang dirancang untuk melindungi data akun. Meskipun dirancang khusus untuk fokus pada lingkungan dengan data akun kartu pembayaran, Anda juga dapat menggunakan PCI DSS untuk melindungi dari ancaman dan mengamankan elemen lain dalam ekosistem pembayaran.

Dewan Standar Keamanan PCI (PCI SSC) memperkenalkan banyak perubahan antara PCI DSS v3.2.1 dan v4.0. Pembaruan ini dibagi menjadi tiga kategori:

1. Persyaratan yang berkembang — Perubahan untuk memastikan bahwa standar tersebut mutakhir dengan ancaman dan teknologi yang muncul, dan perubahan dalam industri pembayaran. Contohnya termasuk persyaratan baru atau modifikasi atau prosedur pengujian, atau penghapusan persyaratan.
2. Klarifikasi atau panduan — Pembaruan kata-kata, penjelasan, definisi, panduan tambahan, atau instruksi untuk meningkatkan pemahaman atau memberikan informasi atau panduan lebih lanjut tentang topik tertentu.
3. Struktur atau format — Reorganisasi konten, termasuk menggabungkan, memisahkan, dan menomori ulang persyaratan untuk menyelaraskan konten.

Untuk informasi lebih lanjut tentang perubahan, lihat Ringkasan perubahan dari PCI DSS Versi 3.2.1 ke 4.0.

Menggunakan kerangka kerja ini untuk mendukung persiapan audit Anda

> **Note**
>
> Framework standar ini menggunakan kontrol terkonsolidasi dari Security Hub sebagai sumber data. Agar berhasil mengumpulkan bukti dari kontrol terkonsolidasi, pastikan Anda mengaktifkan pengaturan temuan kontrol konsolidasi di Security Hub. Untuk informasi

selengkapnya tentang menggunakan Security Hub sebagai tipe sumber data, lihat AWS Security Hubkontrol yang didukung oleh AWS Audit Manager.

Anda dapat menggunakan kerangka kerja PCI DSS V4.0 untuk membantu Anda mempersiapkan audit. Kerangka kerja ini mencakup kumpulan kontrol bawaan dengan deskripsi dan prosedur pengujian. Kontrol ini dikelompokkan ke dalam set kontrol sesuai dengan persyaratan PCI DSS V4.0. Anda juga dapat menyesuaikan kerangka kerja ini dan kontrolnya untuk mendukung audit internal dengan persyaratan khusus.

Dengan menggunakan kerangka kerja sebagai titik awal, Anda dapat membuat penilaian Audit Manager dan mulai mengumpulkan bukti yang relevan untuk audit Anda. Setelah Anda membuat penilaian, Audit Manager mulai menilai AWS sumber daya Anda. Ini dilakukan berdasarkan kontrol yang didefinisikan dalam kerangka PCI DSS V4.0. Saat tiba waktunya untuk audit, Anda—atau delegasi pilihan Anda—dapat meninjau bukti yang dikumpulkan oleh Audit Manager. Anda juga dapat menelusuri folder bukti dalam penilaian Anda dan memilih bukti mana yang ingin Anda sertakan dalam laporan penilaian Anda. Atau, jika Anda mengaktifkan pencari bukti, Anda dapat mencari bukti spesifik dan mengekspornya dalam format CSV, atau membuat laporan penilaian dari hasil penelusuran Anda. Either way, Anda dapat menggunakan laporan penilaian ini untuk menunjukkan bahwa kontrol Anda berfungsi sebagaimana dimaksud.

Rincian kerangka kerja adalah sebagai berikut:

Nama kerangka kerja di AWS Audit Manager	Jumlah kontrol otomatis	Jumlah kontrol manual	Jumlah set kontrol	Layanan AWSdalam ruang lingkup
PCI DSS v4.0	152	128	15	• Amazon API Gateway • Amazon CloudFront • Amazon CloudWatch • Amazon DynamoDB • Amazon Elastic Compute Cloud

Nama kerangka kerja di AWS Audit Manager	Jumlah kontrol otomatis	Jumlah kontrol manual	Jumlah set kontrol	Layanan AWSdalam ruang lingkup
				• OpenSearch Layanan Amazon • Amazon Redshift • Layanan Basis Data Relasional Amazon • Amazon SageMaker • Amazon Simple Storage Service • AWS Backup • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS KMS • AWS Secrets Manager • AWS Security Hub • AWS WAF

Tip

Untuk meninjau AWS Config aturan yang digunakan sebagai pemetaan sumber data dalam kerangka standar ini, unduh file AuditManager_ ConfigDataSourceMappings _PCI-DSS-V4.zip.

Kontrol dalam AWS Audit Manager kerangka kerja ini tidak dimaksudkan untuk memverifikasi apakah sistem Anda sesuai dengan standar PCI DSS. Selain itu, mereka tidak dapat menjamin bahwa Anda akan lulus audit PCI DSS. AWS Audit Managertidak secara otomatis memeriksa kontrol prosedural yang memerlukan pengumpulan bukti manual.

Anda dapat menemukan kerangka kerja ini di bawah tab Kerangka Standar Pustaka kerangka kerja di Audit Manager.

Untuk informasi tentang cara membuat penilaian menggunakan kerangka kerja ini, lihatMembuat penilaian.

Saat Anda menggunakan konsol Audit Manager untuk membuat penilaian dari kerangka kerja standar ini, daftar Layanan AWS dalam cakupan dipilih secara default dan tidak dapat diedit. Ini karena Audit Manager secara otomatis memetakan dan memilih sumber data dan layanan untuk Anda. Pemilihan ini dibuat sesuai dengan persyaratan kerangka kerja PCI DSS V4. Jika Anda perlu mengedit daftar layanan dalam ruang lingkup untuk kerangka kerja ini, Anda dapat melakukannya dengan menggunakan operasi CreateAssessmentatau UpdateAssessmentAPI. Atau, Anda dapat menyesuaikan kerangka kerja standar dan kemudian membuat penilaian dari kerangka kerja khusus.

Untuk petunjuk tentang cara menyesuaikan kerangka kerja ini untuk mendukung persyaratan spesifik Anda, lihat Menyesuaikan kerangka kerja yang ada dan Menyesuaikan kontrol yang ada.

Lebih banyak sumber daya PCI DSS

- Pusat Sumber Daya PCI DSS v4.0
- Dewan Standar Keamanan PCI
- Perpustakaan Dokumen Dewan Standar Keamanan PCI.
- AWSHalaman kepatuhan untuk PCI DSS
- Standar Keamanan Data Industri Kartu Pembayaran (PCI DSS) v4.0 tentang Panduan Kepatuhan AWS
- Ringkasan perubahan dari PCI DSS Versi 3.2.1 ke 4.0

SOC 2

SOC 2 adalah prosedur audit yang memastikan data perusahaan dikelola dengan aman. AWS Audit Managermenyediakan kerangka kerja bawaan yang mendukung SOC 2.

Topik

Apa itu SOC 2?

Sistem dan Kontrol Organisasi (SOC), yang didefinisikan oleh American Institute of Certified Public Accountants (AICPA), adalah nama dari serangkaian laporan yang dihasilkan selama audit. Ini dimaksudkan untuk digunakan oleh organisasi layanan (organisasi yang menyediakan sistem informasi sebagai layanan kepada organisasi lain) untuk mengeluarkan laporan kontrol internal yang divalidasi atas sistem informasi tersebut kepada pengguna layanan tersebut. Laporan berfokus pada kontrol yang dikelompokkan ke dalam lima kategori yang dikenal sebagai Prinsip Layanan Kepercayaan.

AWSLaporan SOC adalah laporan pemeriksaan pihak ketiga independen yang menunjukkan bagaimana AWS mencapai kontrol dan tujuan kepatuhan utama. Tujuan dari laporan ini adalah untuk membantu Anda dan auditor Anda memahami AWS kontrol yang ditetapkan untuk mendukung operasi dan kepatuhan. Ada lima laporan AWS SOC:

- AWSLaporan SOC 1, tersedia untuk AWS pelanggan dari AWS Artifact.
- AWSLaporan Keamanan, Ketersediaan & Kerahasiaan SOC 2, tersedia untuk AWS pelanggan dari. AWS Artifact
- AWSLaporan Keamanan, Ketersediaan & Kerahasiaan SOC 2 tersedia untuk AWS pelanggan dari AWS Artifact(cakupan hanya mencakup Amazon DocumentDB).
- AWSLaporan Privasi Tipe I SOC 2, tersedia untuk AWS pelanggan dari AWS Artifact.
- AWSLaporan Keamanan, Ketersediaan & Kerahasiaan SOC 3, tersedia untuk umum sebagai whitepaper.

Menggunakan kerangka kerja ini untuk mendukung persiapan audit Anda

Anda dapat menggunakan kerangka kerja ini untuk membantu Anda mempersiapkan audit. Kerangka kerja ini mencakup kumpulan kontrol bawaan dengan deskripsi dan prosedur pengujian. Kontrol ini dikelompokkan ke dalam set kontrol sesuai dengan persyaratan SOC 2. Anda juga dapat menyesuaikan kerangka kerja ini dan kontrolnya untuk mendukung audit internal dengan persyaratan khusus.

Dengan menggunakan kerangka kerja sebagai titik awal, Anda dapat membuat penilaian Audit Manager dan mulai mengumpulkan bukti yang relevan untuk audit Anda. Setelah Anda membuat penilaian, Audit Manager mulai menilai AWS sumber daya Anda. Ini dilakukan berdasarkan kontrol yang didefinisikan dalam kerangka kerja. Saat tiba waktunya untuk audit, Anda—atau delegasi pilihan Anda—dapat meninjau bukti yang dikumpulkan oleh Audit Manager. Anda juga dapat menelusuri folder bukti dalam penilaian Anda dan memilih bukti mana yang ingin Anda sertakan dalam laporan penilaian Anda. Atau, jika Anda mengaktifkan pencari bukti, Anda dapat mencari bukti spesifik dan mengekspornya dalam format CSV, atau membuat laporan penilaian dari hasil penelusuran Anda. Either way, Anda dapat menggunakan laporan penilaian ini untuk menunjukkan bahwa kontrol Anda berfungsi sebagaimana dimaksud.

Rincian kerangka kerja adalah sebagai berikut:

Nama kerangka kerja di AWS Audit Manager	Jumlah kontrol otomatis	Jumlah kontrol manual	Jumlah set kontrol	Layanan AWSdalam ruang lingkup
SOC 2	20	41	20	• Amazon Elastic Compute Cloud • AWS Auto Scaling • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Security Hub

> **Tip**
>
> Untuk meninjau AWS Config aturan yang digunakan sebagai pemetaan sumber data dalam kerangka standar ini, unduh file AuditManager_ ConfigDataSourceMappings _SOC2.zip.

Kontrol dalam AWS Audit Manager kerangka kerja ini tidak dimaksudkan untuk memverifikasi apakah sistem Anda sesuai. Selain itu, mereka tidak dapat menjamin bahwa Anda akan lulus audit. AWS Audit Managertidak secara otomatis memeriksa kontrol prosedural yang memerlukan pengumpulan bukti manual.

Anda dapat menemukan kerangka kerja ini di bawah tab Kerangka Standar Pustaka kerangka kerja di Audit Manager.

Untuk petunjuk tentang cara membuat penilaian menggunakan kerangka kerja ini, lihatMembuat penilaian.

Saat Anda menggunakan konsol Audit Manager untuk membuat penilaian dari kerangka kerja standar ini, daftar Layanan AWS dalam cakupan dipilih secara default dan tidak dapat diedit. Ini karena Audit Manager secara otomatis memetakan dan memilih sumber data dan layanan untuk Anda. Pilihan ini dibuat sesuai dengan persyaratan SOC 2. Jika Anda perlu mengedit daftar layanan dalam ruang lingkup untuk kerangka kerja ini, Anda dapat melakukannya dengan menggunakan operasi CreateAssessmentatau UpdateAssessmentAPI. Atau, Anda dapat menyesuaikan kerangka kerja standar dan kemudian membuat penilaian dari kerangka kerja khusus.

Untuk petunjuk tentang cara menyesuaikan kerangka kerja ini untuk mendukung persyaratan spesifik Anda, lihat Menyesuaikan kerangka kerja yang ada dan Menyesuaikan kontrol yang ada.

Lebih banyak sumber daya SOC 2

- AWSHalaman kepatuhan untuk SOC

Pustaka kontrol

Anda dapat mengakses dan mengelola kontrol dari pustaka kontrol di Audit Manager. Anda dapat pergi ke pustaka kontrol kapan saja dengan memilih Pustaka kontrol di panel navigasi di konsol Audit Manager.

Pustaka kontrol berisi katalog kontrol standar dan kontrol khusus.

- Kontrol standar adalah kontrol standar yang disediakan oleh AWS. Anda dapat melihat detail konfigurasi kontrol standar, tetapi Anda tidak dapat mengedit atau menghapusnya. Namun, Anda dapat menyesuaikan kontrol standar apa pun untuk membuat yang baru yang memenuhi persyaratan spesifik Anda.
- Kontrol khusus adalah kontrol khusus yang Anda miliki dan tentukan. Dengan kontrol khusus, Anda dapat menentukan sumber data mana yang ingin Anda kumpulkan bukti. Anda kemudian dapat menambahkan kontrol kustom ke kerangka kustom.

  Untuk mempelajari lebih lanjut tentang cara menambahkan kontrol kustom ke kerangka kerja kustom, lihatPustaka kerangka kerja. Untuk mempelajari lebih lanjut tentang cara membuat penilaian dari kerangka kerja Audit Manager, lihatPenilaian di AWS Audit Manager.

Bagian ini menjelaskan cara membuat dan mengelola kontrol kustom di Audit Manager.

Topik

Mengakses kontrol yang tersedia di AWS Audit Manager

Anda dapat melihat semua kontrol yang tersedia di halaman Control library di konsol Audit Manager. Dari sini, Anda juga dapat membuat kontrol khusus atau menyesuaikan kontrol yang ada.

Anda juga dapat melihat semua kontrol yang tersedia menggunakan Audit Manager API atau AWS Command Line Interface (AWS CLI).

Audit Manager console

Untuk melihat kontrol yang tersedia (konsol)

1. Buka konsol AWS Audit Manager di https://console.aws.amazon.com/auditmanager/home.
2. Di panel navigasi, pilih Control library.
3. Pilih tab Kontrol standar atau tab Kontrol khusus untuk menelusuri kontrol yang tersedia.
4. Pilih nama kontrol apa pun untuk melihat detail untuk kontrol itu.

AWS CLI

Untuk melihat kontrol yang tersedia (AWS CLI)

Jalankan perintah list-controls dan tentukan file. `--control-type` Entah, Anda dapat mengambil daftar kontrol standar. Atau, Anda dapat mengambil daftar kontrol khusus.

```
aws auditmanager list-controls --control-type Standard
```

```
aws auditmanager list-controls --control-type Custom
```

Audit Manager API

Untuk melihat kontrol yang tersedia (API)

Gunakan ListControlsoperasi dan tentukan ControlType. Entah, Anda dapat mengembalikan daftar kontrol standar. Atau, Anda dapat mengembalikan daftar kontrol khusus.

Untuk informasi selengkapnya, pilih salah satu tautan sebelumnya untuk membaca selengkapnya di ReferensiAWS Audit Manager API. Ini termasuk informasi tentang cara menggunakan `ListControls` operasi dan parameter di salah satu SDK khusus bahasa AWS .

Meninjau detail kontrol

Anda dapat meninjau detail kontrol menggunakan konsol Audit Manager, Audit Manager API, atau AWS Command Line Interface (AWS CLI).

Audit Manager console

Untuk melihat detail kontrol (konsol)

1. Buka konsol AWS Audit Manager di https://console.aws.amazon.com/auditmanager/home.
2. Di panel navigasi, pilih Pustaka kontrol untuk melihat daftar kontrol yang tersedia.
3. Pilih tab Kontrol standar atau tab Kontrol khusus untuk menelusuri kontrol yang tersedia.
4. Pilih nama kontrol apa pun untuk melihat detail untuk kontrol itu.

Saat Anda membuka kontrol, Anda melihat halaman detail kontrol. Bagian halaman ini dan isinya dijelaskan di bawah ini.

Bagian ringkasan

Bagian ini memberikan gambaran umum tentang kontrol. Ini termasuk informasi berikut:

- Nama kontrol — Nama kontrol.
- Jenis kontrol - Menentukan apakah kontrol adalah kontrol standar atau kontrol kustom.
- Tag — Jumlah tag yang terkait dengan kontrol.
- Tipe sumber data — Jumlah tipe sumber data yang digunakan untuk kontrol ini.
- Pemetaan — Jumlah atribut pemetaan yang digunakan untuk mengambil data dari sumber data.

Jika Anda melihat kontrol khusus, detail berikut juga ditampilkan:

- Dibuat oleh — Akun yang membuat kontrol kustom.
- Tanggal pembuatan - Tanggal ketika kontrol kustom dibuat.
- Terakhir diperbarui - Tanggal ketika kontrol kustom terakhir diedit.

Tab Detail

Tab ini memberikan ikhtisar dasar kontrol. Ini termasuk informasi berikut:

- Bagian Deskripsi memberikan deskripsi kontrol.
- Bagian Informasi pengujian memberikan deskripsi prosedur pengujian yang direkomendasikan untuk kontrol.
- Bagian Rencana aksi menjelaskan tindakan yang direkomendasikan untuk dilakukan jika kontrol perlu diperbaiki.

Tab sumber data

Tab ini menampilkan informasi tentang sumber data untuk kontrol. Ini termasuk informasi berikut:

- Nama sumber data — Ini hanya berlaku untuk kontrol khusus. Ini mengacu pada nama deskriptif yang Anda berikan setiap sumber data. Anda dapat menggunakan nama ini untuk membedakan antara beberapa sumber data yang termasuk dalam tipe sumber data yang sama.
- Tipe sumber data — Ini menentukan dari mana data bukti berasal.
  - Jika Audit Manager mengumpulkan bukti, sumber data dapat berupa salah satu dari empat jenis: AWS Security Hub,, AWS ConfigAWS CloudTrail, atau panggilanAWS API.
  - Jika Anda mengunggah bukti Anda sendiri, tipe sumber datanya adalah Manual. Deskripsi menunjukkan apakah bukti manual yang diperlukan adalah unggahan File atau respons Teks.
- Pemetaan — Ini adalah atribut pemetaan yang digunakan untuk mengidentifikasi dan mengambil data dari sumber data.
  - Jika tipe sumber data adalah AWS Config, pemetaan adalah nama AWS Config aturan tertentu (misalnya,`EC2_INSTANCE_MANAGED_BY_SSM`). Audit Manager menggunakan pemetaan ini untuk melaporkan hasil pemeriksaan aturan tersebut secara langsung AWS Config.
  - Jika tipe sumber datanya AWS Security Hub, pemetaan adalah nama kontrol Security Hub tertentu (misalnya,`1.1 – Avoid the use of the "root" account`). Audit Manager menggunakan pemetaan ini untuk melaporkan hasil pemeriksaan keamanan tersebut langsung dari Security Hub.
  - Jika tipe sumber data adalah panggilan AWS API, pemetaan adalah nama panggilan API tertentu (misalnya,`ec2_DescribeSecurityGroups`). Audit Manager menggunakan pemetaan ini untuk mengumpulkan respons API.
  - Jika sumber datanya AWS CloudTrail, pemetaan adalah nama CloudTrail peristiwa tertentu (misalnya,`CreateAccessKey`). Audit Manager menggunakan pemetaan ini untuk mengumpulkan aktivitas pengguna terkait dari CloudTrail log Anda.
- Frekuensi — Ini menentukan seberapa sering Audit Manager mengumpulkan bukti dari sumber data. Frekuensi bervariasi tergantung pada jenis sumber data. Untuk informasi selengkapnya, pilih nilai di kolom atau lihatFrekuensi pengumpulan bukti.

Tab tag

Tab ini mencantumkan tag yang terkait dengan kontrol. Ini termasuk informasi berikut:

- Kunci — Kunci tag (misalnya, standar kepatuhan, peraturan, atau kategori).
- Nilai — Nilai tag.

AWS CLI

Untuk melihat detail kontrol (AWS CLI)

1. Untuk mengidentifikasi kontrol yang ingin Anda tinjau, jalankan perintah list-controls dan tentukan. `--control-type` Entah, Anda dapat mengambil daftar kontrol standar. Atau, Anda dapat mengambil daftar kontrol khusus.

   Dalam contoh berikut, ganti *teks placeholder* dengan salah satu atau`Custom`. `Standard`

   ```
   aws auditmanager list-controls --control-type Custom/Standard
   ```

   Respons mengembalikan daftar kontrol. Temukan kontrol yang ingin Anda tinjau, dan catat ID kontrol dan Nama Sumber Daya Amazon (ARN).
2. Untuk mendapatkan detail kontrol, jalankan perintah get-control dan tentukan. `--control-id`

   Dalam contoh berikut, ganti *teks placeholder dengan informasi* Anda sendiri.

   ```
   aws auditmanager get-control --control-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
   ```

   Rincian kontrol dikembalikan dalam format JSON. Untuk memahami data ini, lihat Get-control Output di AWS CLI Command Reference.
3. Untuk melihat tag untuk kontrol, gunakan list-tags-for-resourceperintah dan tentukan `--resource-arn` untuk kontrol.

   Dalam contoh berikut, ganti *teks placeholder dengan informasi* Anda sendiri:

   ```
   aws auditmanager list-tags-for-resource --resource-arn arn:aws:auditmanager:us-east-1:111122223333:control/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
   ```

Untuk informasi selengkapnya tentang tag di Audit Manager, lihat Menandai AWS Audit Manager sumber daya.

Audit Manager API

Untuk melihat detail kontrol (API)

1. Untuk mengidentifikasi kontrol yang ingin Anda tinjau, gunakan ListControlsoperasi dan tentukan ControlType. Entah, Anda dapat mengembalikan daftar kontrol standar. Atau, Anda dapat mengembalikan daftar kontrol khusus.

   Dari respons, temukan kontrol yang ingin Anda tinjau, dan catat ID kontrol dan Nama Sumber Daya Amazon (ARN).
2. Untuk mendapatkan detail kontrol, gunakan GetControloperasi. Dalam permintaan, tentukan ControLid yang Anda dapatkan dari langkah 1.

   Rincian kontrol dikembalikan dalam format JSON. Untuk memahami data ini, lihat Elemen GetControl Respons di ReferensiAWS Audit Manager API.
3. Untuk melihat tag untuk kontrol, gunakan ListTagsForResourceoperasi. Dalam permintaan, tentukan kontrol ResourcEarn yang Anda dapatkan dari langkah 1.

Untuk informasi selengkapnya tentang tag di Audit Manager, lihat Menandai AWS Audit Manager sumber daya.

Untuk informasi selengkapnya tentang operasi API ini, pilih salah satu tautan sebelumnya untuk membaca selengkapnya di ReferensiAWS Audit Manager API. Ini termasuk informasi tentang cara menggunakan operasi dan parameter ini di salah satu SDK khusus bahasa AWS .

Membuat kontrol khusus

Anda dapat menggunakan kontrol khusus untuk mengumpulkan bukti dari sumber data tertentu yang Anda tentukan.

Sama seperti kontrol standar, kontrol kustom mengumpulkan bukti terus-menerus ketika mereka aktif dalam penilaian Anda. Anda juga dapat menambahkan bukti manual ke kontrol kustom apa pun yang Anda buat. Setiap bukti menjadi catatan yang membantu Anda menunjukkan kepatuhan terhadap persyaratan kontrol kustom Anda.

Untuk memulai, berikut adalah beberapa contoh bagaimana Anda dapat menggunakan kontrol khusus:

Gunakan kontrol yang ada sebagai titik awal

Anda dapat menyesuaikan kontrol apa pun di Audit Manager. Ini adalah pilihan yang baik jika kontrol yang ada kurang lebih memenuhi tujuan Anda, tetapi Anda ingin memperluas panduannya atau menyesuaikan beberapa atribut untuk memenuhi kebutuhan spesifik Anda. Misalnya, Anda dapat mengubah seberapa sering kontrol mengumpulkan bukti, dan kemudian mengubah nama kontrol untuk mencerminkan hal ini.

Buat kontrol khusus untuk audit internal

Untuk mendukung audit internal, Anda dapat membuat kontrol khusus yang dibuat khusus yang tidak terkait dengan kerangka kerja atau peraturan kepatuhan tertentu. Ini memberi Anda kebebasan untuk menyesuaikan persyaratan kontrol Anda ke area tertentu, atau mengumpulkan bukti dari sumber daya khusus bisnis. Misalnya, Anda dapat membuat kontrol kustom yang menggunakan AWS Config aturan kustom organisasi Anda sebagai sumber data untuk pengumpulan bukti.

Buat pertanyaan penilaian risiko vendor

Anda dapat menggunakan kontrol khusus untuk mendukung cara Anda mengelola penilaian risiko vendor. Setiap kontrol yang Anda buat dapat mewakili pertanyaan penilaian risiko individu. Dalam hal ini, nama kontrol dapat berupa pertanyaan, dan Anda dapat memberikan jawaban dengan mengunggah file atau memasukkan respons teks sebagai bukti manual.

Ada dua cara untuk membuat kontrol khusus. Anda dapat membuat kontrol baru dari awal atau Anda dapat menyesuaikan kontrol yang ada.

Topik

Membuat kontrol kustom baru dari awal

Anda dapat membuat kontrol kustom baru dari awal dengan mengikuti langkah-langkah ini.

> **Important**
>
> Kami sangat menyarankan agar Anda tidak pernah memasukkan informasi identifikasi sensitif ke dalam bidang bentuk bebas seperti rincian kontrol, informasi pengujian, atau rencana tindakan. Jika Anda membuat kontrol khusus yang berisi informasi sensitif, Anda tidak dapat membagikan kerangka kerja kustom apa pun yang berisi kontrol ini.

Topik

Langkah 1: Tentukan detail kontrol

Mulailah dengan menentukan detail kontrol kustom Anda.

Untuk menentukan detail kontrol

1. Buka konsol AWS Audit Manager di https://console.aws.amazon.com/auditmanager/home.
2. Di panel navigasi, pilih Control library, lalu pilih Create custom control.
3. Di bawah Detail kontrol, masukkan informasi berikut tentang kontrol.
   - Kontrol — Masukkan nama ramah, judul, atau pertanyaan penilaian risiko. Nilai ini membantu Anda mengidentifikasi kontrol Anda di pustaka kontrol.
   - Deskripsi (opsional) — Masukkan detail untuk membantu orang lain memahami tujuan kontrol. Deskripsi ini muncul di halaman detail kontrol.
4. Di bawah Informasi pengujian, masukkan langkah-langkah yang disarankan untuk menguji kontrol.
5. Di bawah Tag, pilih Tambahkan tag baru untuk mengaitkan tag dengan kontrol. Anda dapat menentukan kunci untuk setiap tag yang paling menggambarkan kerangka kepatuhan yang didukung kontrol ini. Kunci tag wajib dan dapat digunakan sebagai kriteria pencarian saat Anda mencari kontrol ini di pustaka kontrol.

6. Pilih Berikutnya.

Langkah 2: Siapkan sumber data

Selanjutnya, tentukan hingga 10 sumber data. Sumber data menentukan dari mana kontrol kustom Anda mengumpulkan bukti.

Jika Anda ingin mengumpulkan bukti otomatis, setiap sumber data harus menyertakan tipe sumber data dan pemetaan sumber data. Detail ini dipetakan ke AWS penggunaan Anda, dan beri tahu Audit Manager tempat mengumpulkan bukti. Jika Anda ingin memberikan bukti Anda sendiri, Anda akan memberi nama sumber data Anda dan kemudian memilih opsi bukti manual.

Important

Agar berhasil menggunakan AWS Config dan Security Hub sebagai sumber data otomatis, pastikan Anda melakukan hal berikut:

- Ikuti petunjuk untuk menyiapkan AWS Configdan menyiapkan Security Hub untuk digunakan dengan Audit Manager.
- Sertakan keduanya AWS Config dan Security Hub sebagai layanan dalam cakupan dalam penilaian Anda.

Audit Manager kemudian dapat mengumpulkan bukti setiap kali evaluasi dilakukan untuk AWS Config aturan atau kontrol Security Hub yang Anda tentukan dalam langkah ini.

Untuk mengatur sumber data

1. Di bawah Nama sumber data, ganti teks placeholder dengan nama deskriptif untuk sumber data.
2. Di bawah metode pengumpulan bukti, pilih bagaimana Anda ingin mengumpulkan bukti untuk kontrol ini.

   a. Jika Anda ingin Audit Manager mengumpulkan bukti, pilih Automated dan ikuti langkah-langkah berikut:

      - Di bawah Jenis sumber data, tentukan dari mana Audit Manager mengumpulkan bukti otomatis.
        - Untuk AWS CloudTrail, pilih kata kunci nama acara dari daftar dropdown.

- Untuk AWS Config, pilih jenis aturan dan kemudian pilih kata kunci pengenal aturan dari daftar dropdown.
- Untuk AWS Security Hub, pilih kontrol Security Hub dari daftar tarik-turun.
- Untuk panggilanAWS API, pilih panggilan API lalu pilih frekuensi pengumpulan bukti.

> **Tip**
>
> Untuk gambaran umum dari setiap jenis sumber data dan tips pemecahan masalah terkait, lihat. Ikhtisar sumber data otomatis
> Jika Anda perlu memvalidasi konfigurasi sumber data Anda dengan pakar domain, tetapkan metode pengumpulan bukti sebagai Manual untuk saat ini. Dengan begitu, Anda dapat membuat kontrol dan menambahkannya ke kerangka kerja sekarang, dan kemudian mengedit kontrol sesuai kebutuhan nanti.

b. Jika Anda ingin memberikan bukti Anda sendiri, pilih Manual dan pilih opsi Bukti Manual.

- Unggah file - Pilih opsi ini jika kontrol memerlukan dokumentasi sebagai bukti.
- Respons teks — Pilih opsi ini jika kontrol memerlukan jawaban atas pertanyaan penilaian risiko.

3. (Opsional) Di bawah Detail tambahan, masukkan deskripsi sumber data dan deskripsi pemecahan masalah.
4. (Opsional) Untuk menambahkan sumber data lain, pilih Tambahkan sumber data dan ulangi langkah 1-3.
5. (Opsional) Untuk menghapus sumber data, pilih Hapus di bagian atas kotak konfigurasi sumber data.
6. Setelah selesai, pilih Berikutnya.

Langkah 3 (Opsional): Tentukan rencana tindakan

Selanjutnya, tentukan tindakan yang harus diambil jika kontrol ini perlu diperbaiki.

Untuk menentukan rencana aksi

1. Di bawah Judul, masukkan judul deskriptif untuk rencana tindakan.
2. Di bawah instruksi Rencana tindakan, masukkan instruksi terperinci untuk rencana tindakan.
3. Pilih Berikutnya.

Langkah 4: Tinjau dan buat kontrol

Tinjau informasi untuk kontrol. Untuk mengubah informasi untuk satu langkah, pilih Edit.

Setelah selesai, pilih Buat kontrol khusus.

Apa yang bisa saya lakukan selanjutnya?

Setelah Anda membuat kontrol kustom baru, Anda dapat menambahkannya ke kerangka kustom. Untuk mempelajari lebih lanjut, lihat Membuat kerangka kerja khusus atauMengedit kerangka kerja khusus.

Setelah Anda menambahkan kontrol kustom ke kerangka kustom, Anda dapat membuat penilaian dari kerangka kustom tersebut dan mulai mengumpulkan bukti. Untuk mempelajari selengkapnya, lihat Membuat penilaian.

Untuk tips pemecahan masalah, lihat. Memecahkan masalah kontrol dan pengaturan kontrol

Menyesuaikan kontrol yang ada

Alih-alih membuat kontrol khusus dari awal, Anda dapat menggunakan kontrol yang ada sebagai titik awal dan menyesuaikannya sesuai dengan kebutuhan Anda. Saat Anda melakukan ini, kontrol yang ada tetap berada di pustaka kontrol, dan kontrol kustom baru dibuat dengan pengaturan khusus Anda.

Anda dapat memilih kontrol yang ada untuk menyesuaikan. Ini bisa berupa kontrol standar atau kontrol khusus.

> **Important**
>
> Kami sangat menyarankan agar Anda tidak pernah memasukkan informasi identifikasi sensitif ke dalam bidang bentuk bebas seperti rincian kontrol, informasi pengujian, atau rencana tindakan. Jika Anda membuat kontrol khusus yang berisi informasi sensitif, Anda tidak dapat membagikan kerangka kerja kustom apa pun yang berisi kontrol ini.

Topik

- Langkah 1: Tentukan detail kontrol
- Langkah 2: Siapkan sumber data
- Langkah 3: (Opsional): Tentukan rencana tindakan

- Langkah 4: Tinjau dan buat kontrol
- Apa yang bisa saya lakukan selanjutnya?

Langkah 1: Tentukan detail kontrol

Rincian kontrol diwarisi dari kontrol asli. Tinjau dan modifikasi detail ini sesuai kebutuhan.

Untuk menentukan detail kontrol

1. Buka konsol AWS Audit Manager di https://console.aws.amazon.com/auditmanager/home.
2. Di panel navigasi, pilih Control library.
3. Pilih kontrol yang ingin Anda sesuaikan dan kemudian pilih Sesuaikan kontrol yang ada.
4. Tentukan nama baru kontrol, dan pilih Sesuaikan.
5. Di bawah Detail kontrol, sesuaikan detail kontrol sesuai kebutuhan.
6. Di bawah informasi Pengujian, sesuaikan informasi pengujian sesuai kebutuhan.
7. Di bawah Tag, sesuaikan tag sesuai kebutuhan.
8. Pilih Berikutnya.

Langkah 2: Siapkan sumber data

Sumber data diwarisi dari kontrol asli. Anda dapat mengubah, menambah, atau menghapus sumber data sesuai kebutuhan.

> **Important**
>
> Agar berhasil menggunakan AWS Config dan Security Hub sebagai sumber data otomatis, pastikan Anda melakukan hal berikut:
>
> - Ikuti petunjuk untuk menyiapkan AWS Configdan menyiapkan Security Hub untuk digunakan dengan Audit Manager.
> - Sertakan keduanya AWS Config dan Security Hub sebagai layanan dalam cakupan dalam penilaian Anda.
>
> Audit Manager kemudian dapat mengumpulkan bukti setiap kali evaluasi dilakukan untuk AWS Config aturan atau kontrol Security Hub yang Anda tentukan dalam langkah ini.

Untuk mengatur sumber data

1. Di bawah Nama sumber data, sesuaikan nama sumber data sesuai kebutuhan.
2. Di bawah metode pengumpulan Bukti, sesuaikan pemilihan sesuai kebutuhan.

   a. Jika Anda ingin Audit Manager mengumpulkan bukti, pilih Automated dan ikuti langkah-langkah berikut:

      - Di bawah tipe sumber data, tinjau dari mana Audit Manager mengumpulkan bukti otomatis, dan memodifikasi sesuai kebutuhan.
        - Untuk AWS CloudTrail, pilih kata kunci nama acara dari daftar dropdown.
        - Untuk AWS Config, pilih jenis aturan dan kemudian pilih kata kunci pengenal aturan dari daftar dropdown.
        - Untuk AWS Security Hub, pilih kontrol Security Hub dari daftar tarik-turun.
        - Untuk panggilanAWS API, pilih panggilan API lalu pilih frekuensi pengumpulan bukti.

      > **Tip**
      >
      > Untuk gambaran umum dari setiap jenis sumber data dan tips pemecahan masalah terkait, lihat. Ikhtisar sumber data otomatis
      > Jika Anda perlu memvalidasi konfigurasi sumber data Anda dengan pakar domain, tetapkan metode pengumpulan bukti sebagai Manual untuk saat ini. Dengan begitu, Anda dapat membuat kontrol dan menambahkannya ke kerangka kerja sekarang, dan kemudian mengedit kontrol sesuai kebutuhan nanti.

   b. Jika Anda ingin memberikan bukti Anda sendiri, pilih Manual dan pilih opsi Bukti Manual.

      - Unggah file - Pilih opsi ini jika kontrol memerlukan dokumentasi sebagai bukti.
      - Respons teks — Pilih opsi ini jika kontrol memerlukan jawaban atas pertanyaan penilaian risiko.

3. (Opsional) Di bawah Rincian tambahan, buat perubahan yang diperlukan pada deskripsi sumber data atau deskripsi pemecahan masalah.
4. (Opsional) Untuk menambahkan sumber data lain, pilih Tambahkan sumber data.
5. (Opsional) Untuk menghapus sumber data, pilih Hapus.
6. Pilih Berikutnya.

Langkah 3: (Opsional): Tentukan rencana tindakan

Rencana aksi diwarisi dari kontrol asli. Anda dapat mengedit rencana tindakan ini sesuai kebutuhan.

Untuk menentukan rencana aksi

1. Di bawah Judul, tinjau judul untuk rencana aksi, dan sesuaikan sesuai kebutuhan.
2. Di bawah Instruksi rencana tindakan, tinjau dan sesuaikan instruksi sesuai kebutuhan.
3. Pilih Berikutnya.

Langkah 4: Tinjau dan buat kontrol

Tinjau informasi untuk kontrol. Untuk mengubah informasi untuk satu langkah, pilih Edit. Setelah selesai, pilih Buat kontrol khusus.

Apa yang bisa saya lakukan selanjutnya?

Setelah Anda membuat kontrol kustom baru, Anda dapat menambahkannya ke kerangka kustom. Untuk mempelajari lebih lanjut, lihat Membuat kerangka kerja khusus atauMengedit kerangka kerja khusus.

Setelah Anda menambahkan kontrol kustom ke kerangka kustom, Anda dapat membuat penilaian dari kerangka kustom tersebut dan mulai mengumpulkan bukti. Untuk mempelajari selengkapnya, lihat Membuat penilaian.

Jika Anda perlu mengedit kontrol khusus, lihatMengedit kontrol khusus.

Untuk tips pemecahan masalah, lihat. Memecahkan masalah kontrol dan pengaturan kontrol

Mengedit kontrol khusus

Anda dapat mengedit kontrol kustom di Audit Manager dengan mengikuti langkah-langkah berikut.

Topik

Langkah 1: Edit detail kontrol

Mulailah dengan meninjau dan mengedit detail kontrol sesuai kebutuhan.

Untuk mengedit detail kontrol

1. Buka konsol AWS Audit Manager di https://console.aws.amazon.com/auditmanager/home.
2. Di panel navigasi, pilih Control library lalu pilih tab Custom controls.
3. Pilih kontrol yang ingin Anda edit dan kemudian pilih Edit.
4. Di bawah Detail kontrol, edit detail kontrol sesuai kebutuhan.
5. Di bawah informasi Pengujian, edit informasi pengujian yang direkomendasikan sesuai kebutuhan.
6. Pilih Berikutnya.

> **Tip**
>
> Untuk mengedit tag untuk kontrol, buka kontrol dan pilih tab tag. Di sana Anda dapat melihat dan mengedit tag yang terkait dengan kontrol.

Langkah 2: Edit sumber data

Selanjutnya, Anda dapat mengedit, menghapus, atau menambahkan sumber data untuk kontrol.

> **Important**
>
> Agar berhasil menggunakan AWS Config dan Security Hub sebagai sumber data otomatis, pastikan Anda melakukan hal berikut:
>
> - Ikuti petunjuk untuk menyiapkan AWS Configdan menyiapkan Security Hub untuk digunakan dengan Audit Manager.
> - Sertakan keduanya AWS Config dan Security Hub sebagai layanan dalam cakupan dalam penilaian Anda.
>
> Audit Manager kemudian dapat mengumpulkan bukti setiap kali evaluasi dilakukan untuk AWS Config aturan atau kontrol Security Hub yang Anda tentukan dalam langkah ini.

Untuk mengedit sumber data

1. Di bawah Nama sumber data, tinjau nama saat ini dan edit sesuai kebutuhan.
2. Di bawah metode pengumpulan Bukti, tinjau pilihan saat ini dan edit sesuai kebutuhan.

   a. Jika Anda ingin Audit Manager mengumpulkan bukti, pilih Automated dan ikuti langkah-langkah berikut:

      - Di bawah Jenis sumber data, tinjau dari mana Audit Manager mengumpulkan bukti otomatis, dan edit sesuai kebutuhan.
        - Untuk AWS CloudTrail, pilih kata kunci nama acara dari daftar dropdown.
        - Untuk AWS Config, pilih jenis aturan dan kemudian pilih kata kunci pengenal aturan dari daftar dropdown.
        - Untuk AWS Security Hub, pilih kontrol Security Hub dari daftar tarik-turun.
        - Untuk panggilanAWS API, pilih panggilan API lalu pilih frekuensi pengumpulan bukti.

      > **Tip**
      >
      > Untuk gambaran umum dari setiap jenis sumber data dan tips pemecahan masalah terkait, lihat. Ikhtisar sumber data otomatis

   b. Jika Anda ingin memberikan bukti Anda sendiri, pilih Manual dan pilih opsi Bukti Manual.

      - Unggah file - Pilih opsi ini jika kontrol memerlukan dokumentasi sebagai bukti.
      - Respons teks — Pilih opsi ini jika kontrol memerlukan jawaban atas pertanyaan penilaian risiko.

3. (Opsional) Di bawah Rincian tambahan, buat perubahan yang diperlukan pada deskripsi sumber data atau deskripsi pemecahan masalah.
4. (Opsional) Untuk menambahkan sumber data lain, pilih Tambahkan sumber data.
5. (Opsional) Untuk menghapus sumber data, pilih Hapus.
6. Pilih Berikutnya.

Langkah 3: (Opsional) Edit rencana tindakan

Selanjutnya, tinjau dan edit rencana tindakan opsional.

Untuk mengedit rencana tindakan

1. Di bawah Judul, edit judul sesuai kebutuhan.
2. Di bawah Instruksi rencana tindakan, edit instruksi sesuai kebutuhan.
3. Pilih Berikutnya.

Langkah 4: Tinjau dan perbarui kontrol

Tinjau informasi untuk kontrol. Untuk mengubah informasi untuk satu langkah, pilih Edit.

Setelah Anda selesai, pilih Simpan perubahan.

> **Note**
>
> Setelah Anda mengedit kontrol, perubahan akan berlaku sebagai berikut di semua penilaian aktif yang menyertakan kontrol:
>
> - Untuk kontrol dengan panggilanAWS API sebagai tipe sumber data, perubahan berlaku pada pukul 00:00 UTC pada hari berikutnya.
> - Untuk semua kontrol lainnya, perubahan segera berlaku.

Menghapus kontrol khusus

Anda dapat menggunakan pustaka kontrol untuk menghapus kontrol kustom yang tidak diinginkan. Setelah Anda menghapus kontrol, itu tidak lagi muncul di pustaka kontrol. Anda juga dapat menghapus kontrol kustom menggunakan Audit Manager API atau AWS Command Line Interface (AWS CLI).

> **Important**
>
> Saat Anda menghapus kontrol kustom, tindakan ini akan menghapus kontrol dari kerangka kerja kustom atau penilaian yang saat ini terkait dengannya. Akibatnya, Audit Manager akan berhenti mengumpulkan bukti untuk kontrol kustom tersebut di semua penilaian Anda. Ini termasuk penilaian yang sebelumnya Anda buat sebelum Anda menghapus kontrol kustom.

Audit Manager console

Untuk menghapus kontrol kustom (konsol)

1. Buka konsol AWS Audit Manager di https://console.aws.amazon.com/auditmanager/home.
2. Di panel navigasi, pilih Control library lalu pilih tab Custom controls.
3. Pilih kontrol yang ingin Anda hapus, lalu pilih Hapus.
4. Di jendela pop-up yang muncul, pilih Hapus untuk mengonfirmasi penghapusan.

AWS CLI

Untuk menghapus kontrol kustom (AWS CLI)

1. Pertama, identifikasi kontrol khusus yang ingin Anda hapus. Untuk melakukan ini, jalankan perintah list-controls dan tentukan as. `--control-type Custom`

   ```
   aws auditmanager list-controls --control-type Custom
   ```

   Respons mengembalikan daftar kontrol kustom. Temukan kontrol yang ingin Anda hapus, dan catat ID kontrol.
2. Selanjutnya, jalankan perintah delete-control dan gunakan `--control-id` parameter untuk menentukan kontrol yang ingin Anda hapus.

   Dalam contoh berikut, ganti *`teks placeholder dengan informasi`* Anda sendiri.

   ```
   aws auditmanager delete-control --control-id a1b2c3d4-5678-90ab-cdef-
   EXAMPLE11111
   ```

Audit Manager API

Untuk menghapus kontrol kustom (API)

1. Gunakan ListControlsoperasi dan tentukan ControlType sebagai`Custom`. Dari respons, temukan kontrol yang ingin Anda hapus dan catat ID kontrol.
2. Gunakan DeleteControloperasi untuk menghapus kontrol kustom. Dalam permintaan, gunakan parameter ControLid untuk menentukan kontrol yang ingin Anda hapus.

Untuk informasi selengkapnya tentang operasi API ini, pilih salah satu tautan sebelumnya untuk membaca selengkapnya di ReferensiAWS Audit Manager API. Ini termasuk informasi tentang cara menggunakan operasi dan parameter ini di salah satu SDK khusus bahasa AWS .

Mengubah frekuensi pengumpulan bukti untuk kontrol

AWS Audit Manager mengumpulkan bukti dari berbagai sumber data pada frekuensi yang berbeda-beda. Frekuensi pengumpulan bukti yang didukung tergantung pada jenis bukti yang dikumpulkan untuk kontrol.

- Untuk panggilanAWS API, Audit Manager mengumpulkan bukti menggunakan panggilan API describe ke panggilan lain Layanan AWS. Anda dapat menentukan frekuensi pengumpulan bukti secara langsung di Audit Manager (hanya untuk kontrol kustom).
- Untuk AWS Config, Audit Manager melaporkan hasil pemeriksaan kepatuhan langsung dari AWS Config. Frekuensi mengikuti pemicu yang didefinisikan dalam AWS Config aturan.
- Untuk AWS Security Hub, Audit Manager melaporkan hasil pemeriksaan kepatuhan langsung dari Security Hub. Frekuensi mengikuti jadwal pemeriksaan Security Hub.
- Untuk AWS CloudTrail, Audit Manager mengumpulkan bukti secara terus menerus dari CloudTrail. Anda tidak dapat mengubah frekuensi untuk jenis bukti ini.

Bagian berikut memberikan informasi lebih lanjut tentang frekuensi pengumpulan bukti untuk setiap jenis sumber data kontrol, dan cara mengubahnya (jika ada).

Topik

Snapshot konfigurasi dari panggilan AWS API

> **Note**
>
> Berikut ini hanya berlaku untuk kontrol khusus. Anda tidak dapat mengubah frekuensi pengumpulan bukti untuk kontrol standar yang menggunakan panggilan API sebagai sumber data.

Jika kontrol kustom menggunakan panggilan AWS API sebagai tipe sumber data, Anda dapat mengubah frekuensi pengumpulan bukti di Audit Manager dengan mengikuti langkah-langkah berikut.

Untuk mengubah frekuensi pengumpulan bukti untuk kontrol kustom dengan sumber data panggilan API

1. Buka konsol AWS Audit Manager di https://console.aws.amazon.com/auditmanager/home.
2. Di panel navigasi, pilih Control library, lalu pilih tab Custom controls.
3. Pilih kontrol khusus yang ingin Anda edit, lalu pilih Edit.
4. Pada halaman Edit detail kontrol, pilih Berikutnya.
5. Temukan kotak sumber data yang ingin Anda edit, dan verifikasi bahwa informasi berikut ini benar:
   - Metode pengumpulan bukti adalah Otomatis.
   - Jenis sumber data adalah panggilanAWS API.
   - Panggilan API yang dipilih adalah panggilan yang ingin Anda ubah frekuensinya.
6. Di bawah Frekuensi, pilih seberapa sering Anda ingin mengumpulkan bukti untuk kontrol kustom.
7. Ulangi langkah 5-6 sesuai kebutuhan untuk sumber data panggilan API tambahan yang ingin Anda edit.
8. Pilih Berikutnya.
9. Pada halaman Edit rencana tindakan, pilih Berikutnya.
10. Pada halaman Tinjau dan perbarui kontrol, tinjau informasi untuk kontrol kustom. Untuk mengubah informasi untuk satu langkah, pilih Edit.
11. Setelah Anda selesai, pilih Simpan perubahan.

Setelah Anda mengedit kontrol dengan panggilanAWS API sebagai tipe sumber data, perubahan akan berlaku pada pukul 00:00 UTC pada hari berikutnya di semua penilaian aktif yang menyertakan kontrol.

Pemeriksaan kepatuhan dari AWS Config

> **Note**
>
> Berikut ini berlaku untuk kontrol standar dan kontrol khusus yang digunakan Aturan AWS Config sebagai sumber data.

Jika kontrol digunakan AWS Config sebagai tipe sumber data, Anda tidak dapat mengubah frekuensi pengumpulan bukti secara langsung di Audit Manager. Ini karena frekuensi mengikuti pemicu yang ditentukan dalam AWS Config aturan.

Ada dua jenis pemicu untuk Aturan AWS Config:

1. Perubahan konfigurasi - AWS Config menjalankan evaluasi untuk aturan ketika jenis sumber daya tertentu dibuat, diubah, atau dihapus.
2. Berkala - AWS Config menjalankan evaluasi untuk aturan pada frekuensi yang Anda pilih (misalnya, setiap 24 jam).

Untuk mempelajari pemicu selengkapnya Aturan AWS Config, lihat Jenis pemicu di PanduanAWS Config Pengembang.

Untuk petunjuk tentang cara mengelola Aturan AWS Config, lihat Mengelola AWS Config aturan Anda.

Pemeriksaan kepatuhan dari Security Hub

> **Note**
>
> Berikut ini berlaku untuk kontrol standar dan kontrol khusus yang menggunakan pemeriksaan Security Hub sebagai sumber data.

Jika kontrol menggunakan Security Hub sebagai tipe sumber data, Anda tidak dapat mengubah frekuensi pengumpulan bukti secara langsung di Audit Manager. Ini karena frekuensi mengikuti jadwal pemeriksaan Security Hub.

- Pemeriksaan berkala berjalan secara otomatis dalam waktu 12 jam setelah proses terbaru. Anda tidak dapat mengubah periodisitas.
- Pemeriksaan yang dipicu perubahan berjalan saat sumber daya terkait mengubah status. Meskipun sumber daya tidak mengubah status, pembaruan pada waktu untuk pemeriksaan yang dipicu perubahan disegarkan setiap 18 jam. Ini membantu menunjukkan bahwa kontrol masih diaktifkan. Secara umum, Security Hub menggunakan aturan yang dipicu perubahan bila memungkinkan.

Untuk mempelajari selengkapnya, lihat Menjadwalkan untuk menjalankan pemeriksaan keamanan di PanduanAWS Security Hub Pengguna.

Log aktivitas pengguna dari AWS CloudTrail

> **Note**
>
> Berikut ini berlaku untuk kontrol standar dan kontrol kustom yang menggunakan log aktivitas AWS CloudTrail pengguna sebagai sumber data.

Anda tidak dapat mengubah frekuensi pengumpulan bukti untuk kontrol yang menggunakan log aktivitas CloudTrail sebagai tipe sumber data. Audit Manager mengumpulkan jenis bukti ini dari CloudTrail secara terus menerus. Frekuensi terus menerus karena aktivitas pengguna dapat terjadi kapan saja sepanjang hari.

Sumber data kontrol yang didukung untuk bukti otomatis

Saat membuat kontrol kustom AWS Audit Manager, Anda dapat mengatur kontrol untuk mengumpulkan bukti otomatis dari jenis sumber data berikut:

- AWS CloudTrail
- AWS Security Hub
- AWS Config
- AWS Panggilan API

Topik berikut merangkum masing-masing tipe sumber data otomatis ini, dan mencantumkan AWS Security Hub kontrol, AWS Config aturan, dan panggilan AWS API spesifik yang didukung oleh Audit Manager.

Topik

Ikhtisar sumber data otomatis

Tabel berikut memberikan gambaran umum dari setiap tipe sumber data otomatis.

Jenis sumber data	Deskripsi	Frekuensi pengumpulan bukti	Untuk menggunakan tipe sumber data ini...	Ketika kontrol ini aktif dalam penilaian...	Kiat pemecahan masalah terkait
AWS CloudTrail	Melacak aktivitas pengguna tertentu.	Terus menerus.	Pilih dari daftar nama acara yang didukung.	Audit Manager memfilter CloudTrail log Anda berdasarkan kata kunci yang Anda pilih. Hasilnya diimpor sebagai bukti aktivitas Pengguna.	Penilaian saya tidak mengumpulkan bukti aktivitas pengguna dari AWS CloudTrail
AWS Config	Menangkap snapshot dari	Berdasarkan pemicu yang	Pilih jenis aturan, lalu pilih aturan.	Audit Manager mendapatkan temuan untuk aturan ini	Penilaian saya tidak

Jenis sumber data	Deskripsi	Frekuensi pengumpulan bukti	Untuk menggunakan tipe sumber data ini...	Ketika kontrol ini aktif dalam penilaian...	Kiat pemecahan masalah terkait
	postur keamanan sumber daya Anda dengan melaporkan temuan dari. AWS Config	didefinisikan dalam AWS Config aturan.	• Untuk aturan terkelola, pilih dari daftar kata kunci aturan terkelola yang didukung. • Untuk aturan khusus, pilih dari daftar aturan yang tersedia.	langsung dari AWS Config. Hasilnya diimpor sebagai bukti pemeriksaan Kepatuhan.	mengumpulkan bukti pemeriksaan kepatuhan dari AWS Config AWS Config masalah integrasi
AWS Security Hub	Menangkap cuplikan postur keamanan sumber daya Anda dengan melaporkan temuan dari Security Hub.	Berdasarkan jadwal pemeriksaan Security Hub.	Pilih dari daftar ID kontrol Security Hub yang didukung.	Audit Manager mendapatkan hasil pemeriksaan keamanan langsung dari Security Hub. Hasilnya diimpor sebagai bukti pemeriksaan Kepatuhan.	Penilaian saya tidak mengumpulkan bukti pemeriksaan kepatuhan dari AWS Security Hub

Jenis sumber data	Deskripsi	Frekuensi pengumpulan bukti	Untuk menggunakan tipe sumber data ini...	Ketika kontrol ini aktif dalam penilaian...	Kiat pemecahan masalah terkait
AWS Panggil API	Mengambil snapshot konfigurasi sumber daya Anda secara langsung melalui panggilan API ke yang ditentukan Layanan AWS.	Harian, mingguan, atau bulanan.	Pilih dari daftar panggilan API yang didukung, lalu pilih frekuensi yang Anda inginkan.	Audit Manager membuat panggilan API berdasarkan frekuensi yang Anda tentukan. Respons diimpor sebagai bukti data Konfigurasi.	Penilaian saya tidak mengumpulkan bukti data konfigurasi untuk panggilan AWS API

Aturan AWS Config didukung oleh AWS Audit Manager

Anda dapat menggunakan Audit Manager untuk menangkap AWS Config evaluasi sebagai bukti audit. Saat membuat atau mengedit kontrol kustom, Anda dapat menentukan satu atau beberapa AWS Config aturan sebagai pemetaan sumber data untuk pengumpulan bukti. AWS Config melakukan pemeriksaan kepatuhan berdasarkan aturan ini, dan Audit Manager melaporkan hasilnya sebagai bukti pemeriksaan kepatuhan.

Selain aturan terkelola, Anda juga dapat memetakan aturan kustom Anda ke sumber data kontrol.

Note

- Audit Manager tidak mengumpulkan bukti dari AWS Config aturan terkait layanan, kecuali aturan terkait layanan dari Paket Kesesuaian dan dari. AWS OrganizationsUntuk informasi selengkapnya, lihat bagian Pemecahan Masalah dari panduan ini.
- Audit Manager tidak mengelola AWS Config aturan untuk Anda. Sebelum Anda memulai pengumpulan bukti, kami sarankan Anda meninjau parameter AWS Config aturan Anda saat ini. Kemudian, validasi parameter tersebut terhadap persyaratan kerangka kerja yang Anda pilih. Jika diperlukan, Anda dapat memperbarui parameter aturan AWS Configagar selaras dengan persyaratan kerangka kerja. Ini akan membantu memastikan bahwa penilaian Anda mengumpulkan bukti pemeriksaan kepatuhan yang benar untuk kerangka kerja tersebut.

  Misalnya, anggaplah Anda membuat penilaian untuk CIS v1.2.0. Kerangka kerja ini memiliki kontrol bernama 1.9 — Pastikan kebijakan kata sandi IAM membutuhkan panjang minimum 14 atau lebih. Dalam AWS Config, iam-password-policyaturan memiliki `MinimumPasswordLength` parameter yang memeriksa panjang kata sandi. Nilai default untuk parameter ini adalah 14 karakter. Akibatnya, aturan tersebut sejalan dengan persyaratan kontrol. Jika Anda tidak menggunakan nilai parameter default, pastikan bahwa nilai yang Anda gunakan sama dengan atau lebih besar dari persyaratan 14 karakter dari CIS v1.2.0. Anda dapat menemukan detail parameter default untuk setiap aturan terkelola dalam AWS Config dokumentasi.

Topik

- Menggunakan aturan AWS Config terkelola dengan Audit Manager
- Menggunakan aturan AWS Config khusus dengan Audit Manager
- Mengatasi masalah AWS Config integrasi dengan Audit Manager

Menggunakan aturan AWS Config terkelola dengan Audit Manager

326 aturan AWS Config terkelola saat ini didukung oleh Audit Manager. Anda dapat menggunakan salah satu kata kunci pengenal aturan terkelola berikut saat menyiapkan sumber data untuk kontrol kustom. Untuk informasi selengkapnya tentang salah satu aturan terkelola yang tercantum di bawah ini, pilih item dari daftar atau lihat AturanAWS Config Terkelola di PanduanAWS Config Pengguna.

> **Tip**
>
> Bila Anda memilih aturan terkelola di konsol Audit Manager selama pembuatan kontrol kustom, pastikan Anda mencari salah satu kata kunci pengenal aturan berikut, dan bukan nama aturan. Untuk informasi tentang perbedaan antara nama aturan dan pengidentifikasi aturan, dan cara menemukan pengenal untuk aturan terkelola, lihat bagian Pemecahan masalah pada panduan pengguna ini.

Kata kunci aturan AWS Config terkelola yang didukung

- ACCESS_KEYS_DIPUTAR
- ACCOUNT_PART_OF_ORGANIZATIONS
- ACM_CERTIFICATE_EXPIRATION_CHECK
- ACM_CERTIFICATE_RSA_CHECK
- ALB_DESYNC_MODE_CHECK
- ALB_HTTP_DROP_INVALID_HEADER_ENABLED
- ALB_HTTP_TO_HTTP_REDIRECTION_CHECK
- ALB_WAF_ENABLED
- API_GW_ASSOCIATED_WITH_WAF
- API_GW_CACHE_ENABLED_AND_ENCRYPTED
- API_GW_ENDPOINT_TYPE_CHECK
- API_GW_EXECUTION_LOGGING_ENABLED
- API_GW_SSL_ENABLED
- API_GW_XRAY_ENABLED
- API_GWV2_ACCESS_LOGS_ENABLED
- API_GWV2_AUTHORIZATION_TYPE_CONFIGURATED
- DISETUJUI_AMIS_BY_ID
- DISETUJUI_AMIS_BY_TAG
- APPSYNC_ASSOCIATED_WITH_WAF
- APPSYNC_CACHE_ENCRYPTION_AT_REST
- APPSYNC_LOGGING_ENABLED

Kata kunci aturan AWS Config terkelola yang didukung

- AURORA_LAST_BACKUP_RECOVERY_POINT_CREATED
- AURORA_MYSQL_BACKTRACKING_ENABLED
- AURORA_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- AUTOSCALING_CAPACITY_REBALANCING
- AUTOSCALING_GROUP_ELB_HEALTHCHECK_REQUIRED
- AUTOSCALING_LAUNCH_CONFIG_HOP_LIMIT
- AUTOSCALING_LAUNCH_CONFIG_PUBLIC_IP_DISABLED
- AUTOSCALING_LAUNCHCONFIG_REQUIRES_IMDSV2
- TEMPLAT AUTOSCALING_LAUNCH_
- AUTOSCALING_MULTIPLE_AZ
- AUTOSCALING_MULTIPLE_INSTANCE_TYPES
- BACKUP_PLAN_MIN_FREQUENCY_AND_MIN_RETENTION_CHECK
- BACKUP_RECOVERY_POINT_ENCRYPTED
- BACKUP_RECOVERY_POINT_MANUAL_DELETION_DISABLED
- BACKUP_RECOVERY_POINT_MINIMUM_RETENTION_CHECK
- BEANSTALK_ENHANCED_HEALTH_REPORTING_ENABLED
- CLB_DESYNC_MODE_CHECK
- CLB_MULTIPLE_AZ
- CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED
- CLOUD_TRAIL_ENABLED
- CLOUD_TRAIL_ENCRYPTION_ENABLED
- CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED
- CLOUDFORMATION_STACK_DRIFT_DETECTION_CHECK
- CLOUDFORMATION_STACK_NOTIFICATION_CHECK
- CLOUDFRONT_ACCESSLOGS_ENABLED
- CLOUDFRONT_ASSOCIATED_WITH_WAF
- CLOUDFRONT_CUSTOM_SSL_CERTIFICATE
- CLOUDFRONT_DEFAULT_ROOT_OBJECT_CONFIGURATED
- CLOUDFRONT_NO_DEPRECATED_SSL_PROTOCOLS

Kata kunci aturan AWS Config terkelola yang didukung

- CLOUDFRONT_ORIGIN_ACCESS_IDENTITY_ENABLED
- CLOUDFRONT_ORIGIN_FAILOVER_ENABLED
- CLOUDFRONT_S3_ORIGIN_ACCESS_CONTROL_ENABLED
- CLOUDFRONT_S3_ORIGIN_NON_EXISTENT_BUCKET
- CLOUDFRONT_SECURITY_POLICY_CHECK
- CLOUDFRONT_SNI_ENABLED
- CLOUDFRONT_TRAFFIC_TO_ORIGIN_ENCRYPTED
- CLOUDFRONT_VIEWER_POLICY_HTTPS
- CLOUDTRAIL_S3_DATAEVENTS_ENABLED
- CLOUDTRAIL_SECURITY_TRAIL_ENABLED
- CLOUDWATCH_ALARM_ACTION_CHECK
- CLOUDWATCH_ALARM_ACTION_ENABLED_CHECK
- CLOUDWATCH_ALARM_RESOURCE_CHECK
- CLOUDWATCH_ALARM_SETTINGS_CHECK
- CLOUDWATCH_LOG_GROUP_ENCRYPTED
- CMK_BACKING_KEY_ROTATION_ENABLED
- CODEBUILD_PROJECT_ARTIFACT_ENCRYPTION
- CODEBUILD_PROJECT_ENVIRONMENT_PRIVILEGED_CHECK
- CODEBUILD_PROJECT_ENVVAR_ AWSCRED_CHECK
- CODEBUILD_PROJECT_LOGGING_ENABLED
- CODEBUILD_PROJECT_S3_LOGS_ENCRYPTED
- CODEBUILD_PROJECT_SOURCE_REPO_URL_CHECK
- CODEPLOY_AUTO_ROLLBACK_MONITOR_ENABLED
- CODEPLOY_EC2_MINIMUM_HEALTHY_HOSTS_CONFIGURATED
- CODEPLOY_LAMBDA_ALLATONCE_TRAFFIC_SHIFT_DISABLED
- CODEPIPELINE_DEPLOYMENT_COUNT_CHECK
- CODEPIPELINE_REGION_FANOUT_CHECK
- CUSTOM_SCHEMA_REGISTRY_POLICY_ATTACHED
- CW_LOGGROUP_RETENTION_PERIOD_CHECK

Kata kunci aturan AWS Config terkelola yang didukung

- DAX_ENCRYPTION_ENABLED
- DB_INSTANCE_BACKUP_ENABLED
- DESIRED_INSTANCE_TENANCY
- DESIRED_INSTANCE_TYPE
- DMS_REPLICATION_NOT_PUBLIC
- DYNAMODB_AUTOSCALING_ENABLED
- DYNAMODB_IN_BACKUP_PLAN
- DYNAMODB_LAST_BACKUP_RECOVERY_POINT_CREATED
- DYNAMODB_PITR_ENABLED
- DYNAMODB_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- DYNAMODB_TABLE_ENCRYPTED_KMS
- DYNAMODB_TABLE_ENCRYPTION_ENABLED
- DYNAMODB_THROUGHPUT_LIMIT_CHECK
- EBS_IN_BACKUP_PLAN
- EBS_LAST_BACKUP_RECOVERY_POINT_CREATED
- EBS_OPTIMIZED_INSTANCE
- EBS_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- EBS_SNAPSHOT_PUBLIC_RESTORABLE_CHECK
- EC2_CLIENT_VPN_NOT_AUTHORIZE_SEMUA
- EC2_EBS_ENCRYPTION_BY_DEFAULT
- EC2_IMDSV2_PERIKSA
- EC2_INSTANCE_DETAILED_MONITORING_ENABLED
- EC2_INSTANCE_MANAGED_BY_SSM
- EC2_INSTANCE_MULTIPLE_ENI_CHECK
- EC2_INSTANCE_NO_PUBLIC_IP
- EC2_INSTANCE_PROFILE_ATTACHED
- EC2_LAST_BACKUP_RECOVERY_POINT_CREATED
- EC2_LAUNCH_TEMPLATE_PUBLIC_IP_DISABLED
- EC2_MANAGEDINSTANCE_APPLICATIONS_BLACKLISTED

Kata kunci aturan AWS Config terkelola yang didukung

- EC2_MANAGEDINSTANCE_APPLICATIONS_REQUIRED
- EC2_MANAGEDINSTANCE_ASSOCIATION_COMPLIANCE_STATUS_CHECK
- EC2_MANAGEDINSTANCE_INVENTORY_BLACKLISTED
- EC2_MANAGEDINSTANCE_PATCH_COMPLIANCE_STATUS_CHECK
- EC2_MANAGEDINSTANCE_PLATFORM_CHECK
- EC2_TIDAK_AMAZON_KEY_PASANGAN
- EC2_PARAVIRTUAL_INSTANCE_CHECK
- EC2_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- EC2_SECURITY_GROUP_ATTACHED_TO_ENI
- EC2_SECURITY_GROUP_ATTACHED_TO_ENI_PERIODIC
- EC2_STOPPED_INSTANCE
- EC2_TOKEN_HOP_LIMIT_CHECK
- EC2_TRANSIT_GATEWAY_AUTO_VPC_ATTACH_DISABLED
- EC2_VOLUME_INUSE_PERIKSA
- ECR_PRIVATE_IMAGE_SCANNING_ENABLED
- ECR_PRIVATE_LIFECYCLE_POLICY_CONFIGURATED
- ECR_PRIVATE_TAG_IMMUTABILITY_ENABLED
- ECS_ AWSVPC_NETWORKING _DIAKTIFKAN
- ECS_CONTAINER_INSIGHTS_ENABLED
- ECS_CONTAINERS_NONPRIVILEGED
- ECS_CONTAINERS_READONLY_ACCESS
- ECS_FARGATE_LATEST_PLATFORM_VERSION
- ECS_NO_ENVIRONMENT_SECRETS
- ECS_TASK_DEFINITION_LOG_CONFIGURATION
- ECS_TASK_DEFINITION_MEMORY_HARD_LIMIT
- ECS_TASK_DEFINITION_NONROOT_USER
- ECS_TASK_DEFINITION_PID_MODE_CHECK
- ECS_TASK_DEFINITION_USER_FOR_HOST_MODE_CHECK
- EFS_ACCESS_POINT_ENFORCE_ROOT_DIRECTORY

Kata kunci aturan AWS Config terkelola yang didukung

- EFS_ACCESS_POINT_ENFORCE_USER_IDENTITY
- EFS_ENCRYPTED_CHECK
- EFS_IN_BACKUP_PLAN
- EFS_LAST_BACKUP_RECOVERY_POINT_CREATED
- EFS_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- EIP_TERLAMPIR
- EKS_CLUSTER_LOGGING_ENABLED
- EKS_CLUSTER_OLDEST_SUPPORTED_VERSION
- EKS_CLUSTER_SUPPORTED_VERSION
- EKS_ENDPOINT_NO_PUBLIC_ACCESS
- EKS_SECRETS_ENCRYPTED
- ELASTIC_BEANSTALK_LOGS_TO_CLOUDWATCH
- ELASTIC_BEANSTALK_MANAGED_UPDATES_ENABLED
- ELASTICACHE_AUTO_MINOR_VERSION_UPGRADE_CHECK
- ELASTICACHE_RBAC_AUTH_ENABLED
- ELASTICACHE_REDIS_CLUSTER_AUTOMATIC_BACKUP_CHECK
- ELASTICACHE_REPL_GRP_AUTO_FAILOVER_ENABLED
- ELASTICACHE_REPL_GRP_ENCRYPTED_AT_REST
- ELASTICACHE_REPL_GRP_ENCRYPTED_IN_TRANSIT
- ELASTICACHE_REPL_GRP_REDIS_AUTH_ENABLED
- ELASTICACHE_SUBNET_GROUP_CHECK
- ELASTICACHE_SUPPORTED_ENGINE_VERSION
- ELASTICSEARCH_ENCRYPTED_AT_REST
- ELASTICSEARCH_IN_VPC_ONLY
- ELASTICSEARCH_LOGS_TO_CLOUDWATCH
- ELASTICSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK
- ELB_ACM_CERTIFICATE_REQUIRED
- ELB_CROSS_ZONE_LOAD_BALANCING_ENABLED
- ELB_CUSTOM_SECURITY_POLICY_SSL_CHECK

Kata kunci aturan AWS Config terkelola yang didukung

- ELB_DELETION_PROTECTION_ENABLED
- ELB_LOGGING_ENABLED
- ELB_PREDEFINED_SECURITY_POLICY_SSL_CHECK
- ELB_TLS_HTTPS_LISTENERS_ONLY
- ELBV2_ACM_CERTIFICATE_REQUIRED
- ELBV2_MULTIPLE_AZ
- EMR_KERBEROS_ENABLED
- EMR_MASTER_NO_PUBLIC_IP
- TERENKRIPTED_VOLUME
- FMS_SHIELD_RESOURCE_POLICY_CHECK
- FMS_WEBACL_RESOURCE_POLICY_CHECK
- FMS_WEBACL_RULEGROUP_ASSOCIATION_CHECK
- FSX_LAST_BACKUP_RECOVERY_POINT_CREATED
- FSX_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- GUARDDUTY_ENABLED_CENTRALIZED
- GUARDDUTY_NON_ARCHIVED_FINDS
- IAM_CUSTOMER_POLICY_BLOCKED_KMS_ACTIONS
- IAM_GROUP_HAS_USERS_CHECK
- IAM_INLINE_POLICY_BLOCKED_KMS_ACTIONS
- IAM_NO_INLINE_POLICY_CHECK
- IAM_PASSWORD_POLICY
- IAM_POLICY_BLACKLISTED_CHECK
- IAM_POLICY_IN_USE
- IAM_POLICY_NO_STATEMENTS_WITH_ADMIN_ACCESS
- IAM_POLICY_NO_STATEMENTS_WITH_FULL_ACCESS
- IAM_ROLE_MANAGED_POLICY_CHECK
- IAM_ROOT_ACCESS_KEY_CHECK
- IAM_USER_GROUP_MEMBERSHIP_CHECK
- IAM_USER_MFA_ENABLED

Kata kunci aturan AWS Config terkelola yang didukung

- IAM_USER_NO_POLICIES_CHECK
- IAM_USER_UNUSED_CREDENTIALS_CHECK
- INCOMING_SSH_DISABLED
- INSTANCES_IN_VPC
- KINESIS_STREAM_ENCRYPTED
- INTERNET_GATEWAY_AUTHORIZED_VPC_ONLY
- KMS_CMK_NOT_SCHEDULED_FOR_DELETION
- LAMBDA_CONCURRENCY_PERIKSA
- LAMBDA_DLQ_PERIKSA
- LAMBDA_FUNCTION_PUBLIC_ACCESS_FORBIDLED
- LAMBDA_FUNCTION_SETTINGS_CHECK
- LAMBDA_INSIDE_VPC
- LAMBDA_VPC_MULTI_AZ_PERIKSA
- MACIE_STATUS_CHECK
- MFA_ENABLED_FOR_IAM_CONSOLE_ACCESS
- MQ_AUTOMATIC_MINOR_VERSION_UPGRADE_ENABLED
- MQ_CLOUDWATCH_AUDIT_LOGGING_ENABLED
- MQ_NO_PUBLIC_ACCESS
- MULTI_REGION_CLOUD_TRAIL_ENABLED
- NACL_NO_UNRESTRICTED_SSH_RDP
- NETFW_LOGGING_ENABLED
- NETFW_MULTI_AZ_ENABLED
- NETFW_POLICY_DEFAULT_ACTION_FRAGMENT_PACKETS
- NETFW_POLICY_DEFAULT_ACTION_FULL_PACKETS
- NETFW_POLICY_RULE_GROUP_ASSOCIATED
- NETFW_STATELESS_RULE_GROUP_NOT_EMPTY
- NLB_CROSS_ZONE_LOAD_BALANCING_ENABLED
- NO_UNRESTRICTED_ROUTE_TO_IGW
- OPENSEARCH_ACCESS_CONTROL_ENABLED

Kata kunci aturan AWS Config terkelola yang didukung

- OPENSEARCH_AUDIT_LOGGING_ENABLED
- OPENSEARCH_DATA_NODE_FAULT_TOLERANCE
- OPENSEARCH_ENCRYPTED_AT_REST
- OPENSEARCH_HTTPS_DIPERLUKAN
- OPENSEARCH_IN_VPC_ONLY
- OPENSEARCH_LOGS_TO_CLOUDWATCH
- OPENSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK
- RDS_AUTOMATIC_MINOR_VERSION_UPGRADE_ENABLED
- RDS_CLUSTER_DEFAULT_ADMIN_CHECK
- RDS_CLUSTER_DELETION_PROTECTION_ENABLED
- RDS_CLUSTER_IAM_AUTHENTICATION_ENABLED
- RDS_CLUSTER_MULTI_AZ_ENABLED
- RDS_DB_SECURITY_GROUP_NOT_ALLOWED
- RDS_ENHANCED_MONITORING_ENABLED
- RDS_IN_BACKUP_PLAN
- RDS_INSTANCE_DEFAULT_ADMIN_CHECK
- RDS_INSTANCE_DELETION_PROTECTION_ENABLED
- RDS_INSTANCE_IAM_AUTHENTICATION_ENABLED
- RDS_INSTANCE_PUBLIC_ACCESS_CHECK
- RDS_LAST_BACKUP_RECOVERY_POINT_CREATED
- RDS_LOGGING_ENABLED
- RDS_MULTI_AZ_SUPPORT
- RDS_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- RDS_SNAPSHOT_ENCRYPTED
- RDS_SNAPSHOTS_PUBLIC_DILARANG
- RDS_STORAGE_TERENKRIPSI
- REDSHIFT_BACKUP_ENABLED
- REDSHIFT_REQUIRE_TLS_SSL
- REDSHIFT_CLUSTER_CONFIGURATION_CHECK

Kata kunci aturan AWS Config terkelola yang didukung

- REDSHIFT_CLUSTER_MAINTENANCESETTINGS_CHECK
- REDSHIFT_CLUSTER_PUBLIC_ACCESS_CHECK
- REDSHIFT_AUDIT_LOGGING_ENABLED
- REDSHIFT_CLUSTER_KMS_ENABLED
- REDSHIFT_DEFAULT_ADMIN_CHECK
- REDSHIFT_DEFAULT_DB_NAME_CHECK
- REDSHIFT_ENHANCED_VPC_ROUTING_ENABLED
- REQUIRED_TAGS
- DIBATAS_INCOMING_TRAFFIC
- ROOT_ACCOUNT_HARDWARE_MFA_ENABLED
- ROOT_ACCOUNT_MFA_ENABLED
- S3_ACCOUNT_LEVEL_PUBLIC_ACCESS_BLOCKS_PERIODIC
- S3_ACCOUNT_LEVEL_PUBLIC_ACCESS_BLOCKS
- S3_BUCKET_ACL_DILARANG
- S3_BUCKET_BLACKLISTED_ACTIONS_DILARANG
- S3_BUCKET_DEFAULT_LOCK_ENABLED
- S3_BUCKET_LEVEL_PUBLIC_ACCESS_DILARANG
- S3_BUCKET_LOGGING_ENABLED
- S3_BUCKET_POLICY_GRANTEE_CHECK
- S3_BUCKET_POLICY_NOT_MORE_PERMISIF
- S3_BUCKET_PUBLIC_READ_DILARANG
- S3_BUCKET_PUBLIC_WRITE_DILARANG
- S3_BUCKET_REPLICATION_ENABLED
- S3_BUCKET_SERVER_SIDE_ENCRYPTION_ENABLED
- S3_BUCKET_SSL_REQUESTS_ONLY
- S3_BUCKET_VERSIONING_ENABLED
- S3_DEFAULT_ENCRYPTION_KMS
- S3_EVENT_NOTIFICATIONS_ENABLED
- S3_LAST_BACKUP_RECOVERY_POINT_CREATED

Kata kunci aturan AWS Config terkelola yang didukung

- S3_LIFECYCLE_POLICY_CHECK
- S3_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- S3_VERSION_LIFECYCLE_POLICY_CHECK
- SAGEMAKER_ENDPOINT_CONFIGURATION_KMS_KEY_CONFIGURATED
- SAGEMAKER_NOTEBOOK_INSTANCE_INSIDE_VPC
- SAGEMAKER_NOTEBOOK_INSTANCE_KMS_KEY_CONFIGURATED
- SAGEMAKER_NOTEBOOK_INSTANCE_ROOT_ACCESS_CHECK
- SAGEMAKER_NOTEBOOK_NO_DIRECT_INTERNET_ACCESS
- SECRETSMANAGER_ROTATION_ENABLED_CHECK
- SECRETSMANAGER_SCHEDULED_ROTATION_SUCCESS_CHECK
- SECRETSMANAGER_SECRET_PERIODIC_ROTATION
- SECRETSMANAGER_SECRET_UNUSED
- SECRETSMANAGER_USING_CMK
- SECURITY_ACCOUNT_INFORMATION_DISEDIAKAN
- SECURITYHUB_ENAB_ENABLED
- SERVICE_VPC_ENDPOINT_ENABLED
- SES_MALWARE_SCANNING_ENABLED
- SHIELD_ADVANCED_ENABLED_AUTORENEW
- SHIELD_DRT_ACCESS
- SNS_ENCRYPTED_KMS
- SNS_TOPIC_MESSAGE_DELIVERY_NOTIFICATION_ENABLED
- SSM_DOCUMENT_NOT_PUBLIC
- STEP_FUNCTIONS_STATE_MACHINE_LOGGING_ENABLED
- STORAGEGATEWAY_LAST_BACKUP_RECOVERY_POINT_CREATED
- STORAGEGATEWAY_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- SUBNET_AUTO_ASSIGN_PUBLIC_IP_DISABLED
- VIRTUALMACHINE_LAST_BACKUP_RECOVERY_POINT_CREATED
- VIRTUALMACHINE_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- VPC_DEFAULT_SECURITY_GROUP_CLOSED

Kata kunci aturan AWS Config terkelola yang didukung

- VPC_FLOW_LOGS_ENABLED
- VPC_NETWORK_ACL_UNUSED_CHECK
- VPC_PEERING_DNS_RESOLUTION_CHECK
- VPC_SG_OPEN_ONLY_TO_AUTHORIZED_PORTS
- VPC_VPN_2_TUNNELS_UP
- WAF_CLASSIC_LOGGING_ENABLED
- WAF_GLOBAL_RULEGROUP_NOT_EMPTY
- WAF_GLOBAL_RULE_NOT_EMPTY
- WAF_GLOBAL_WEBACL_NOT_EMPTY
- WAF_REGIONAL_RULEGROUP_NOT_EMPTY
- WAF_REGIONAL_RULE_NOT_EMPTY
- WAF_REGIONAL_WEBACL_NOT_EMPTY
- WAFV2_LOGGING_ENABLED
- WAFV2_RULEGROUP_NOT_EMPTY
- WAFV2_WEBACL_NOT_EMPTY

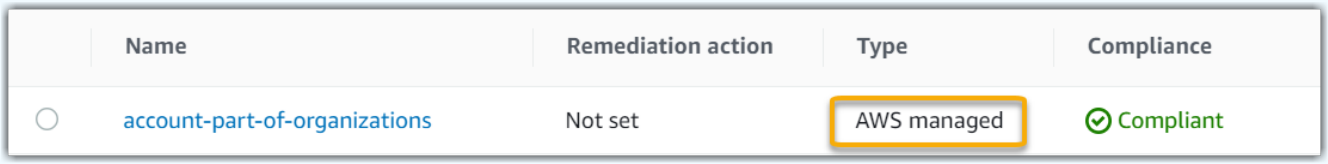
Menggunakan aturan AWS Config khusus dengan Audit Manager

Sekarang Anda dapat menggunakan aturan AWS Config kustom sebagai sumber data untuk pelaporan audit. Ketika kontrol memiliki sumber data yang dipetakan ke AWS Config aturan, Audit Manager menambahkan evaluasi yang dibuat oleh AWS Config aturan.

Aturan khusus yang dapat Anda gunakan bergantung pada Akun AWS cara Anda masuk ke Audit Manager. Jika Anda dapat mengakses aturan kustom AWS Config, Anda dapat menggunakannya sebagai pemetaan sumber data di Audit Manager.

- Untuk individu Akun AWS — Anda dapat menggunakan salah satu aturan khusus yang Anda buat dengan akun Anda.
- Untuk akun yang merupakan bagian dari organisasi — Anda dapat menggunakan salah satu aturan kustom tingkat anggota Anda. Atau, Anda dapat menggunakan salah satu aturan kustom tingkat organisasi yang tersedia untuk Anda. AWS Config

Untuk petunjuk tentang cara membuat kontrol yang menggunakan aturan kustom sebagai sumber data, lihat Membuat kontrol baru dari awal dan Menyesuaikan kontrol yang ada.

> **Tip**
>
> Perlu diingat bahwa aturan terkelola tidak ditampilkan dalam daftar tarik-turun aturan kustom di Audit Manager.
> Jika Anda ingin memverifikasi apakah AWS Config aturan adalah aturan terkelola atau aturan khusus, Anda dapat melakukannya menggunakan AWS Config konsol. Dari menu navigasi kiri, pilih Aturan dan cari aturan di tabel. Jika itu adalah aturan terkelola, kolom Type menunjukkan AWS managed.
>
> 
>
>
> Untuk memetakan aturan terkelola sebagai sumber data, Anda dapat mencari kata kunci pengenal aturan terkelola di Audit Manager di daftar dropdown aturan terkelola. Untuk informasi selengkapnya, lihat bagian Pemecahan Masalah dari panduan ini.

Setelah memetakan aturan kustom sebagai sumber data untuk kontrol, Anda dapat mengaitkan kontrol tersebut dengan kerangka kerja khusus di Audit Manager. Untuk petunjuk tentang cara membuat kerangka kerja khusus yang menggunakan kontrol kustom Anda, lihat Membuat kerangka kerja baru dari awal dan Menyesuaikan kerangka kerja yang ada. Untuk petunjuk tentang cara menambahkan kontrol Anda ke kerangka kustom yang ada, lihat Mengedit kerangka kerja yang ada.

Untuk informasi tentang membuat aturan kustom di AWS Config, lihat Mengembangkan aturan kustom untuk AWS Config di PanduanAWS Config Pengembang.

Mengatasi masalah AWS Config integrasi dengan Audit Manager

Untuk menemukan jawaban atas pertanyaan dan masalah umum, lihat AWS Config integrasi di bagian Pemecahan Masalah di panduan ini.

AWS Security Hub kontrol yang didukung oleh AWS Audit Manager

Audit Manager memungkinkan Anda melaporkan hasil pemeriksaan kepatuhan langsung dari Security Hub. Untuk melakukannya, Anda menentukan satu atau beberapa kontrol Security Hub sebagai pemetaan sumber data saat mengonfigurasi kontrol kustom di Audit Manager.

> **Note**
>
> - Audit Manager tidak mengumpulkan bukti dari AWS Config aturan terkait layanan yang dibuat oleh Security Hub. Untuk informasi selengkapnya, lihat bagian Pemecahan Masalah dari panduan ini.
> - Pada 9 November 2022, Security Hub meluncurkan pemeriksaan keamanan otomatis yang selaras dengan persyaratan Tolok Ukur AWS Yayasan Center for Internet Security (CIS) versi 1.4.0, Level 1 dan 2 (CIS v1.4.0). Di Security Hub, standar CIS v1.4.0 didukung selain standar CIS v1.2.0.

Topik

- Menggunakan kontrol Security Hub dengan Audit Manager
- Kontrol Security Hub yang Didukung

Menggunakan kontrol Security Hub dengan Audit Manager

> **Tip**
>
> Kami menyarankan Anda mengaktifkan pengaturan temuan kontrol konsolidasi di Security Hub jika belum diaktifkan. Jika Anda mengaktifkan Security Hub pada atau setelah 23 Februari 2003, pengaturan ini diaktifkan secara default.

Ketika temuan konsolidasi diaktifkan, Security Hub menghasilkan satu temuan untuk setiap pemeriksaan keamanan (bahkan ketika pemeriksaan yang sama berlaku untuk beberapa standar). Setiap temuan Security Hub dikumpulkan sebagai satu penilaian sumber daya unik di Audit Manager. Akibatnya, temuan konsolidasi menghasilkan penurunan total penilaian sumber daya unik yang dilakukan Audit Manager untuk temuan Security Hub. Untuk alasan ini, menggunakan temuan konsolidasi seringkali dapat mengakibatkan pengurangan biaya penggunaan Audit Manager Anda, tanpa mengorbankan kualitas dan ketersediaan bukti. Untuk informasi selengkapnya tentang harga, lihat AWS Audit Manager Harga.

Contoh bukti saat temuan konsolidasi dihidupkan atau dimatikan

Contoh berikut menunjukkan perbandingan cara Audit Manager mengumpulkan dan menyajikan bukti tergantung pada setelan Security Hub Anda.

When consolidated findings is turned on

Katakanlah Anda telah mengaktifkan tiga standar keamanan berikut di Security Hub: AWS FSBP, PCI DSS, dan CIS Benchmark v1.2.0.

- Ketiga standar ini menggunakan kontrol yang sama (IAM.4) dengan AWS Config aturan dasar yang sama (iam-root-access-key-check).
- Karena pengaturan temuan kontrol terkonsolidasi diaktifkan, Security Hub menghasilkan satu temuan tunggal untuk kontrol ini.
- Security Hub mengirimkan temuan konsolidasi ke Audit Manager untuk kontrol ini.
- Temuan konsolidasi dihitung sebagai salah satu penilaian sumber daya unik di Audit Manager. Akibatnya, satu bukti ditambahkan ke penilaian Anda.

Berikut adalah contoh bagaimana bukti itu mungkin terlihat:


```
{
    "SchemaVersion": "2018-10-08",
    "Id": "arn:aws:securityhub:us-west-2:111122223333:security-control/IAM.4/
finding/09876543-p0o9-i8u7-y6t5-098765432109",
    "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/securityhub",
    "ProductName": "Security Hub",
    "CompanyName": "AWS",
    "Region": "us-west-2",
    "GeneratorId": "security-control/IAM.4",
    "AwsAccountId": "111122223333",
    "Types": [
        "Software and Configuration Checks/Industry and Regulatory Standards"
    ],
    "FirstObservedAt": "2023-10-25T11:32:24.861Z",
    "LastObservedAt": "2023-11-02T11:59:19.546Z",
    "CreatedAt": "2023-10-25T11:32:24.861Z",
    "UpdatedAt": "2023-11-02T11:59:15.127Z",
    "Severity": {
        "Label": "INFORMATIONAL",
        "Normalized": 0,
        "Original": "INFORMATIONAL"
```

```
    },
    "Title": "IAM root user access key should not exist",
    "Description": "This AWS control checks whether the root user access key is
 available.",
    "Remediation": {
        "Recommendation": {
            "Text": "For information on how to correct this issue, consult the AWS
 Security Hub controls documentation.",
            "Url": "https://docs.aws.amazon.com/console/securityhub/IAM.4/
remediation"
        }
    },
    "ProductFields": {
        "RelatedAWSResources:0/name": "securityhub-iam-root-access-key-
check-000270f5",
        "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
        "aws/securityhub/ProductName": "Security Hub",
        "aws/securityhub/CompanyName": "AWS",
        "Resources:0/Id": "arn:aws:iam::111122223333:root",
        "aws/securityhub/FindingId": "arn:aws:securityhub:us-west-2::product/aws/
securityhub/arn:aws:securityhub:us-west-2:111122223333:security-control/IAM.4/
finding/09876543-p0o9-i8u7-y6t5-098765432109"
    },
    "Resources": [{
        "Type": "AwsAccount",
        "Id": "AWS::::Account:111122223333",
        "Partition": "aws",
        "Region": "us-west-2"
    }],
    "Compliance": {
        "Status": "PASSED",
        "RelatedRequirements": [
            "CIS AWS Foundations Benchmark v1.2.0/1.12"
        ],
        "SecurityControlId": "IAM.4",
        "AssociatedStandards": [{
                "StandardsId": "ruleset/cis-aws-foundations-benchmark/v/1.2.0"
            },
            {
                "StandardsId": "standards/aws-foundational-security-best-practices/
v/1.0.0"
            }
        ]
    },
```

```
    "WorkflowState": "NEW",
    "Workflow": {
        "Status": "RESOLVED"
    },
    "RecordState": "ACTIVE",
    "FindingProviderFields": {
        "Severity": {
            "Label": "INFORMATIONAL",
            "Original": "INFORMATIONAL"
        },
        "Types": [
            "Software and Configuration Checks/Industry and Regulatory Standards"
        ]
    },
    "ProcessedAt": "2023-11-02T11:59:20.980Z"
}
```

When consolidated findings is turned off

Katakanlah Anda telah mengaktifkan tiga standar keamanan berikut di Security Hub: AWS FSBP, PCI DSS, dan CIS Benchmark v1.2.0.

- Ketiga standar ini menggunakan kontrol yang sama (IAM.4) dengan AWS Config aturan dasar yang sama (iam-root-access-key-check).
- Karena pengaturan temuan konsolidasi dimatikan, Security Hub menghasilkan temuan terpisah per pemeriksaan keamanan untuk setiap standar yang diaktifkan (dalam hal ini, tiga temuan).
- Security Hub mengirimkan tiga temuan khusus standar terpisah ke Audit Manager untuk kontrol ini.
- Ketiga temuan tersebut dihitung sebagai tiga penilaian sumber daya unik di Audit Manager. Akibatnya, tiga bukti terpisah ditambahkan ke penilaian Anda.

Berikut adalah contoh bagaimana bukti itu mungkin terlihat. Perhatikan bahwa dalam contoh ini, masing-masing dari tiga muatan berikut memiliki ID kontrol keamanan yang sama (*`SecurityControlId":"IAM.4"`*). Untuk alasan ini, kontrol penilaian yang mengumpulkan bukti ini di Audit Manager (IAM.4) menerima tiga bukti terpisah ketika temuan berikut datang dari Security Hub.

Bukti untuk IAM.4 (FSBP)

```
{
```

```
  "version":"0",
  "id":"12345678-1q2w-3e4r-5t6y-123456789012",
  "detail-type":"Security Hub Findings - Imported",
  "source":"aws.securityhub",
  "account":"111122223333",
  "time":"2023-10-27T18:55:59Z",
  "region":"us-west-2",
  "resources":[
     "arn:aws:securityhub:us-west-2::product/aws/securityhub/arn:aws:securityhub:us-
west-2:111122223333:subscription/aws-foundational-security-best-practices/v/1.0.0/
Lambda.1/finding/b5e68d5d-43c3-46c8-902d-51cb0d4da568"
  ],
  "detail":{
     "findings":[
        {
           "SchemaVersion":"2018-10-08",
           "Id":"arn:aws:securityhub:us-west-2:111122223333:subscription/aws-
foundational-security-best-practices/v/1.0.0/IAM.4/finding/8e2e05a2-4d50-4c2e-
a78f-3cbe9402d17d",
           "ProductArn":"arn:aws:securityhub:us-west-2::product/aws/securityhub",
           "ProductName":"Security Hub",
           "CompanyName":"AWS",
           "Region":"us-west-2",
           "GeneratorId":"aws-foundational-security-best-practices/v/1.0.0/IAM.4",
           "AwsAccountId":"111122223333",
           "Types":[
              "Software and Configuration Checks/Industry and Regulatory Standards/
AWS-Foundational-Security-Best-Practices"
           ],
           "FirstObservedAt":"2020-10-05T19:18:47.848Z",
           "LastObservedAt":"2023-11-01T14:12:04.106Z",
           "CreatedAt":"2020-10-05T19:18:47.848Z",
           "UpdatedAt":"2023-11-01T14:11:53.720Z",
           "Severity":{
              "Product":0,
              "Label":"INFORMATIONAL",
              "Normalized":0,
              "Original":"INFORMATIONAL"
           },
           "Title":"IAM.4 IAM root user access key should not exist",
           "Description":"This AWS control checks whether the root user access key
 is available.",
           "Remediation":{
              "Recommendation":{
```

```
                "Text":"For information on how to correct this issue, consult the
 AWS Security Hub controls documentation.",
                "Url":"https://docs.aws.amazon.com/console/securityhub/IAM.4/
remediation"
             }
          },
          "ProductFields":{
             "StandardsArn":"arn:aws:securityhub:::standards/aws-foundational-
security-best-practices/v/1.0.0",
             "StandardsSubscriptionArn":"arn:aws:securityhub:us-
west-2:111122223333:subscription/aws-foundational-security-best-practices/v/1.0.0",
             "ControlId":"IAM.4",
             "RecommendationUrl":"https://docs.aws.amazon.com/console/securityhub/
IAM.4/remediation",
             "RelatedAWSResources:0/name":"securityhub-iam-root-access-key-
check-67cbb1c4",
             "RelatedAWSResources:0/type":"AWS::Config::ConfigRule",
             "StandardsControlArn":"arn:aws:securityhub:us-
west-2:111122223333:control/aws-foundational-security-best-practices/v/1.0.0/IAM.4",
             "aws/securityhub/ProductName":"Security Hub",
             "aws/securityhub/CompanyName":"AWS",
             "Resources:0/Id":"arn:aws:iam::111122223333:root",
             "aws/securityhub/FindingId":"arn:aws:securityhub:us-west-2::product/
aws/securityhub/arn:aws:securityhub:us-west-2:111122223333:subscription/aws-
foundational-security-best-practices/v/1.0.0/IAM.4/finding/8e2e05a2-4d50-4c2e-
a78f-3cbe9402d17d"
          },
          "Resources":[
             {
                "Type":"AwsAccount",
                "Id":"AWS::::Account:111122223333",
                "Partition":"aws",
                "Region":"us-west-2"
             }
          ],
          "Compliance":{
             "Status":"PASSED",
             "SecurityControlId":"IAM.4",
             "AssociatedStandards":[
                {
                   "StandardsId":"standards/aws-foundational-security-best-
practices/v/1.0.0"
                }
             ]
```

```
            },
            "WorkflowState":"NEW",
            "Workflow":{
               "Status":"RESOLVED"
            },
            "RecordState":"ACTIVE",
            "FindingProviderFields":{
               "Severity":{
                  "Label":"INFORMATIONAL",
                  "Original":"INFORMATIONAL"
               },
               "Types":[
                  "Software and Configuration Checks/Industry and Regulatory
 Standards/AWS-Foundational-Security-Best-Practices"
               ]
            },
            "ProcessedAt":"2023-11-01T14:12:07.395Z"
         }
      ]
   }
}
```

Bukti untuk IAM.4 (CIS 1.2)

```
{
  "version":"0",
  "id":"12345678-1q2w-3e4r-5t6y-123456789012",
  "detail-type":"Security Hub Findings - Imported",
  "source":"aws.securityhub",
  "account":"111122223333",
  "time":"2023-10-27T18:55:59Z",
  "region":"us-west-2",
  "resources":[
     "arn:aws:securityhub:us-west-2::product/aws/securityhub/arn:aws:securityhub:us-
west-2:111122223333:subscription/aws-foundational-security-best-practices/v/1.0.0/
Lambda.1/finding/1dd8f2f8-cf1b-47c9-a875-8d7387fc9c23"
  ],
  "detail":{
     "findings":[
        {
           "SchemaVersion":"2018-10-08",
```

```
            "Id":"arn:aws:securityhub:us-west-2:111122223333:subscription/cis-aws-
foundations-benchmark/v/1.2.0/1.12/finding/1dd8f2f8-cf1b-47c9-a875-8d7387fc9c23",
            "ProductArn":"arn:aws:securityhub:us-west-2::product/aws/securityhub",
            "ProductName":"Security Hub",
            "CompanyName":"AWS",
            "Region":"us-west-2",
            "GeneratorId":"arn:aws:securityhub:::ruleset/cis-aws-foundations-
benchmark/v/1.2.0/rule/1.12",
            "AwsAccountId":"111122223333",
            "Types":[
               "Software and Configuration Checks/Industry and Regulatory Standards/
CIS AWS Foundations Benchmark"
            ],
            "FirstObservedAt":"2020-10-05T19:18:47.775Z",
            "LastObservedAt":"2023-11-01T14:12:07.989Z",
            "CreatedAt":"2020-10-05T19:18:47.775Z",
            "UpdatedAt":"2023-11-01T14:11:53.720Z",
            "Severity":{
               "Product":0,
               "Label":"INFORMATIONAL",
               "Normalized":0,
               "Original":"INFORMATIONAL"
            },
            "Title":"1.12 Ensure no root user access key exists",
            "Description":"The root user is the most privileged user in an AWS
 account. AWS Access Keys provide programmatic access to a given AWS account. It is
 recommended that all access keys associated with the root user be removed.",
            "Remediation":{
               "Recommendation":{
                  "Text":"For information on how to correct this issue, consult the
 AWS Security Hub controls documentation.",
                  "Url":"https://docs.aws.amazon.com/console/securityhub/IAM.4/
remediation"
               }
            },
            "ProductFields":{
               "StandardsGuideArn":"arn:aws:securityhub:::ruleset/cis-aws-
foundations-benchmark/v/1.2.0",
               "StandardsGuideSubscriptionArn":"arn:aws:securityhub:us-
west-2:111122223333:subscription/cis-aws-foundations-benchmark/v/1.2.0",
               "RuleId":"1.12",
               "RecommendationUrl":"https://docs.aws.amazon.com/console/securityhub/
IAM.4/remediation",
```

```
              "RelatedAWSResources:0/name":"securityhub-iam-root-access-key-
check-67cbb1c4",
              "RelatedAWSResources:0/type":"AWS::Config::ConfigRule",
              "StandardsControlArn":"arn:aws:securityhub:us-
west-2:111122223333:control/cis-aws-foundations-benchmark/v/1.2.0/1.12",
              "aws/securityhub/ProductName":"Security Hub",
              "aws/securityhub/CompanyName":"AWS",
              "Resources:0/Id":"arn:aws:iam::111122223333:root",
              "aws/securityhub/FindingId":"arn:aws:securityhub:us-west-2::product/
aws/securityhub/arn:aws:securityhub:us-west-2:111122223333:subscription/cis-aws-
foundations-benchmark/v/1.2.0/1.12/finding/1dd8f2f8-cf1b-47c9-a875-8d7387fc9c23"
           },
           "Resources":[
              {
                 "Type":"AwsAccount",
                 "Id":"AWS::::Account:111122223333",
                 "Partition":"aws",
                 "Region":"us-west-2"
              }
           ],
           "Compliance":{
              "Status":"PASSED",
              "SecurityControlId":"IAM.4",
              "AssociatedStandards":[
                 {
                    "StandardsId":"ruleset/cis-aws-foundations-benchmark/v/1.2.0"
                 }
              ]
           },
           "WorkflowState":"NEW",
           "Workflow":{
              "Status":"RESOLVED"
           },
           "RecordState":"ACTIVE",
           "FindingProviderFields":{
              "Severity":{
                 "Label":"INFORMATIONAL",
                 "Original":"INFORMATIONAL"
              },
              "Types":[
                 "Software and Configuration Checks/Industry and Regulatory
 Standards/CIS AWS Foundations Benchmark"
              ]
           },
```

```
            "ProcessedAt":"2023-11-01T14:12:13.436Z"
         }
      ]
   }
}
```

Bukti untuk PCI.IAM.1 (PCI DSS)

```
{
  "version":"0",
  "id":"12345678-1q2w-3e4r-5t6y-123456789012",
  "detail-type":"Security Hub Findings - Imported",
  "source":"aws.securityhub",
  "account":"111122223333",
  "time":"2023-10-27T18:55:59Z",
  "region":"us-west-2",
  "resources":[
     "arn:aws:securityhub:us-west-2::product/aws/securityhub/arn:aws:securityhub:us-
west-2:111122223333:subscription/aws-foundational-security-best-practices/v/1.0.0/
Lambda.1/finding/1dd8f2f8-cf1b-47c9-a875-8d7387fc9c23"
  ],
  "detail":{
     "findings":[
        {
           "SchemaVersion":"2018-10-08",
           "Id":"arn:aws:securityhub:us-west-2:111122223333:subscription/pci-dss/
v/3.2.1/PCI.IAM.1/finding/3c75f651-6e2e-44f4-8e22-297d5c2d0c8b",
           "ProductArn":"arn:aws:securityhub:us-west-2::product/aws/securityhub",
           "ProductName":"Security Hub",
           "CompanyName":"AWS",
           "Region":"us-west-2",
           "GeneratorId":"pci-dss/v/3.2.1/PCI.IAM.1",
           "AwsAccountId":"111122223333",
           "Types":[
              "Software and Configuration Checks/Industry and Regulatory Standards/
PCI-DSS"
           ],
           "FirstObservedAt":"2020-10-05T19:18:47.788Z",
           "LastObservedAt":"2023-11-01T14:12:02.413Z",
           "CreatedAt":"2020-10-05T19:18:47.788Z",
           "UpdatedAt":"2023-11-01T14:11:53.720Z",
           "Severity":{
              "Product":0,
```

```
            "Label":"INFORMATIONAL",
            "Normalized":0,
            "Original":"INFORMATIONAL"
         },
         "Title":"PCI.IAM.1 IAM root user access key should not exist",
         "Description":"This AWS control checks whether the root user access key
 is available.",
         "Remediation":{
            "Recommendation":{
               "Text":"For information on how to correct this issue, consult the
 AWS Security Hub controls documentation.",
               "Url":"https://docs.aws.amazon.com/console/securityhub/IAM.4/
remediation"
            }
         },
         "ProductFields":{
            "StandardsArn":"arn:aws:securityhub:::standards/pci-dss/v/3.2.1",
            "StandardsSubscriptionArn":"arn:aws:securityhub:us-
west-2:111122223333:subscription/pci-dss/v/3.2.1",
            "ControlId":"PCI.IAM.1",
            "RecommendationUrl":"https://docs.aws.amazon.com/console/securityhub/
IAM.4/remediation",
            "RelatedAWSResources:0/name":"securityhub-iam-root-access-key-
check-67cbb1c4",
            "RelatedAWSResources:0/type":"AWS::Config::ConfigRule",
            "StandardsControlArn":"arn:aws:securityhub:us-
west-2:111122223333:control/pci-dss/v/3.2.1/PCI.IAM.1",
            "aws/securityhub/ProductName":"Security Hub",
            "aws/securityhub/CompanyName":"AWS",
            "Resources:0/Id":"arn:aws:iam::111122223333:root",
            "aws/securityhub/FindingId":"arn:aws:securityhub:us-west-2::product/
aws/securityhub/arn:aws:securityhub:us-west-2:111122223333:subscription/pci-dss/
v/3.2.1/PCI.IAM.1/finding/3c75f651-6e2e-44f4-8e22-297d5c2d0c8b"
         },
         "Resources":[
            {
               "Type":"AwsAccount",
               "Id":"AWS::::Account:111122223333",
               "Partition":"aws",
               "Region":"us-west-2"
            }
         ],
         "Compliance":{
            "Status":"PASSED",
```

```
            "RelatedRequirements":[
               "PCI DSS 2.1",
               "PCI DSS 2.2",
               "PCI DSS 7.2.1"
            ],
            "SecurityControlId":"IAM.4",
            "AssociatedStandards":[
               {
                  "StandardsId":"standards/pci-dss/v/3.2.1"
               }
            ]
         },
         "WorkflowState":"NEW",
         "Workflow":{
            "Status":"RESOLVED"
         },
         "RecordState":"ACTIVE",
         "FindingProviderFields":{
            "Severity":{
               "Label":"INFORMATIONAL",
               "Original":"INFORMATIONAL"
            },
            "Types":[
               "Software and Configuration Checks/Industry and Regulatory
 Standards/PCI-DSS"
            ]
         },
         "ProcessedAt":"2023-11-01T14:12:05.950Z"
      }
   ]
  }
}
```


Kontrol Security Hub yang Didukung

Kontrol Security Hub berikut saat ini didukung oleh Audit Manager. Anda dapat menggunakan salah satu kata kunci ID kontrol khusus standar berikut saat menyiapkan sumber data untuk kontrol kustom.

Standar keamanan	Kata kunci yang didukung di Audit Manager (ID kontrol standar di Security Hub)	Dokumentasi kontrol terkait (ID kontrol keamanan yang sesuai di Security Hub)
CIS v1.2.0	1.2	IAM.5
CIS v1.2.0	1.3	IAM.8
CIS v1.2.0	1.4	IAM.3
CIS v1.2.0	1.5	IAM.11
CIS v1.2.0	1.6	IAM.12
CIS v1.2.0	1.7	IAM.13
CIS v1.2.0	1.8	IAM.14
CIS v1.2.0	1.9	IAM.15
CIS v1.2.0	1.10	IAM.16
CIS v1.2.0	1.11	IAM.17
CIS v1.2.0	1.12	IAM.4
CIS v1.2.0	1.13	IAM.9
CIS v1.2.0	1.14	IAM.6
CIS v1.2.0	1.16	IAM.2
CIS v1.2.0	1.20	IAM.18
CIS v1.2.0	1.22	IAM.1
CIS v1.2.0	2.1	CloudTrail.1

Standar keamanan	Kata kunci yang didukung di Audit Manager (ID kontrol standar di Security Hub)	Dokumentasi kontrol terkait (ID kontrol keamanan yang sesuai di Security Hub)
CIS v1.2.0	2.2	CloudTrail.4
CIS v1.2.0	2.3	CloudTrail.6
CIS v1.2.0	2.4	CloudTrail.5
CIS v1.2.0	2.5	Konfigurasi.1
CIS v1.2.0	2.6	CloudTrail.7
CIS v1.2.0	2.7	CloudTrail.2
CIS v1.2.0	2.8	KMS.4
CIS v1.2.0	2.9	EC2.6
CIS v1.2.0	3.1	CloudWatch.2
CIS v1.2.0	3.2	CloudWatch.3
CIS v1.2.0	3.3	CloudWatch.1
CIS v1.2.0	3.4	CloudWatch.4
CIS v1.2.0	3.5	CloudWatch.5
CIS v1.2.0	3.6	CloudWatch.6
CIS v1.2.0	3.7	CloudWatch.7
CIS v1.2.0	3.8	CloudWatch.8
CIS v1.2.0	3.9	CloudWatch.9

Standar keamanan	Kata kunci yang didukung di Audit Manager (ID kontrol standar di Security Hub)	Dokumentasi kontrol terkait (ID kontrol keamanan yang sesuai di Security Hub)
CIS v1.2.0	3.10	CloudWatch.10
CIS v1.2.0	3.11	CloudWatch.11
CIS v1.2.0	3.12	CloudWatch.12
CIS v1.2.0	3.13	CloudWatch.13
CIS v1.2.0	3.14	CloudWatch.14
CIS v1.2.0	4.1	EC2.13
CIS v1.2.0	4.2	EC2.14
CIS v1.2.0	4.3	EC2.2
PCI DSS	PCI. AutoScaling.1	AutoScaling.1
PCI DSS	PCI. CloudTrail.1	CloudTrail.1
PCI DSS	PCI. CloudTrail.2	CloudTrail.2
PCI DSS	PCI. CloudTrail.3	CloudTrail.3
PCI DSS	PCI. CloudTrail.4	CloudTrail.4

Standar keamanan	Kata kunci yang didukung di Audit Manager (ID kontrol standar di Security Hub)	Dokumentasi kontrol terkait (ID kontrol keamanan yang sesuai di Security Hub)
PCI DSS	PCI. CodeBuild .1	CodeBuild.1
PCI DSS	PCI. CodeBuild .2	CodeBuild.2
PCI DSS	PCI.config.1	Konfigurasi.1
PCI DSS	PCI.CW.1	CloudWatch.1
PCI DSS	PCI.DMS.1	DMS.1
PCI DSS	PCI.EC2.1	EC2.1
PCI DSS	PCI.EC2.2	EC2.2
PCI DSS	PCI.EC2.3	EC2.3
PCI DSS	PCI.EC2.4	EC2.12
PCI DSS	PCI.EC2.5	EC2.13
PCI DSS	PCI.EC2.6	EC2.6
PCI DSS	PCI.elbv2.1	ELB.1
PCI DSS	PCI.ES.1	ES.1
PCI DSS	PCI.ES.2	ES.2
PCI DSS	PCI. GuardDuty .1	GuardDuty.1

Standar keamanan	Kata kunci yang didukung di Audit Manager (ID kontrol standar di Security Hub)	Dokumentasi kontrol terkait (ID kontrol keamanan yang sesuai di Security Hub)
PCI DSS	PCI.IAM.1	IAM.1
PCI DSS	PCI.IAM.2	IAM.2
PCI DSS	PCI.IAM.3	IAM.3
PCI DSS	PCI.IAM.4	IAM.4
PCI DSS	PCI.IAM.5	IAM.9
PCI DSS	PCI.IAM.6	IAM.6
PCI DSS	PCI.IAM.7	PCI.IAM.7
PCI DSS	PCI.IAM.8	PCI.IAM8.
PCI DSS	PCI.KMS.1	PCI.KMS.4
PCI DSS	PCI.Lambda.1	Lambda.1
PCI DSS	PCI.Lambda.2	Lambda.3
PCI DSS	PCI.openSearch.1	Opensearch.1
PCI DSS	PCI.openSearch.2	Opensearch.2
PCI DSS	PCI.RDS.1	RDS.1
PCI DSS	PCI.RDS.2	RDS.2
PCI DSS	PCI.redshift.1	Pergeseran merah.1

Standar keamanan	Kata kunci yang didukung di Audit Manager (ID kontrol standar di Security Hub)	Dokumentasi kontrol terkait (ID kontrol keamanan yang sesuai di Security Hub)
PCI DSS	PCI.S3.1	S3.1
PCI DSS	PCI.S3.2	S3.2
PCI DSS	PCI.S3.3	S3.3
PCI DSS	PCI.S3.4	S3.4
PCI DSS	PCI.S3.5	S3.5
PCI DSS	PCI.S3.6	S3.1
PCI DSS	PCI. SageMaker .1	SageMaker.1
PCI DSS	PCI.SSM.1	SSM.1
PCI DSS	PCI.SSM.2	SSM.2
PCI DSS	PCI.SSM.3	SSM.3
AWS Praktik Terbaik Keamanan Dasar	Akun.1	Akun.1
AWS Praktik Terbaik Keamanan Dasar	Akun.2	Akun.2
AWS Praktik Terbaik Keamanan Dasar	ACM.1	ACM.1
AWS Praktik Terbaik Keamanan Dasar	ACM.2	ACM.2
AWS Praktik Terbaik Keamanan Dasar	ApiGateway.1	ApiGateway.1
AWS Praktik Terbaik Keamanan Dasar	ApiGateway.2	ApiGateway.2

Standar keamanan	Kata kunci yang didukung di Audit Manager (ID kontrol standar di Security Hub)	Dokumentasi kontrol terkait (ID kontrol keamanan yang sesuai di Security Hub)
AWS Praktik Terbaik Keamanan Dasar	ApiGateway.3	ApiGateway.3
AWS Praktik Terbaik Keamanan Dasar	ApiGateway.4	ApiGateway.4
AWS Praktik Terbaik Keamanan Dasar	ApiGateway.5	ApiGateway.5
AWS Praktik Terbaik Keamanan Dasar	ApiGateway.8	ApiGateway.8
AWS Praktik Terbaik Keamanan Dasar	ApiGateway.9	ApiGateway.9
AWS Praktik Terbaik Keamanan Dasar	AppSync.2	AppSync.2
AWS Praktik Terbaik Keamanan Dasar	AppSync.5	AppSync.5
AWS Praktik Terbaik Keamanan Dasar	Athena.1	Athena.1
AWS Praktik Terbaik Keamanan Dasar	AutoScaling.1	AutoScaling.1
AWS Praktik Terbaik Keamanan Dasar	AutoScaling.2	AutoScaling.2
AWS Praktik Terbaik Keamanan Dasar	AutoScaling.3	AutoScaling.3
AWS Praktik Terbaik Keamanan Dasar	AutoScaling.4	AutoScaling.4
AWS Praktik Terbaik Keamanan Dasar	Penskalaan otomatis.5	Penskalaan otomatis.5
AWS Praktik Terbaik Keamanan Dasar	AutoScaling.6	AutoScaling.6
AWS Praktik Terbaik Keamanan Dasar	AutoScaling.9	AutoScaling.9
AWS Praktik Terbaik Keamanan Dasar	Cadangan.1	Backup.1

Standar keamanan	Kata kunci yang didukung di Audit Manager (ID kontrol standar di Security Hub)	Dokumentasi kontrol terkait (ID kontrol keamanan yang sesuai di Security Hub)
AWS Praktik Terbaik Keamanan Dasar	CloudFormation.1	CloudFormation.1
AWS Praktik Terbaik Keamanan Dasar	CloudFront.1	CloudFront.1
AWS Praktik Terbaik Keamanan Dasar	CloudFront.2	CloudFront.2
AWS Praktik Terbaik Keamanan Dasar	CloudFront.3	CloudFront.3
AWS Praktik Terbaik Keamanan Dasar	CloudFront.4	CloudFront.4
AWS Praktik Terbaik Keamanan Dasar	CloudFront.5	CloudFront.5
AWS Praktik Terbaik Keamanan Dasar	CloudFront.6	CloudFront.6
AWS Praktik Terbaik Keamanan Dasar	CloudFront.7	CloudFront.7
AWS Praktik Terbaik Keamanan Dasar	CloudFront.8	CloudFront.8
AWS Praktik Terbaik Keamanan Dasar	CloudFront.9	CloudFront.9
AWS Praktik Terbaik Keamanan Dasar	CloudFront.10	CloudFront.10
AWS Praktik Terbaik Keamanan Dasar	CloudFront.12	CloudFront.12
AWS Praktik Terbaik Keamanan Dasar	CloudFront.13	CloudFront.13
AWS Praktik Terbaik Keamanan Dasar	CloudTrail.1	CloudTrail.1
AWS Praktik Terbaik Keamanan Dasar	CloudTrail.2	CloudTrail.2
AWS Praktik Terbaik Keamanan Dasar	CloudTrail.3	CloudTrail.3

Standar keamanan	Kata kunci yang didukung di Audit Manager (ID kontrol standar di Security Hub)	Dokumentasi kontrol terkait (ID kontrol keamanan yang sesuai di Security Hub)
AWS Praktik Terbaik Keamanan Dasar	CloudTrail.4	CloudTrail.4
AWS Praktik Terbaik Keamanan Dasar	CloudTrail.5	CloudTrail.5
AWS Praktik Terbaik Keamanan Dasar	CloudTrail.6	CloudTrail.6
AWS Praktik Terbaik Keamanan Dasar	CloudTrail.7	CloudTrail.7
AWS Praktik Terbaik Keamanan Dasar	CloudWatch.1	CloudWatch.1
AWS Praktik Terbaik Keamanan Dasar	CloudWatch.2	CloudWatch.2
AWS Praktik Terbaik Keamanan Dasar	CloudWatch.3	CloudWatch.3
AWS Praktik Terbaik Keamanan Dasar	CloudWatch.4	CloudWatch.4
AWS Praktik Terbaik Keamanan Dasar	CloudWatch.5	CloudWatch.5
AWS Praktik Terbaik Keamanan Dasar	CloudWatch.6	CloudWatch.6
AWS Praktik Terbaik Keamanan Dasar	CloudWatch.7	CloudWatch.7
AWS Praktik Terbaik Keamanan Dasar	CloudWatch.8	CloudWatch.8
AWS Praktik Terbaik Keamanan Dasar	CloudWatch.9	CloudWatch.9
AWS Praktik Terbaik Keamanan Dasar	CloudWatch.10	CloudWatch.10
AWS Praktik Terbaik Keamanan Dasar	CloudWatch.11	CloudWatch.11
AWS Praktik Terbaik Keamanan Dasar	CloudWatch.12	CloudWatch.12
AWS Praktik Terbaik Keamanan Dasar	CloudWatch.13	CloudWatch.13

Standar keamanan	Kata kunci yang didukung di Audit Manager (ID kontrol standar di Security Hub)	Dokumentasi kontrol terkait (ID kontrol keamanan yang sesuai di Security Hub)
AWS Praktik Terbaik Keamanan Dasar	CloudWatch.14	CloudWatch.14
AWS Praktik Terbaik Keamanan Dasar	CloudWatch.15	CloudWatch.15
AWS Praktik Terbaik Keamanan Dasar	CloudWatch.16	CloudWatch.16
AWS Praktik Terbaik Keamanan Dasar	CloudWatch.17	CloudWatch.17
AWS Praktik Terbaik Keamanan Dasar	CodeBuild.1	CodeBuild.1
AWS Praktik Terbaik Keamanan Dasar	CodeBuild.2	CodeBuild.2
AWS Praktik Terbaik Keamanan Dasar	CodeBuild.3	CodeBuild.3
AWS Praktik Terbaik Keamanan Dasar	CodeBuild.4	CodeBuild.4
AWS Praktik Terbaik Keamanan Dasar	CodeBuild.5	CodeBuild.5
AWS Praktik Terbaik Keamanan Dasar	Konfigurasi.1	Konfigurasi.1
AWS Praktik Terbaik Keamanan Dasar	DMS.1	DMS.1
AWS Praktik Terbaik Keamanan Dasar	DMS.6	DMS.6
AWS Praktik Terbaik Keamanan Dasar	DMS.7	DMS.7
AWS Praktik Terbaik Keamanan Dasar	DMS.8	DMS.8
AWS Praktik Terbaik Keamanan Dasar	DMS.9	DMS.9
AWS Praktik Terbaik Keamanan Dasar	DokumenDB.1	DokumenDB.1
AWS Praktik Terbaik Keamanan Dasar	DokumenDB.2	DokumenDB.2

Standar keamanan	Kata kunci yang didukung di Audit Manager (ID kontrol standar di Security Hub)	Dokumentasi kontrol terkait (ID kontrol keamanan yang sesuai di Security Hub)
AWS Praktik Terbaik Keamanan Dasar	DokumenDB.3	DokumenDB.3
AWS Praktik Terbaik Keamanan Dasar	DokumenDB.4	DokumenDB.4
AWS Praktik Terbaik Keamanan Dasar	DokumenDB.5	DokumenDB.5
AWS Praktik Terbaik Keamanan Dasar	DynamoDB.1	DynamoDB.1
AWS Praktik Terbaik Keamanan Dasar	DynamoDB.2	DynamoDB.2
AWS Praktik Terbaik Keamanan Dasar	DynamoDB.3	DynamoDB.3
AWS Praktik Terbaik Keamanan Dasar	DynamoDB.4	DynamoDB.4
AWS Praktik Terbaik Keamanan Dasar	DynamoDb.6	DynamoDb.6
AWS Praktik Terbaik Keamanan Dasar	EC2.1	EC2.1
AWS Praktik Terbaik Keamanan Dasar	EC2.2	EC2.2
AWS Praktik Terbaik Keamanan Dasar	EC2.3	EC2.3
AWS Praktik Terbaik Keamanan Dasar	EC2.4	EC2.4
AWS Praktik Terbaik Keamanan Dasar	EC2.6	EC2.6
AWS Praktik Terbaik Keamanan Dasar	EC2.7	EC2.7
AWS Praktik Terbaik Keamanan Dasar	EC2.8	EC2.8
AWS Praktik Terbaik Keamanan Dasar	EC2.9	EC2.9
AWS Praktik Terbaik Keamanan Dasar	EC2.10	EC2.10

Standar keamanan	Kata kunci yang didukung di Audit Manager (ID kontrol standar di Security Hub)	Dokumentasi kontrol terkait (ID kontrol keamanan yang sesuai di Security Hub)
AWS Praktik Terbaik Keamanan Dasar	EC2.12	EC2.12
AWS Praktik Terbaik Keamanan Dasar	EC2.13	EC2.13
AWS Praktik Terbaik Keamanan Dasar	EC2.14	EC2.14
AWS Praktik Terbaik Keamanan Dasar	EC2.15	EC2.15
AWS Praktik Terbaik Keamanan Dasar	EC2.16	EC2.16
AWS Praktik Terbaik Keamanan Dasar	EC2.17	EC2.17
AWS Praktik Terbaik Keamanan Dasar	EC2.18	EC2.18
AWS Praktik Terbaik Keamanan Dasar	EC2.19	EC2.19
AWS Praktik Terbaik Keamanan Dasar	EC2.20	EC2.20
AWS Praktik Terbaik Keamanan Dasar	EC2.21	EC2.21
AWS Praktik Terbaik Keamanan Dasar	EC2.22	EC2.22
AWS Praktik Terbaik Keamanan Dasar	EC2.23	EC2.23
AWS Praktik Terbaik Keamanan Dasar	EC2.24	EC2.24
AWS Praktik Terbaik Keamanan Dasar	EC2.25	EC2.25
AWS Praktik Terbaik Keamanan Dasar	EC2.28	EC2.28
AWS Praktik Terbaik Keamanan Dasar	EC2.51	EC2.51
AWS Praktik Terbaik Keamanan Dasar	ECR.1	ECR.1

Standar keamanan	Kata kunci yang didukung di Audit Manager (ID kontrol standar di Security Hub)	Dokumentasi kontrol terkait (ID kontrol keamanan yang sesuai di Security Hub)
AWS Praktik Terbaik Keamanan Dasar	ECR.2	ECR.2
AWS Praktik Terbaik Keamanan Dasar	ECR.3	ECR.3
AWS Praktik Terbaik Keamanan Dasar	ECS.1	ECS.1
AWS Praktik Terbaik Keamanan Dasar	ECS.2	ECS.2
AWS Praktik Terbaik Keamanan Dasar	ECS.3	ECS.3
AWS Praktik Terbaik Keamanan Dasar	ECS.4	ECS.4
AWS Praktik Terbaik Keamanan Dasar	DLS.5	ECS.5
AWS Praktik Terbaik Keamanan Dasar	ECS.8	ECS.8
AWS Praktik Terbaik Keamanan Dasar	ECS.9	ECS.9
AWS Praktik Terbaik Keamanan Dasar	ECS.10	ECS.10
AWS Praktik Terbaik Keamanan Dasar	ECS.12	ECS.12
AWS Praktik Terbaik Keamanan Dasar	EFS.1	EFS.1
AWS Praktik Terbaik Keamanan Dasar	EFS.2	EFS.2
AWS Praktik Terbaik Keamanan Dasar	EFS.3	EFS.3
AWS Praktik Terbaik Keamanan Dasar	EFS.4	EFS.4
AWS Praktik Terbaik Keamanan Dasar	EKS.1	EKS.1
AWS Praktik Terbaik Keamanan Dasar	EKS.2	EKS.2

Standar keamanan	Kata kunci yang didukung di Audit Manager (ID kontrol standar di Security Hub)	Dokumentasi kontrol terkait (ID kontrol keamanan yang sesuai di Security Hub)
AWS Praktik Terbaik Keamanan Dasar	EKS.8	EKS.8
AWS Praktik Terbaik Keamanan Dasar	ElastiCache.1	ElastiCache.1
AWS Praktik Terbaik Keamanan Dasar	ElastiCache.2	ElastiCache.2
AWS Praktik Terbaik Keamanan Dasar	ElastiCache.3	ElastiCache.3
AWS Praktik Terbaik Keamanan Dasar	ElastiCache.4	ElastiCache.4
AWS Praktik Terbaik Keamanan Dasar	ElastiCache.5	ElastiCache.5
AWS Praktik Terbaik Keamanan Dasar	ElastiCache.6	ElastiCache.6
AWS Praktik Terbaik Keamanan Dasar	ElastiCache.7	ElastiCache.7
AWS Praktik Terbaik Keamanan Dasar	ElasticBeanstalk.1	ElasticBeanstalk.1
AWS Praktik Terbaik Keamanan Dasar	ElasticBeanstalk.2	ElasticBeanstalk.2
AWS Praktik Terbaik Keamanan Dasar	ElasticBeanstalk.3	ElasticBeanstalk.3
AWS Praktik Terbaik Keamanan Dasar	ELB.1	ELB.1
AWS Praktik Terbaik Keamanan Dasar	ELB.2	ELB.2
AWS Praktik Terbaik Keamanan Dasar	ELB.3	ELB.3
AWS Praktik Terbaik Keamanan Dasar	ELB.4	ELB.4

Standar keamanan	Kata kunci yang didukung di Audit Manager (ID kontrol standar di Security Hub)	Dokumentasi kontrol terkait (ID kontrol keamanan yang sesuai di Security Hub)
AWS Praktik Terbaik Keamanan Dasar	ELB.5	ELB.5
AWS Praktik Terbaik Keamanan Dasar	ELB.6	ELB.6
AWS Praktik Terbaik Keamanan Dasar	ELB.7	ELB.7
AWS Praktik Terbaik Keamanan Dasar	ELB.8	ELB.8
AWS Praktik Terbaik Keamanan Dasar	ELB.9	ELB.9
AWS Praktik Terbaik Keamanan Dasar	ELB.10	ELB.10
AWS Praktik Terbaik Keamanan Dasar	ELB.12	ELB.12
AWS Praktik Terbaik Keamanan Dasar	ELB.13	ELB.13
AWS Praktik Terbaik Keamanan Dasar	ELB.14	ELB.14
AWS Praktik Terbaik Keamanan Dasar	ELB.16	ELB.16
AWS Praktik Terbaik Keamanan Dasar	ELBV2.1	ELB.1
AWS Praktik Terbaik Keamanan Dasar	EMR.1	EMR.1
AWS Praktik Terbaik Keamanan Dasar	EMR.2	EMR.2
AWS Praktik Terbaik Keamanan Dasar	ES.1	ES.1
AWS Praktik Terbaik Keamanan Dasar	ES.2	ES.2
AWS Praktik Terbaik Keamanan Dasar	ES.3	ES.3
AWS Praktik Terbaik Keamanan Dasar	ES.4	ES.4

Standar keamanan	Kata kunci yang didukung di Audit Manager (ID kontrol standar di Security Hub)	Dokumentasi kontrol terkait (ID kontrol keamanan yang sesuai di Security Hub)
AWS Praktik Terbaik Keamanan Dasar	ES.5	ES.5
AWS Praktik Terbaik Keamanan Dasar	ES.6	ES.6
AWS Praktik Terbaik Keamanan Dasar	ES.7	ES.7
AWS Praktik Terbaik Keamanan Dasar	ES.8	ES.8
AWS Praktik Terbaik Keamanan Dasar	EventBridge.3	EventBridge3.
AWS Praktik Terbaik Keamanan Dasar	EventBridge.4	EventBridge.4
AWS Praktik Terbaik Keamanan Dasar	FSX.1	FSX.1
AWS Praktik Terbaik Keamanan Dasar	GuardDuty.1	GuardDuty.1
AWS Praktik Terbaik Keamanan Dasar	IAM.1	IAM.1
AWS Praktik Terbaik Keamanan Dasar	IAM.2	IAM.2
AWS Praktik Terbaik Keamanan Dasar	IAM.3	IAM.3
AWS Praktik Terbaik Keamanan Dasar	IAM.4	IAM.4
AWS Praktik Terbaik Keamanan Dasar	IAM.5	IAM.5
AWS Praktik Terbaik Keamanan Dasar	IAM.6	IAM.6
AWS Praktik Terbaik Keamanan Dasar	IAM.7	IAM.7
AWS Praktik Terbaik Keamanan Dasar	IAM.8	IAM.8
AWS Praktik Terbaik Keamanan Dasar	IAM.9	IAM.9

Standar keamanan	Kata kunci yang didukung di Audit Manager (ID kontrol standar di Security Hub)	Dokumentasi kontrol terkait (ID kontrol keamanan yang sesuai di Security Hub)
AWS Praktik Terbaik Keamanan Dasar	IAM.10	IAM.10
AWS Praktik Terbaik Keamanan Dasar	IAM.11	IAM.11
AWS Praktik Terbaik Keamanan Dasar	IAM.12	IAM.12
AWS Praktik Terbaik Keamanan Dasar	IAM.13	IAM.13
AWS Praktik Terbaik Keamanan Dasar	IAM.14	IAM.14
AWS Praktik Terbaik Keamanan Dasar	IAM.15	IAM.15
AWS Praktik Terbaik Keamanan Dasar	IAM.16	IAM.16
AWS Praktik Terbaik Keamanan Dasar	IAM.17	IAM.17
AWS Praktik Terbaik Keamanan Dasar	IAM.18	IAM.18
AWS Praktik Terbaik Keamanan Dasar	IAM.19	IAM.19
AWS Praktik Terbaik Keamanan Dasar	IAM.21	IAM.21
AWS Praktik Terbaik Keamanan Dasar	IAM.22	IAM.22
AWS Praktik Terbaik Keamanan Dasar	Kinesis.1	Kinesis.1
AWS Praktik Terbaik Keamanan Dasar	KMS.1	KMS.1
AWS Praktik Terbaik Keamanan Dasar	KMS.2	KMS.2
AWS Praktik Terbaik Keamanan Dasar	KMS.3	KMS.3
AWS Praktik Terbaik Keamanan Dasar	KMS.4	KMS.4

Standar keamanan	Kata kunci yang didukung di Audit Manager (ID kontrol standar di Security Hub)	Dokumentasi kontrol terkait (ID kontrol keamanan yang sesuai di Security Hub)
AWS Praktik Terbaik Keamanan Dasar	Lambda.1	Lambda.1
AWS Praktik Terbaik Keamanan Dasar	Lambda.2	Lambda.2
AWS Praktik Terbaik Keamanan Dasar	Lambda.3	Lambda.3
AWS Praktik Terbaik Keamanan Dasar	Lambda.5	Lambda.5
AWS Praktik Terbaik Keamanan Dasar	Macie.1	Macie.1
AWS Praktik Terbaik Keamanan Dasar	MQ.5	MQ.5
AWS Praktik Terbaik Keamanan Dasar	MQ.6	MQ.6
AWS Praktik Terbaik Keamanan Dasar	MSK.1	MSK.1
AWS Praktik Terbaik Keamanan Dasar	MSK.2	MSK.2
AWS Praktik Terbaik Keamanan Dasar	Neptunus.1	Neptunus.1
AWS Praktik Terbaik Keamanan Dasar	Neptunus.2	Neptunus.2
AWS Praktik Terbaik Keamanan Dasar	Neptunus.3	Neptunus.3
AWS Praktik Terbaik Keamanan Dasar	Neptunus.4	Neptunus.4
AWS Praktik Terbaik Keamanan Dasar	Neptunus.5	Neptunus.5
AWS Praktik Terbaik Keamanan Dasar	Neptunus.6	Neptunus.6
AWS Praktik Terbaik Keamanan Dasar	Neptunus.7	Neptunus.7
AWS Praktik Terbaik Keamanan Dasar	Neptunus.8	Neptunus.8

Standar keamanan	Kata kunci yang didukung di Audit Manager (ID kontrol standar di Security Hub)	Dokumentasi kontrol terkait (ID kontrol keamanan yang sesuai di Security Hub)
AWS Praktik Terbaik Keamanan Dasar	Neptunus.9	Neptunus.9
AWS Praktik Terbaik Keamanan Dasar	NetworkFirewall.1	NetworkFirewall.1
AWS Praktik Terbaik Keamanan Dasar	NetworkFirewall.2	NetworkFirewall.2
AWS Praktik Terbaik Keamanan Dasar	NetworkFirewall.3	NetworkFirewall.3
AWS Praktik Terbaik Keamanan Dasar	NetworkFirewall.4	NetworkFirewall.4
AWS Praktik Terbaik Keamanan Dasar	NetworkFirewall.5	NetworkFirewall.5
AWS Praktik Terbaik Keamanan Dasar	NetworkFirewall.6	NetworkFirewall.6
AWS Praktik Terbaik Keamanan Dasar	NetworkFirewall.9	NetworkFirewall.9
AWS Praktik Terbaik Keamanan Dasar	Opensearch.1	Opensearch.1
AWS Praktik Terbaik Keamanan Dasar	Opensearch.2	Opensearch.2
AWS Praktik Terbaik Keamanan Dasar	Opensearch.3	Opensearch.3
AWS Praktik Terbaik Keamanan Dasar	Opensearch.4	Opensearch.4
AWS Praktik Terbaik Keamanan Dasar	Opensearch.5	Opensearch.5

Standar keamanan	Kata kunci yang didukung di Audit Manager (ID kontrol standar di Security Hub)	Dokumentasi kontrol terkait (ID kontrol keamanan yang sesuai di Security Hub)
AWS Praktik Terbaik Keamanan Dasar	Opensearch.6	Opensearch.6
AWS Praktik Terbaik Keamanan Dasar	Opensearch.7	Opensearch.7
AWS Praktik Terbaik Keamanan Dasar	Opensearch.8	Opensearch.8
AWS Praktik Terbaik Keamanan Dasar	Opensearch.10	Opensearch.10
AWS Praktik Terbaik Keamanan Dasar	PCA.1	PCA.1
AWS Praktik Terbaik Keamanan Dasar	RDS.1	RDS.1
AWS Praktik Terbaik Keamanan Dasar	RDS.2	RDS.2
AWS Praktik Terbaik Keamanan Dasar	RDS.3	RDS.3
AWS Praktik Terbaik Keamanan Dasar	RDS.4	RDS.4
AWS Praktik Terbaik Keamanan Dasar	RDS.5	RDS.5
AWS Praktik Terbaik Keamanan Dasar	RDS.6	RDS.6
AWS Praktik Terbaik Keamanan Dasar	RDS.7	RDS.7
AWS Praktik Terbaik Keamanan Dasar	RDS.8	RDS.8
AWS Praktik Terbaik Keamanan Dasar	RDS.9	RDS.9
AWS Praktik Terbaik Keamanan Dasar	RDS.10	RDS.10
AWS Praktik Terbaik Keamanan Dasar	RDS.11	RDS.11
AWS Praktik Terbaik Keamanan Dasar	RDS.12	RDS.12

Standar keamanan	Kata kunci yang didukung di Audit Manager (ID kontrol standar di Security Hub)	Dokumentasi kontrol terkait (ID kontrol keamanan yang sesuai di Security Hub)
AWS Praktik Terbaik Keamanan Dasar	RDS.13	RDS.13
AWS Praktik Terbaik Keamanan Dasar	RDS.14	RDS.14
AWS Praktik Terbaik Keamanan Dasar	RDS.15	RDS.15
AWS Praktik Terbaik Keamanan Dasar	RDS.16	RDS.16
AWS Praktik Terbaik Keamanan Dasar	RDS.17	RDS.17
AWS Praktik Terbaik Keamanan Dasar	RDS.18	RDS.18
AWS Praktik Terbaik Keamanan Dasar	RDS.19	RDS.19
AWS Praktik Terbaik Keamanan Dasar	RDS.20	RDS.20
AWS Praktik Terbaik Keamanan Dasar	RDS.21	RDS.21
AWS Praktik Terbaik Keamanan Dasar	RDS.22	RDS.22
AWS Praktik Terbaik Keamanan Dasar	RDS.23	RDS.23
AWS Praktik Terbaik Keamanan Dasar	RDS.24	RDS.24
AWS Praktik Terbaik Keamanan Dasar	RDS.25	RDS.25
AWS Praktik Terbaik Keamanan Dasar	RDS.26	RDS.26
AWS Praktik Terbaik Keamanan Dasar	RDS.27	RDS.27
AWS Praktik Terbaik Keamanan Dasar	RDS.34	RDS.34
AWS Praktik Terbaik Keamanan Dasar	RDS.35	RDS.35

Standar keamanan	Kata kunci yang didukung di Audit Manager (ID kontrol standar di Security Hub)	Dokumentasi kontrol terkait (ID kontrol keamanan yang sesuai di Security Hub)
AWS Praktik Terbaik Keamanan Dasar	Pergeseran merah.1	Pergeseran merah.1
AWS Praktik Terbaik Keamanan Dasar	Pergeseran merah.2	Pergeseran merah.2
AWS Praktik Terbaik Keamanan Dasar	Pergeseran merah.3	Pergeseran merah.3
AWS Praktik Terbaik Keamanan Dasar	Pergeseran merah.4	Pergeseran merah.4
AWS Praktik Terbaik Keamanan Dasar	Pergeseran Merah.6	Pergeseran Merah.6
AWS Praktik Terbaik Keamanan Dasar	Pergeseran Merah.7	Pergeseran Merah.7
AWS Praktik Terbaik Keamanan Dasar	Pergeseran Merah.8	Pergeseran Merah.8
AWS Praktik Terbaik Keamanan Dasar	Pergeseran Merah.9	Pergeseran Merah.9
AWS Praktik Terbaik Keamanan Dasar	Pergeseran Merah.10	Pergeseran Merah.10
AWS Praktik Terbaik Keamanan Dasar	Route53.2	Route53.2
AWS Praktik Terbaik Keamanan Dasar	S3.1	S3.1
AWS Praktik Terbaik Keamanan Dasar	S3.2	S3.2

Standar keamanan	Kata kunci yang didukung di Audit Manager (ID kontrol standar di Security Hub)	Dokumentasi kontrol terkait (ID kontrol keamanan yang sesuai di Security Hub)
AWS Praktik Terbaik Keamanan Dasar	S3.3	S3.3
AWS Praktik Terbaik Keamanan Dasar	S3.4	S3.4
AWS Praktik Terbaik Keamanan Dasar	S3.5	S3.5
AWS Praktik Terbaik Keamanan Dasar	S3.6	S3.6
AWS Praktik Terbaik Keamanan Dasar	S3.7	S3.7
AWS Praktik Terbaik Keamanan Dasar	S3.8	S3.8
AWS Praktik Terbaik Keamanan Dasar	S3.9	S3.9
AWS Praktik Terbaik Keamanan Dasar	S3.11	S3.11
AWS Praktik Terbaik Keamanan Dasar	S3.12	S3.12
AWS Praktik Terbaik Keamanan Dasar	S3.13	S3.13
AWS Praktik Terbaik Keamanan Dasar	S3.14	S3.14
AWS Praktik Terbaik Keamanan Dasar	S3.15	S3.15
AWS Praktik Terbaik Keamanan Dasar	S3.17	S3.17
AWS Praktik Terbaik Keamanan Dasar	S3.19	S3.19
AWS Praktik Terbaik Keamanan Dasar	S3.19	S3.20
AWS Praktik Terbaik Keamanan Dasar	SageMaker.1	SageMaker.1
AWS Praktik Terbaik Keamanan Dasar	SageMaker.2	SageMaker.2

Standar keamanan	Kata kunci yang didukung di Audit Manager (ID kontrol standar di Security Hub)	Dokumentasi kontrol terkait (ID kontrol keamanan yang sesuai di Security Hub)
AWS Praktik Terbaik Keamanan Dasar	SageMaker.3	SageMaker.3
AWS Praktik Terbaik Keamanan Dasar	SecretsManager.1	SecretsManager.1
AWS Praktik Terbaik Keamanan Dasar	SecretsManager.2	SecretsManager.2
AWS Praktik Terbaik Keamanan Dasar	SecretsManager.3	SecretsManager.3
AWS Praktik Terbaik Keamanan Dasar	SecretsManager.4	SecretsManager.4
AWS Praktik Terbaik Keamanan Dasar	SNS.1	SNS.1
AWS Praktik Terbaik Keamanan Dasar	SNS.2	SNS.2
AWS Praktik Terbaik Keamanan Dasar	SQS.1	SQS.1
AWS Praktik Terbaik Keamanan Dasar	SSM.1	SSM.1
AWS Praktik Terbaik Keamanan Dasar	SSM.2	SSM.2
AWS Praktik Terbaik Keamanan Dasar	SSM.3	SSM.3
AWS Praktik Terbaik Keamanan Dasar	SSM.4	SSM.4
AWS Praktik Terbaik Keamanan Dasar	StepFunctions.1	StepFunctions.1
AWS Praktik Terbaik Keamanan Dasar	WAF.1	WAF.1
AWS Praktik Terbaik Keamanan Dasar	WAF.2	WAF.2

Standar keamanan	Kata kunci yang didukung di Audit Manager (ID kontrol standar di Security Hub)	Dokumentasi kontrol terkait (ID kontrol keamanan yang sesuai di Security Hub)
AWS Praktik Terbaik Keamanan Dasar	WAF.3	WAF.3
AWS Praktik Terbaik Keamanan Dasar	WAF.4	WAF.4
AWS Praktik Terbaik Keamanan Dasar	WAF.6	WAF.6
AWS Praktik Terbaik Keamanan Dasar	WAF.7	WAF.7
AWS Praktik Terbaik Keamanan Dasar	WAF.8	WAF.8
AWS Praktik Terbaik Keamanan Dasar	WAF.10	WAF.10
AWS Praktik Terbaik Keamanan Dasar	WAF.11	WAF.11
AWS Praktik Terbaik Keamanan Dasar	WAF.12	WAF.12

Panggilan API didukung oleh AWS Audit Manager

Audit Manager membuat panggilan API Layanan AWS untuk mengumpulkan snapshot detail konfigurasi untuk AWS sumber daya Anda. Anda dapat menentukan panggilan API ini sebagai pemetaan sumber data saat mengonfigurasi kontrol kustom di Audit Manager.

Untuk setiap sumber daya yang berada dalam lingkup panggilan API, Audit Manager menangkap snapshot konfigurasi dan mengubahnya menjadi bukti. Ini menghasilkan satu bukti per sumber daya, sebagai lawan dari satu bukti per panggilan API.

Misalnya, jika panggilan `ec2_DescribeRouteTables` API menangkap snapshot konfigurasi dari lima tabel rute, Anda akan mendapatkan total lima bukti untuk satu panggilan API. Setiap bukti adalah snapshot dari konfigurasi tabel rute individu.

Di halaman ini

- Panggilan API yang didukung untuk sumber data kontrol kustom
- Panggilan API berpaginasi
- Panggilan API yang digunakan dalam kerangka kerja AWS License Manager standar

Panggilan API yang didukung untuk sumber data kontrol kustom

Dalam kontrol kustom, Anda dapat menggunakan salah satu panggilan API berikut sebagai sumber data. Audit Manager kemudian dapat menggunakan panggilan API ini untuk mengumpulkan bukti tentang AWS penggunaan Anda.

Panggilan API yang didukung	Bagaimana Audit Manager menggunakan API ini untuk mengumpulkan bukti
acm_ GetAccountConfiguration	Kumpulkan snapshot dari opsi konfigurasi akun yang terkait dengan Anda Akun AWS.
acm_ ListCertificates	Ambil daftar ARN sertifikat dan nama domain.
cloudtrail_ DescribeTrails	Kumpulkan snapshot pengaturan untuk satu atau beberapa jalur yang terkait dengan Wilayah saat ini untuk Anda. Akun AWS
cloudwatch_ DescribeAlarms	Kumpulkan snapshot konfigurasi alarm yang digunakan untuk Anda. Akun AWS
config_ DescribeConfigRules	Ambil detail tentang AWS Config aturan Anda.
config_ DescribeDeliveryChannels	Kumpulkan snapshot konfigurasi untuk saluran pengiriman di dalam Anda Akun AWS.
directconnect_ DescribeDirectConnectGateways	Ambil daftar semua AWS Direct Connect gateway Anda.
directconnect_ DescribeVirtualGateways	Ambil daftar gateway pribadi virtual yang dimiliki oleh Anda. Akun AWS
docdb_ DescribeCertificates	Kumpulkan daftar sertifikat untuk Anda Akun AWS.
docdb_deskripsidB ClusterParameterGroups	Kumpulkan daftar `DBClusterParameterGroup` deskripsi untuk Anda Akun AWS.

Panggilan API yang didukung	Bagaimana Audit Manager menggunakan API ini untuk mengumpulkan bukti
docdb_describedBinstances	Kumpulkan informasi tentang instans Amazon DynamoDB yang disediakan untuk Anda. Akun AWS
dinamodb_ DescribeTable	Kumpulkan snapshot konfigurasi untuk tabel DynamoDB di tabel Anda. Akun AWS Saat Anda menggunakan API ini sebagai sumber data, Anda tidak perlu memberikan nama tabel DynamoDB tertentu. Sebagai gantinya, Audit Manager menggunakan `ListTables` operasi untuk mencantumkan semua tabel Anda. Untuk setiap tabel yang terdaftar, Audit Manager kemudian melakukan `DescribeTable` operasi untuk menghasilkan bukti untuk sumber daya tersebut.
dinamodb_ ListBackups	Ambil daftar cadangan DynamoDB yang terkait dengan Anda. Akun AWS
dinamodb_ ListGlobalTables	Ambil daftar semua tabel global yang saat ini ada di Anda Akun AWS.
dinamodb_ ListTables	Ambil daftar semua nama tabel yang terkait dengan titik akhir Anda Akun AWS dan Anda saat ini.
ec2_ DescribeAddresses	Kumpulkan snapshot alamat IP Elastis Anda.
ec2_ DescribeCustomerGateways	Kumpulkan snapshot gateway pelanggan VPN Anda.
ec2_ DescribeEgressOnlyInternetGateways	Kumpulkan snapshot dari gateway internet khusus egress-Anda.
ec2_ DescribeFlowLogs	Kumpulkan snapshot dari flow log Anda.
ec2_ DescribeInstances	Kumpulkan snapshot dari instans Anda.

Panggilan API yang didukung	Bagaimana Audit Manager menggunakan API ini untuk mengumpulkan bukti
ec2_ DescribeInternetGateways	Kumpulkan snapshot gateway internet Anda.
ec2_ DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations	Kumpulkan deskripsi asosiasi antara grup antarmuka virtual dan tabel rute gateway lokal di Anda Akun AWS.
ec2_ DescribeLocalGateways	Kumpulkan snapshot gateway lokal Anda.
ec2_ DescribeLocalGatewayVirtualInterfaces	Kumpulkan snapshot dari antarmuka virtual gateway lokal Anda.
ec2_ DescribeNatGateways	Kumpulkan snapshot gateway NAT Anda.
ec2_ DescribeNetworkAcls	Kumpulkan snapshot dari ACL jaringan Anda.
ec2_ DescribeRouteTables	Kumpulkan snapshot dari tabel rute Anda.
ec2_ DescribeSecurityGroups	Kumpulkan snapshot grup keamanan Anda.
ec2_ DescribeTransitGateways	Kumpulkan snapshot gateway transit Anda.
ec2_ DescribeVolumes	Kumpulkan snapshot dari titik akhir VPC Anda.
ec2_ DescribeVpcs	Kumpulkan snapshot dari VPC Anda.
ec2_ DescribeVpcEndpoints	Kumpulkan snapshot dari titik akhir VPC Anda.
ec2_ DescribeVpcPeeringConnections	Kumpulkan snapshot koneksi VPN Anda.
ec2_ DescribeVpnConnections	Kumpulkan snapshot koneksi VPN Anda.
ec2_ DescribeVpnGateways	Kumpulkan snapshot gateway pribadi virtual Anda.

Panggilan API yang didukung	Bagaimana Audit Manager menggunakan API ini untuk mengumpulkan bukti
ec2_ GetEbsDefaultKmsKeyId	Kumpulkan snapshot default AWS KMS key untuk enkripsi EBS untuk Anda Akun AWS di Wilayah saat ini.
ec2_ GetEbsEncryptionBy Default	Jelaskan apakah enkripsi EBS secara default diaktifkan untuk Anda Akun AWS di Wilayah saat ini.
ecs_ DescribeClusters	Kumpulkan snapshot dari cluster ECS Anda.
eks_ DescribeAddonVersions	Kumpulkan snapshot versi add-on Anda.
elastisis_ DescribeCacheClust ers	Kumpulkan snapshot dari cluster yang Anda sediakan.
elastisis_ DescribeServiceUpd ates	Kumpulkan snapshot pembaruan layanan untuk Amazon ElastiCache.
elasticfilesystem_ DescribeA ccessPoints	Kumpulkan snapshot dari titik akses Amazon EFS di situs Anda Akun AWS.
elasticfilesystem_ DescribeF ileSystems	Kumpulkan snapshot sistem file Amazon EFS Anda.
elasticloadbalancingv2_ DescribeLoadBalancers	Kumpulkan snapshot penyeimbang beban di Anda. Akun AWS
ElasticLoadBalanci ngV2_DescribessIPolicies	Kumpulkan snapshot kebijakan yang Anda gunakan untuk negosiasi SSL.
elasticloadbalancingv2_ DescribeTargetGroups	Kumpulkan snapshot dari kelompok target ELB Anda.
elasticmapreduce_ ListSecur ityConfigurations	Ambil daftar konfigurasi keamanan yang terlihat oleh Anda Akun AWS, bersama dengan tanggal dan waktu pembuatannya, dan namanya.
acara_ ListConnections	Ambil daftar EventBridge koneksi Amazon di Anda Akun AWS.

Panggilan API yang didukung	Bagaimana Audit Manager menggunakan API ini untuk mengumpulkan bukti
acara_ ListEventBuses	Ambil daftar bus EventBridge acara Amazon di Anda Akun AWS, termasuk bus acara default, bus acara khusus, dan bus acara mitra.
acara_ ListEventSources	Ambil daftar sumber acara mitra yang telah dibagikan dengan Anda Akun AWS.
acara_ ListRules	Ambil daftar EventBridge aturan Amazon Anda.
selang pembakar_ ListDeliveryStreams	Ambil daftar aliran pengiriman Anda.
fsx_ DescribeFileSystems	Kumpulkan snapshot dari sistem file yang dimiliki oleh Anda Akun AWS.
penjagaan_ ListDetectors	Ambil daftar sumber daya GuardDuty detektor Amazon Anda. `detectorIds`
iam_ GenerateCredentialReport	Buat laporan kredenal untuk Anda Akun AWS.
iam_ GetAccountPasswordPolicy	Kumpulkan snapshot kebijakan kata sandi untuk Anda Akun AWS.
iam_ GetAccountSummary	Kumpulkan snapshot penggunaan entitas IAM dan kuota IAM di Anda. Akun AWS
iam_ ListGroupPolicies	Ambil daftar kebijakan sebaris yang disematkan dalam grup IAM yang tersedia di grup Anda. Akun AWS
iam_ ListGroups	Ambil daftar grup IAM yang terkait dengan awalan jalur yang tersedia di Anda. Akun AWS
iam_ ID ListOpen ConnectProviders	Ambil daftar objek sumber daya penyedia OpenID Connect (OIDC) IAM yang didefinisikan dalam objek sumber daya penyedia OpenID Connect (OIDC). Akun AWS

Panggilan API yang didukung	Bagaimana Audit Manager menggunakan API ini untuk mengumpulkan bukti
iam_ ListPolicies	Mengambil daftar semua kebijakan terkelola yang tersedia di Anda Akun AWS, termasuk kebijakan terkelola yang ditentuka n pelanggan Anda sendiri dan semua kebijakan yang dikelola AWS.
iam_ ListRoles	Ambil daftar peran IAM yang terkait dengan awalan jalur yang tersedia di Anda. Akun AWS
IAM_ListSamlProviders	Ambil daftar objek sumber daya penyedia SAMP yang didefinis ikan dalam IAM di file Anda. Akun AWS
iam_ ListUsers	Ambil daftar pengguna IAM di Anda. Akun AWS
iam_ MFADevices ListVirtual	Ambil daftar perangkat MFA virtual yang didefinisikan dalam perangkat MFA Anda. Akun AWS
kafka_ ListClusters	Ambil daftar cluster MSK Amazon di Anda. Akun AWS
kafka_ ListKafkaVersions	Ambil daftar objek versi Apache Kafka di Anda. Akun AWS
kinesis_ ListStreams	Ambil daftar aliran data Kinesis Anda.
kms_ GetKeyPolicy	Audit Manager menggunakan API ini untuk mengumpulkan snapshot dari kebijakan utama untuk Anda Akun AWS. AWS KMS keys Saat Anda menggunakan API ini sebagai sumber data, Anda tidak perlu memberikan nama yang spesifik AWS KMS key. Sebagai gantinya, Audit Manager menggunakan `ListKeys` operasi untuk mencantumkan semua kunci KMS Anda. Untuk setiap kunci KMS yang terdaftar, Audit Manager kemudian melakukan `GetKeyPolicy` operasi untuk menghasilkan bukti untuk sumber daya tersebut.

Panggilan API yang didukung	Bagaimana Audit Manager menggunakan API ini untuk mengumpulkan bukti
kms_ GetKeyRotationStatus	Audit Manager menggunakan API ini untuk mengumpulkan snapshot apakah rotasi otomatis diaktifkan untuk AWS KMS keys di Anda Akun AWS. Saat Anda menggunakan API ini sebagai sumber data, Anda tidak perlu memberikan nama yang spesifik AWS KMS key. Sebagai gantinya, Audit Manager menggunakan `ListKeys` operasi untuk mencantumkan semua kunci KMS Anda. Untuk setiap kunci KMS yang terdaftar, Audit Manager kemudian melakukan `GetKeyRotationStatus` operasi untuk menghasilkan bukti untuk sumber daya tersebut.
kms_ ListKeys	Ambil daftar AWS KMS keys di Anda Akun AWS.
lambda_ ListFunctions	Ambil daftar fungsi Lambda di Akun AWSAnda, dengan konfigurasi khusus versi masing-masing.
RDS_DescribedBClusters	Kumpulkan snapshot dari cluster Amazon Aurora DB yang ada dan cluster DB multi-AZ di Anda. Akun AWS
RDS_DescribedBinstances	Kumpulkan snapshot dari instans RDS yang disediakan di Anda. Akun AWS
pergeseran merah_ DescribeClusters	Kumpulkan snapshot dari cluster Amazon Redshift yang disediakan di Anda. Akun AWS

Panggilan API yang didukung	Bagaimana Audit Manager menggunakan API ini untuk mengumpulkan bukti
s3_ GetBucketEncryption	Kumpulkan snapshot yang menunjukkan konfigurasi enkripsi default untuk bucket S3 Anda. Saat menggunakan API ini sebagai sumber data, Anda tidak perlu memberikan nama bucket S3 tertentu. Sebagai gantinya, Audit Manager menggunakan `ListBuckets` operasi untuk mencantumkan semua bucket Anda. Untuk setiap bucket yang terdaftar, Audit Manager kemudian melakukan `GetBucketEncryption` operasi untuk menghasilkan bukti untuk sumber daya tersebut. Audit Manager hanya dapat memberikan status enkripsi untuk bucket yang dibuat Wilayah AWS sama dengan penilaian Anda. Jika Anda perlu melihat status enkripsi semua bucket S3 Anda di beberapa Wilayah AWS, kami sarankan Anda membuat penilaian di masing-masing Wilayah AWS tempat Anda memiliki bucket S3.
s3_ ListBuckets	Ambil daftar ember S3 di. Akun AWS
sns_ ListTopics	Ambil daftar topik SNS di Anda. Akun AWS
sqs_ ListQueues	Ambil daftar antrian SQS di Anda. Akun AWS

Panggilan API berpaginasi

Banyak yang Layanan AWS mengumpulkan dan menyimpan sejumlah besar data. Akibatnya, ketika panggilan`list`,`describe`, atau `get` API mencoba mengembalikan data Anda, mungkin ada banyak hasil. Jika jumlah data terlalu besar untuk dikembalikan dalam satu respons, hasilnya dapat dipecah menjadi potongan-potongan yang lebih mudah dikelola melalui penggunaan pagination. Ini membagi hasil menjadi “halaman” data, membuat tanggapan lebih mudah ditangani.

Beberapa panggilan API yang didukung Audit Manager diberi paginasi. Ini berarti bahwa mereka mengembalikan sebagian hasil pada awalnya, dan memerlukan permintaan berikutnya untuk mengembalikan seluruh hasil yang ditetapkan. Misalnya, operasi Amazon RDS DescribedBInstances

mengembalikan hingga 100 instance sekaligus, dan permintaan berikutnya diperlukan untuk mengembalikan halaman hasil berikutnya.

Per 08 Maret 2023, Audit Manager mendukung panggilan API paginasi sebagai sumber data untuk pengumpulan bukti. Sebelumnya, jika panggilan API paginasi digunakan sebagai sumber data, hanya sebagian sumber daya Anda yang dikembalikan dalam respons API (hingga 100 hasil). Sekarang, Audit Manager memanggil operasi API paginasi beberapa kali, dan mendapatkan setiap halaman hasil hingga semua sumber daya dikembalikan. Untuk setiap sumber daya, Audit Manager kemudian menangkap snapshot konfigurasi dan menyimpannya sebagai bukti. Karena kumpulan sumber daya lengkap Anda sekarang ditangkap dalam respons API, kemungkinan besar Anda akan melihat peningkatan jumlah bukti yang dikumpulkan.

Audit Manager menangani pagination panggilan API untuk Anda secara otomatis. Jika Anda membuat kontrol khusus yang menggunakan panggilan API paginasi sebagai sumber data, Anda tidak perlu menentukan parameter pagination apa pun.

Panggilan API yang digunakan dalam kerangka kerja AWS License Manager standar

Dalam kerangka AWS License Managerstandar, Audit Manager menggunakan aktivitas kustom yang dipanggil `GetLicenseManagerSummary` untuk mengumpulkan bukti. Aktivitas ini memanggil tiga API License Manager berikut:

- ListLicenseConfigurations
- ListAssociationsForLicenseConfiguration
- ListUsageForLicenseConfiguration

Data yang dikembalikan kemudian diubah menjadi bukti dan dilampirkan pada kontrol yang relevan dalam penilaian Anda.

Contoh

Katakanlah Anda menggunakan dua produk berlisensi (SQL Service 2017 dan Oracle Database Enterprise Edition). Pertama, `GetLicenseManagerSummary` aktivitas memanggil ListLicenseConfigurationsAPI, yang menyediakan detail konfigurasi lisensi di akun Anda. Selanjutnya, ia menambahkan data kontekstual tambahan untuk setiap konfigurasi lisensi dengan memanggil ListUsageForLicenseConfigurationdan. ListAssociationsForLicenseConfiguration Akhirnya, ia mengubah data konfigurasi lisensi menjadi bukti dan melampirkannya ke kontrol masing-masing dalam kerangka kerja (4.5 - Lisensi terkelola pelanggan untuk SQL Server 2017 dan 3.0.4 - Lisensi terkelola pelanggan untuk Oracle Database Enterprise Edition).

Jika Anda menggunakan produk berlisensi yang tidak tercakup oleh kontrol apa pun dalam kerangka kerja, data konfigurasi lisensi tersebut dilampirkan sebagai bukti kontrol berikut: 5.0 - Lisensi terkelola pelanggan untuk lisensi lain.

AWS CloudTrail nama acara yang didukung oleh AWS Audit Manager

Anda dapat menangkap peristiwa AWS CloudTrail manajemen dan acara layanan global sebagai bukti di Audit Manager. Untuk melakukan ini, Anda menentukan nama CloudTrail acara sebagai kata kunci pemetaan sumber data saat Anda membuat kontrol khusus.

> **Note**
>
> Audit Manager hanya menangkap peristiwa manajemen dan acara layanan global. Peristiwa data dan wawasan peristiwa tidak tersedia sebagai bukti. Untuk informasi selengkapnya tentang berbagai jenis CloudTrail acara, lihat CloudTrail konsep di PanduanAWS CloudTrail Pengguna.

Sebagai pengecualian di atas, CloudTrail peristiwa berikut tidak didukung oleh Audit Manager:

- kms_ GenerateDataKey
- KMS_Dekripsi
- sts_ AssumeRole
- kinesisvideo_ GetDataEndpoint
- kinesisvideo_ GetSignalingChannelEndpoint
- kinesisvideo_ DescribeSignalingChannel
- kinesisvideo_ DescribeStream

Per 11 Mei 2023, Audit Manager tidak lagi mendukung CloudTrail peristiwa hanya-baca sebagai kata kunci untuk pengumpulan bukti. Kami menghapus total 3.135 kata kunci read-only. Karena pelanggan dan Layanan AWS keduanya melakukan panggilan baca ke API, acara hanya-baca menjadi berisik. Akibatnya, kata kunci read-only mengumpulkan banyak bukti yang tidak dapat diandalkan atau relevan untuk audit. Kata kunci hanya-baca termasuk`List`,`Describe`, dan panggilan `Get` API (misalnya, GetObjectdan ListBucketsuntuk Amazon S3). Jika Anda menggunakan salah satu kata kunci ini untuk pengumpulan bukti, Anda tidak perlu melakukan apa pun. Kata kunci

secara otomatis dihapus dari konsol Audit Manager dan dari penilaian Anda, dan bukti tidak lagi dikumpulkan untuk kata kunci ini.

Pengaturan AWS Audit Manager

Anda dapat meninjau dan mengonfigurasi AWS Audit Manager pengaturan Anda kapan saja.

Untuk mengakses pengaturan Anda

1. Buka konsol AWS Audit Manager di https://console.aws.amazon.com/auditmanager/home.
2. Pada panel navigasi kiri, pilih Pengaturan.

Pengaturan berikut tersedia:

- Pengaturan umum
  - Izin
  - Enkripsi data
  - Administrator yang didelegasikan (opsional)
  - AWS Config (opsional)
  - Security Hub (opsional)
  - Menonaktifkan AWS Audit Manager
- Pengaturan penilaian
  - Pemilik audit default (opsional)
  - Tujuan laporan penilaian (opsional)
  - Pemberitahuan (opsional)
- Pengaturan pencari bukti
  - Pencari bukti (opsional)
  - Tujuan ekspor (opsional)

Pengaturan umum

Tab Pengaturan umum adalah tampilan default halaman pengaturan di konsol Audit Manager. Gunakan tab ini untuk meninjau dan memperbarui pengaturan Audit Manager umum Anda.

Topik

- Izin

- Enkripsi data
- Administrator yang didelegasikan (opsional)
- AWS Config (opsional)
- Security Hub (opsional)
- Menonaktifkan AWS Audit Manager

Izin

AWS Audit Managermenggunakan peran terkait layanan untuk terhubung ke sumber data atas nama Anda. Untuk informasi selengkapnya, lihat Menggunakan peran terkait layanan untuk AWS Audit Manager.

Untuk meninjau detail peran terkait layanan yang digunakan Audit Manager, pilih Lihat izin peran terkait layanan IAM.

Untuk informasi selengkapnya tentang peran terkait layanan, lihat Menggunakan peran terkait layanan di Panduan Pengguna IAM.

Enkripsi data

Audit Manager secara otomatis membuat unik Kunci yang dikelola AWS untuk penyimpanan data Anda yang aman. Secara default, data Audit Manager Anda dienkripsi dengan kunci KMS ini. Atau, jika Anda ingin menyesuaikan pengaturan enkripsi data Anda, Anda dapat menentukan kunci terkelola pelanggan enkripsi simetris Anda sendiri. Menggunakan tombol KMS Anda sendiri memberi Anda lebih banyak fleksibilitas, termasuk kemampuan untuk membuat, memutar, dan menonaktifkan kunci.

> **Important**
>
> Untuk menghasilkan laporan penilaian dan hasil pencarian pencari bukti ekspor berhasil, kunci yang dikelola pelanggan Anda (jika Anda memberikannya) harus Wilayah AWS sama dengan penilaian Anda. Untuk daftar Wilayah Audit Manager, lihat AWS Audit Managertitik akhir dan kuota di Referensi Umum Amazon Web Services.

Anda dapat memperbarui setelan enkripsi data menggunakan konsol Audit Manager, AWS Command Line Interface (AWS CLI), atau Audit Manager API.

Audit Manager console

Untuk memperbarui pengaturan enkripsi data Anda (konsol)

1. Dari tab Pengaturan umum, buka bagian Enkripsi data.
2. Untuk menggunakan kunci KMS default yang disediakan oleh Audit Manager, kosongkan kotak centang Sesuaikan pengaturan enkripsi (lanjutan).
3. Untuk menggunakan kunci terkelola pelanggan, pilih kotak centang Kustomisasi pengaturan enkripsi (lanjutan). Anda kemudian dapat memilih kunci KMS yang ada, atau membuat yang baru.

AWS CLI

Untuk memperbarui pengaturan enkripsi data Anda (AWS CLI)

Jalankan perintah update-settings dan gunakan `--kms-key` parameter untuk menentukan kunci yang dikelola pelanggan Anda sendiri.

Dalam contoh berikut, ganti *teks placeholder dengan informasi* Anda sendiri.

```
aws auditmanager update-settings --kms-key arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab
```

Audit Manager API

Untuk memperbarui pengaturan enkripsi data (API)

Panggil UpdateSettingsoperasi dan gunakan parameter KMSKey untuk menentukan kunci yang dikelola pelanggan Anda sendiri.

Untuk informasi selengkapnya, pilih tautan sebelumnya untuk membaca selengkapnya di Referensi API Audit Manager. Ini termasuk informasi tentang cara menggunakan operasi dan parameter ini di salah satu SDK khusus bahasaAWS.

> **Note**
>
> Saat Anda mengubah setelan enkripsi data Audit Manager, perubahan ini berlaku untuk penilaian baru apa pun yang Anda buat. Ini termasuk laporan penilaian dan ekspor pencari bukti yang Anda buat dari penilaian baru Anda.

Perubahan tidak berlaku untuk penilaian yang sudah ada yang Anda buat sebelum mengubah setelan enkripsi. Ini termasuk laporan penilaian baru dan ekspor CSV yang Anda buat dari penilaian yang ada, selain laporan penilaian yang ada dan ekspor CSV. Penilaian yang ada — dan semua laporan penilaian dan ekspor CSV mereka — terus menggunakan kunci KMS lama.
Jika identitas IAM yang menghasilkan laporan penilaian tidak dapat menggunakan kunci KMS lama, berikan izin di tingkat kebijakan utama. Untuk petunjuk, lihat Mengizinkan pengguna di akun lain menggunakan kunci KMS di Panduan AWS Key Management Service Pengembang.

Untuk petunjuk tentang cara membuat kunci, lihat Membuat kunci di Panduan AWS Key Management Service Pengguna.

Administrator yang didelegasikan (opsional)

Jika Anda menggunakan AWS Organizations dan ingin mengaktifkan dukungan multi-akun untuk Audit Manager, Anda dapat menetapkan akun anggota di organisasi Anda sebagai administrator yang didelegasikan untuk Audit Manager.

Prasyarat

- Akun Anda harus menjadi bagian dari organisasi. Untuk informasi selengkapnya, lihat Membuat dan mengelola organisasi di Panduan AWS Organizations Pengguna.
- Sebelum Anda menunjuk administrator yang didelegasikan, Anda harus mengaktifkan semua fitur di organisasi Anda. Anda juga harus mengonfigurasi setelan Security Hub organisasi Anda. Dengan cara ini, Audit Manager dapat mengumpulkan bukti Security Hub dari akun anggota Anda.
- Akun administrator yang didelegasikan harus memiliki akses pada kunci KMS yang Anda berikan saat menyiapkan Audit Manager. Untuk meninjau dan mengubah setelan enkripsi Anda, lihatEnkripsi data.

Pertimbangan penting bagi administrator yang didelegasikan di Audit Manager

Perhatikan faktor-faktor berikut yang menentukan bagaimana administrator yang didelegasikan beroperasi di Audit Manager:

Penggunaan akun manajemen

Anda tidak dapat menggunakan akun AWS Organizations manajemen sebagai administrator yang didelegasikan di Audit Manager.

Menggunakan administrator yang didelegasikan di beberapa Wilayah AWS

Jika Anda ingin mengaktifkan Audit Manager di lebih dari satuWilayah AWS, Anda harus menetapkan akun administrator yang didelegasikan secara terpisah di setiap Wilayah. Dalam pengaturan Audit Manager Anda, Anda harus menggunakan akun administrator yang didelegasikan yang sama di semua Wilayah.

Tugas pembersihan pencari bukti

Sebelum Anda menggunakan akun manajemen untuk menghapus atau mengubah administrator yang didelegasikan, pastikan akun administrator yang didelegasikan saat ini masuk ke Audit Manager dan menonaktifkan pencari bukti. Menonaktifkan pencari bukti secara otomatis menghapus penyimpanan data peristiwa yang dibuat di akun saat pencari bukti diaktifkan.

Jika tugas ini tidak selesai, penyimpanan data acara tetap ada di akun mereka. Dalam hal ini, kami menyarankan agar administrator yang didelegasikan asli menggunakan CloudTrail Lake untuk menghapus penyimpanan data acara secara manual.

Tugas pembersihan ini diperlukan untuk memastikan bahwa Anda tidak berakhir dengan beberapa penyimpanan data acara. Audit Manager mengabaikan penyimpanan data peristiwa yang tidak digunakan setelah Anda menghapus atau mengubah akun administrator yang didelegasikan. Namun, jika Anda tidak menghapus penyimpanan data peristiwa yang tidak digunakan, penyimpanan data acara terus menimbulkan biaya penyimpanan dari CloudTrail Lake.

Penghapusan data

Saat Anda menghapus akun administrator yang didelegasikan untuk Audit Manager, data untuk akun tersebut tidak akan dihapus. Jika Anda ingin menghapus data sumber daya untuk akun administrator yang didelegasikan, Anda harus melakukan tugas itu secara terpisah sebelum menghapus akun. Anda juga dapat melakukan ini di konsol Audit Manager. Atau, Anda dapat menggunakan salah satu operasi delete API yang disediakan oleh Audit Manager. Untuk daftar operasi penghapusan yang tersedia, lihat Penghapusan data Audit Manager.

Pada saat ini, Audit Manager tidak menyediakan opsi untuk menghapus bukti untuk administrator tertentu yang didelegasikan. Sebagai gantinya, ketika akun manajemen Anda membatalkan pendaftaran Audit Manager, kami melakukan pembersihan untuk akun administrator yang didelegasikan saat ini pada saat deregistrasi.

Untuk solusi untuk masalah umum Organizations dan administrator yang didelegasikan di Audit Manager, lihatMemecahkan masalah administrator dan masalah yang didelegasikan AWS Organizations.

Mengelola akun administrator yang didelegasikan untuk Audit Manager

Anda dapat meninjau dan mengubah pengaturan akun administrator yang didelegasikan sebagai berikut.

Tambahkan administrator yang didelegasikan

Anda dapat menambahkan administrator yang didelegasikan menggunakan konsol Audit Manager, AWS Command Line Interface (AWS CLI), atau Audit Manager API.

> **Note**
>
> Setelah menambahkan administrator yang didelegasikan di setelan Audit Manager, akun manajemen Anda tidak dapat lagi membuat penilaian tambahan di Audit Manager. Selain itu, pengumpulan bukti berhenti untuk setiap penilaian yang ada yang dibuat oleh akun manajemen. Audit Manager mengumpulkan dan melampirkan bukti ke akun administrator yang didelegasikan, yang merupakan akun utama untuk mengelola penilaian organisasi Anda.

Audit Manager console

Untuk menambahkan administrator yang didelegasikan (konsol)

1. Dari tab Pengaturan umum, buka bagian Administrator yang didelegasikan.
2. Di bawah ID akun administrator yang didelegasikan, masukkan ID akun administrator yang didelegasikan.
3. Pilih Delegasikan.

AWS CLI

Untuk menambahkan administrator yang didelegasikan () AWS CLI

Jalankan register-organization-admin-accountperintah dan gunakan `--admin-account-id` parameter untuk menentukan ID akun administrator yang didelegasikan.

Dalam contoh berikut, ganti *teks placeholder dengan informasi* Anda sendiri.

```
aws auditmanager register-organization-admin-account --admin-account-id 111122223333
```

Audit Manager API

Untuk menambahkan administrator (API) yang didelegasikan saat ini

Panggil RegisterOrganizationAdminAccountoperasi dan gunakan adminAccountIdparameter untuk menentukan ID akun administrator yang didelegasikan.

Untuk informasi selengkapnya, pilih tautan sebelumnya untuk membaca selengkapnya di Referensi API Audit Manager. Ini termasuk informasi tentang cara menggunakan operasi dan parameter ini di salah satu SDK khusus bahasaAWS.

Mengubah administrator yang didelegasikan

Anda dapat mengubah administrator yang didelegasikan menggunakan konsol Audit Manager, AWS Command Line Interface (AWS CLI), atau Audit Manager API.

> **Warning**
>
> Ketika Anda mengubah administrator yang didelegasikan, Anda terus memiliki akses ke bukti yang sebelumnya Anda kumpulkan di bawah akun administrator yang didelegasikan lama. Namun, Audit Manager berhenti mengumpulkan dan melampirkan bukti ke akun administrator lama yang didelegasikan.

Audit Manager console

Untuk mengubah administrator yang didelegasikan saat ini (konsol)

1. (Opsional) Jika administrator (akun A) yang didelegasikan saat ini mengaktifkan pencari bukti, lakukan tugas pembersihan berikut:

   - Sebelum menetapkan akun B sebagai administrator baru yang didelegasikan, pastikan akun A masuk ke Audit Manager dan menonaktifkan pencari bukti.

     Menonaktifkan pencari bukti secara otomatis menghapus penyimpanan data peristiwa yang dibuat saat akun Pencari bukti yang diaktifkan. Jika Anda tidak menyelesaikan

langkah ini, maka akun A harus pergi ke CloudTrail Lake dan secara manual menghapus penyimpanan data acara. Jika tidak, penyimpanan data acara tetap berada di akun A dan terus dikenakan biaya penyimpanan CloudTrail Danau.

2. Dari tab Pengaturan umum, buka bagian Administrator yang didelegasikan dan pilih Hapus.
3. Di jendela pop-up yang muncul, pilih Hapus untuk mengonfirmasi.
4. Di bawah ID akun administrator yang didelegasikan, masukkan ID akun administrator yang didelegasikan baru.
5. Pilih Delegasikan.

AWS CLI

Sebelum Anda mulai

Jika administrator (akun A) yang didelegasikan saat ini mengaktifkan pencari bukti, lakukan tugas pembersihan berikut:

Sebelum menetapkan akun B sebagai administrator baru yang didelegasikan, pastikan akun A masuk ke Audit Manager dan menonaktifkan pencari bukti.

Menonaktifkan pencari bukti secara otomatis menghapus penyimpanan data peristiwa yang dibuat saat akun Pencari bukti yang diaktifkan. Jika Anda tidak menyelesaikan langkah ini, maka akun A harus pergi ke CloudTrail Lake dan secara manual menghapus penyimpanan data acara. Jika tidak, penyimpanan data acara tetap berada di akun A dan terus dikenakan biaya penyimpanan CloudTrail Danau.

Untuk mengubah administrator yang didelegasikan saat ini () AWS CLI

Pertama, jalankan deregister-organization-admin-accountperintah menggunakan `--admin-account-id` parameter untuk menentukan ID akun dari administrator yang didelegasikan saat ini.

Dalam contoh berikut, ganti *`teks placeholder dengan informasi`* Anda sendiri.

```
aws auditmanager deregister-organization-admin-account --admin-account-
id 111122223333
```

Kemudian, jalankan register-organization-admin-accountperintah menggunakan `--admin-account-id` parameter untuk menentukan ID akun administrator yang didelegasikan baru.

Dalam contoh berikut, ganti *teks placeholder dengan informasi* Anda sendiri.

```
aws auditmanager register-organization-admin-account --admin-account-id 444455556666
```

Audit Manager API

Sebelum Anda mulai

Jika administrator (akun A) yang didelegasikan saat ini mengaktifkan pencari bukti, lakukan tugas pembersihan berikut:

Sebelum menetapkan akun B sebagai administrator baru yang didelegasikan, pastikan akun A masuk ke Audit Manager dan menonaktifkan pencari bukti.

Menonaktifkan pencari bukti secara otomatis menghapus penyimpanan data peristiwa yang dibuat saat akun Pencari bukti yang diaktifkan. Jika Anda tidak menyelesaikan langkah ini, maka akun A harus pergi ke CloudTrail Lake dan secara manual menghapus penyimpanan data acara. Jika tidak, penyimpanan data acara tetap berada di akun A dan terus dikenakan biaya penyimpanan CloudTrail Danau.

Untuk mengubah administrator yang didelegasikan (API) saat ini

Pertama, panggil DeregisterOrganizationAdminAccountoperasi dan gunakan adminAccountIdparameter untuk menentukan ID akun dari administrator yang didelegasikan saat ini.

Kemudian, panggil RegisterOrganizationAdminAccountoperasi dan gunakan adminAccountIdparameter untuk menentukan ID akun administrator yang didelegasikan baru.

Untuk informasi selengkapnya, pilih tautan sebelumnya untuk membaca selengkapnya di Referensi API Audit Manager. Ini termasuk informasi tentang cara menggunakan operasi dan parameter ini di salah satu SDK khusus bahasaAWS.

Menghapus administrator yang didelegasikan

Anda dapat menghapus administrator yang didelegasikan menggunakan konsol Audit Manager, AWS Command Line Interface (AWS CLI), atau Audit Manager API.

> **Warning**
>
> Saat menghapus administrator yang didelegasikan, Anda tetap memiliki akses ke bukti yang sebelumnya Anda kumpulkan di bawah akun administrator yang didelegasikan tersebut. Namun, Audit Manager berhenti mengumpulkan dan melampirkan bukti ke akun administrator lama yang didelegasikan.

Audit Manager console

Untuk menghapus administrator yang didelegasikan saat ini (konsol)

1. (Opsional) Jika administrator yang didelegasikan saat ini mengaktifkan pencari bukti, lakukan tugas pembersihan berikut:

   - Pastikan akun administrator yang didelegasikan saat ini masuk ke Audit Manager dan menonaktifkan pencari bukti.

     Menonaktifkan pencari bukti secara otomatis menghapus penyimpanan data peristiwa yang dibuat di akun mereka saat mereka mengaktifkan pencari bukti. Jika langkah ini tidak selesai, akun administrator yang didelegasikan harus menggunakan CloudTrail Lake untuk menghapus penyimpanan data peristiwa secara manual. Jika tidak, penyimpanan data acara tetap ada di akun mereka dan terus dikenakan biaya penyimpanan CloudTrail Danau.
2. Dari tab Pengaturan umum, buka bagian Administrator yang didelegasikan dan pilih Hapus.
3. Di jendela pop-up yang muncul, pilih Hapus untuk mengonfirmasi.

AWS CLI

Sebelum Anda mulai

Jika administrator yang didelegasikan saat ini mengaktifkan pencari bukti, lakukan tugas pembersihan berikut:

Pastikan akun administrator yang didelegasikan saat ini masuk ke Audit Manager dan menonaktifkan pencari bukti.

Menonaktifkan pencari bukti secara otomatis menghapus penyimpanan data peristiwa yang dibuat di akun mereka saat mereka mengaktifkan pencari bukti. Jika langkah ini tidak selesai,

akun administrator yang didelegasikan harus menggunakan CloudTrail Lake untuk menghapus penyimpanan data peristiwa secara manual. Jika tidak, penyimpanan data acara tetap ada di akun mereka dan terus dikenakan biaya penyimpanan CloudTrail Danau.

Untuk menghapus administrator yang didelegasikan saat ini () AWS CLI

Jalankan deregister-organization-admin-accountperintah dan gunakan `--admin-account-id` parameter untuk menentukan ID akun administrator yang didelegasikan.

Dalam contoh berikut, ganti *`teks placeholder dengan informasi`* Anda sendiri.

```
aws auditmanager deregister-organization-admin-account --admin-account-
id 111122223333
```

Audit Manager API

Sebelum Anda mulai

Jika administrator yang didelegasikan saat ini mengaktifkan pencari bukti, lakukan tugas pembersihan berikut:

Pastikan akun administrator yang didelegasikan saat ini masuk ke Audit Manager dan menonaktifkan pencari bukti.

Menonaktifkan pencari bukti secara otomatis menghapus penyimpanan data peristiwa yang dibuat di akun mereka saat mereka mengaktifkan pencari bukti. Jika langkah ini tidak selesai, akun administrator yang didelegasikan harus menggunakan CloudTrail Lake untuk menghapus penyimpanan data peristiwa secara manual. Jika tidak, penyimpanan data acara tetap ada di akun mereka dan terus dikenakan biaya penyimpanan CloudTrail Danau.

Untuk menghapus administrator (API) yang didelegasikan saat ini

Panggil DeregisterOrganizationAdminAccountoperasi dan gunakan adminAccountIdparameter untuk menentukan ID akun administrator yang didelegasikan.

Untuk informasi selengkapnya, pilih tautan sebelumnya untuk membaca selengkapnya di Referensi API Audit Manager. Ini termasuk informasi tentang cara menggunakan operasi dan parameter ini di salah satu SDK khusus bahasaAWS.

AWS Config (opsional)

Anda dapat mengizinkan Audit Manager untuk mengumpulkan temuan dariAWS Config. Bila AWS Config diaktifkan, Audit Manager dapat menangkap snapshot dari postur keamanan sumber daya Anda dengan melaporkan hasil pemeriksaan aturan langsung dariAWS Config. Kami menyarankan Anda AWS Config untuk mengaktifkan pengalaman yang optimal di Audit Manager.

Untuk mengaktifkanAWS Config, pilih Aktifkan AWS Config untuk pergi ke layanan itu. Untuk petunjuk tentang cara mengaktifkanAWS Config, lihat Menyiapkan AWS Config di Panduan AWS Config Pengembang.

Security Hub (opsional)

Anda dapat mengizinkan Audit Manager untuk mengimpor AWS Security Hub temuan untuk standar kepatuhan yang didukung. Saat Security Hub diaktifkan, Audit Manager dapat menangkap snapshot dari postur keamanan sumber daya Anda dengan hasil pemeriksaan keamanan langsung dari Security Hub. Kami menyarankan Anda mengaktifkan Security Hub untuk pengalaman optimal di Audit Manager.

Untuk mengaktifkan Security Hub, pilih Aktifkan Security Hub untuk membuka layanan tersebut. Untuk petunjuk tentang cara mengaktifkan Security Hub, lihat Menyiapkan AWS Security Hub di Panduan Pengguna Security Hub.

Menonaktifkan AWS Audit Manager

Anda dapat menonaktifkan Audit Manager jika Anda tidak lagi ingin menggunakan layanan. Ketika Anda menonaktifkan Audit Manager, Anda juga memiliki opsi untuk menghapus semua data Anda.

Secara default, data Anda tidak akan dihapus saat Anda menonaktifkan Audit Manager. Data bukti Anda disimpan selama dua tahun sejak pembuatannya. Sumber daya Audit Manager Anda yang lain (termasuk penilaian, kontrol kustom, dan kerangka kerja kustom) dipertahankan tanpa batas waktu, dan akan tersedia jika Anda mengaktifkan kembali Audit Manager di masa mendatang. Untuk informasi selengkapnya tentang retensi data, lihat Perlindungan Data dalam panduan ini.

Jika Anda memilih untuk menghapus data, Audit Manager menghapus semua data bukti bersama dengan semua sumber daya Audit Manager yang Anda buat (termasuk penilaian, kontrol kustom, dan kerangka kerja kustom). Semua data Anda dihapus dalam waktu tujuh hari setelah menonaktifkan Audit Manager.

⚠ Warning

- Saat Anda menonaktifkan Audit Manager, akses Anda dicabut dan layanan tidak lagi mengumpulkan bukti untuk penilaian yang ada. Anda tidak dapat mengakses apa pun di layanan kecuali Anda mengaktifkan kembali Audit Manager.
- Menghapus semua data adalah tindakan permanen. Jika Anda memutuskan untuk mengaktifkan kembali Audit Manager di masa mendatang, data Anda tidak akan dapat dipulihkan.

Anda dapat menonaktifkan Audit Manager menggunakan konsol Audit Manager, AWS Command Line Interface (AWS CLI), atau Audit Manager API.

Audit Manager console

Untuk menonaktifkan Audit Manager (konsol)

1. Dari tab Pengaturan umum, buka AWS Audit Manager bagian Nonaktifkan.
2. Pilih Disable (Nonaktifkan).
3. Di jendela pop-up, tinjau pengaturan penyimpanan data Anda saat ini.
    a. Untuk melanjutkan pilihan Anda saat ini, pilih Nonaktifkan Audit Manager.
    b. Untuk mengubah pilihan Anda saat ini, lakukan langkah-langkah berikut:
        i. Pilih Batal untuk kembali ke halaman pengaturan.
        ii. Untuk menggunakan pengaturan penyimpanan data default, matikan Hapus semua data. Seleksi ini menyimpan data bukti selama dua tahun sejak pembuatannya, dan mempertahankan sumber daya Audit Manager lainnya tanpa batas waktu.
        iii. Untuk menghapus data Anda, aktifkan Hapus semua data.
        iv. Pilih Nonaktifkan, lalu pilih Nonaktifkan Audit Manager untuk mengonfirmasi pilihan Anda.

AWS CLI

Sebelum Anda mulai

Sebelum menonaktifkan Audit Manager, Anda dapat menjalankan perintah update-settings untuk menyetel kebijakan penyimpanan data pilihan Anda. Secara default, Audit Manager menyimpan data Anda. Jika Anda ingin meminta penghapusan data Anda, gunakan `--deregistration-policy` parameter dengan `deleteResources` nilai yang disetel ke. `ALL`

```
aws auditmanager update-settings --deregistration-policy deleteResources=ALL
```

Untuk menonaktifkan Audit Manager (AWS CLI)

Saat Anda siap menonaktifkan Audit Manager, jalankan perintah deregister-account.

```
aws auditmanager deregister-account
```

Audit Manager API

Sebelum Anda mulai

Sebelum menonaktifkan Audit Manager, Anda dapat menggunakan operasi UpdateSettingsAPI untuk menyetel kebijakan penyimpanan data pilihan Anda. Secara default, Audit Manager menyimpan data Anda. Jika Anda ingin menghapus data Anda, Anda dapat menggunakan DeregistrationPolicyatribut untuk meminta penghapusan data Anda.

Untuk menonaktifkan Audit Manager (API)

Ketika Anda siap untuk menonaktifkan Audit Manager, hubungi DeregisterAccountoperasi.

Untuk informasi selengkapnya, pilih tautan sebelumnya untuk membaca selengkapnya di Referensi API Audit Manager. Ini termasuk informasi tentang cara menggunakan operasi dan parameter ini di salah satu SDK khusus bahasaAWS.

Untuk mengaktifkan kembali Audit Manager setelah Anda menonaktifkannya

Buka beranda layanan Audit Manager dan ikuti langkah-langkah untuk mengatur Audit Manager sebagai pengguna baru. Untuk informasi selengkapnya, lihat Menyiapkan AWS Audit Manager.

> **Tip**
>
> - Jika Anda memilih untuk menghapus data saat menonaktifkan Audit Manager, Anda harus menunggu hingga data dihapus sebelum dapat mengaktifkan kembali layanan. Tergantung pada berapa banyak data yang Anda miliki, ini bisa memakan waktu hingga tujuh hari.

Namun, jangan ragu untuk mencoba mengaktifkan kembali Audit Manager sebelum itu. Dalam banyak kasus, data dihapus hanya dalam satu jam.

- Jika Anda memilih untuk tidak menghapus data saat Anda menonaktifkan Audit Manager, penilaian yang ada dipindahkan ke keadaan tidak aktif dan berhenti mengumpulkan bukti sebagai hasilnya. Untuk mulai mengumpulkan bukti lagi untuk penilaian yang sudah ada sebelumnya, edit penilaian dan pilih Simpan tanpa membuat perubahan apa pun.

Pengaturan penilaian

Gunakan tab ini untuk meninjau dan memperbarui pengaturan penilaian Anda.

Topik

Pemilik audit default (opsional)

Anda dapat menentukan pemilik audit default yang memiliki akses utama ke penilaian Anda di Audit Manager.

Anda dapat memperbarui setelan ini menggunakan konsol Audit Manager, AWS Command Line Interface (AWS CLI), atau Audit Manager API.

Audit Manager console

Anda dapat memilih dari yang Akun AWS tercantum dalam tabel, atau menggunakan bilah pencarian untuk mencari yang lainAkun AWS.

Untuk memperbarui setelan pemilik audit default (konsol)

1. Dari tab Pengaturan penilaian, buka bagian Pemilik audit default dan pilih Edit.
2. Untuk menambahkan pemilik audit default, pilih kotak centang di samping nama akun di bawah Pemilik audit.
3. Untuk menghapus pemilik audit default, kosongkan kotak centang di samping nama akun di bawah Pemilik audit.

4. Setelah selesai, pilih Simpan.

AWS CLI

Untuk memperbarui setelan pemilik audit default Anda (AWS CLI)

Jalankan perintah update-settings dan gunakan `--default-process-owners` parameter untuk menentukan pemilik audit.

Dalam contoh berikut, ganti *`teks placeholder dengan informasi`* Anda sendiri. Perhatikan bahwa hanya `roleType` bisa`PROCESS_OWNER`.

```
aws auditmanager update-settings --default-process-owners
 roleType=PROCESS_OWNER,roleArn=arn:aws:iam::111122223333:role/Administrator
```

Audit Manager API

Untuk memperbarui setelan pemilik audit default (API)

Panggil UpdateSettingsoperasi dan gunakan defaultProcessOwnersparameter untuk menentukan pemilik audit default. Perhatikan bahwa hanya `roleType` bisa`PROCESS_OWNER`.

Untuk informasi selengkapnya tentang pemilik audit, lihat Pemilik audit di bagian Konsep dan terminologi panduan ini.

Tujuan laporan penilaian (opsional)

Saat membuat laporan penilaian, Audit Manager akan menerbitkan laporan tersebut ke bucket S3 pilihan Anda. Bucket S3 ini disebut sebagai tujuan laporan penilaian. Anda dapat memilih bucket Amazon S3 tempat Audit Manager menyimpan laporan penilaian Anda.

Anda dapat memperbarui setelan ini menggunakan konsol Audit Manager, AWS Command Line Interface (AWS CLI), atau Audit Manager API.

Audit Manager console

Untuk memperbarui setelan tujuan laporan penilaian (konsol)

1. Dari tab Pengaturan penilaian, buka bagian Tujuan laporan penilaian.

2. Untuk menggunakan bucket Amazon S3 yang sudah ada, pilih nama bucket dari menu tarik-turun.
3. Untuk membuat bucket Amazon S3 baru, pilih Buat bucket baru.
4. Setelah selesai, pilih Simpan.

AWS CLI

Untuk memperbarui setelan tujuan laporan penilaian Anda (AWS CLI)

Jalankan perintah update-settings dan gunakan `--default-assessment-reports-destination` parameter untuk menentukan bucket S3.

Dalam contoh berikut, ganti *`teks placeholder dengan informasi`* Anda sendiri:

```
aws auditmanager update-settings --default-assessment-reports-destination
 destinationType=S3,destination=s3://doc-example-destination-bucket
```

Audit Manager API

Untuk memperbarui setelan tujuan laporan penilaian (API)

Panggil UpdateSettingsoperasi dan gunakan parameter defaultAssessmentReportsTujuan untuk menentukan bucket S3.

Untuk petunjuk tentang cara membuat bucket S3, lihat Membuat bucket di Panduan Pengguna Amazon S3.

Kiat konfigurasi untuk tujuan laporan penilaian Anda

Untuk memastikan keberhasilan pembuatan laporan penilaian Anda, kami sarankan Anda memverifikasi konfigurasi berikut untuk tujuan laporan penilaian Anda.

Ember Wilayah yang Sama

Kami menyarankan Anda menggunakan bucket S3 yang Wilayah AWS sama dengan penilaian Anda. Bila Anda menggunakan bucket dan penilaian wilayah yang sama, laporan penilaian Anda dapat menyertakan hingga 22.000 item bukti. Sebaliknya, saat Anda menggunakan bucket dan penilaian lintas wilayah, hanya 3.500 item bukti yang dapat disertakan.

Wilayah AWS

Kunci terkelola pelanggan Anda (jika Anda memberikannya) harus sesuai dengan Wilayah penilaian Anda dan bucket tujuan laporan penilaian S3 Anda. Wilayah AWS Untuk petunjuk tentang cara mengubah kunci KMS, lihat AWS Audit Managerpengaturan, Enkripsi data. Untuk petunjuk tentang cara mengubah bucket S3, lihat AWS Audit Managerpengaturan, Tujuan laporan penilaian. Untuk daftar Wilayah Audit Manager yang didukung, lihat AWS Audit Managertitik akhir dan kuota di Referensi Umum Amazon Web Services.

Enkripsi ember S3

Jika tujuan laporan penilaian Anda memiliki kebijakan bucket yang memerlukan enkripsi sisi server (SSE) menggunakan SSE-KMS, maka kunci KMS yang digunakan dalam kebijakan bucket tersebut harus sesuai dengan kunci KMS yang dikonfigurasi dalam setelan enkripsi data Audit Manager. Jika Anda belum mengonfigurasi kunci KMS di setelan Audit Manager, dan kebijakan bucket tujuan laporan penilaian Anda memerlukan SSE, pastikan kebijakan bucket mengizinkan SSE-S3. Untuk petunjuk tentang cara mengonfigurasi kunci KMS yang digunakan untuk enkripsi data, lihat Pengaturan enkripsi data.

Ember S3 lintas akun

Menggunakan bucket S3 lintas akun sebagai tujuan laporan penilaian Anda tidak didukung di konsol Audit Manager. Anda dapat menentukan bucket lintas akun sebagai tujuan laporan penilaian Anda dengan menggunakan AWS CLI atau salah satu AWS SDK, tetapi untuk mempermudah, sebaiknya Anda tidak melakukannya. Jika Anda memilih untuk menggunakan bucket S3 lintas akun sebagai tujuan laporan penilaian Anda, pertimbangkan poin-poin berikut.

- Secara default, objek S3—seperti laporan penilaian—dimiliki oleh objek yang mengunggah objek. Akun AWS Anda dapat menggunakan setelan Kepemilikan Objek S3 untuk mengubah perilaku default ini sehingga objek baru apa pun yang ditulis oleh akun dengan daftar kontrol akses (ACL) yang `bucket-owner-full-control` dikalengkan secara otomatis menjadi milik pemilik bucket.

  Meskipun ini bukan persyaratan, kami menyarankan Anda untuk membuat perubahan berikut pada pengaturan bucket lintas akun Anda. Membuat perubahan ini memastikan bahwa pemilik bucket memiliki kendali penuh atas laporan penilaian yang Anda publikasikan ke bucket mereka.

  - Setel kepemilikan objek bucket S3 ke pilihan pemilik bucket, bukan penulis objek default
  - Tambahkan kebijakan bucket untuk memastikan bahwa objek yang diunggah ke bucket tersebut `bucket-owner-full-control` memiliki ACL

- Untuk mengizinkan Audit Manager mempublikasikan laporan dalam bucket S3 lintas akun, Anda harus menambahkan kebijakan bucket S3 berikut ke tujuan laporan penilaian Anda. Ganti *teks placeholder* dengan informasi Anda sendiri. `Principal`Elemen dalam kebijakan ini adalah pengguna atau peran yang memiliki penilaian dan membuat laporan penilaian. `Resource`Ini menentukan bucket S3 lintas akun tempat laporan diterbitkan.

```
{
  "Version": "2012-10-17",
  "Statement": [
      {
          "Sid": "Allow cross account assessment report publishing",
          "Effect": "Allow",
          "Principal": {
              "AWS":
 "arn:aws:iam::AssessmentOwnerAccountId:user/AssessmentOwnerUserName"
          },
          "Action": [
              "s3:ListBucket",
              "s3:PutObject",
              "s3:GetObject",
              "s3:GetBucketLocation",
              "s3:PutObjectAcl",
              "s3:DeleteObject"
          ],
          "Resource": [
              "arn:aws:s3:::CROSS-ACCOUNT-BUCKET",
              "arn:aws:s3:::CROSS-ACCOUNT-BUCKET/*"
          ]
      }
  ]
}
```

Pemberitahuan (opsional)

Audit Manager dapat mengirim notifikasi ke topik Amazon SNS yang Anda tentukan dalam setelan ini. Jika Anda berlangganan topik SNS tersebut, Anda akan menerima notifikasi saat masuk ke Audit Manager.

Anda dapat memperbarui setelan ini menggunakan konsol Audit Manager, AWS Command Line Interface (AWS CLI), atau Audit Manager API.

Audit Manager console

Untuk memperbarui setelan notifikasi (konsol)

1. Dari tab Pengaturan penilaian, buka bagian Pemberitahuan.
2. Untuk menggunakan topik SNS yang ada, pilih nama topik dari menu tarik-turun.
3. Untuk membuat topik SNS baru, pilih Buat topik baru.
4. Setelah selesai, pilih Simpan.

AWS CLI

Untuk memperbarui setelan notifikasi Anda (AWS CLI)

Jalankan perintah update-settings dan gunakan `--sns-topic` parameter untuk menentukan topik SNS.

Dalam contoh berikut, ganti *`teks placeholder dengan informasi`* Anda sendiri:

```
aws auditmanager update-settings --sns-topic arn:aws:sns:us-east-1:111122223333:my-assessment-topic
```

Audit Manager API

Untuk memperbarui setelan notifikasi (API)

Panggil UpdateSettingsoperasi dan gunakan parameter SNStopic untuk menentukan topik SNS.

> **Note**
>
> Anda dapat menggunakan topik SNS standar atau topik FIFO (first-in-first-out) SNS. Meskipun Audit Manager mendukung pengiriman pemberitahuan ke topik FIFO, urutan pengiriman pesan tidak dijamin.
> Jika Anda ingin menggunakan topik Amazon SNS yang tidak Anda miliki, konfigurasikan kebijakan AWS Identity and Access Management (IAM) Anda untuk ini. Lebih khusus lagi, Anda harus mengonfigurasinya untuk memungkinkan penerbitan dari Amazon Resource Name (ARN) topik. Untuk informasi selengkapnya tentang IAM, lihat Identitas dan manajemen akses untuk AWS Audit Manager.

Untuk mempelajari lebih lanjut tentang daftar tindakan yang memanggil notifikasi di Audit Manager, lihatNotifikasi di AWS Audit Manager.

Untuk petunjuk tentang cara membuat topik Amazon SNS, lihat Membuat topik Amazon SNS di Panduan Pengguna Amazon SNS.

Pengaturan pencari bukti

Gunakan tab ini untuk meninjau dan memperbarui pengaturan pencari bukti Anda.

Topik

Pencari bukti (opsional)

Kami sangat menyarankan agar Anda mengaktifkan pencari bukti. Mengaktifkan fitur ini diperlukan jika Anda ingin menjalankan kueri penelusuran pada bukti Anda.

Ikuti langkah-langkah ini untuk mengaktifkan, menonaktifkan, atau memeriksa status pencari bukti.

Aktifkan pencari bukti

Anda harus mengaktifkan pencari bukti di setiap Wilayah AWS tempat Anda ingin mencari bukti. Jika Anda adalah administrator yang didelegasikan untuk Audit Manager, aktifkan pencari bukti untuk mencari bukti untuk semua akun anggota di organisasi Anda.

Izin yang diperlukan untuk mengaktifkan pencari bukti

Untuk mengaktifkan pencari bukti, Anda memerlukan izin untuk membuat dan mengelola penyimpanan data acara di CloudTrail Lake. Untuk menggunakan fitur ini, Anda memerlukan izin untuk melakukan kueri CloudTrail Lake. Untuk contoh kebijakan izin yang dapat Anda gunakan, lihat Mengizinkan akses administrator penuh.

Jika Anda memerlukan bantuan dengan izin, hubungi AWS administrator Anda. Jika Anda seorang AWS administrator, Anda dapat menyalin pernyataan izin yang diperlukan dan melampirkannya ke kebijakan IAM.

Meminta untuk mengaktifkan pencari bukti

Anda dapat menyelesaikan tugas ini menggunakan konsol Audit Manager, AWS Command Line Interface (AWS CLI), atau Audit Manager API.

Audit Manager console

Untuk meminta mengaktifkan pencari bukti (konsol)

1. Buka konsol AWS Audit Manager di https://console.aws.amazon.com/auditmanager/home.
2. Dari tab Pengaturan pencari bukti, buka bagian Pencari bukti.
3. Pilih Kebijakan izin yang diperlukan, lalu Lihat izin CloudTrail Danau untuk melihat izin pencari bukti yang diperlukan. Jika Anda belum memiliki izin ini, Anda dapat menyalin pernyataan kebijakan ini dan melampirkannya ke kebijakan IAM.
4. Pilih Aktifkan.
5. Di jendela pop-up, pilih Permintaan untuk mengaktifkan.

AWS CLI

Untuk meminta mengaktifkan pencari bukti (AWS CLI)

Jalankan perintah update-settings dengan parameter. `--evidence-finder-enabled`

```
aws auditmanager update-settings --evidence-finder-enabled
```

Audit Manager API

Untuk meminta mengaktifkan pencari bukti (API)

Panggil UpdateSettingsoperasi dan gunakan evidenceFinderEnabledparameter.

Untuk informasi selengkapnya, pilih tautan sebelumnya untuk membaca selengkapnya di Referensi API Audit Manager. Ini termasuk informasi tentang cara menggunakan operasi dan parameter ini di salah satu SDK khusus bahasaAWS.

Konfirmasikan status pencari bukti

Setelah Anda mengirimkan permintaan Anda, dibutuhkan waktu hingga 10 menit untuk mengaktifkan pencari bukti dan membuat penyimpanan data acara. Segera setelah penyimpanan data acara dibuat, semua bukti baru dicerna ke dalam penyimpanan data acara bergerak maju.

Ketika pencari bukti diaktifkan dan penyimpanan data acara dibuat, kami mengisi kembali penyimpanan data acara yang baru dibuat dengan bukti masa lalu Anda hingga dua tahun. Proses ini terjadi secara otomatis dan membutuhkan waktu hingga tujuh hari untuk menyelesaikannya.

Anda dapat memeriksa status pencari bukti saat ini menggunakan konsol Audit Manager, Audit Manager APIAWS CLI, atau Audit Manager.

Audit Manager console

Untuk melihat status pencari bukti saat ini (konsol)

1. Buka konsol AWS Audit Manager di https://console.aws.amazon.com/auditmanager/home.
2. Pada panel navigasi kiri, pilih Pengaturan.
3. Di bawah Aktifkan pencari bukti — opsional, tinjau status saat ini.

   Setiap status didefinisikan sebagai berikut:

   - Pencari bukti tidak diaktifkan — Anda belum berhasil mengaktifkan pencari bukti.
   - Anda telah meminta untuk mengaktifkan pencari bukti — Permintaan Anda sedang menunggu penyimpanan data acara yang sedang dibuat.
   - Pencari bukti diaktifkan - Penyimpanan data acara telah dibuat. Anda sekarang dapat menggunakan pencari bukti.

     Tergantung berapa banyak bukti yang Anda miliki, dibutuhkan hingga tujuh hari untuk mengisi kembali penyimpanan data acara baru dengan data bukti masa lalu Anda. Panel informasi biru menunjukkan bahwa pengisian ulang data sedang berlangsung. Jangan ragu untuk mulai menjelajahi pencari bukti sementara itu. Namun, perlu diingat bahwa tidak semua data tersedia sampai pengisian ulang selesai.
   - Anda telah meminta untuk menonaktifkan pencari bukti — Permintaan Anda sedang menunggu penyimpanan data acara dihapus.
   - Pencari bukti telah dinonaktifkan - Pencari bukti telah dinonaktifkan secara permanen dan penyimpanan data acara dihapus.

AWS CLI

Untuk melihat status pencari bukti saat ini (AWS CLI)

Jalankan perintah get-settings dengan `--attribute` parameter yang disetel ke. `EVIDENCE_FINDER_ENABLEMENT`

```
aws auditmanager get-settings --attribute EVIDENCE_FINDER_ENABLEMENT
```

Ini mengembalikan informasi berikut:

EnablementStatus

Atribut ini menunjukkan status pencari bukti saat ini.

- `ENABLE_IN_PROGRESS`— Anda meminta untuk mengaktifkan pencari bukti. Penyimpanan data peristiwa saat ini sedang dibuat untuk mendukung kueri pencari bukti.
- `ENABLED`— Penyimpanan data peristiwa telah dibuat dan pencari bukti diaktifkan. Sebaiknya tunggu tujuh hari hingga penyimpanan data acara diisi kembali dengan data bukti masa lalu Anda. Anda dapat menggunakan pencari bukti sementara itu, tetapi tidak semua data tersedia sampai pengisian ulang selesai.
- `DISABLE_IN_PROGRESS`— Anda meminta untuk menonaktifkan pencari bukti, dan permintaan Anda menunggu penyimpanan data acara dihapus.
- `DISABLED`— Anda menonaktifkan pencari bukti secara permanen dan penyimpanan data acara dihapus. Anda tidak dapat mengaktifkan kembali pencari bukti setelah titik ini.

BackfillStatus

Atribut ini menunjukkan status pengisian ulang data bukti saat ini.

- `NOT_STARTED`— Isi ulang belum dimulai.
- `IN_PROGRESS`— Isi ulang sedang berlangsung. Ini membutuhkan waktu hingga tujuh hari untuk menyelesaikannya, tergantung pada jumlah data bukti.
- `COMPLETED`— Isi ulang selesai. Semua bukti masa lalu Anda sekarang dapat ditanyakan.

Audit Manager API

Untuk melihat status pencari bukti (API) saat ini

Panggil GetSettingsoperasi dengan `attribute` parameter yang disetel ke`EVIDENCE_FINDER_ENABLEMENT`. Ini mengembalikan informasi berikut:

EnablementStatus

Atribut ini menunjukkan status pencari bukti saat ini.

- `ENABLE_IN_PROGRESS`- Anda meminta untuk mengaktifkan pencari bukti. Penyimpanan data peristiwa saat ini sedang dibuat untuk mendukung kueri pencari bukti.
- `ENABLED`- Sebuah penyimpanan data acara telah dibuat dan pencari bukti diaktifkan. Sebaiknya tunggu tujuh hari hingga penyimpanan data acara diisi kembali dengan data bukti masa lalu Anda. Anda dapat menggunakan pencari bukti sementara itu, tetapi tidak semua data tersedia sampai pengisian ulang selesai.
- `DISABLE_IN_PROGRESS`- Anda meminta untuk menonaktifkan pencari bukti, dan permintaan Anda menunggu penghapusan penyimpanan data acara.
- `DISABLED`- Anda menonaktifkan pencari bukti secara permanen dan penyimpanan data acara dihapus. Anda tidak dapat mengaktifkan kembali pencari bukti setelah titik ini.

BackfillStatus

Atribut ini menunjukkan status pengisian ulang data bukti saat ini.

- `NOT_STARTED`berarti bahwa pengurukan belum dimulai.
- `IN_PROGRESS`berarti bahwa isi ulang sedang berlangsung. Ini membutuhkan waktu hingga tujuh hari untuk menyelesaikannya, tergantung pada jumlah data bukti.
- `COMPLETED`berarti bahwa isi ulang selesai. Semua bukti masa lalu Anda sekarang dapat ditanyakan.

Untuk informasi selengkapnya, lihat evidenceFinderEnablementdi Referensi API Audit Manager.

Nonaktifkan pencari bukti

Jika Anda tidak lagi ingin menggunakan pencari bukti, Anda dapat menonaktifkan fitur ini kapan saja.

> **Warning**
>
> Menonaktifkan pencari bukti akan menghapus penyimpanan data peristiwa CloudTrail Lake yang dibuat Audit Manager. Akibatnya, Anda tidak dapat mengaktifkan kembali fitur tersebut. Untuk menggunakan kembali pencari bukti setelah Anda menonaktifkannya, Anda harus

menonaktifkannya AWS Audit Manager, dan kemudian mengaktifkan kembali layanan sepenuhnya.

Izin yang diperlukan untuk menonaktifkan pencari bukti

Untuk menonaktifkan pencari bukti, Anda memerlukan izin untuk menghapus penyimpanan data peristiwa di CloudTrail Lake. Untuk contoh kebijakan yang dapat Anda gunakan, lihat Izin untuk menonaktifkan pencari bukti.

Jika Anda memerlukan bantuan dengan izin, hubungi AWS administrator Anda. Jika Anda seorang AWS administrator, Anda dapat melampirkan pernyataan izin yang diperlukan ke kebijakan IAM.

Menonaktifkan pencari bukti

Anda dapat menyelesaikan tugas ini menggunakan konsol Audit Manager, AWS Command Line Interface (AWS CLI), atau Audit Manager API.

Audit Manager console

Untuk menonaktifkan pencari bukti (konsol)

1. Di bagian Pencari bukti pada halaman pengaturan Audit Manager, pilih Nonaktifkan.
2. Di jendela pop-up yang muncul, masukkan **`Yes`** untuk mengonfirmasi keputusan Anda.
3. Pilih Permintaan untuk menonaktifkan.

AWS CLI

Untuk menonaktifkan pencari bukti (AWS CLI)

Jalankan perintah update-settings dengan parameter. `--no-evidence-finder-enabled`

```
aws auditmanager update-settings --no-evidence-finder-enabled
```

Audit Manager API

Untuk menonaktifkan pencari bukti (API)

Panggil UpdateSettingsoperasi dan gunakan evidenceFinderEnabledparameter.

Untuk informasi selengkapnya, pilih tautan sebelumnya untuk membaca selengkapnya di Referensi API Audit Manager. Ini termasuk informasi tentang cara menggunakan operasi dan parameter ini di salah satu SDK khusus bahasaAWS.

Tujuan ekspor (opsional)

Saat menjalankan kueri di pencari bukti, Anda dapat mengekspor hasil penelusuran ke file nilai yang dipisahkan koma (CSV). Gunakan pengaturan ini untuk memilih bucket S3 default tempat Audit Manager menyimpan file yang diekspor.

Anda dapat memperbarui setelan ini menggunakan konsol Audit Manager, AWS Command Line Interface (AWS CLI), atau Audit Manager API.

> **Important**
>
> Bucket S3 Anda harus memiliki kebijakan izin yang diperlukan agar CloudTrail dapat menulis file ekspor ke dalamnya. Lebih khusus lagi, kebijakan bucket harus menyertakan `s3:PutObject` tindakan dan bucket ARN, dan daftar CloudTrail sebagai kepala layanan. Kami memberikan contoh kebijakan izin yang dapat Anda gunakan. Untuk petunjuk tentang cara melampirkan kebijakan ini ke bucket S3, lihat Menambahkan kebijakan bucket menggunakan konsol Amazon S3.
> Untuk tips selengkapnya, lihat tips konfigurasi untuk tujuan ekspor Anda di halaman ini.

Audit Manager console

Untuk memperbarui setelan tujuan ekspor (konsol)

1. Dari tab Pengaturan pencari bukti, buka bagian tujuan Ekspor.
2. Pilih salah satu opsi berikut:
   - Jika Anda ingin menghapus bucket S3 saat ini, pilih Hapus untuk menghapus pengaturan Anda.
   - Jika Anda ingin menyimpan bucket S3 default untuk pertama kalinya, lanjutkan ke langkah 3.
3. Tentukan bucket S3 tempat Anda ingin menyimpan file yang diekspor.
   - Pilih Browse S3 untuk memilih dari daftar bucket Anda.

- Atau, Anda dapat memasukkan URI bucket dalam format ini: **`s3://bucketname/prefix`**

> **Tip**
>
> Agar bucket tujuan tetap teratur, Anda dapat membuat folder opsional untuk ekspor CSV Anda. Untuk melakukannya, tambahkan garis miring (**`/`**) dan awalan ke nilai di kotak URI Sumber Daya (misalnya,). **`/evidenceFinderCSVExports`** Audit Manager kemudian menyertakan awalan ini saat menambahkan file CSV ke bucket, dan Amazon S3 menghasilkan jalur yang ditentukan oleh awalan. Untuk informasi selengkapnya tentang awalan di Amazon S3, lihat Mengatur objek di konsol Amazon S3 di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

4. Setelah selesai, pilih Simpan.

Untuk petunjuk tentang cara membuat bucket S3, lihat Membuat bucket di Panduan Pengguna Amazon S3.

AWS CLI

Untuk memperbarui setelan tujuan ekspor Anda (AWS CLI)

Jalankan perintah update-settings dan gunakan `--default-export-destination` parameter untuk menentukan bucket S3.

Dalam contoh berikut, ganti *`teks placeholder dengan informasi`* Anda sendiri:

```
aws auditmanager update-settings --default-export-destination
 destinationType=S3,destination=s3://doc-example-destination-bucket
```

Untuk petunjuk tentang cara membuat bucket S3, lihat create-bucket di Command Reference. AWS CLI

Audit Manager API

Untuk memperbarui setelan tujuan ekspor (API)

Panggil UpdateSettingsoperasi dan gunakan defaultExportDestinationparameter untuk menentukan bucket S3.

Untuk petunjuk tentang cara membuat bucket S3, lihat CreateBucketdi Referensi API Amazon S3.

Kiat konfigurasi untuk tujuan ekspor Anda

Untuk memastikan ekspor file berhasil, kami sarankan Anda memverifikasi konfigurasi berikut untuk tujuan ekspor Anda.

Wilayah AWS

Kunci Wilayah AWS yang dikelola pelanggan Anda (jika Anda memberikannya) harus sesuai dengan Wilayah penilaian Anda. Untuk petunjuk tentang cara mengubah kunci KMS, lihat setelan enkripsi data Audit Manager.

Ember S3 lintas akun

Menggunakan bucket S3 lintas akun sebagai tujuan ekspor Anda tidak didukung di konsol Audit Manager. Anda dapat menentukan bucket lintas akun menggunakan AWS CLI atau salah satu AWS SDK, tetapi untuk kesederhanaan, kami menyarankan Anda untuk tidak melakukan ini. Jika Anda memilih untuk menggunakan bucket S3 lintas akun sebagai tujuan ekspor Anda, pertimbangkan poin-poin berikut.

- Secara default, objek S3—seperti ekspor CSV—dimiliki oleh objek yang mengunggah objek. Akun AWS Anda dapat menggunakan setelan Kepemilikan Objek S3 untuk mengubah perilaku default ini, sehingga objek baru apa pun yang ditulis oleh akun dengan daftar kontrol akses (ACL) yang `bucket-owner-full-control` dikalengkan secara otomatis menjadi milik pemilik bucket.

  Meskipun ini bukan persyaratan, kami menyarankan Anda untuk membuat perubahan berikut pada pengaturan bucket lintas akun Anda. Membuat perubahan ini memastikan bahwa pemilik bucket memiliki kendali penuh atas file yang diekspor yang Anda publikasikan ke bucket mereka.

  - Setel kepemilikan objek bucket S3 ke pilihan pemilik bucket, bukan penulis objek default
  - Tambahkan kebijakan bucket untuk memastikan bahwa objek yang diunggah ke bucket tersebut `bucket-owner-full-control` memiliki ACL
- Untuk mengizinkan Audit Manager mengekspor file ke bucket S3 lintas akun, Anda harus menambahkan kebijakan bucket S3 berikut ke bucket tujuan ekspor. Ganti *`teks placeholder`* dengan informasi Anda sendiri. `Principal`Elemen dalam kebijakan ini adalah pengguna atau peran yang memiliki penilaian dan mengekspor file. `Resource`Ini menentukan bucket S3 lintas akun tempat file diekspor.

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

```
  "Statement": [
      {
          "Sid": "Allow cross account file exports",
          "Effect": "Allow",
          "Principal": {
              "AWS":
 "arn:aws:iam::AssessmentOwnerAccountId:user/AssessmentOwnerUserName"
          },
          "Action": [
              "s3:ListBucket",
              "s3:PutObject",
              "s3:GetObject",
              "s3:GetBucketLocation",
              "s3:PutObjectAcl",
              "s3:DeleteObject"
          ],
          "Resource": [
              "arn:aws:s3:::CROSS-ACCOUNT-BUCKET",
              "arn:aws:s3:::CROSS-ACCOUNT-BUCKET/*"
          ]
      }
  ]
}
```

Notifikasi di AWS Audit Manager

AWS Audit Managerdapat memberitahu Anda tentang tindakan pengguna melalui Amazon Simple Notification Service (Amazon SNS).

Audit Manager mengirimkan notifikasi saat salah satu peristiwa berikut terjadi:

- Pemilik audit mendelegasikan set kontrol untuk ditinjau.
- Seorang delegasi mengirimkan kontrol yang ditinjau kembali ke pemilik audit.
- Pemilik audit melengkapi peninjauan set kontrol.

Prasyarat

Sebelum Anda menyiapkan notifikasi Amazon SNS di Audit Manager, pastikan Anda menyelesaikan langkah-langkah berikut.

1. Buat topik di Amazon SNS jika Anda belum memilikinya. Untuk instruksi, lihat Membuat topik Amazon SNS dalam Panduan Developer Layanan Notifikasi Sederhana Amazon.
2. Berlangganan setidaknya satu titik akhir ke topik. Misalnya, jika Anda ingin menerima notifikasi melalui pesan teks, berlangganlah titik akhir SMS ke topik tersebut. Titik akhir SMS adalah nomor ponsel. Untuk menerima notifikasi melalui email, berlangganlah titik akhir email ke topik tersebut. Titik akhir email adalah alamat email.

   Untuk informasi lebih lanjut, lihat Memulai di Panduan Developer Amazon Simple Notification Service.
3. (Opsional) Jika topik Anda menggunakanAWS Key Management Service (OpsionalAWS KMS) untuk enkripsi sisi server (Opsional), Anda harus menambahkan izin untukAWS KMS key kebijakan. Untuk contoh kebijakan yang dapat Anda gunakan, lihat Izin untuk kunci KMS yang dilampirkan ke topik SNS.

Mengonfigurasi notifikasi diAWS Audit Manager

Ikuti langkah-langkah ini untuk mengonfigurasi notifikasi Anda diAWS Audit Manager.

Untuk mengonfigurasi notifikasi diAWS Audit Manager

1. Buka konsol AWS Audit Manager di https://console.aws.amazon.com/auditmanager/home.
2. Di panel navigasi kiri, pilih Pengaturan.
3. Pada Notifikasi - Opsional, tentukan topik SNS yang ingin Anda gunakan untuk menerima notifikasi.
   - Untuk menggunakan topik yang ada, pilih nama topik dari menu tarik-turun.
   - Untuk membuat topik baru, pilih Buat topik baru. Ini membawa Anda ke konsol Amazon SNS tempat Anda dapat membuat topik.
4. Setelah selesai, pilih Simpan.

> **Catatan**
>
> - Anda dapat menggunakan topik SNS standar atau topik FIFO (first-in-first-out) SNS. Audit Manager mendukung pengiriman pemberitahuan ke topik FIFO. Namun, urutan pesan yang dikirim tidak dijamin.
> - Jika Anda ingin menggunakan topik Amazon SNS yang tidak dimiliki, Anda harus mengonfigurasi kebijakanAWS Identity and Access Management (IAM) Anda. Lebih khusus lagi, Anda harus mengonfigurasi kebijakan Anda untuk mengizinkan publikasi dari Amazon Resource Name (ARN) dari topik tersebut. Untuk informasi lebih lanjut, lihat Identity and access management untukAWS Audit Manager.

Pemecahan Masalah

Untuk menemukan jawaban atas pertanyaan dan masalah umum, lihat Memecahkan masalah pemberitahuan di bagian Pemecahan Masalah pada panduan ini.

Pemecahan masalah di AWS Audit Manager

Anda dapat menggunakan informasi berikut untuk memecahkan masalah yang Anda temui saat bekerja dengan. AWS Audit Manager

Jika masalah yang Anda temui berada di luar cakupan informasi berikut, atau jika masih ada setelah Anda mencoba menyelesaikannya, hubungi AWS Support.

Topik

Pemecahan masalah penilaian dan pengumpulan bukti

Anda dapat menggunakan informasi di halaman ini untuk menyelesaikan masalah penilaian umum dan pengumpulan bukti di Audit Manager.

Topik

- Apa yang terjadi jika saya menghapus akun dalam lingkup dari organisasi saya?
- Saya tidak dapat mengedit layanan dalam ruang lingkup untuk penilaian saya
- Apa perbedaan antara layanan dalam lingkup dan tipe sumber data?
- Pembuatan penilaian saya gagal
- Saya menonaktifkan dan kemudian mengaktifkan kembali Audit Manager, dan sekarang penilaian saya yang sudah ada sebelumnya tidak lagi mengumpulkan bukti

Saya membuat penilaian tetapi saya belum dapat melihat bukti apa pun

Jika Anda tidak dapat melihat bukti apa pun, kemungkinan Anda tidak menunggu setidaknya 24 jam setelah Anda membuat penilaian atau ada kesalahan konfigurasi.

Kami menyarankan Anda memeriksa hal-hal berikut:

1. Pastikan 24 jam berlalu sejak Anda membuat penilaian. Bukti otomatis tersedia 24 jam setelah Anda membuat penilaian.
2. Pastikan bahwa Anda menggunakan Audit Manager Wilayah AWS sama dengan Layanan AWS yang Anda harapkan untuk melihat buktinya.
3. Jika Anda berharap untuk melihat bukti pemeriksaan kepatuhan dari AWS Config danAWS Security Hub, pastikan bahwa konsol Security Hub AWS Config dan Security Hub menampilkan hasil untuk pemeriksaan ini. Hasil AWS Config dan Security Hub akan ditampilkan sama dengan Wilayah AWS yang Anda gunakan Audit Manager.

Jika Anda masih tidak dapat melihat bukti dalam penilaian Anda dan itu bukan karena salah satu masalah ini, periksa penyebab potensial lainnya yang dijelaskan di halaman ini.

Penilaian saya tidak mengumpulkan bukti pemeriksaan kepatuhan dari AWS Security Hub

Jika Anda tidak melihat bukti pemeriksaan kepatuhan untuk AWS Security Hub kontrol, ini bisa disebabkan oleh salah satu masalah berikut.

Konfigurasi tidak ada di AWS Security Hub

> Masalah ini dapat disebabkan jika Anda melewatkan beberapa langkah konfigurasi saat Anda mengaktifkanAWS Security Hub.

Pastikan Anda mengaktifkan Security Hub dan mengonfigurasi pengaturan Anda sebagai berikut.

Mengonfirmasi setelan Security Hub Anda untuk satu Akun AWS

Jika Anda menggunakan satuAkun AWS, periksa yang berikut ini:

- Konfirmasikan bahwa Anda mengaktifkan AWS Config dan mengonfigurasi perekaman sumber daya untuk akun Anda.
- Konfirmasikan bahwa Anda mengaktifkan standar keamanan PCI DSS untuk akun Anda.
- Konfirmasikan bahwa Anda mengaktifkan pengaturan temuan kontrol konsolidasi di Security Hub.

Mengonfirmasi setelan Security Hub untuk suatu organisasi

Jika Anda menggunakan Organizations, periksa hal berikut:

- Konfirmasikan bahwa Anda mengaktifkan AWS Config dan mengonfigurasi rekaman sumber daya untuk organisasi Anda.
- Konfirmasikan bahwa Anda mengaktifkan standar keamanan PCI DSS untuk setiap akun anggota organisasi.
- Konfirmasikan bahwa Anda mengaktifkan pengaturan temuan kontrol konsolidasi di Security Hub.
- Konfirmasikan bahwa akun administrator yang didelegasikan yang Anda gunakan di Security Hub sama dengan yang Anda gunakan di Audit Manager.
- Konfirmasikan bahwa Anda mengaktifkan akun organisasi sebagai akun anggota Security Hub.

Nama kontrol Security Hub dimasukkan secara tidak benar di **`ControlMappingSource`**

Bila Anda menggunakan Audit Manager API untuk membuat kontrol kustom, Anda dapat menentukan kontrol Security Hub sebagai pemetaan sumber data untuk pengumpulan bukti. Untuk melakukan ini, Anda memasukkan ID kontrol sebagai `keywordValue`.

Jika Anda tidak melihat bukti pemeriksaan kepatuhan untuk kontrol Security Hub, bisa jadi bukti tersebut salah `keywordValue` dimasukkan ke dalam Anda`ControlMappingSource`. `keywordValue`Ini peka huruf besar/kecil. Jika Anda salah memasukkannya, Audit Manager mungkin tidak mengenali aturan tersebut. Akibatnya, Anda mungkin tidak mengumpulkan bukti pemeriksaan kepatuhan untuk kontrol tersebut seperti yang diharapkan.

Untuk memperbaiki masalah ini, perbarui kontrol khusus dan revisi. `keywordValue` Format kata kunci Security Hub yang benar bervariasi. Untuk akurasi, rujuk daftar kata kunci kontrol Security Hub yang didukung.

`AuditManagerSecurityHubFindingsReceiver` EventBridge Aturan Amazon tidak ada

Saat Anda mengaktifkan Audit Manager, aturan bernama akan `AuditManagerSecurityHubFindingsReceiver` dibuat dan diaktifkan secara otomatis di Amazon EventBridge. Aturan ini memungkinkan Audit Manager mengumpulkan temuan Security Hub sebagai bukti.

Jika aturan ini tidak terdaftar dan diaktifkan di Wilayah AWS tempat Anda menggunakan Security Hub, Audit Manager tidak dapat mengumpulkan temuan Security Hub untuk Wilayah tersebut.

Untuk mengatasi masalah ini, buka EventBridge konsol dan konfirmasikan bahwa `AuditManagerSecurityHubFindingsReceiver` aturan ada di konsol AndaAkun AWS. Jika aturan tidak ada, kami sarankan Anda menonaktifkan Audit Manager dan kemudian mengaktifkan kembali layanan. Jika tindakan ini tidak menyelesaikan masalah, atau jika menonaktifkan Audit Manager bukan pilihan, hubungi AWS Support untuk bantuan.

AWS ConfigAturan terkait layanan yang dibuat oleh Security Hub

Perlu diingat bahwa Audit Manager tidak mengumpulkan bukti dari AWS Configaturan terkait layanan yang dibuat Security Hub. Ini adalah jenis AWS Config aturan terkelola tertentu yang diaktifkan dan dikendalikan oleh layanan Security Hub. Security Hub membuat instance aturan terkait layanan ini di AWS lingkungan Anda, meskipun instance lain dari aturan yang sama sudah ada. Akibatnya, untuk mencegah duplikasi bukti, Audit Manager tidak mendukung pengumpulan bukti dari aturan terkait layanan.

Penilaian saya tidak mengumpulkan bukti pemeriksaan kepatuhan dari AWS Config

Jika Anda tidak melihat bukti pemeriksaan kepatuhan untuk suatu AWS Config aturan, ini bisa disebabkan oleh salah satu masalah berikut.

Pengidentifikasi aturan dimasukkan secara tidak benar di **`ControlMappingSource`**

Saat menggunakan Audit Manager API untuk membuat kontrol kustom, Anda dapat menentukan AWS Config aturan sebagai pemetaan sumber data untuk pengumpulan bukti. `keywordValue`Yang Anda tentukan tergantung pada jenis aturan.

Jika Anda tidak melihat bukti pemeriksaan kepatuhan untuk suatu AWS Config aturan, bisa jadi `keywordValue` itu salah dimasukkan dalam aturan Anda`ControlMappingSource`. `keywordValue`Ini peka huruf besar/kecil. Jika Anda salah memasukkannya, Audit Manager mungkin tidak mengenali aturan tersebut. Akibatnya, Anda mungkin tidak mengumpulkan bukti pemeriksaan kepatuhan untuk aturan tersebut sebagaimana dimaksud.

Untuk memperbaiki masalah ini, perbarui kontrol khusus dan revisi. `keywordValue`

- Untuk aturan kustom, pastikan bahwa `keywordValue` memiliki `Custom_` awalan diikuti oleh nama aturan kustom. Format nama aturan kustom dapat bervariasi. Untuk akurasi, kunjungi AWS Configkonsol untuk memverifikasi nama aturan kustom Anda.
- Untuk aturan terkelola, pastikan bahwa itu `keywordValue` adalah pengenal aturan di`ALL_CAPS_WITH_UNDERSCORES`. Sebagai contoh, `CLOUDWATCH_LOG_GROUP_ENCRYPTED`. Untuk akurasi, rujuk daftar kata kunci aturan terkelola yang didukung.

> **Note**
>
> Untuk beberapa aturan terkelola, pengidentifikasi aturan berbeda dari nama aturan. Misalnya, pengidentifikasi aturan untuk restricted-ssh adalah. `INCOMING_SSH_DISABLED` Pastikan untuk menggunakan pengenal aturan, bukan nama aturan. Untuk menemukan pengenal aturan, pilih aturan dari daftar aturan terkelola dan cari nilai pengenalnya.

Aturannya adalah aturan terkait layanan AWS Config

Anda dapat menggunakan aturan terkelola dan aturan khusus sebagai pemetaan sumber data untuk pengumpulan bukti. Namun, Audit Manager tidak mengumpulkan bukti dari sebagian besar aturan terkait layanan.

Hanya ada dua jenis aturan terkait layanan yang Audit Manager mengumpulkan bukti dari:

- Aturan terkait layanan dari Paket Kesesuaian
- Aturan terkait layanan dari AWS Organizations

Audit Manager tidak mengumpulkan bukti dari aturan terkait layanan lainnya, khususnya aturan apa pun dengan Nama Sumber Daya Amazon (ARN) yang berisi awalan berikut: `arn:aws:config:*:*:config-rule/aws-service-rule/...`

Alasan Audit Manager tidak mengumpulkan bukti dari sebagian besar AWS Config aturan terkait layanan adalah untuk mencegah duplikat bukti dalam penilaian Anda. Aturan terkait layanan

adalah jenis aturan terkelola tertentu yang memungkinkan orang lain Layanan AWS membuat AWS Config aturan di akun Anda. Misalnya, beberapa kontrol Security Hub menggunakan aturan AWS Config terkait layanan untuk menjalankan pemeriksaan keamanan. Untuk setiap kontrol Security Hub yang menggunakan AWS Config aturan terkait layanan, Security Hub membuat instance dari AWS Config aturan yang diperlukan di lingkungan AndaAWS. Ini terjadi bahkan jika aturan asli sudah ada di akun Anda. Oleh karena itu, untuk menghindari pengumpulan bukti yang sama dari aturan yang sama dua kali, Audit Manager mengabaikan aturan terkait layanan dan tidak mengumpulkan bukti darinya.

AWS Configtidak diaktifkan dan disertakan sebagai layanan dalam cakupan

AWS Configharus diaktifkan di AndaAkun AWS. Itu juga harus dimasukkan sebagai layanan dalam ruang lingkup penilaian Anda. Setelah Anda mengatur dengan AWS Config cara ini, Audit Manager mengumpulkan bukti setiap kali evaluasi AWS Config aturan terjadi.

Pertama, pastikan bahwa Anda mengaktifkan AWS Config diAkun AWS. Untuk petunjuk, lihat Mengaktifkan dan mengatur AWS Config.

Selanjutnya, pastikan bahwa Anda termasuk AWS Config sebagai layanan dalam ruang lingkup penilaian Anda. Untuk meninjau layanan saat ini dalam cakupan penilaian Anda, lihat Tinjau penilaian, Layanan AWS tab. Untuk mengedit daftar layanan dalam lingkup penilaian, lihat Mengedit Layanan AWS dalam cakupan.

AWS ConfigAturan mengevaluasi konfigurasi sumber daya sebelum Anda menyiapkan penilaian

Jika AWS Config aturan Anda disiapkan untuk mengevaluasi perubahan konfigurasi untuk sumber daya tertentu, Anda mungkin melihat ketidakcocokan antara evaluasi AWS Config dan bukti di Audit Manager. Hal ini terjadi jika evaluasi aturan terjadi sebelum Anda mengatur kontrol dalam penilaian Audit Manager Anda. Dalam hal ini, Audit Manager tidak menghasilkan bukti sampai sumber daya yang mendasarinya mengubah status lagi dan memicu evaluasi ulang aturan.

Sebagai solusinya, Anda dapat menavigasi ke aturan di AWS Config konsol dan mengevaluasi ulang aturan secara manual. Ini memanggil evaluasi baru dari semua sumber daya yang berkaitan dengan aturan itu.

Penilaian saya tidak mengumpulkan bukti aktivitas pengguna dari AWS CloudTrail

Bila Anda menggunakan Audit Manager API untuk membuat kontrol kustom, Anda dapat menentukan nama CloudTrail peristiwa sebagai pemetaan sumber data untuk pengumpulan bukti. Untuk melakukannya, Anda memasukkan nama acara sebagai `keywordValue`.

Jika Anda tidak melihat bukti aktivitas pengguna untuk suatu CloudTrail peristiwa, bisa jadi bukti tersebut salah `keywordValue` dimasukkan ke dalam acara Anda`ControlMappingSource`. `keywordValue`Ini peka huruf besar/kecil. Jika Anda salah memasukkannya, Audit Manager mungkin tidak mengenali nama acara. Akibatnya, Anda mungkin tidak mengumpulkan bukti aktivitas pengguna untuk peristiwa tersebut sebagaimana dimaksud.

Untuk memperbaiki masalah ini, perbarui kontrol khusus dan revisi. `keywordValue` Pastikan bahwa acara tersebut ditulis sebagai`serviceprefix_ActionName`. Sebagai contoh, `cloudtrail_StartLogging`. Untuk akurasi, tinjau Layanan AWS awalan dan nama tindakan di Referensi Otorisasi Layanan.

Penilaian saya tidak mengumpulkan bukti data konfigurasi untuk panggilan AWS API

Saat menggunakan Audit Manager API untuk membuat kontrol kustom, Anda dapat menentukan panggilan AWS API sebagai pemetaan sumber data untuk pengumpulan bukti. Untuk melakukannya, Anda memasukkan panggilan API sebagai `keywordValue`.

Jika Anda tidak melihat bukti data konfigurasi untuk panggilan AWS API, bisa jadi kesalahan `keywordValue` dimasukkan ke dalam panggilan Anda`ControlMappingSource`. `keywordValue`Kasus sensitif. Jika Anda salah memasukkannya, Audit Manager mungkin tidak mengenali panggilan API. Akibatnya, Anda mungkin tidak mengumpulkan bukti data konfigurasi untuk panggilan API tersebut sebagaimana dimaksud.

Untuk memperbaiki masalah ini, perbarui kontrol khusus dan revisi. `keywordValue` Pastikan bahwa panggilan API ditulis sebagai`serviceprefix_ActionName`. Sebagai contoh, `iam_ListGroups`. Untuk akurasi, rujuk daftar panggilan API yang didukung.

Penilaian saya tidak mengumpulkan bukti dari yang lain Layanan AWS

Jika Layanan AWS tidak dipilih sebagai cakupan penilaian Anda, Audit Manager tidak mengumpulkan bukti dari sumber daya yang terkait dengan layanan tersebut. Ini juga terjadi jika an Layanan AWS dipilih tetapi Anda belum mengaktifkannya di lingkungan Anda.

Jika Anda membuat penilaian dari kerangka kerja khusus, Anda dapat mengedit layanan dalam ruang lingkup penilaian Anda. Anda kemudian dapat menentukan tambahan Layanan AWS yang ingin Anda kumpulkan bukti. Setelah Anda menambahkan layanan ini, bukti akan tersedia setelah 24 jam.

> **Note**
>
> Jika Anda membuat penilaian dari kerangka kerja standar, daftar Layanan AWS dalam lingkup telah dipilih sebelumnya dan tidak dapat diedit. Ini karena ketika Anda membuat penilaian dari kerangka kerja standar, Audit Manager secara otomatis memetakan dan memilih sumber data dan layanan yang relevan untuk Anda. Pemilihan dilakukan berdasarkan persyaratan kerangka standar. Perhatikan bahwa, untuk kerangka kerja standar yang hanya berisi kontrol manual, tidak Layanan AWS ada ruang lingkup.
> Solusi untuk mengedit lingkup Layanan AWS in sambil tetap membuat penilaian berdasarkan kerangka kerja standar adalah dengan menyesuaikan kerangka kerja standar. Dengan menggunakan solusi ini, Anda dapat menggunakan kerangka kerja yang Anda sesuaikan untuk membuat penilaian baru. Dalam penilaian ini, Anda kemudian dapat menentukan mana yang Layanan AWS berada dalam ruang lingkup.

Bukti saya dihasilkan pada interval yang berbeda, dan saya tidak yakin seberapa sering dikumpulkan

Kontrol dalam penilaian Audit Manager dipetakan ke berbagai sumber data. Setiap sumber data memiliki frekuensi pengumpulan bukti yang berbeda. Akibatnya, tidak ada one-size-fits-all jawaban untuk seberapa sering bukti dikumpulkan. Beberapa sumber data mengevaluasi kepatuhan, sedangkan yang lain hanya menangkap status sumber daya dan mengubah data tanpa penentuan kepatuhan.

Berikut ini adalah ringkasan dari berbagai jenis sumber data dan seberapa sering mereka mengumpulkan bukti.

Jenis sumber data	Deskripsi	Frekuensi pengumpulan bukti	Ketika kontrol ini aktif dalam penilaian
AWS CloudTrail	Melacak aktivitas pengguna tertentu.	Terus menerus	Audit Manager memfilter CloudTrail log Anda berdasarkan kata kunci yang Anda pilih. Log yang diproses diimpor sebagai bukti aktivitas Pengguna.
AWS Security Hub	Menangkap snapshot postur keamanan sumber daya Anda dengan melaporkan temuan dari Security Hub.	Berdasarkan jadwal pemeriksaan Security Hub (biasanya sekitar setiap 12 jam)	Audit Manager mengambil temuan keamanan langsung dari Security Hub. Temuan ini diimpor sebagai bukti pemeriksaan Kepatuhan.
AWS Config	Menangkap snapshot dari postur keamanan sumber daya Anda dengan melaporkan temuan dari. AWS Config	Berdasarkan pengaturan yang didefinisikan dalam AWS Config aturan	Audit Manager mengambil evaluasi aturan langsung dariAWS Config. Evaluasi diimpor sebagai bukti pemeriksaan Kepatuhan.
AWSPanggilan API	Mengambil snapshot konfigurasi sumber daya Anda secara langsung melalui panggilan API ke yang ditentukanLayanan AWS.	Harian, mingguan, atau bulanan	Audit Manager membuat panggilan API berdasarkan frekuensi yang Anda tentukan. Respons diimpor sebagai bukti data Konfigurasi.

Terlepas dari frekuensi pengumpulan bukti, bukti baru dikumpulkan secara otomatis selama penilaian aktif. Untuk informasi lebih lanjut, lihat Frekuensi pengumpulan bukti.

Untuk mempelajari lebih lanjut, lihat Sumber data kontrol yang didukung untuk bukti otomatis dan Mengubah frekuensi pengumpulan bukti untuk kontrol.

Apa yang terjadi jika saya menghapus akun dalam lingkup dari organisasi saya?

Ketika akun dalam cakupan dihapus dari organisasi Anda, Audit Manager tidak lagi mengumpulkan bukti untuk akun tersebut. Namun, akun terus ditampilkan dalam penilaian Anda di bawah Akun AWStab. Untuk menghapus akun dari daftar akun dalam ruang lingkup, edit penilaian. Akun yang dihapus tidak lagi ditampilkan dalam daftar selama pengeditan, dan Anda dapat menyimpan perubahan tanpa cakupan akun itu.

Saya tidak dapat mengedit layanan dalam ruang lingkup untuk penilaian saya

Saat Anda menggunakan konsol Audit Manager untuk membuat penilaian dari kerangka kerja standar, daftar lingkup Layanan AWS dalam dipilih secara default. Daftar ini tidak dapat diedit. Ini karena Audit Manager secara otomatis memetakan dan memilih sumber data dan layanan untuk Anda. Pemilihan ini dibuat sesuai dengan persyaratan kerangka standar. Jika kerangka kerja standar yang Anda pilih hanya berisi kontrol manual, tidak Layanan AWS ada dalam cakupan penilaian Anda, dan Anda tidak dapat menambahkan layanan apa pun ke penilaian Anda.

Jika Anda perlu mengedit daftar layanan dalam cakupan, gunakan operasi UpdateAssessmentAPI yang disediakan oleh Audit Manager. Atau, Anda dapat menyesuaikan kerangka kerja standar dan kemudian membuat penilaian dari kerangka kerja khusus.

Apa perbedaan antara layanan dalam lingkup dan tipe sumber data?

Layanan dalam lingkup adalah layanan Layanan AWS yang ditentukan sebagai bagian dari penilaian Anda. Ketika layanan berada dalam ruang lingkup, Audit Manager mengumpulkan bukti tentang penggunaan Anda atas layanan tersebut dan sumber dayanya.

Tipe sumber data menunjukkan dari mana tepatnya bukti dikumpulkan. Jika Anda mengunggah bukti Anda sendiri, tipe sumber datanya adalah Manual. Jika Audit Manager mengumpulkan bukti, sumber data dapat menjadi salah satu dari empat jenis.

1. AWS Security Hub— Menangkap snapshot postur keamanan sumber daya Anda dengan melaporkan temuan dari Security Hub.
2. AWS Config— Menangkap snapshot dari postur keamanan sumber daya Anda dengan melaporkan temuan dari. AWS Config
3. AWS CloudTrail— Melacak aktivitas pengguna tertentu untuk sumber daya.
4. AWSPanggilan API — Mengambil snapshot konfigurasi sumber daya Anda secara langsung melalui panggilan API ke spesifikLayanan AWS.

Berikut adalah dua contoh untuk menggambarkan perbedaan antara layanan dalam lingkup dan tipe sumber data.

Contoh 1

Katakanlah Anda ingin mengumpulkan bukti untuk kontrol yang diberi nama 4.1.2 - Larang akses tulis publik ke bucket S3. Kontrol ini memeriksa tingkat akses kebijakan bucket S3 Anda. Untuk kontrol ini, Audit Manager menggunakan AWS Config aturan khusus (s3- bucket-public-write-prohibited) untuk mencari evaluasi bucket S3 Anda. Dalam contoh ini, berikut ini benar:

- Layanan dalam cakupan adalah Amazon S3
- Sumber daya yang sedang dinilai adalah bucket S3 Anda
- Tipe sumber datanya adalah AWS Config
- Pemetaan sumber data adalah AWS Config aturan khusus () `s3-bucket-public-write-prohibited`

Contoh 2

Katakanlah Anda ingin mengumpulkan bukti untuk kontrol HIPAA yang diberi nama 164.308 (a) (5) (ii) (C). Kontrol ini memerlukan prosedur pemantauan untuk mendeteksi login yang tidak tepat. Untuk kontrol ini, Audit Manager menggunakan CloudTrail log untuk mencari semua peristiwa login AWS Management Console. Dalam contoh ini, berikut ini benar:

- Layanan dalam lingkup adalah IAM
- Sumber daya yang sedang dinilai adalah pengguna Anda
- Tipe sumber datanya adalah CloudTrail
- Pemetaan sumber data adalah CloudTrail peristiwa tertentu () `ConsoleLogin`

Pembuatan penilaian saya gagal

Jika pembuatan penilaian Anda gagal, itu bisa jadi karena Anda memilih terlalu banyak Akun AWS dalam lingkup penilaian Anda. Jika Anda menggunakanAWS Organizations, Audit Manager dapat mendukung hingga sekitar 150 akun anggota dalam lingkup penilaian tunggal. Jika Anda melebihi angka ini, pembuatan penilaian mungkin gagal. Sebagai solusinya, Anda dapat menjalankan beberapa penilaian dengan cakupan akun berbeda untuk setiap penilaian.

Saya menonaktifkan dan kemudian mengaktifkan kembali Audit Manager, dan sekarang penilaian saya yang sudah ada sebelumnya tidak lagi mengumpulkan bukti

Saat Anda menonaktifkan Audit Manager dan memilih untuk tidak menghapus data, penilaian yang ada akan beralih ke keadaan tidak aktif dan berhenti mengumpulkan bukti. Ini berarti bahwa ketika Anda mengaktifkan kembali Audit Manager, penilaian yang Anda buat sebelumnya tetap tersedia. Namun, mereka tidak secara otomatis melanjutkan pengumpulan bukti.

Untuk mulai mengumpulkan bukti lagi untuk penilaian yang sudah ada sebelumnya, edit penilaian dan pilih Simpan tanpa membuat perubahan apa pun.

Memecahkan masalah laporan penilaian

Anda dapat menggunakan informasi di halaman ini untuk menyelesaikan masalah laporan penilaian umum di Audit Manager.

Topik

- Laporan penilaian saya gagal dihasilkan
- Saya mengikuti daftar periksa di atas, dan laporan penilaian saya masih gagal dihasilkan
- Saya mendapatkan kesalahan akses ditolak ketika saya mencoba membuat laporan
- Saya tidak dapat membuka zip laporan penilaian
- Ketika saya memilih nama bukti dalam laporan, saya tidak diarahkan ke rincian bukti
- Pembuatan laporan penilaian saya macet dalam status Sedang berlangsung, dan saya tidak yakin bagaimana pengaruhnya terhadap penagihan saya
- Lihat juga

Laporan penilaian saya gagal dihasilkan

Laporan penilaian Anda mungkin gagal dihasilkan karena sejumlah alasan. Anda dapat mulai memecahkan masalah ini dengan memeriksa penyebab yang paling sering. Gunakan daftar periksa berikut untuk memulai.

1. Periksa apakah ada Wilayah AWS informasi Anda yang tidak cocok:
   a. Apakah kunci Wilayah AWS yang dikelola pelanggan Anda sesuai dengan Wilayah AWS penilaian Anda?

      Jika Anda memberikan kunci KMS Anda sendiri untuk enkripsi data Audit Manager, kuncinya harus Wilayah AWS sama dengan penilaian Anda. Untuk mengatasi masalah ini, ubah kunci KMS ke kunci yang berada di Wilayah yang sama dengan penilaian Anda. Untuk petunjuk tentang cara mengubah kunci KMS, lihat AWS Audit Managerpengaturan, Enkripsi data.

   b. Apakah kunci Wilayah AWS yang dikelola pelanggan Anda cocok dengan bucket S3 Anda? Wilayah AWS

      Jika Anda memberikan kunci KMS sendiri untuk enkripsi data Audit Manager, kunci harus sama Wilayah AWS dengan bucket S3 yang Anda gunakan sebagai tujuan laporan penilaian Anda. Untuk mengatasi masalah ini, Anda dapat mengubah kunci KMS atau bucket S3 sehingga keduanya berada di Wilayah yang sama dengan penilaian Anda. Untuk petunjuk tentang cara mengubah kunci KMS, lihat AWS Audit Managerpengaturan, Enkripsi data. Untuk petunjuk tentang cara mengubah bucket S3, lihat AWS Audit Managerpengaturan, Tujuan laporan penilaian.

2. Periksa izin bucket S3 yang Anda gunakan sebagai tujuan laporan penilaian:
   a. Apakah entitas IAM yang menghasilkan laporan penilaian memiliki izin yang diperlukan untuk bucket S3?

      Entitas IAM harus memiliki izin bucket S3 yang diperlukan untuk mempublikasikan laporan di bucket tersebut. Kami memberikan contoh kebijakan yang dapat Anda gunakan. Untuk petunjuk tentang cara menentukan bucket S3 yang berbeda, lihat AWS Audit Managerpengaturan, Tujuan laporan penilaian.

   b. Apakah bucket S3 memiliki kebijakan bucket yang memerlukan enkripsi sisi server (SSE) menggunakan SSE-KMS?

      Jika ya, kunci KMS yang digunakan dalam kebijakan bucket tersebut harus cocok dengan kunci KMS yang ditentukan dalam setelan enkripsi data Audit Manager Anda. Jika Anda

tidak mengonfigurasi kunci KMS di setelan Audit Manager, dan kebijakan bucket S3 Anda memerlukan SSE, pastikan kebijakan bucket mengizinkan SSE-S3. Untuk petunjuk tentang cara mengubah kunci KMS, lihat AWS Audit Managerpengaturan, Enkripsi data. Untuk petunjuk tentang cara mengubah bucket S3, lihat AWS Audit Managerpengaturan, Tujuan laporan penilaian.

Jika Anda masih tidak berhasil membuat laporan penilaian, tinjau masalah berikut di halaman ini.

Saya mengikuti daftar periksa di atas, dan laporan penilaian saya masih gagal dihasilkan

Audit Manager membatasi berapa banyak bukti yang dapat Anda tambahkan ke laporan penilaian. Batasannya didasarkan pada Wilayah AWS penilaian Anda, Wilayah bucket S3 yang digunakan sebagai tujuan laporan penilaian Anda, dan apakah penilaian Anda menggunakan pelanggan yang dikelolaAWS KMS key.

1. Batasnya adalah 22.000 untuk laporan wilayah yang sama (di mana bucket dan penilaian S3 sama) Wilayah AWS
2. Batasnya adalah 3.500 untuk laporan Lintas wilayah (di mana bucket dan penilaian S3 berbeda) Wilayah AWS
3. Batasnya adalah 3.500 jika penilaian menggunakan kunci KMS yang dikelola pelanggan

Jika Anda mencoba membuat laporan yang berisi lebih banyak bukti dari ini, operasi mungkin gagal.

Sebagai solusinya, Anda dapat menghasilkan beberapa laporan penilaian daripada satu laporan penilaian yang lebih besar. Dengan melakukan ini, Anda dapat mengekspor bukti dari penilaian Anda ke dalam batch berukuran lebih mudah dikelola.

Saya mendapatkan kesalahan akses ditolak ketika saya mencoba membuat laporan

Anda akan mendapatkan `access denied` kesalahan jika penilaian Anda dibuat oleh akun administrator yang didelegasikan bahwa kunci KMS yang ditentukan dalam pengaturan Audit Manager Anda bukan milik. Untuk menghindari kesalahan ini, saat Anda menunjuk administrator yang didelegasikan untuk Audit Manager, pastikan akun administrator yang didelegasikan memiliki akses pada kunci KMS yang Anda berikan saat menyiapkan Audit Manager.

Anda mungkin juga menerima `access denied` kesalahan jika tidak memiliki izin menulis untuk bucket S3 yang Anda gunakan sebagai tujuan laporan penilaian.

Jika Anda mendapatkan `access denied` kesalahan, pastikan Anda memenuhi persyaratan berikut:

- Kunci KMS Anda di setelan Audit Manager memberikan izin kepada administrator yang didelegasikan. Anda dapat mengonfigurasinya dengan mengikuti petunjuk di Mengizinkan pengguna di akun lain menggunakan kunci KMS di Panduan AWS Key Management Service Pengembang. Untuk petunjuk tentang cara meninjau dan mengubah setelan enkripsi Anda di Audit Manager, lihat Enkripsi data.
- Anda memiliki kebijakan izin yang memberi Anda akses menulis untuk bucket S3 yang Anda gunakan sebagai tujuan laporan penilaian. Lebih khusus lagi, kebijakan izin Anda berisi `s3:PutObject` tindakan, menentukan ARN bucket S3, dan menyertakan kunci KMS yang digunakan untuk mengenkripsi laporan penilaian Anda. Untuk contoh kebijakan yang dapat Anda gunakan, lihat Contoh kebijakan berbasis identitas untuk. AWS Audit Manager

> **Note**
>
> Jika Anda mengubah setelan enkripsi data Audit Manager, perubahan ini berlaku untuk penilaian baru yang Anda buat selanjutnya. Ini termasuk laporan penilaian apa pun yang Anda buat dari penilaian baru Anda.
> Perubahan tidak berlaku untuk penilaian yang sudah ada yang Anda buat sebelum mengubah setelan enkripsi. Ini termasuk laporan penilaian baru yang Anda buat dari penilaian yang ada, selain laporan penilaian yang ada. Penilaian yang ada — dan semua laporan penilaian mereka — terus menggunakan kunci KMS lama. Jika identitas IAM yang menghasilkan laporan penilaian tidak memiliki izin untuk menggunakan kunci KMS lama, Anda dapat memberikan izin di tingkat kebijakan utama.

Saya tidak dapat membuka zip laporan penilaian

Jika Anda tidak dapat membuka zip laporan penilaian di Windows, kemungkinan Windows Explorer tidak dapat mengekstraknya karena jalur filenya memiliki beberapa folder bersarang atau nama panjang. Ini karena, di bawah sistem penamaan file Windows, jalur folder, nama file, dan ekstensi file tidak dapat melebihi 259 karakter. Jika tidak, ini menghasilkan `Destination Path Too Long` kesalahan.

Untuk mengatasi masalah ini, coba pindahkan file zip ke folder induk dari lokasi saat ini. Anda kemudian dapat mencoba lagi untuk mengekstraknya dari sana. Atau, Anda juga dapat mencoba memperpendek nama file zip atau mengekstraknya ke lokasi lain yang memiliki jalur file yang lebih pendek.

Ketika saya memilih nama bukti dalam laporan, saya tidak diarahkan ke rincian bukti

Masalah ini mungkin terjadi jika Anda berinteraksi dengan laporan penilaian di browser, atau menggunakan pembaca PDF default yang diinstal pada sistem operasi Anda. Beberapa browser dan pembaca PDF default sistem tidak mengizinkan pembukaan tautan relatif. Ini berarti bahwa, meskipun hyperlink mungkin berfungsi dalam ringkasan laporan penilaian PDF (seperti nama kontrol hyperlink dalam daftar isi), hyperlink diabaikan saat Anda mencoba menavigasi dari PDF ringkasan penilaian ke PDF detail bukti terpisah.

Jika Anda mengalami masalah ini, kami sarankan Anda menggunakan pembaca PDF khusus untuk berinteraksi dengan laporan penilaian Anda. Untuk pengalaman yang andal, kami sarankan Anda menginstal dan menggunakan Adobe Acrobat Reader, yang dapat Anda unduh di situs web Adobe. Pembaca PDF lainnya juga tersedia, tetapi Adobe Acrobat Reader telah terbukti bekerja secara konsisten dan andal dengan laporan penilaian Audit Manager.

Pembuatan laporan penilaian saya macet dalam status Sedang berlangsung, dan saya tidak yakin bagaimana pengaruhnya terhadap penagihan saya

Pembuatan laporan penilaian tidak berdampak pada penagihan. Anda hanya ditagih berdasarkan bukti yang dikumpulkan penilaian Anda. Untuk informasi selengkapnya tentang harga, lihat AWS Audit Manager Harga.

Lihat juga

Halaman-halaman berikut berisi panduan pemecahan masalah tentang membuat laporan penilaian dari pencari bukti:

- Saya tidak dapat membuat beberapa laporan penilaian dari hasil pencarian saya
- Saya tidak dapat menambahkan hasil pencarian individual ke laporan penilaian
- Tidak semua hasil pencari bukti saya termasuk dalam laporan penilaian

- Saya ingin membuat laporan penilaian dari hasil pencarian saya, tetapi pernyataan kueri saya gagal

Memecahkan masalah kontrol dan pengaturan kontrol

Anda dapat menggunakan informasi di halaman ini untuk mengatasi masalah umum dengan kontrol di Audit Manager.

Masalah umum

- Saya tidak dapat melihat kontrol atau set kontrol apa pun dalam penilaian saya
- Saya tidak dapat mengunggah bukti manual ke kontrol

AWS Configmasalah integrasi

- Saya perlu menggunakan beberapa AWS Config aturan sebagai sumber data untuk satu kontrol
- Opsi aturan khusus tidak tersedia saat saya mengonfigurasi sumber data kontrol
- Opsi aturan khusus tersedia, tetapi tidak ada aturan yang muncul di daftar dropdown
- Beberapa aturan khusus tersedia, tetapi saya tidak dapat melihat aturan yang ingin saya gunakan
- Saya tidak dapat melihat aturan terkelola yang ingin saya gunakan
- Saya ingin membagikan kerangka kerja khusus, tetapi memiliki kontrol yang menggunakan AWS Config aturan khusus sebagai sumber data. Dapatkah penerima mengumpulkan bukti untuk kontrol ini?
- Apa yang terjadi ketika aturan khusus diperbaruiAWS Config? Apakah saya perlu mengambil tindakan apa pun di Audit Manager?

Saya tidak dapat melihat kontrol atau set kontrol apa pun dalam penilaian saya

Singkatnya, untuk melihat kontrol untuk penilaian, Anda harus ditentukan sebagai pemilik audit untuk penilaian itu. Selain itu, Anda memerlukan izin IAM yang diperlukan untuk melihat dan mengelola sumber daya Audit Manager terkait.

Jika Anda memerlukan akses ke kontrol dalam penilaian, mintalah salah satu pemilik audit untuk penilaian tersebut untuk menentukan Anda sebagai pemilik audit. Anda dapat menentukan pemilik audit saat membuat atau mengedit penilaian.

Pastikan juga bahwa Anda memiliki izin yang diperlukan untuk mengelola penilaian. Kami menyarankan agar pemilik audit menggunakan AWSAuditManagerAdministratorAccesskebijakan tersebut. Jika Anda memerlukan bantuan dengan izin IAM, hubungi administrator atau Support AWS Anda. Untuk informasi selengkapnya tentang cara melampirkan kebijakan ke identitas IAM, lihat Menambahkan Izin ke Pengguna dan Menambahkan dan menghapus izin identitas IAM di Panduan Pengguna IAM.

Saya tidak dapat mengunggah bukti manual ke kontrol

Jika Anda tidak dapat mengunggah bukti secara manual ke kontrol, kemungkinan besar karena kontrol dalam status tidak aktif.

Untuk mengunggah bukti manual ke kontrol, Anda harus terlebih dahulu mengubah status kontrol menjadi Sedang ditinjau atau Ditinjau. Untuk informasi selengkapnya, lihat Memperbarui status kontrol.

> **Important**
>
> Masing-masing hanya Akun AWS dapat mengunggah hingga 100 file bukti secara manual ke kontrol setiap hari. Melebihi kuota harian ini menyebabkan unggahan manual tambahan gagal untuk kontrol itu. Jika Anda perlu mengunggah sejumlah besar bukti manual ke satu kontrol, unggah bukti Anda dalam batch selama beberapa hari.

Saya perlu menggunakan beberapa AWS Config aturan sebagai sumber data untuk satu kontrol

Anda dapat menggunakan kombinasi aturan terkelola dan aturan khusus untuk satu kontrol. Untuk melakukan ini, siapkan beberapa sumber data untuk kontrol, dan pilih jenis aturan pilihan Anda untuk masing-masing. Anda dapat menentukan hingga 10 sumber data untuk satu kontrol kustom.

Opsi aturan khusus tidak tersedia saat saya mengonfigurasi sumber data kontrol

Ini berarti Anda tidak memiliki izin untuk melihat aturan khusus untuk organisasi Akun AWS atau Anda. Lebih khusus lagi, Anda tidak memiliki izin untuk melakukan DescribeConfigRulesoperasi di konsol Audit Manager.

Untuk mengatasi masalah ini, hubungi AWS administrator Anda untuk bantuan. Jika Anda seorang AWS administrator, Anda dapat memberikan izin untuk pengguna atau grup Anda dengan mengelola kebijakan IAM Anda.

Opsi aturan khusus tersedia, tetapi tidak ada aturan yang muncul di daftar dropdown

Ini berarti bahwa tidak ada aturan khusus yang diaktifkan dan tersedia untuk digunakan di organisasi Akun AWS atau Anda.

Jika Anda belum memiliki aturan khususAWS Config, Anda dapat membuatnya. Untuk petunjuk, lihat aturan AWS Config khusus di Panduan AWS Config Pengembang.

Jika Anda mengharapkan untuk melihat aturan khusus, periksa item pemecahan masalah berikut.

Beberapa aturan khusus tersedia, tetapi saya tidak dapat melihat aturan yang ingin saya gunakan

Jika Anda tidak dapat melihat aturan khusus yang Anda harapkan untuk ditemukan, ini mungkin disebabkan oleh salah satu masalah berikut.

Akun Anda dikecualikan dari aturan

Ada kemungkinan bahwa akun administrator yang didelegasikan yang Anda gunakan dikecualikan dari aturan.

Akun manajemen organisasi Anda (atau salah satu akun administrator yang AWS Config didelegasikan) dapat membuat aturan organisasi khusus menggunakan AWS Command Line Interface (AWS CLI). Ketika mereka melakukannya, mereka dapat menentukan daftar akun yang akan dikecualikan dari aturan. Jika akun Anda ada di daftar ini, aturan tidak tersedia di Audit Manager.

Untuk mengatasi masalah ini, hubungi AWS Config administrator Anda untuk bantuan. Jika Anda seorang AWS Config administrator, Anda dapat memperbarui daftar akun yang dikecualikan dengan menjalankan put-organization-config-ruleperintah.

Aturan tidak berhasil dibuat dan diaktifkan di AWS Config

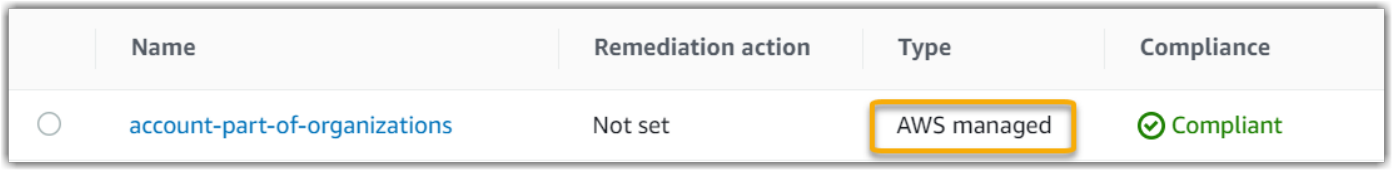
Mungkin juga aturan kustom tidak dibuat dan diaktifkan dengan sukses. Jika terjadi kesalahan saat membuat aturan, atau aturan tidak diaktifkan, aturan tersebut tidak akan muncul dalam daftar aturan yang tersedia di Audit Manager.

Untuk bantuan dengan masalah ini, kami sarankan Anda menghubungi AWS Config administrator Anda.

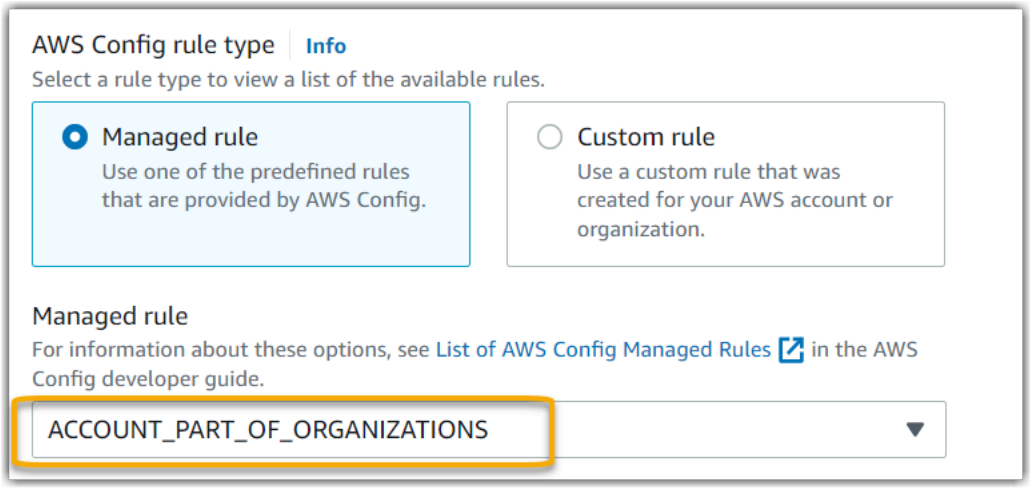
Aturannya adalah aturan yang dikelola

Jika Anda tidak dapat menemukan aturan yang Anda cari di bawah daftar dropdown aturan kustom, ada kemungkinan bahwa aturan tersebut adalah aturan terkelola.

Anda dapat menggunakan AWS Configkonsol untuk memverifikasi apakah aturan adalah aturan terkelola. Untuk melakukannya, pilih Aturan di menu navigasi kiri dan cari aturan di tabel. Jika aturan adalah aturan terkelola, kolom Type menunjukkan AWSdikelola.

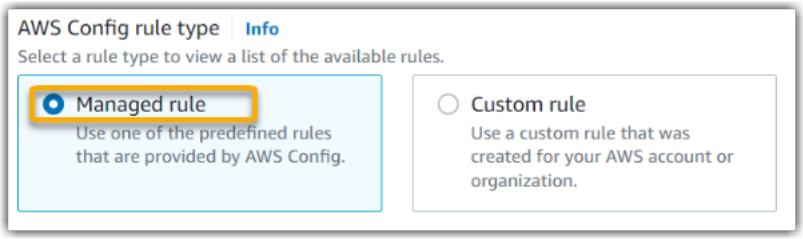


Setelah mengonfirmasi bahwa itu adalah aturan terkelola, kembali ke Audit Manager dan pilih Aturan terkelola sebagai jenis aturan. Kemudian, cari kata kunci pengidentifikasi aturan terkelola di daftar dropdown aturan terkelola.



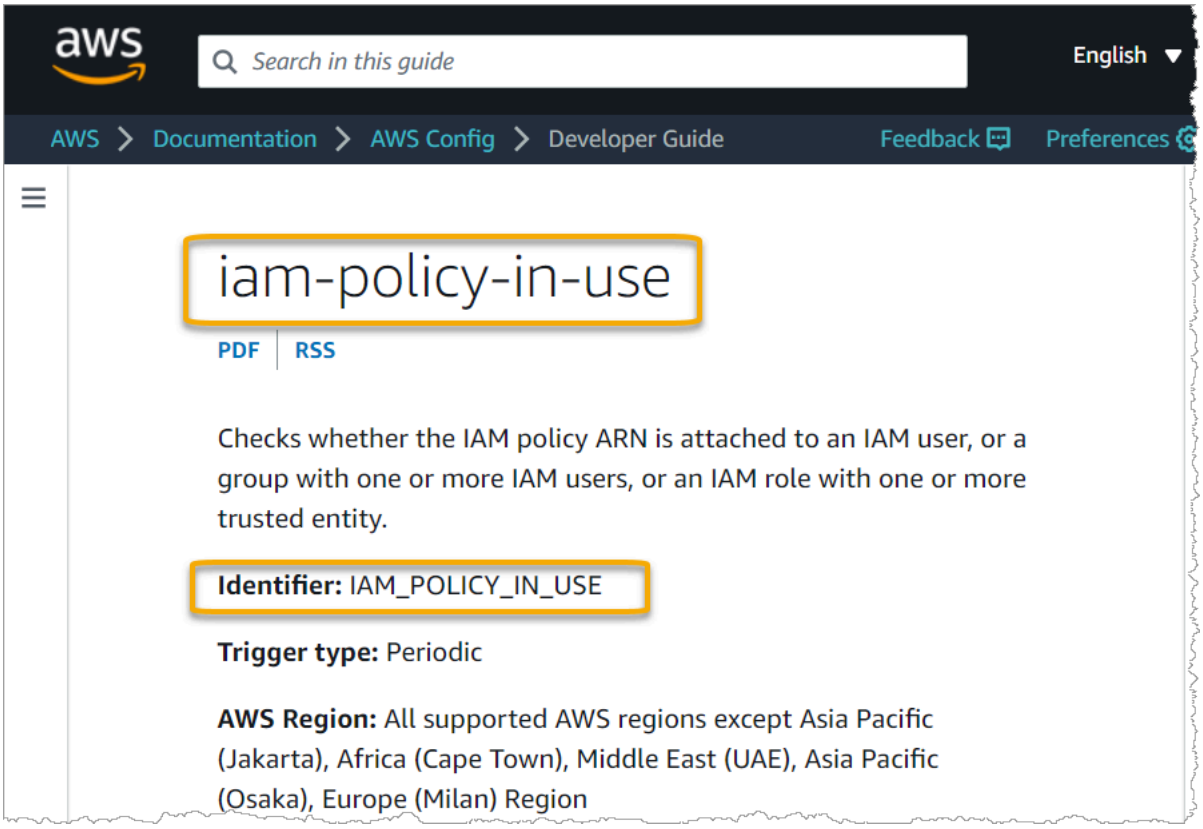
Saya tidak dapat melihat aturan terkelola yang ingin saya gunakan

Sebelum memilih aturan dari daftar tarik-turun di konsol Audit Manager, pastikan Anda memilih Aturan terkelola sebagai jenis aturan.

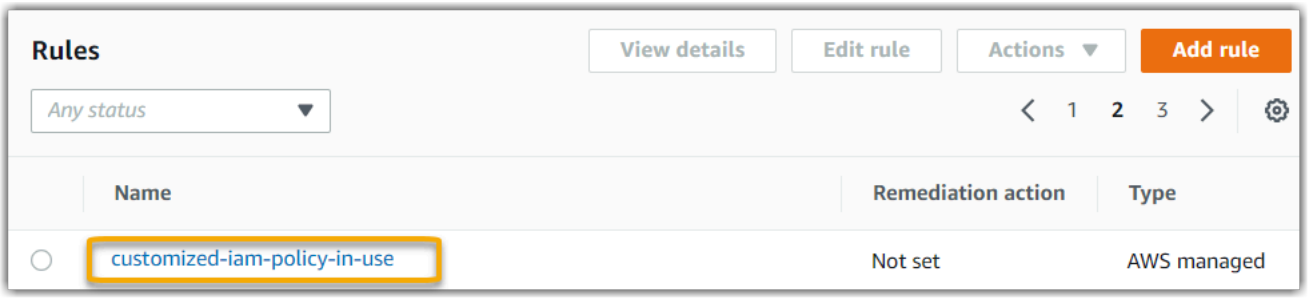


Jika Anda masih tidak dapat melihat aturan terkelola yang Anda harapkan untuk ditemukan, ada kemungkinan bahwa Anda sedang mencari nama aturan. Sebagai gantinya, Anda harus mencari pengenal aturan.

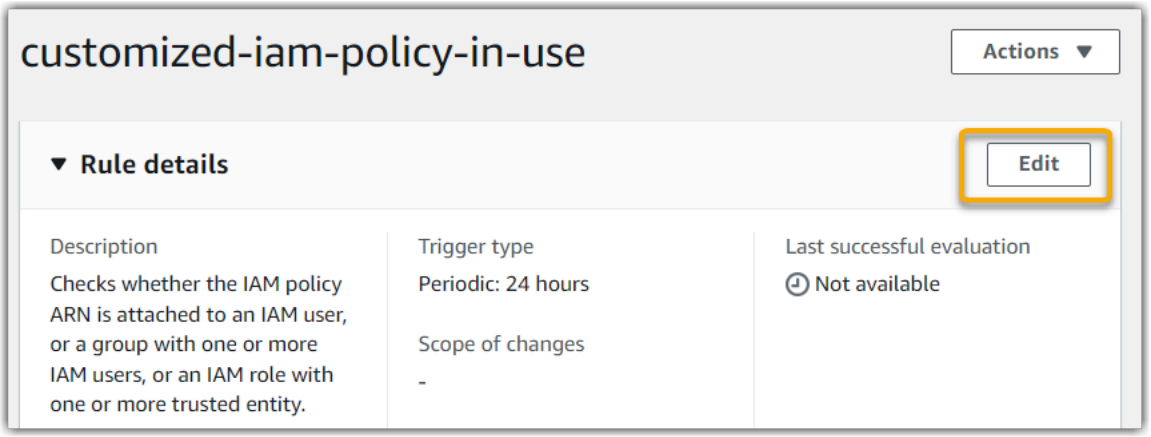
Jika Anda menggunakan aturan terkelola default, nama dan pengenalnya serupa. Namanya dalam huruf kecil dan menggunakan tanda hubung (misalnya,). `iam-policy-in-use` Pengidentifikasi dalam huruf besar dan menggunakan garis bawah (misalnya,). `IAM_POLICY_IN_USE` Untuk menemukan pengenal aturan terkelola default, tinjau daftar kata kunci aturan AWS Config terkelola yang didukung dan ikuti tautan untuk aturan yang ingin Anda gunakan. Ini membawa Anda ke AWS Config dokumentasi untuk aturan terkelola itu. Dari sini, Anda dapat melihat nama dan pengenal. Cari kata kunci pengenal di daftar dropdown Audit Manager.



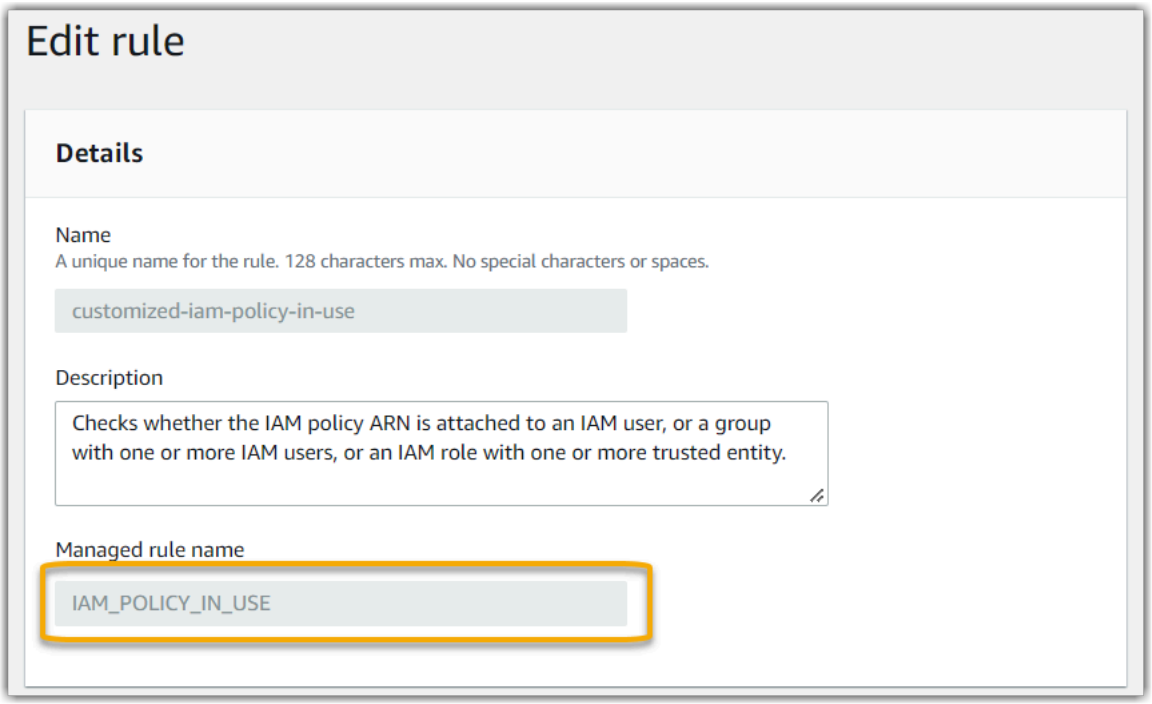
Jika Anda menggunakan aturan terkelola yang disesuaikan, Anda dapat menggunakan AWS Configkonsol untuk menemukan pengenal aturan. Misalnya, katakanlah Anda ingin menggunakan aturan terkelola yang disebut`customized-iam-policy-in-use`. Untuk menemukan pengenal untuk aturan ini, buka AWS Config konsol, pilih Aturan di menu navigasi kiri, dan pilih aturan dalam tabel.



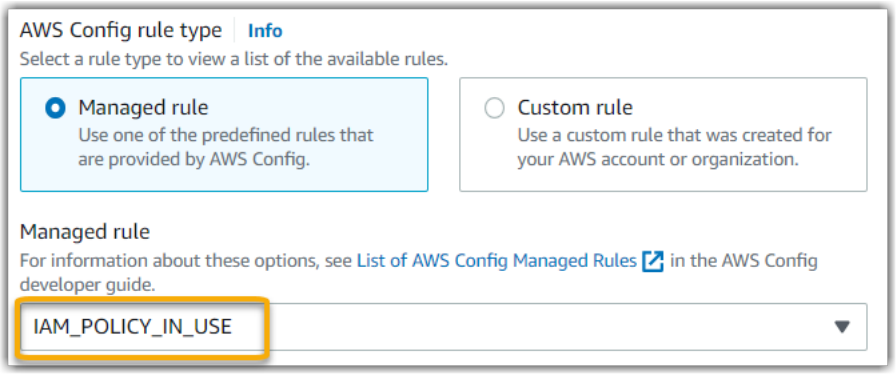
Pilih Edit untuk membuka detail tentang aturan terkelola.



Di bagian Detail, Anda dapat menemukan pengenal sumber tempat aturan terkelola dibuat dari (`IAM_POLICY_IN_USE`).



Sekarang Anda dapat kembali ke konsol Audit Manager dan memilih kata kunci pengenal yang sama dari daftar dropdown.



Saya ingin membagikan kerangka kerja khusus, tetapi memiliki kontrol yang menggunakan AWS Config aturan khusus sebagai sumber data. Dapatkah penerima mengumpulkan bukti untuk kontrol ini?

Ya, penerima dapat mengumpulkan bukti untuk kontrol ini, tetapi beberapa langkah diperlukan untuk mencapai ini.

Agar Audit Manager mengumpulkan bukti menggunakan AWS Config aturan sebagai pemetaan sumber data, berikut ini harus benar. Ini berlaku untuk aturan terkelola dan aturan khusus.

1. Aturan harus ada di AWS lingkungan penerima
2. Aturan harus diaktifkan di AWS lingkungan penerima

Ingat bahwa AWS Config aturan kustom di akun Anda kemungkinan belum ada di AWS lingkungan penerima. Selain itu, ketika penerima menerima permintaan berbagi, Audit Manager tidak membuat ulang aturan kustom Anda di akun mereka. Agar penerima dapat mengumpulkan bukti menggunakan aturan kustom Anda sebagai pemetaan sumber data, mereka harus membuat aturan kustom yang sama dalam contoh mereka. AWS Config Setelah penerima membuat dan kemudian mengaktifkan aturan, Audit Manager dapat mengumpulkan bukti dari sumber data tersebut.

Kami menyarankan Anda berkomunikasi dengan penerima untuk memberi tahu mereka jika ada aturan khusus yang perlu dibuat dalam contoh merekaAWS Config.

Apa yang terjadi ketika aturan khusus diperbaruiAWS Config? Apakah saya perlu mengambil tindakan apa pun di Audit Manager?

Untuk pembaruan aturan di AWS lingkungan Anda

Jika Anda memperbarui aturan kustom dalam AWS lingkungan Anda, tidak ada tindakan yang diperlukan di Audit Manager. Audit Manager mendeteksi dan menangani pembaruan aturan seperti yang dijelaskan dalam tabel berikut. Audit Manager tidak memberi tahu Anda saat pembaruan aturan terdeteksi.

Skenario	Apa yang dilakukan Audit Manager	Apa yang perlu Anda lakukan
Aturan khusus diperbarui dalam contoh AndaAWS Config.	Audit Manager terus melaporkan temuan untuk aturan tersebut menggunakan definisi aturan yang diperbarui.	Tidak ada tindakan yang diperlukan.
Aturan kustom dihapus dalam contoh AndaAWS Config.	Audit Manager menghentikan pelaporan temuan untuk aturan yang dihapus.	Tidak ada tindakan yang diperlukan. Jika mau, Anda dapat mengedit kontrol khusus yang menggunakan aturan yang dihapus sebagai pemetaan sumber data. Melakukannya membantu membersihkan pengaturan sumber data Anda dengan menghapus aturan yang dihapus. Jika tidak, nama aturan yang dihapus tetap sebagai pemetaan sumber data yang tidak digunakan.

Untuk pembaruan aturan di luar AWS lingkungan Anda

Jika aturan kustom diperbarui di luar AWS lingkungan Anda, Audit Manager tidak mendeteksi pembaruan aturan. Ini adalah sesuatu yang perlu dipertimbangkan jika Anda menggunakan kerangka kerja kustom bersama. Ini karena, dalam skenario ini, pengirim dan penerima masing-masing bekerja di AWS lingkungan yang terpisah. Tabel berikut memberikan tindakan yang disarankan untuk skenario ini.

Peran Anda	Skenario	Tindakan yang disarankan
Sender	• Anda berbagi kerangka kerja yang menggunakan aturan kustom sebagai pemetaan sumber data. • Setelah membagikan kerangka kerja, Anda memperbarui atau menghapus salah satu aturan tersebutAWS Config.	Beri tahu penerima tentang pembaruan Anda. Dengan begitu, mereka dapat menerapkan pembaruan yang sama dan tetap sinkron dengan definisi aturan terbaru.
Penerir	• Anda menerima kerangka kerja bersama yang menggunakan aturan kustom sebagai pemetaan sumber data. • Setelah Anda membuat ulang aturan kustom dalam instance AndaAWS Config, pengirim memperbarui atau menghapus salah satu aturan tersebut.	Buat pembaruan aturan yang sesuai dalam contoh Anda sendiriAWS Config.

Memecahkan masalah dasbor

Anda dapat menggunakan informasi di halaman ini untuk mengatasi masalah dasbor umum di Audit Manager.

Topik

- Tidak ada data di dasbor saya
- Opsi unduhan CSV tidak tersedia
- Saya tidak melihat file yang diunduh saat mencoba mengunduh file CSV
- Domain kontrol atau kontrol tertentu hilang dari dasbor
- Cuplikan harian menunjukkan jumlah bukti yang bervariasi setiap hari. Apakah ini normal?

Tidak ada data di dasbor saya

Jika angka dalam widget snapshot harian menampilkan tanda hubung (-), ini menunjukkan bahwa tidak ada data yang tersedia. Anda harus memiliki setidaknya satu penilaian aktif untuk melihat data

di dasbor. Untuk memulai, buat penilaian. Setelah periode 24 jam, data penilaian Anda akan mulai muncul di dasbor.

> **Note**
>
> Jika angka dalam widget snapshot harian menampilkan nol (0), ini menunjukkan bahwa penilaian aktif Anda (atau penilaian yang Anda pilih) tidak memiliki bukti yang tidak sesuai.

Opsi unduhan CSV tidak tersedia

Opsi ini hanya tersedia untuk penilaian individu. Pastikan Anda menerapkan the section called "Penilaian filter" ke dasbor, lalu coba lagi. Perlu diingat bahwa Anda hanya dapat mengunduh satu file CSV dalam satu waktu.

Saya tidak melihat file yang diunduh saat mencoba mengunduh file CSV

Jika domain kontrol berisi sejumlah besar kontrol, mungkin ada penundaan singkat sementara Audit Manager membuat file CSV. Setelah file dihasilkan, ia mengunduh secara otomatis.

Jika Anda masih tidak melihat file yang diunduh, pastikan koneksi internet Anda berfungsi normal dan Anda menggunakan versi terbaru dari browser web Anda. Selain itu, periksa folder unduhan terbaru Anda. File diunduh ke lokasi default yang ditentukan oleh browser Anda. Jika ini tidak menyelesaikan masalah Anda, coba unduh file menggunakan browser lain.

Domain kontrol atau kontrol tertentu hilang dari dasbor

Ini mungkin berarti bahwa penilaian aktif Anda (atau penilaian tertentu) tidak memiliki data yang relevan untuk domain kontrol atau kontrol tersebut.

Domain kontrol ditampilkan di dasbor hanya jika kedua kriteria berikut terpenuhi:

- Penilaian aktif Anda (atau penilaian tertentu) berisi setidaknya satu kontrol yang terkait dengan domain tersebut
- Setidaknya satu kontrol dalam domain itu mengumpulkan bukti pada tanggal di bagian atas dasbor

Kontrol ditampilkan dalam domain hanya jika mengumpulkan bukti pada tanggal di bagian atas dasbor.

Cuplikan harian menunjukkan jumlah bukti yang bervariasi setiap hari. Apakah ini normal?

Tidak semua bukti dikumpulkan setiap hari. Kontrol dalam penilaian Audit Manager dipetakan ke sumber data yang berbeda, dan masing-masing dapat memiliki jadwal pengumpulan bukti yang berbeda. Akibatnya, diharapkan snapshot harian menampilkan jumlah bukti yang bervariasi setiap hari. Untuk informasi selengkapnya tentang frekuensi pengumpulan bukti, lihat Bagaimana AWS Audit Manager mengumpulkan bukti.

Memecahkan masalah administrator dan masalah yang didelegasikan AWS Organizations

Anda dapat menggunakan informasi di halaman ini untuk menyelesaikan masalah administrator umum yang didelegasikan di Audit Manager.

Topik

- Saya tidak dapat mengatur Audit Manager dengan akun administrator yang didelegasikan
- Saat membuat penilaian, saya tidak dapat melihat akun dari organisasi saya dalam cakupan Akun
- Saya mendapatkan kesalahan akses ditolak ketika saya mencoba membuat laporan penilaian menggunakan akun administrator yang didelegasikan
- Apa yang terjadi di Audit Manager jika saya memutuskan tautan akun anggota dari organisasi saya?
- Apa yang terjadi jika saya menautkan kembali akun anggota ke organisasi saya?
- Apa yang terjadi jika saya memigrasikan akun anggota dari satu organisasi ke organisasi lain?

Saya tidak dapat mengatur Audit Manager dengan akun administrator yang didelegasikan

Meskipun beberapa administrator yang didelegasikan didukungAWS Organizations, Audit Manager hanya mengizinkan satu administrator yang didelegasikan. Jika Anda mencoba menunjuk beberapa administrator yang didelegasikan di Audit Manager, Anda menerima pesan galat berikut:

- Konsol: `You have exceeded the allowed number of delegated administrators for the delegated service`

- CLI: `An error occurred (ValidationException) when calling the RegisterAccount operation: Cannot change delegated Admin for an active account 11111111111 from 2222222222222 to 333333333333`

Pilih satu akun individual yang ingin Anda gunakan sebagai administrator yang didelegasikan di Audit Manager. Pastikan Anda mendaftarkan akun administrator yang didelegasikan di Organizations terlebih dahulu, lalu tambahkan akun yang sama dengan administrator yang didelegasikan di Audit Manager.

Saat membuat penilaian, saya tidak dapat melihat akun dari organisasi saya dalam cakupan Akun

Jika ingin penilaian Audit Manager menyertakan beberapa akun dari organisasi, Anda harus menentukan administrator yang didelegasikan.

Pastikan Anda mengonfigurasi akun administrator yang didelegasikan untuk Audit Manager. Untuk petunjuk, lihat Pengaturan, Administrator yang didelegasikan.

Beberapa masalah yang perlu diingat:

- Anda tidak dapat menggunakan akun AWS Organizations manajemen sebagai administrator yang didelegasikan di Audit Manager.
- Jika Anda ingin mengaktifkan Audit Manager di lebih dari satuWilayah AWS, Anda harus menetapkan akun administrator yang didelegasikan secara terpisah di setiap Wilayah. Di setelan Audit Manager Anda, tentukan akun administrator yang didelegasikan yang sama di semua Wilayah.
- Saat Anda menunjuk administrator yang didelegasikan, pastikan akun administrator yang didelegasikan memiliki akses pada kunci KMS yang Anda berikan saat menyiapkan Audit Manager. Untuk mempelajari cara meninjau dan mengubah setelan enkripsi, lihat Enkripsi data.

Saya mendapatkan kesalahan akses ditolak ketika saya mencoba membuat laporan penilaian menggunakan akun administrator yang didelegasikan

Anda akan mendapatkan `access denied` kesalahan jika penilaian Anda dibuat oleh akun administrator yang didelegasikan bahwa kunci KMS yang ditentukan dalam pengaturan Audit Manager Anda bukan milik. Untuk menghindari kesalahan ini, saat Anda menunjuk administrator

yang didelegasikan untuk Audit Manager, pastikan akun administrator yang didelegasikan memiliki akses pada kunci KMS yang Anda berikan saat menyiapkan Audit Manager.

Anda mungkin juga menerima `access denied` kesalahan jika tidak memiliki izin menulis untuk bucket S3 yang Anda gunakan sebagai tujuan laporan penilaian.

Jika Anda mendapatkan `access denied` kesalahan, pastikan Anda memenuhi persyaratan berikut:

- Kunci KMS Anda di setelan Audit Manager memberikan izin kepada administrator yang didelegasikan. Anda dapat mengonfigurasinya dengan mengikuti petunjuk di Mengizinkan pengguna di akun lain menggunakan kunci KMS di Panduan AWS Key Management Service Pengembang. Untuk petunjuk tentang cara meninjau dan mengubah setelan enkripsi Anda di Audit Manager, lihat Enkripsi data.
- Anda memiliki kebijakan izin yang memberi Anda akses menulis untuk tujuan laporan penilaian. Lebih khusus lagi, kebijakan izin Anda berisi `s3:PutObject` tindakan, menentukan ARN bucket S3, dan menyertakan kunci KMS yang digunakan untuk mengenkripsi laporan penilaian Anda. Untuk contoh kebijakan yang dapat Anda gunakan, lihat Contoh kebijakan berbasis identitas untuk. AWS Audit Manager

> **Note**
>
> Jika Anda mengubah setelan enkripsi data Audit Manager, perubahan ini berlaku untuk penilaian baru yang Anda buat selanjutnya. Ini termasuk laporan penilaian apa pun yang Anda buat dari penilaian baru Anda.
> Perubahan tidak berlaku untuk penilaian yang sudah ada yang Anda buat sebelum mengubah setelan enkripsi. Ini termasuk laporan penilaian baru yang Anda buat dari penilaian yang ada, selain laporan penilaian yang ada. Penilaian yang ada — dan semua laporan penilaian mereka — terus menggunakan kunci KMS lama. Jika identitas IAM yang menghasilkan laporan penilaian tidak memiliki izin untuk menggunakan kunci KMS lama, Anda dapat memberikan izin di tingkat kebijakan utama.

Apa yang terjadi di Audit Manager jika saya memutuskan tautan akun anggota dari organisasi saya?

Saat Anda memutuskan tautan akun anggota dari organisasi, Audit Manager menerima pemberitahuan tentang acara ini. Audit Manager kemudian secara otomatis menghapusnya Akun

AWS dari akun dalam daftar cakupan penilaian Anda yang ada. Saat Anda menentukan cakupan penilaian baru yang bergerak maju, akun yang tidak ditautkan tidak lagi muncul dalam daftar yang memenuhi syarat. Akun AWS

Saat Audit Manager menghapus akun anggota yang tidak ditautkan dari akun dalam daftar cakupan penilaian Anda, Anda tidak akan diberi tahu tentang perubahan ini. Selain itu, akun anggota yang tidak ditautkan tidak diberi tahu bahwa Audit Manager tidak lagi diaktifkan di akun mereka.

Apa yang terjadi jika saya menautkan kembali akun anggota ke organisasi saya?

Saat Anda menautkan kembali akun anggota ke organisasi Anda, akun tersebut tidak secara otomatis ditambahkan ke cakupan penilaian Audit Manager yang ada. Namun, akun anggota yang ditautkan kembali sekarang muncul sebagai memenuhi syarat Akun AWS saat Anda menentukan akun dalam lingkup penilaian Anda.

- Untuk penilaian yang ada, Anda dapat mengedit cakupan penilaian secara manual untuk menambahkan akun anggota yang ditautkan kembali. Untuk petunjuk, lihat Mengedit Akun AWS dalam ruang lingkup.
- Untuk penilaian baru, Anda dapat menambahkan akun yang ditautkan ulang selama penyiapan penilaian. Untuk petunjuk, lihat Menentukan Akun AWS dalam ruang lingkup.

Apa yang terjadi jika saya memigrasikan akun anggota dari satu organisasi ke organisasi lain?

Jika akun anggota mengaktifkan Audit Manager di organisasi 1 dan kemudian bermigrasi ke organisasi 2, Audit Manager tidak diaktifkan untuk organisasi 2 sebagai hasilnya.

Memecahkan masalah pencari bukti

Gunakan informasi di halaman ini untuk menyelesaikan masalah pencari bukti umum di Audit Manager.

Masalah pencari bukti umum

- Saya tidak dapat mengaktifkan pencari bukti
- Saya mengaktifkan pencari bukti, tetapi saya tidak melihat bukti masa lalu di hasil pencarian saya

- Saya tidak dapat menonaktifkan pencari bukti
- Kueri penelusuran saya gagal

Masalah laporan penilaian pencari bukti

- Saya tidak dapat membuat beberapa laporan penilaian dari hasil pencarian saya
- Saya tidak dapat menyertakan bukti spesifik dari hasil pencarian saya
- Tidak semua hasil pencari bukti saya termasuk dalam laporan penilaian
- Saya ingin membuat laporan penilaian dari hasil pencarian saya, tetapi pernyataan kueri saya gagal
- Sumber daya lainnya

Pencari bukti masalah ekspor CSV

- Ekspor CSV saya gagal
- Saya tidak dapat mengekspor bukti spesifik dari hasil pencarian saya
- Saya tidak dapat mengekspor beberapa file CSV sekaligus

Saya tidak dapat mengaktifkan pencari bukti

Alasan umum mengapa Anda tidak dapat mengaktifkan pencari bukti termasuk situasi berikut:

Anda kehilangan izin

Jika Anda mencoba mengaktifkan pencari bukti untuk pertama kalinya, pastikan Anda memiliki izin yang diperlukan. Izin ini memungkinkan Anda membuat dan mengelola penyimpanan data acara di CloudTrail Lake, yang diperlukan untuk mendukung permintaan pencarian pencari bukti. Izin juga memungkinkan Anda menjalankan kueri penelusuran di pencari bukti.

Jika Anda memerlukan bantuan dengan izin, hubungi AWS administrator Anda. Jika Anda seorang AWS administrator, Anda dapat menyalin pernyataan izin yang diperlukan dan melampirkannya ke kebijakan IAM.

Anda menggunakan akun manajemen Organizations

Ingatlah bahwa Anda tidak dapat menggunakan akun manajemen untuk mengaktifkan pencari bukti. Masuk sebagai akun administrator yang didelegasikan, dan coba lagi.

Anda sebelumnya menonaktifkan pencari bukti

Mengaktifkan kembali pencari bukti saat ini tidak didukung. Jika sebelumnya Anda menonaktifkan pencari bukti, Anda tidak dapat mengaktifkannya lagi.

Saya mengaktifkan pencari bukti, tetapi saya tidak melihat bukti masa lalu di hasil pencarian saya

Saat Anda mengaktifkan pencari bukti, dibutuhkan hingga 7 hari untuk semua data bukti masa lalu Anda tersedia.

Selama periode 7 hari ini, penyimpanan data acara diisi kembali dengan data bukti bernilai dua tahun terakhir Anda. Ini berarti bahwa jika Anda menggunakan pencari bukti segera setelah Anda mengaktifkannya, tidak semua hasil tersedia sampai pengisian ulang selesai.

Untuk petunjuk tentang cara memeriksa status pengisian ulang data, lihat Mengonfirmasi status pencari bukti.

Saya tidak dapat menonaktifkan pencari bukti

Ini bisa disebabkan oleh salah satu alasan berikut.

Anda kehilangan izin

Jika Anda mencoba menonaktifkan pencari bukti, pastikan Anda memiliki izin yang diperlukan. Izin ini memungkinkan Anda untuk memperbarui dan menghapus penyimpanan data peristiwa di CloudTrail Lake, yang diperlukan untuk menonaktifkan pencari bukti.

Jika Anda memerlukan bantuan dengan izin, hubungi AWS administrator Anda. Jika Anda seorang AWS administrator, Anda dapat menyalin pernyataan izin yang diperlukan dan melampirkannya ke kebijakan IAM.

Permintaan untuk mengaktifkan pencari bukti masih berlangsung

Saat Anda meminta untuk mengaktifkan pencari bukti, kami membuat penyimpanan data peristiwa untuk mendukung kueri pencari bukti. Anda tidak dapat menonaktifkan pencari bukti saat penyimpanan data acara sedang dibuat.

Untuk melanjutkan, tunggu hingga penyimpanan data acara dibuat, dan coba lagi. Untuk informasi selengkapnya, lihat Mengonfirmasi status pencari bukti.

Anda sudah diminta untuk menonaktifkan pencari bukti

Saat Anda meminta untuk menonaktifkan pencari bukti, kami menghapus penyimpanan data peristiwa yang digunakan untuk kueri pencari bukti. Jika Anda mencoba lagi untuk menonaktifkan pencari bukti saat penyimpanan data peristiwa sedang dihapus, Anda mendapatkan pesan kesalahan.

Dalam hal ini, tidak diperlukan tindakan. Tunggu hingga penyimpanan data acara dihapus. Segera setelah ini selesai, pencari bukti dinonaktifkan. Untuk informasi selengkapnya, lihat Mengonfirmasi status pencari bukti.

Kueri penelusuran saya gagal

Permintaan pencarian yang gagal dapat disebabkan oleh salah satu alasan berikut.

Anda kehilangan izin

Verifikasi bahwa pengguna memiliki izin yang diperlukan untuk menjalankan kueri penelusuran dan mengakses hasil pencarian. Secara khusus, Anda memerlukan izin untuk CloudTrail tindakan berikut:

- StartQuery
- DescribeQuery
- CancelQuery
- GetQueryResults

Jika Anda memerlukan bantuan dengan izin, hubungi AWS administrator Anda. Jika Anda seorang AWS administrator, Anda dapat menyalin pernyataan izin yang diperlukan dan melampirkannya ke kebijakan IAM.

Anda menjalankan jumlah kueri maksimum

Anda dapat menjalankan hingga 5 kueri sekaligus. Jika Anda menjalankan jumlah maksimum kueri bersamaan, ini menghasilkan kesalahan. `MaxConcurrentQueriesException` Jika Anda mendapatkan pesan kesalahan ini, tunggu sebentar hingga beberapa kueri selesai, lalu jalankan kueri lagi.

Pernyataan kueri Anda memiliki kesalahan validasi

Jika Anda menggunakan API atau CLI untuk melakukan StartQueryoperasi CloudTrail Lake, pastikan bahwa Anda `queryStatement` valid. Jika pernyataan kueri memiliki kesalahan

validasi, sintaks yang salah, atau kata kunci yang tidak didukung, ini menghasilkan file. `InvalidQueryStatementException`

Untuk informasi selengkapnya tentang menulis kueri, lihat Membuat atau mengedit kueri di Panduan AWS CloudTrail Pengguna.

Untuk contoh sintaks yang valid, tinjau contoh pernyataan kueri berikut yang dapat digunakan untuk menanyakan penyimpanan data peristiwa Audit Manager.

Contoh 1: Selidiki bukti dan status kepatuhannya

Contoh ini menemukan bukti dengan status kepatuhan apa pun di semua penilaian dalam akun, dalam rentang tanggal yang ditentukan.

```
SELECT eventData.evidenceId, eventData.resourceArn,
 eventData.resourceComplianceCheck FROM $EDS_ID WHERE eventTime > '2022-11-02
 00:00:00.000' AND eventTime < '2022-11-03 00:00:00.000'
```

Contoh 2: Tentukan bukti yang tidak sesuai untuk kontrol

Contoh ini menemukan semua bukti yang tidak sesuai dalam rentang tanggal tertentu untuk penilaian dan kontrol tertentu.

```
SELECT * FROM $EDS_ID WHERE eventData.assessmentId = '11aa33bb-55cc-77dd-99ee-
ff22gg44hh66' AND eventTime > '2022-10-27 22:05:00.000' AND eventTime
 < '2022-11-03 22:05:00.000' AND eventData.resourceComplianceCheck IN
 ('NON_COMPLIANT','FAILED','WARNING') AND eventData.controlId IN ('aa11bb22-cc33-
dd44-ee55-ff66gg77hh88')
```

Contoh 3: Hitung bukti dengan nama

Contoh ini mencantumkan bukti total untuk penilaian dalam rentang tanggal tertentu, dikelompokkan berdasarkan nama dan diurutkan berdasarkan jumlah bukti.

```
SELECT eventData.eventName as eventName, COUNT(*) as totalEvidence FROM  $EDS_ID
 WHERE eventData.assessmentId = '11aa33bb-55cc-77dd-99ee-ff22gg44hh66' AND eventTime
 > '2022-10-27 22:05:00.000' AND eventTime < '2022-11-03 22:05:00.000' GROUP BY
 eventData.eventName ORDER BY totalEvidence DESC
```

Contoh 4: Jelajahi bukti berdasarkan sumber data dan layanan

Contoh ini menemukan semua bukti dalam rentang tanggal tertentu untuk sumber data dan layanan tertentu.

```
SELECT * FROM $EDS_ID WHERE eventTime > '2022-10-27 22:05:00.000' AND eventTime
 < '2022-11-03 22:05:00.000' AND eventData.service IN ('dynamodb') AND
 eventData.dataSource IN ('AWS API calls')
```

Contoh 5: Jelajahi bukti yang sesuai dengan sumber data dan domain kontrol

Contoh ini menemukan bukti yang sesuai untuk domain kontrol tertentu, di mana bukti berasal dari sumber data yang bukan AWS Config.

```
SELECT * FROM $EDS_ID WHERE eventData.resourceComplianceCheck IN
('PASSED','COMPLIANT') AND eventData.controlDomainName IN ('Logging and
monitoring','Data security and privacy') AND eventData.dataSource NOT IN ('AWS
Config')
```

Pengecualian API lainnya

StartQueryAPI mungkin gagal karena beberapa alasan lain. Untuk daftar lengkap kemungkinan kesalahan dan deskripsi, lihat StartQuery Kesalahan dalam Referensi AWS CloudTrail API.

Saya tidak dapat membuat beberapa laporan penilaian dari hasil pencarian saya

Kesalahan ini disebabkan oleh menjalankan terlalu banyak kueri CloudTrail Danau secara bersamaan.

Kesalahan ini dapat terjadi jika Anda mengelompokkan hasil pencarian dan mencoba untuk segera menghasilkan laporan penilaian untuk setiap item baris dalam hasil yang dikelompokkan. Saat Anda mendapatkan hasil penelusuran dan menghasilkan laporan penilaian, setiap tindakan akan memanggil kueri. Anda hanya dapat menjalankan hingga 5 kueri sekaligus. Jika Anda menjalankan jumlah maksimum kueri bersamaan, `MaxConcurrentQueriesException` kesalahan dikembalikan.

Untuk mencegah kesalahan ini, pastikan Anda tidak membuat terlalu banyak laporan penilaian sekaligus. Jika Anda menjalankan jumlah maksimum kueri bersamaan, `MaxConcurrentQueriesException` kesalahan dikembalikan. Jika Anda mendapatkan pesan galat ini, tunggu beberapa menit hingga laporan penilaian yang sedang berlangsung selesai.

Anda dapat memeriksa status laporan penilaian Anda dari halaman pusat unduhan di konsol Audit Manager. Setelah laporan Anda selesai, kembali ke hasil yang dikelompokkan dalam pencari bukti. Anda kemudian dapat terus mendapatkan hasil dan menghasilkan laporan penilaian untuk setiap item baris.

Saya tidak dapat menyertakan bukti spesifik dari hasil pencarian saya

Semua hasil pencarian Anda disertakan dalam laporan penilaian. Anda tidak dapat menambahkan baris individual secara selektif dari kumpulan hasil penelusuran Anda.

Jika Anda hanya ingin menyertakan hasil penelusuran tertentu dalam laporan penilaian, sebaiknya Anda mengedit filter penelusuran saat ini. Dengan cara ini, Anda dapat mempersempit hasil Anda untuk menargetkan hanya bukti yang ingin Anda sertakan dalam laporan.

Tidak semua hasil pencari bukti saya termasuk dalam laporan penilaian

Saat Anda membuat laporan penilaian, ada batasan berapa banyak bukti yang dapat Anda tambahkan. Batasannya didasarkan pada Wilayah AWS penilaian Anda, Wilayah bucket S3 yang digunakan sebagai tujuan laporan penilaian Anda, dan apakah penilaian Anda menggunakan pelanggan yang dikelolaAWS KMS key.

1. Batasnya adalah 22.000 untuk laporan wilayah yang sama (di mana bucket dan penilaian S3 sama) Wilayah AWS
2. Batasnya adalah 3.500 untuk laporan Lintas wilayah (di mana bucket dan penilaian S3 berbeda) Wilayah AWS
3. Batasnya adalah 3.500 jika penilaian menggunakan kunci KMS yang dikelola pelanggan

Jika Anda melebihi batas ini, laporan masih dibuat. Namun, Audit Manager hanya menambahkan 3.500 atau 22.000 item bukti pertama ke dalam laporan.

Untuk mencegah masalah ini, kami sarankan Anda mengedit filter pencarian Anda saat ini. Dengan cara ini, Anda dapat mengurangi hasil pencarian Anda dengan menargetkan sejumlah kecil bukti. Jika diperlukan, Anda dapat mengulangi metode ini dan menghasilkan beberapa laporan penilaian alih-alih satu laporan yang lebih besar.

Saya ingin membuat laporan penilaian dari hasil pencarian saya, tetapi pernyataan kueri saya gagal

Jika Anda menggunakan CreateAssessmentReportAPI dan pernyataan kueri Anda mengembalikan pengecualian validasi, periksa tabel di bawah ini untuk panduan tentang cara memperbaikinya.

> **Note**
>
> Meskipun pernyataan kueri berfungsi CloudTrail, kueri yang sama mungkin tidak valid untuk pembuatan laporan penilaian di Audit Manager. Ini karena beberapa perbedaan dalam validasi kueri antara kedua layanan.

Klausul	Isu	Solusi	Catatan
`SELECT`	`SELECT`Klausa berisi nama kolom	Hapus `SELECT` klausa dan ganti dengan`SELECT eventJson` .	Hanya `SELECT eventJson` didukung. Validasi ini ditangani oleh Audit Manager.
`FROM`	`FROM`Klausa berisi ID penyimpanan data peristiwa yang tidak valid atau ID penyimpanan data peristiwa yang disediakan tidak cocok dengan ID penyimpanan data peristiwa di setelan Audit Manager Anda	Hapus `FROM` klausa dan ganti dengan`FROM` *`edsID`*, di mana nilai `edsID` cocok dengan ID penyimpanan data peristiwa yang ditentukan dalam setelan Audit Manager Anda. Anda dapat mengambil ARN penyimpanan data peristiwa dari pengaturan Audit Manager Anda. Untuk informasi selengkapnya, lihat GetSettings dalam Referensi API AWS Audit Manager.	Validasi ini ditangani oleh Audit Manager.

Klausul	Isu	Solusi	Catatan
`GROUP BY`	Sebuah `GROUP BY` klausa hadir dalam query	Hapus `GROUP BY` klausa.	Validasi ini ditangani oleh Audit Manager.
`HAVING`	Sebuah `HAVING` klausa hadir dalam query	Hapus `HAVING` klausa.	Validasi ini ditangani oleh Audit Manager.
`LIMIT`	`LIMIT`Klausul berisi nilai yang melebihi batas maksimum yang diizinkan	Jika `LIMIT` klausa ada, pastikan nilainya sama dengan atau kurang dari batas maksimum yang didukung: • Untuk laporan wilayah yang sama, batasnya adalah 22.000 • Untuk laporan lintas wilayah, batasnya adalah 3.500 • Untuk laporan di mana penilaian terkait menggunakan pelanggan yang dikelolaAWS KMS key, batasnya adalah 3.500	Di konsol, tidak ada batasan jumlah hasil bukti yang dapat dikembalikan. Namun, saat membuat laporan penilaian , batas berlaku untuk jumlah bukti yang dapat Anda sertakan. Jika tidak ada `LIMIT` nilai yang diberikan dalam pernyataan kueri Anda, batas maksimum default diterapkan. Validasi ini ditangani oleh Audit Manager.
`ORDER BY`	`ORDER BY`Klausa berisi fungsi Agregat atau Alias yang tidak ada dalam klausa `SELECT`	Pastikan `ORDER BY` klausa tidak berisi kondisi apa pun menggunakan fungsi Agregat atau Alias.	Validasi ini ditangani oleh API. CloudTrail StartQuery

Klausul	Isu	Solusi	Catatan

`WHERE`	`WHERE`Klausul tersebut berisi lebih dari satu `assessmentId`
	
	atau
	
	`WHERE`Klausa berisi `assessmentId` yang tidak cocok dengan `assessmentId` permintaan Anda `createAssessmentReport`
	
	atau
	
	`WHERE`Klausa berisi nama kolom yang tidak didukung
		Pastikan bahwa hanya satu AssessMentID yang ditentukan, dan cocok dengan parameter AssesmentID yang Anda tentukan dalam permintaan API. `createAssessmentReport`
		
		Hapus nama kolom yang tidak didukung.
			Validasi ini ditangani oleh API. CloudTrail StartQuery

Contoh

Contoh berikut menunjukkan bagaimana Anda dapat menggunakan `queryStatement` parameter saat memanggil CreateAssessmentReportoperasi. Sebelum Anda menggunakan kueri ini, ganti *`teks placeholder`* dengan milik `edsId` Anda dan nilai. `assessmentId`

Contoh 1: Buat laporan (Batas wilayah yang sama berlaku)

Contoh ini membuat laporan yang menyertakan hasil untuk bucket S3 yang dibuat antara 22-23 Januari 2022.

```
SELECT eventJson FROM 12345678-abcd-1234-abcd-123456789012 WHERE eventData.assessmentId
 = '11aa33bb-55cc-77dd-99ee-ff22gg44hh66' AND eventTime > '2022-01-22 00:00:00.000' AND
 eventTime < '2022-01-23 00:00:00.000' AND eventName='CreateBucket' LIMIT 22000
```

Contoh 2: Membuat laporan (Batas lintas wilayah berlaku)

Contoh ini membuat laporan yang mencakup semua hasil untuk penyimpanan dan penilaian data peristiwa yang ditentukan, tanpa rentang tanggal yang ditentukan.

```
SELECT eventJson FROM 12345678-abcd-1234-abcd-123456789012 WHERE eventData.assessmentId
 = '11aa33bb-55cc-77dd-99ee-ff22gg44hh66' LIMIT 7000
```

Contoh 3: Buat laporan (di bawah batas default)

Contoh ini membuat laporan yang mencakup semua hasil untuk penyimpanan dan penilaian data peristiwa yang ditentukan, dengan batas yang berada di bawah maksimum default.

```
SELECT eventJson FROM 12345678-abcd-1234-abcd-123456789012 WHERE eventData.assessmentId
 = '11aa33bb-55cc-77dd-99ee-ff22gg44hh66' LIMIT 2000
```

Sumber daya lainnya

Halaman berikut berisi panduan pemecahan masalah umum tentang laporan penilaian:

- Memecahkan masalah laporan penilaian

Ekspor CSV saya gagal

Ekspor CSV Anda mungkin gagal karena sejumlah alasan. Anda dapat memecahkan masalah ini dengan memeriksa penyebab yang paling sering.

Pertama, pastikan Anda memenuhi prasyarat untuk menggunakan fitur ekspor CSV:

Anda berhasil mengaktifkan pencari bukti

Jika Anda belum mengaktifkan pencari bukti, Anda tidak dapat menjalankan kueri penelusuran dan mengekspor hasil penelusuran Anda.

Isi ulang penyimpanan data acara Anda selesai

Jika Anda menggunakan pencari bukti segera setelah Anda mengaktifkannya, dan pengurukan bukti masih berlangsung, mungkin ada beberapa hasil yang tidak tersedia. Untuk memeriksa status isi ulang, lihat Konfirmasi status pencari bukti.

Kueri penelusuran Anda berhasil

Audit Manager tidak dapat mengekspor hasil kueri yang gagal. Untuk memecahkan masalah kueri yang gagal, lihat. Kueri penelusuran saya gagal

Setelah Anda mengonfirmasi bahwa Anda memenuhi prasyarat, gunakan daftar periksa berikut untuk memeriksa potensi masalah:

1. Periksa status kueri penelusuran Anda:
   a. Apakah kueri dibatalkan? Pencari bukti menampilkan sebagian hasil yang diproses sebelum kueri dibatalkan. Namun, Audit Manager tidak mengekspor sebagian hasil ke bucket S3 atau pusat unduhan.
   b. Apakah kueri sudah berjalan selama lebih dari satu jam? Kueri yang berjalan lebih dari satu jam mungkin habis. Pencari bukti menampilkan sebagian hasil yang diproses sebelum waktu kueri habis. Namun, Audit Manager tidak mengekspor sebagian hasil. Untuk menghindari batas waktu, Anda dapat mengurangi jumlah bukti yang dipindai dengan mengedit kueri penelusuran untuk menentukan rentang waktu yang lebih sempit.
2. Periksa nama dan URI bucket S3 tujuan ekspor Anda:
   a. Apakah ember yang Anda tentukan ada? Jika Anda memasukkan URI bucket secara manual, pastikan Anda tidak salah mengetik apa pun. Kesalahan ketik atau URI yang salah dapat mengakibatkan `RESOURCE_NOT_FOUND` kesalahan saat Audit Manager mencoba mengekspor file CSV ke Amazon S3.
3. Periksa izin bucket S3 tujuan ekspor Anda:
   a. Apakah Anda memiliki izin menulis untuk ember S3? Anda harus memiliki akses tulis untuk bucket S3 yang Anda gunakan sebagai tujuan ekspor. Lebih khusus lagi, kebijakan izin IAM harus menyertakan `s3:PutObject` tindakan dan bucket ARN, dan daftar CloudTrail sebagai prinsipal layanan. Kami memberikan contoh kebijakan yang dapat Anda gunakan. Untuk petunjuk tentang cara menggunakan bucket S3 yang berbeda, lihat Mengekspor setelan tujuan.
4. Periksa apakah ada Wilayah AWS informasi Anda yang tidak cocok:
   a. Apakah kunci Wilayah AWS yang dikelola pelanggan Anda sesuai dengan Wilayah AWS penilaian Anda? Jika Anda memberikan kunci terkelola pelanggan untuk enkripsi data, itu harus Wilayah AWS sama dengan penilaian Anda. Untuk petunjuk tentang cara mengubah kunci KMS, lihat Pengaturan enkripsi data.
5. Periksa izin akun administrator yang didelegasikan:
   a. Apakah kunci terkelola pelanggan di setelan Audit Manager memberikan izin kepada administrator yang didelegasikan? Jika Anda menggunakan akun administrator yang didelegasikan dan Anda menentukan kunci terkelola pelanggan untuk enkripsi data, pastikan administrator yang didelegasikan memiliki akses pada kunci KMS tersebut. Untuk petunjuk, lihat Mengizinkan pengguna di akun lain menggunakan kunci KMS di Panduan AWS Key

Management Service Pengembang. Untuk meninjau dan mengubah setelan enkripsi Anda di Audit Manager, lihat Pengaturan enkripsi data.

> **Note**
>
> Jika Anda mengubah setelan enkripsi data Audit Manager, perubahan ini berlaku untuk penilaian baru yang Anda buat untuk selanjutnya. Ini termasuk file CSV apa pun yang Anda ekspor dari penilaian baru Anda.
> Perubahan tidak berlaku untuk penilaian yang sudah ada yang Anda buat sebelum mengubah setelan enkripsi. Ini termasuk ekspor CSV baru dari penilaian yang ada, selain ekspor CSV yang ada. Penilaian yang ada — dan semua ekspor CSV mereka — terus menggunakan kunci KMS lama. Jika identitas IAM yang mengekspor file CSV tidak memiliki izin untuk menggunakan kunci KMS lama, Anda dapat memberikan izin di tingkat kebijakan utama.

Saya tidak dapat mengekspor bukti spesifik dari hasil pencarian saya

Semua hasil pencarian Anda disertakan dalam hasil.

Jika Anda hanya ingin menyertakan bukti spesifik dalam file CSV, kami sarankan Anda mengedit filter penelusuran saat ini. Dengan cara ini, Anda dapat mempersempit hasil Anda untuk menargetkan hanya bukti yang ingin Anda ekspor.

Saya tidak dapat mengekspor beberapa file CSV sekaligus

Kesalahan ini disebabkan oleh menjalankan terlalu banyak kueri CloudTrail Danau secara bersamaan.

Ini dapat terjadi jika Anda mengelompokkan hasil pencarian dan mencoba untuk segera mengekspor file CSV untuk setiap item baris dalam hasil yang dikelompokkan. Saat Anda mendapatkan hasil penelusuran dan mengekspor file CSV, masing-masing tindakan ini akan memanggil kueri. Anda hanya dapat menjalankan hingga lima kueri sekaligus. Jika Anda menjalankan jumlah maksimum kueri bersamaan, `MaxConcurrentQueriesException` kesalahan dikembalikan.

Untuk mencegah kesalahan ini, pastikan Anda tidak mengekspor terlalu banyak file CSV sekaligus.

Untuk mengatasi kesalahan ini, tunggu hingga ekspor CSV Anda yang sedang berlangsung selesai. Sebagian besar ekspor memakan waktu beberapa menit. Namun, jika Anda mengekspor data dalam

jumlah yang sangat besar, mungkin diperlukan waktu hingga satu jam untuk menyelesaikan ekspor. Jangan ragu untuk menjauh dari pencari bukti saat ekspor sedang berlangsung.

Anda dapat memeriksa status ekspor dari pusat unduhan di konsol Audit Manager. Setelah file yang diekspor siap, kembali ke hasil yang dikelompokkan dalam pencari bukti. Anda kemudian dapat terus mendapatkan hasil dan mengekspor file CSV untuk setiap item baris.

Memecahkan masalah berbagi kerangka kerja

Anda dapat menggunakan informasi di halaman ini untuk menyelesaikan masalah berbagi kerangka kerja umum di Audit Manager.

Topik

Status permintaan berbagi terkirim saya ditampilkan sebagai Gagal

Jika Anda mencoba membagikan kerangka kerja khusus dan operasi gagal, kami sarankan Anda memeriksa yang berikut ini:

1. Pastikan Audit Manager diaktifkan di penerima Akun AWS dan di Wilayah yang ditentukan. Untuk daftar AWS Audit Manager Wilayah yang didukung, lihat AWS Audit Managertitik akhir dan kuota di Referensi Umum Amazon Web Services.
2. Pastikan Anda memasukkan Akun AWS ID yang benar saat menentukan akun penerima.
3. Pastikan Anda tidak menentukan akun AWS Organizations manajemen sebagai penerima. Anda dapat berbagi kerangka kerja khusus dengan administrator yang didelegasikan, tetapi jika Anda mencoba berbagi kerangka kerja khusus dengan akun manajemen, operasi gagal.
4. Jika Anda menggunakan kunci yang dikelola pelanggan untuk mengenkripsi data Audit Manager Anda, pastikan kunci KMS Anda diaktifkan. Jika kunci KMS Anda dinonaktifkan dan Anda mencoba membagikan kerangka kerja khusus, operasi gagal. Untuk petunjuk tentang cara

mengaktifkan kunci KMS yang dinonaktifkan, lihat Mengaktifkan dan menonaktifkan kunci di Panduan Pengembang. AWS Key Management Service

Permintaan berbagi saya memiliki titik biru di sebelahnya. Apa artinya ini?

Pemberitahuan titik biru menunjukkan bahwa permintaan berbagi membutuhkan perhatian Anda.

Pemberitahuan titik biru untuk pengirim

Titik notifikasi biru muncul di sebelah permintaan berbagi terkirim dengan status Kedaluwarsa. Audit Manager menampilkan notifikasi titik biru sehingga Anda dapat mengingatkan penerima untuk mengambil tindakan atas permintaan berbagi sebelum berakhir.

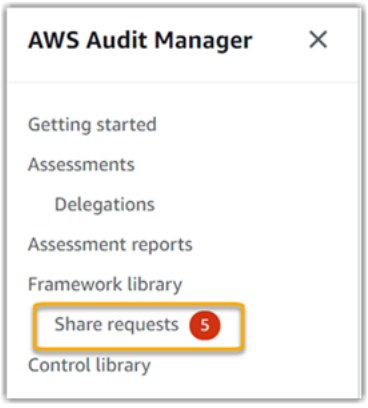
Agar titik notifikasi biru menghilang, penerima harus menerima atau menolak permintaan. Titik biru juga menghilang jika Anda mencabut permintaan berbagi.

Anda dapat menggunakan prosedur berikut untuk memeriksa permintaan berbagi yang kedaluwarsa, dan mengirim pengingat opsional kepada penerima untuk mengambil tindakan.

Untuk melihat notifikasi untuk permintaan terkirim

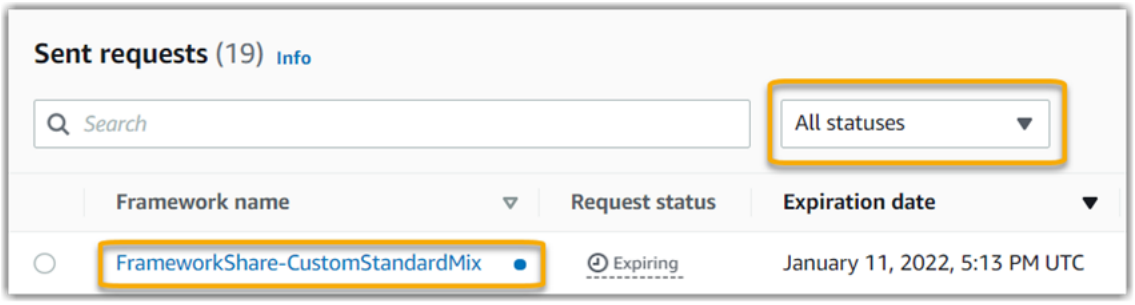
1. Buka konsol AWS Audit Manager di https://console.aws.amazon.com/auditmanager/home.
2. Jika Anda memiliki pemberitahuan permintaan berbagi, Audit Manager akan menampilkan titik merah di sebelah ikon menu navigasi.

3. Perluas panel navigasi dan lihat di sebelah Permintaan Bagikan. Lencana notifikasi menunjukkan jumlah permintaan berbagi yang perlu diperhatikan.



4. Pilih Bagikan permintaan, lalu pilih tab Permintaan terkirim.

5. Cari titik biru untuk mengidentifikasi permintaan berbagi yang kedaluwarsa dalam 30 hari ke depan. Atau, Anda juga dapat melihat permintaan berbagi kedaluwarsa dengan memilih Kedaluwarsa dari dropdown filter Semua status.



6. (Opsional) Ingatkan penerima bahwa mereka perlu mengambil tindakan atas permintaan berbagi sebelum berakhir. Langkah ini bersifat opsional, karena Audit Manager mengirimkan notifikasi di konsol untuk memberi tahu penerima saat permintaan berbagi aktif atau kedaluwarsa. Namun, Anda juga dapat mengirim pengingat Anda sendiri ke penerima menggunakan saluran komunikasi pilihan Anda.

Pemberitahuan titik biru untuk penerima

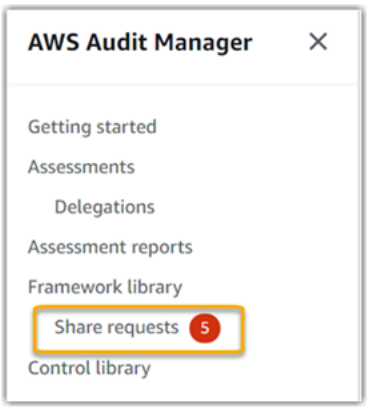
Titik notifikasi biru muncul di sebelah permintaan berbagi yang diterima dengan status Aktif atau Kedaluwarsa. Audit Manager menampilkan notifikasi titik biru untuk mengingatkan Anda untuk mengambil tindakan atas permintaan berbagi sebelum berakhir. Agar titik notifikasi biru menghilang, Anda harus menerima atau menolak permintaan. Titik biru juga menghilang jika pengirim mencabut permintaan berbagi.

Anda dapat menggunakan prosedur berikut untuk memeriksa permintaan berbagi yang aktif dan kedaluwarsa.

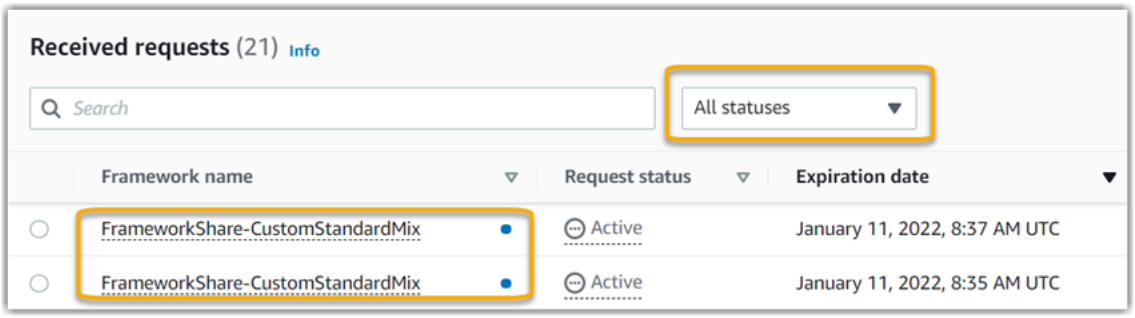
Untuk melihat notifikasi untuk permintaan yang diterima

1. Buka konsol AWS Audit Manager di https://console.aws.amazon.com/auditmanager/home.
2. Jika Anda memiliki pemberitahuan permintaan berbagi, Audit Manager akan menampilkan titik merah di sebelah ikon menu navigasi.

3. Perluas panel navigasi dan lihat di sebelah Permintaan Bagikan. Lencana notifikasi menunjukkan jumlah permintaan berbagi yang perlu Anda perhatikan.



4. Pilih Berbagi permintaan. Secara default, halaman ini terbuka di tab Permintaan Diterima.
5. Identifikasi permintaan berbagi yang memerlukan tindakan Anda dengan mencari item dengan titik biru.



6. (Opsional) Untuk hanya melihat permintaan yang kedaluwarsa dalam 30 hari ke depan, cari daftar tarik-turun Semua status dan pilih Kedaluwarsa.

Kerangka kerja bersama saya memiliki kontrol yang menggunakan AWS Config aturan khusus sebagai sumber data. Dapatkah penerima mengumpulkan bukti untuk kontrol ini?

Ya, penerima Anda dapat mengumpulkan bukti untuk kontrol ini, tetapi beberapa langkah diperlukan untuk mencapai ini.

Agar Audit Manager mengumpulkan bukti menggunakan AWS Config aturan sebagai pemetaan sumber data, berikut ini harus benar. Kriteria ini berlaku untuk aturan terkelola dan aturan khusus.

- Aturan harus ada di AWS lingkungan penerima.
- Aturan harus diaktifkan di AWS lingkungan penerima.

Ingat bahwa AWS Config aturan di akun Anda kemungkinan belum ada di AWS lingkungan penerima. Selain itu, ketika penerima menerima permintaan berbagi, Audit Manager tidak membuat ulang aturan kustom Anda di akun mereka. Agar penerima dapat mengumpulkan bukti menggunakan aturan kustom Anda sebagai pemetaan sumber data, mereka harus membuat aturan kustom yang sama dalam contoh mereka. AWS Config Setelah penerima membuat dan kemudian mengaktifkan aturanAWS Config, Audit Manager dapat mengumpulkan bukti dari sumber data tersebut.

Kami menyarankan Anda berkomunikasi dengan penerima untuk memberi tahu mereka jika ada AWS Config aturan khusus yang harus dibuat dalam contoh merekaAWS Config.

Saya memperbarui aturan khusus yang digunakan dalam kerangka kerja bersama. Apakah saya perlu mengambil tindakan apa pun?

Untuk pembaruan aturan di AWS lingkungan Anda

Bila Anda memperbarui aturan kustom dalam AWS lingkungan Anda, tidak ada tindakan yang diperlukan di Audit Manager. Audit Manager mendeteksi dan menangani pembaruan aturan dengan cara yang dijelaskan dalam tabel berikut. Audit Manager tidak memberi tahu Anda saat pembaruan aturan terdeteksi.

Skenario	Apa yang dilakukan Audit Manager	Apa yang perlu Anda lakukan
Aturan khusus diperbaru i dalam contoh AndaAWS Config.	Audit Manager terus melaporkan temuan untuk aturan tersebut menggunakan definisi aturan yang diperbarui.	Tidak ada tindakan yang diperlukan.
Aturan kustom dihapus dalam contoh AndaAWS Config.	Audit Manager menghenti kan pelaporan temuan untuk aturan yang dihapus.	Tidak ada tindakan yang diperlukan. Jika mau, Anda dapat mengedit kontrol khusus yang menggunakan aturan yang dihapus sebagai pemetaan sumber data. Anda kemudian dapat menghapus aturan yang dihapus untuk membersih

Skenario	Apa yang dilakukan Audit Manager	Apa yang perlu Anda lakukan
		kan pengaturan sumber data kontrol Anda. Jika tidak, nama aturan yang dihapus tetap sebagai pemetaan sumber data yang tidak digunakan.

Untuk pembaruan aturan di luar AWS lingkungan Anda

Di AWS lingkungan penerima, Audit Manager tidak mendeteksi pembaruan aturan. Ini karena pengirim dan penerima masing-masing bekerja di lingkungan yang terpisahAWS. Tabel berikut memberikan tindakan yang disarankan untuk skenario ini.

Peran Anda	Skenario	Tindakan yang disarankan
Sender	• Anda berbagi kerangka kerja yang menggunakan aturan kustom sebagai pemetaan sumber data. • Setelah membagikan kerangka kerja, Anda memperbarui atau menghapus salah satu aturan tersebutAWS Config.	Hubungi penerima untuk memberi tahu mereka tentang pembaruan. Dengan begitu, mereka dapat membuat pembaruan yang sama dan tetap sinkron dengan definisi aturan terbaru.
Penerir	• Anda menerima kerangka kerja bersama yang menggunakan aturan kustom sebagai pemetaan sumber data. • Setelah Anda membuat ulang aturan kustom dalam instance AndaAWS Config, pengirim memperbarui atau menghapus salah satu aturan tersebut.	Buat pembaruan aturan yang sesuai dalam contoh Anda sendiriAWS Config.

Memecahkan masalah pemberitahuan

Anda dapat menggunakan informasi di halaman ini untuk mengatasi masalah pemberitahuan umum di Audit Manager.

Topik

Saya menentukan topik Amazon SNS di Audit Manager, tetapi saya tidak menerima pemberitahuan apa pun

Jika topik Amazon SNS Anda menggunakan AWS KMS enkripsi sisi server (SSE), Anda mungkin kehilangan izin yang diperlukan untuk kebijakan utama Anda. AWS KMS Anda mungkin juga gagal menerima pemberitahuan jika Anda tidak berlangganan titik akhir ke topik Anda.

Jika Anda tidak menerima notifikasi, pastikan Anda melakukan hal berikut:

- Anda melampirkan kebijakan izin yang diperlukan ke kunci KMS Anda. Contoh kebijakan tersedia di halaman Pemberitahuan panduan ini.
- Anda berlangganan titik akhir ke topik yang mengirimkan notifikasi. Ketika Anda berlangganan titik akhir email ke topik, Anda menerima email yang meminta Anda untuk mengonfirmasi langganan Anda. Anda harus mengonfirmasi langganan Anda untuk mulai menerima pemberitahuan email. Untuk informasi selengkapnya, lihat Memulai di Panduan Pengembang Amazon SNS.

Saya menentukan topik FIFO, tetapi saya tidak menerima pemberitahuan dalam urutan yang diharapkan

Audit Manager mendukung pengiriman pemberitahuan ke topik FIFO SNS. Namun, urutan di mana Audit Manager mengirimkan pemberitahuan ke topik FIFO Anda tidak dijamin.

Memecahkan masalah izin dan akses

Anda dapat menggunakan informasi di halaman ini untuk menyelesaikan masalah izin umum di Audit Manager.

Topik

Saya mengikuti prosedur penyiapan Audit Manager, tetapi saya tidak memiliki cukup hak IAM

Pengguna, peran, atau grup yang Anda gunakan untuk mengakses Audit Manager harus memiliki izin yang diperlukan. Selain itu, kebijakan berbasis identitas Anda tidak boleh terlalu membatasi. Jika tidak, konsol tidak akan berfungsi sebagaimana dimaksud. Prosedur Pengaturan dalam panduan ini memberikan kebijakan yang memberikan izin minimum yang diperlukan untuk menyiapkan Audit Manager. Bergantung pada kasus penggunaan Anda, Anda mungkin memerlukan izin yang lebih luas dan tidak terlalu ketat. Misalnya, kami menyarankan agar pemilik audit memiliki akses administrator. Ini agar mereka dapat memodifikasi pengaturan Audit Manager dan mengelola sumber daya seperti penilaian, kerangka kerja, kontrol, dan laporan penilaian. Pengguna lain, seperti delegasi, mungkin hanya memerlukan akses manajemen atau akses hanya-baca.

Pastikan Anda menambahkan izin yang sesuai untuk pengguna, peran, atau grup Anda. Untuk pemilik audit, kebijakan yang disarankan adalah AWSAuditManagerAdministratorAccess. Untuk delegasi, Anda dapat menggunakan contoh ini yang disediakan di halaman contoh kebijakan IAM. Anda dapat menggunakan contoh kebijakan ini sebagai titik awal, dan membuat perubahan seperlunya agar sesuai dengan kebutuhan Anda.

Kami menyarankan Anda meluangkan waktu untuk menyesuaikan izin Anda untuk memenuhi persyaratan spesifik Anda. Jika Anda memerlukan bantuan dengan izin IAM, hubungi administrator atau Support AWS Anda.

Saya menentukan seseorang sebagai pemilik audit, tetapi mereka masih belum memiliki akses penuh ke penilaian. Mengapa ini?

Menentukan seseorang sebagai pemilik audit saja tidak memberi mereka akses penuh ke penilaian. Pemilik audit juga harus memiliki izin IAM yang diperlukan untuk mengakses dan mengelola sumber daya Audit Manager. Dengan kata lain, selain menentukan pengguna sebagai pemilik audit, Anda juga harus melampirkan kebijakan IAM yang diperlukan kepada pengguna tersebut. Ide di balik ini adalah bahwa, dengan mewajibkan keduanya, Audit Manager memastikan bahwa Anda memiliki kendali penuh atas semua spesifikasi setiap penilaian.

> **Note**
>
> Untuk pemilik audit, kami sarankan Anda menggunakan AWSAuditManagerAdministratorAccesskebijakan ini. Untuk informasi selengkapnya, lihat Kebijakan yang disarankan untuk persona pengguna di Audit Manager.

Saya tidak dapat melakukan tindakan di Audit Manager

Jika Anda tidak memiliki izin yang diperlukan untuk menggunakan AWS Audit Manager konsol atau operasi Audit Manager API, kemungkinan besar Anda akan mengalami `AccessDeniedException` kesalahan.

Untuk mengatasi masalah ini, Anda harus menghubungi administrator Anda untuk mendapatkan bantuan. Administrator Anda adalah orang yang memberi Anda kredensi masuk Anda.

Saya ingin mengizinkan orang di luar saya Akun AWS untuk mengakses sumber daya Audit Manager saya

Anda dapat membuat peran yang dapat digunakan para pengguna di akun lain atau orang-orang di luar organisasi Anda untuk mengakses sumber daya Anda. Anda dapat menentukan siapa 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 akses kepada orang ke sumber daya Anda.

Untuk mempelajari selengkapnya, periksa hal berikut:

- Untuk mengetahui apakah Audit Manager mendukung fitur ini, lihatBagaimana AWS Audit Manager bekerja dengan IAM.

- Untuk mempelajari cara memberikan akses ke sumber daya di seluruh Akun AWS yang Anda miliki, silakan lihat Menyediakan akses ke pengguna IAM di Akun AWS lainnya yang Anda miliki di Panduan Pengguna IAM.
- Untuk mempelajari cara memberikan akses ke sumber daya Anda ke pihak ketiga Akun AWS, silakan lihat Menyediakan akses ke akun Akun AWS yang dimiliki oleh pihak ketiga dalam Panduan Pengguna IAM.
- Untuk mempelajari cara memberikan akses melalui federasi identitas, silakan lihat Menyediakan akses ke pengguna terautentikasi eksternal (gabungan identitas) di Panduan Pengguna IAM .
- Untuk mempelajari perbedaan antara penggunaan kebijakan peran dan kebijakan berbasis sumber daya untuk akses lintas akun, silakan lihat Bagaimana peran IAM berbeda dari kebijakan berbasis sumber daya di Panduan Pengguna IAM.

Lihat juga

Halaman berikut berisi panduan pemecahan masalah untuk masalah lain yang dapat disebabkan oleh izin yang hilang:

- Saya tidak dapat melihat kontrol atau set kontrol apa pun dalam penilaian saya
- Opsi aturan khusus tidak tersedia saat saya mengonfigurasi sumber data kontrol
- Saya mendapatkan kesalahan akses ditolak ketika saya mencoba membuat laporan penilaian
- Saya mendapatkan kesalahan akses ditolak ketika saya mencoba membuat laporan penilaian menggunakan akun administrator yang didelegasikan
- Saya tidak dapat mengaktifkan pencari bukti
- Saya tidak dapat menonaktifkan pencari bukti
- Kueri penelusuran saya gagal di pencari bukti
- Saya menentukan topik Amazon SNS di Audit Manager, tetapi saya tidak menerima pemberitahuan apa pun

Kuota dan batasan untukAWS Audit Manager

AndaAkun AWS memiliki kuota default, yang sebelumnya disebut sebagai batasan, untuk masing-masing layananLayanan AWS. Kecuali dinyatakan lain, setiap kuota bersifat khusus per Wilayah. Anda dapat meminta kenaikan untuk beberapa kuota, dan kuota lainnya tidak dapat ditingkatkan.

Sebagian besar kuota Audit Manager, tetapi tidak semuanya, tercantum di bawahAWS Audit Manager namespace di konsol Service Quotas. Untuk mempelajari cara meminta kenaikan kuota, lihatMengelola kuota Audit Manager.

Kuota Audit Manager Default

AWS Audit ManagerKuota berikut adalahAkun AWS per Wilayah.

Penilaian

- Jumlah penilaian aktif per akun: 100

Laporan penilaian

- Jumlah item bukti yang dapat Anda tambahkan ke laporan penilaian:
  - Untuk laporan wilayah yang sama (di mana penilaian dan tujuan laporan penilaian S3 bucket adalah samaWilayah AWS): 22.000
  - Untuk laporan lintas wilayah (di mana penilaian dan tujuan laporan penilaian S3 bucket berbedaWilayah AWS): 3.500
  - Untuk laporan di mana penilaian terkait menggunakan pelanggan yang dikelolaAWS KMS key: 3.500

Kontrol

- Jumlah kontrol khusus per akun: 500

Bukti

- Ukuran maksimum dari satu file bukti manual: 100 MB
- Jumlah unggahan bukti manual harian per kontrol: 100

> **Tip**
>
> Jika Anda perlu mengunggah sejumlah besar bukti manual ke satu kontrol, kami sarankan Anda mengunggah bukti Anda dalam batch selama beberapa hari.

Kerangka

- Jumlah kerangka kerja khusus per akun: 100

> **Note**
>
> Kuota kerangka kerja berlaku untuk semua kerangka kerja kustom bersama di perpustakaan kerangka kerja Anda, terlepas dari siapa yang membuat kerangka kerja.

Penerima kerangka kerja khusus bersama

- Jumlah akun penerima aktif: 100

Akses API

- Jumlah Transaksi per detik (TPS) di semua API: 20 TPS

Mengelola kuota Audit Manager

AWS Audit Managerterintegrasi dengan Service Quotas,Layanan AWS yang memungkinkan Anda melihat dan mengelola kuota dari lokasi pusat. Untuk informasi selengkapnya, lihat Apa itu Service Quotas? di Panduan Pengguna Service Quotas. Service Quotas memudahkan Anda untuk mencari nilai kuota Audit Manager Anda.

Untuk melihat kuota layanan Audit Manager menggunakan konsol

1. Buka konsol Service Quotas di https://console.aws.amazon.com/servicequotas/.
2. Di panel navigasi, pilih Layanan AWS.
3. Dari Layanan AWSdaftar, cari dan pilih AWS Audit Manager.

4. Di daftar Kuota layanan, Anda dapat melihat nama kuota layanan, nilai yang diterapkan (jika tersedia), nilaiAWS default, dan apakah kuota dapat disesuaikan.
5. Untuk melihat informasi tambahan tentang service quotas, seperti deskripsi, pilih nama kuota.
6. (Opsional) Untuk meminta peningkatan kuota, pilih kuota yang ingin Anda tingkatkan, kemudian pilih Meminta peningkatan kuota, masukkan atau pilih informasi yang diperlukan, dan pilih Minta.

Untuk informasi lebih lanjut, lihat Meminta peningkatan kuota di Panduan Pengguna Service Quotas.

Keamanan di AWS Audit Manager

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 dari 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 ProgramAWS Kepatuhan ProgramAWS Kepatuhan . Untuk mempelajari tentang program kepatuhan yang berlaku AWS Audit Manager, lihat AWS Layanan dalam Lingkup olehAWS Layanan 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 Audit Manager. Topik berikut menunjukkan cara mengonfigurasi Audit Manager untuk memenuhi tujuan keamanan dan kepatuhan Anda. Anda juga mempelajari cara menggunakan AWS layanan lain yang membantu Anda memantau dan mengamankan sumber daya Audit Manager Anda.

Topik

Perlindungan data di AWS Audit Manager

Model tanggung jawab AWS bersama model berlaku untuk perlindungan data di AWS Audit Manager. Seperti yang dijelaskan dalam model AWS ini, bertanggung jawab untuk melindungi infrastruktur global yang menjalankan semua AWS Cloud. Anda bertanggung jawab untuk memelihara kendali atas isi yang dihost 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 GDPRAWS di Blog KeamananAWS .

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

- Gunakan autentikasi multi-faktor (MFA) pada setiap akun.
- Gunakan SSL/TLS untuk berkomunikasi dengan sumber daya. AWS Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Siapkan API dan pencatatan aktivitas pengguna dengan AWS CloudTrail.
- Gunakan solusi AWS enkripsi, bersama dengan semua kontrol keamanan default di dalamnya 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 Audit Manager 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.

Selain rekomendasi di atas, kami merekomendasikan secara khusus agar pelanggan Audit Manager tidak menyertakan informasi identifikasi sensitif di bidang bentuk bebas saat membuat penilaian, kontrol kustom, kerangka kerja khusus, dan komentar delegasi.

Penghapusan data Audit Manager

Ada beberapa cara agar data Audit Manager dapat dihapus.

Penghapusan data saat menonaktifkan Audit Manager

Ketika Anda menonaktifkan Audit Manager, Anda dapat memutuskan apakah Anda ingin menghapus semua data Audit Manager Anda. Jika Anda memilih untuk menghapus data, data tersebut akan dihapus dalam waktu 7 hari setelah menonaktifkan Audit Manager. Setelah data Anda dihapus, Anda tidak dapat memulihkannya.

Penghapusan data otomatis

Beberapa data Audit Manager dihapus secara otomatis setelah periode waktu tertentu. Audit Manager menyimpan data pelanggan sebagai berikut.

Tipe data	Periode retensi data	Catatan
Bukti	Data disimpan selama 2 tahun sejak saat pembuatan	Termasuk bukti otomatis dan bukti manual
Sumber daya yang dibuat pelanggan	Data disimpan tanpa batas	Termasuk penilaian, laporan penilaian, kontrol kustom, dan kerangka kerja khusus

Penghapusan data manual

Anda dapat menghapus sumber daya Audit Manager individual kapan saja. Untuk petunjuk, lihat yang berikut ini:

- Menghapus penilaian
  - Lihat juga: DeleteAssessmentdi ReferensiAWS Audit Manager API
- Menghapus kerangka kerja khusus
  - Lihat juga: DeleteAssessmentFrameworkdi ReferensiAWS Audit Manager API
- Menghapus permintaan berbagi
  - Lihat juga: DeleteAssessmentFrameworkSharedi ReferensiAWS Audit Manager API
- Menghapus laporan penilaian
  - Lihat juga: DeleteAssessmentReportdi ReferensiAWS Audit Manager API
- Menghapus kontrol khusus
  - Lihat juga: DeleteControldi ReferensiAWS Audit Manager API

Untuk menghapus data sumber daya lain yang mungkin telah Anda buat saat menggunakan Audit Manager, lihat berikut ini:

- Menghapus penyimpanan data acara di PanduanAWS CloudTrail Pengguna
- Menghapus bucket di Panduan Pengguna Amazon Simple Storage Service (Amazon S3)

Enkripsi diam

Untuk mengenkripsi data saat istirahat, Audit Manager menggunakan enkripsi sisi server Kunci yang dikelola AWS untuk semua penyimpanan data dan lognya.

Data Anda dienkripsi di bawah kunci yang dikelola pelanggan atau Kunci milik AWS, tergantung pada pengaturan yang Anda pilih. Jika Anda tidak memberikan kunci terkelola pelanggan, Audit Manager menggunakan kunci Kunci milik AWS untuk mengenkripsi konten Anda. Semua metadata layanan di DynamoDB dan Amazon S3 di Audit Manager dienkripsi menggunakan file. Kunci milik AWS

Audit Manager mengenkripsi data sebagai berikut:

- Metadata layanan yang disimpan di Amazon S3 dienkripsi di bawah menggunakan SSE-KMS. Kunci milik AWS
- Metadata layanan yang disimpan di DynamoDB adalah sisi server yang dienkripsi menggunakan KMS dan file. Kunci milik AWS
- Konten Anda yang disimpan di DynamoDB dienkripsi sisi klien menggunakan kunci yang dikelola pelanggan atau kunci. Kunci milik AWSKunci KMS didasarkan pada pengaturan yang Anda pilih.

- Konten Anda yang disimpan di Amazon S3 di Audit Manager dienkripsi menggunakan SSE-KMS. Kunci KMS didasarkan pada pilihan Anda, dan bisa berupa kunci yang dikelola pelanggan atau kunci. Kunci milik AWS
- Laporan penilaian yang dipublikasikan ke bucket S3 Anda dienkripsi sebagai berikut:
  - Jika Anda memberikan kunci terkelola pelanggan, data Anda dienkripsi menggunakan SSE-KMS.
  - Jika Anda menggunakan Kunci milik AWS, data Anda dienkripsi menggunakan SSE-S3.

Enkripsi dalam bergerak

Audit Manager menyediakan endpoint yang aman dan pribadi untuk mengenkripsi data dalam perjalanan. Endpoint yang aman dan pribadi memungkinkan AWS untuk melindungi integritas permintaan API ke Audit Manager.

Transit antar layanan

Secara default, semua komunikasi antar layanan dilindungi dengan menggunakan enkripsi Transport Layer Security (TLS).

Manajemen kunci

Audit Manager mendukung kunci terkelola Kunci milik AWS dan pelanggan untuk mengenkripsi semua sumber daya Audit Manager (penilaian, kontrol, kerangka kerja, bukti, dan laporan penilaian yang disimpan ke bucket S3 di akun Anda).

Kami menyarankan Anda menggunakan kunci yang dikelola pelanggan. Dengan demikian, Anda dapat melihat dan mengelola kunci enkripsi yang melindungi data Anda, termasuk melihat log penggunaannya AWS CloudTrail. Ketika Anda memilih kunci yang dikelola pelanggan, Audit Manager membuat hibah pada kunci KMS sehingga dapat digunakan untuk mengenkripsi konten Anda.

> **Warning**
>
> Setelah menghapus atau menonaktifkan kunci KMS yang digunakan untuk mengenkripsi sumber daya Audit Manager, Anda tidak dapat lagi mendekripsi sumber daya yang dienkripsi di bawah kunci KMS tersebut, yang berarti bahwa data menjadi tidak dapat dipulihkan.

Menghapus kunci KMS di AWS Key Management Service (AWS KMS) bersifat merusak dan berpotensi berbahaya. Untuk informasi selengkapnya tentang menghapus kunci KMS, lihat Menghapus AWS KMS keysdi Panduan Pengguna.AWS Key Management Service

Anda dapat menentukan setelan enkripsi saat mengaktifkan Audit Manager menggunakan AWS Management Console, Audit Manager API, atau AWS Command Line Interface (AWS CLI). Untuk petunjuk, lihat Aktifkan AWS Audit Manager.

Anda dapat meninjau dan mengubah pengaturan enkripsi Anda kapan saja. Untuk petunjuk, lihat Enkripsi data.

Untuk informasi selengkapnya tentang cara mengatur kunci terkelola pelanggan, lihat Membuat kunci di PanduanAWS Key Management Service Pengguna.

Identitas dan manajemen akses untuk AWS Audit Manager

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 Audit Manager. IAM adalah Layanan AWS yang dapat Anda gunakan tanpa biaya tambahan.

Topik

- Audiens
- Mengautentikasi dengan identitas
- Mengelola akses menggunakan kebijakan
- Bagaimana AWS Audit Manager bekerja dengan IAM
- Contoh kebijakan berbasis identitas untuk AWS Audit Manager
- Pencegahan confused deputy lintas layanan
- AWS kebijakan terkelola untuk AWS Audit Manager
- Memecahkan masalah AWS Audit Manager identitas dan akses
- Menggunakan peran terkait layanan untuk AWS Audit Manager

Audiens

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

Pengguna layanan — Jika Anda menggunakan layanan Audit Manager untuk melakukan pekerjaan Anda, administrator Anda memberi Anda kredensi dan izin yang Anda butuhkan. Saat Anda menggunakan lebih banyak fitur Audit Manager untuk melakukan pekerjaan Anda, Anda mungkin memerlukan izin tambahan. Memahami cara akses dikelola dapat membantu Anda meminta izin yang tepat dari administrator Anda. Jika Anda tidak dapat mengakses fitur di Audit Manager, lihatMemecahkan masalah AWS Audit Manager identitas dan akses.

Administrator layanan - Jika Anda bertanggung jawab atas sumber daya Audit Manager di perusahaan Anda, Anda mungkin memiliki akses penuh ke Audit Manager. Tugas Anda adalah menentukan fitur dan sumber daya Audit Manager mana yang harus diakses pengguna layanan Anda. Kemudian, Anda harus mengirimkan permintaan kepada administrator IAM Anda 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 dengan Audit Manager, lihatBagaimana AWS Audit Manager bekerja dengan IAM.

Administrator IAM - Jika Anda administrator IAM, Anda mungkin ingin mempelajari detail tentang cara menulis kebijakan untuk mengelola akses ke Audit Manager. Untuk melihat contoh kebijakan berbasis identitas Audit Manager yang dapat Anda gunakan di IAM, lihat. Contoh kebijakan berbasis identitas untuk AWS Audit Manager

Mengautentikasi dengan identitas

Otentikasi adalah cara Anda masuk AWS menggunakan kredensyal 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 gabungan, 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 PanduanAWS 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 lebih lanjut, lihat Autentikasi multi-faktor dalam Panduan PenggunaAWS IAM Identity Center dan Menggunakan autentikasi multi-faktor (MFA) di AWS dalam Panduan Pengguna IAM.

Akun AWS pengguna root

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 Anda. Lindungi kredensial pengguna root Anda dan gunakan kredensial tersebut untuk melakukan tugas yang hanya dapat dilakukan pengguna root. Untuk daftar tugas lengkap yang mengharuskan Anda masuk sebagai pengguna root, lihat Tugas yang memerlukan kredensial pengguna root dalam Panduan Pengguna IAM.

Identitas terfederasi

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

Identitas federasi adalah pengguna dari direktori pengguna perusahaan Anda, penyedia identitas web, direktori Pusat Identitas AWS Directory Service, atau pengguna mana pun yang mengakses Layanan AWS dengan menggunakan kredensil yang disediakan melalui sumber identitas. Ketika identitas federasi mengakses Akun AWS, mereka mengambil peran, dan peran memberikan kredensyal sementara.

Untuk pengelolaan akses terpusat, sebaiknya Anda menggunakan AWS IAM Identity Center. Anda dapat membuat pengguna dan grup di Pusat Identitas IAM, atau Anda dapat menghubungkan dan menyinkronkan ke sekumpulan pengguna dan grup di sumber identitas Anda sendiri untuk digunakan di semua aplikasi Akun AWS dan aplikasi Anda. Untuk informasi tentang Pusat Identitas IAM, lihat Apa yang dimaksud Pusat Identitas IAM? dalam Panduan PenggunaAWS IAM Identity Center .

Pengguna dan grup IAM

Pengguna IAM adalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus untuk satu orang atau aplikasi. Jika memungkinkan, sebaiknya andalkan kredensial temporer, dan bukan membuat pengguna IAM yang memiliki kredensial jangka panjang seperti kata sandi dan kunci akses. Namun, jika Anda memiliki kasus penggunaan khusus yang memerlukan kredensial jangka panjang dengan pengguna IAM, sebaiknya rotasikan 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 kumpulan pengguna IAM. Anda tidak dapat masuk sebagai grup. Anda dapat menggunakan grup untuk menentukan izin untuk beberapa pengguna sekaligus. Grup membuat izin lebih mudah dikelola untuk sekelompok besar pengguna. Misalnya, Anda dapat memiliki grup yang bernama IAMAdmins dan memberikan izin kepada grup tersebut untuk mengelola sumber daya IAM.

Pengguna berbeda dari peran. Pengguna secara unik terkait dengan satu orang atau aplikasi, tetapi peran tersebut dimaksudkan untuk dapat diambil oleh siapa pun yang membutuhkannya. Pengguna memiliki kredensial jangka panjang permanen, tetapi peran memberikan kredensial sementara. Untuk mempelajari selengkapnya, silakan 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 metode untuk menggunakan peran, lihat Menggunakan peran IAM dalam Panduan Pengguna IAM.

Peran IAM dengan kredensial sementara berguna dalam situasi berikut:

- Akses pengguna gabungan – Untuk menetapkan izin ke sebuah identitas gabungan, Anda dapat membuat peran dan menentukan izin untuk peran tersebut. Saat identitas terfederasi diautentikasi, identitas tersebut dikaitkan dengan peran dan diberikan izin yang ditentukan oleh peran. Untuk informasi tentang peran untuk federasi, lihat Membuat peran untuk Penyedia Identitas pihak ketiga dalam Panduan Pengguna IAM. Jika Anda menggunakan Pusat Identitas IAM, Anda mengonfigurasi sekumpulan izin. Untuk mengontrol apa yang dapat diakses identitas Anda setelah identitas tersebut diautentikasi, Pusat Identitas IAM mengaitkan izin yang ditetapkan ke peran dalam IAM. Untuk informasi tentang rangkaian izin, lihat Rangkaian izin dalam Panduan PenggunaAWS 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 (pengguna utama tepercaya) dengan akun berbeda untuk mengakses sumber daya yang ada 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 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.
- Akses lintas layanan — Beberapa Layanan AWS menggunakan fitur lain Layanan AWS. Contoh, ketika Anda melakukan panggilan dalam layanan, umumnya layanan tersebut menjalankan aplikasi di Amazon EC2 atau menyimpan objek di Amazon S3. Suatu layanan mungkin melakukan hal tersebut menggunakan izin pengguna utama panggilan, 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 tindakan yang kemudian memulai 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 Meneruskan sesi akses.
  - Peran IAM – Peran layanan adalah peran IAM yang diambil layanan untuk melakukan tindakan atas nama Anda. Administrator IAM dapat membuat, memodifikasi, dan menghapus

peran layanan dari dalam IAM. Untuk informasi selengkapnya, lihat Membuat 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 AWSLayanan tersebut dapat mengambil peran untuk melakukan sebuah 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 di 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 Ikhtisar kebijakan JSON dalam Panduan Pengguna IAM.

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

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

Kebijakan IAM mendefinisikan izin untuk suatu tindakan terlepas dari metode yang Anda gunakan untuk operasi. Sebagai contoh, anggap saja 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 pengguna dan peran, di sumber daya mana, dan dengan ketentuan 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 terkelola. 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 AWSKebijakan 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 dalam Panduan Pengguna IAM.

Kebijakan berbasis sumber daya

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

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

Daftar kontrol akses (ACL)

Daftar kontrol akses (ACL) mengendalikan pengguna utama mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACL sama dengan kebijakan berbasis sumber daya, meskipun tidak menggunakan format dokumen kebijakan JSON.

Amazon S3, AWS WAF, dan Amazon VPC adalah contoh layanan yang mendukung ACL. Untuk mempelajari ACL selengkapnya, silakan lihat Gambaran umum daftar kontrol akses (ACL) di Panduan Developer Layanan Penyimpanan Ringkas Amazon.

Tipe kebijakan lain

AWS mendukung jenis kebijakan tambahan yang kurang umum. Tipe-tipe kebijakan ini dapat mengatur izin maksimum yang diberikan kepada Anda berdasarkan tipe kebijakan yang lebih umum.

- Batasan izin – Batasan izin adalah fitur lanjutan di mana Anda menetapkan izin maksimum yang dapat diberikan oleh kebijakan berbasis identitas kepada entitas IAM (pengguna 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 secara eksplisit terhadap salah satu kebijakan ini akan mengesampingkan izin tersebut. 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 dalam organisasi, Anda dapat menerapkan kebijakan kontrol layanan (SCP) ke sebagian atau semua akun Anda. SCP membatasi izin untuk entitas di akun anggota, termasuk masing-masing. Pengguna root akun AWSUntuk informasi selengkapnya tentang Organisasi dan SCP, lihat Cara kerja SCP dalam Panduan PenggunaAWS Organizations .
- Kebijakan sesi – Kebijakan sesi adalah kebijakan lanjutan yang Anda teruskan sebagai parameter saat Anda membuat sesi sementara secara terprogram untuk peran atau pengguna gabungan. 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 di salah satu kebijakan ini akan membatalkan izin tersebut. Untuk informasi selengkapnya, lihat Kebijakan sesi dalam Panduan Pengguna IAM.

Berbagai jenis kebijakan

Jika beberapa jenis kebijakan diberlakukan untuk satu 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 Audit Manager bekerja dengan IAM

Sebelum Anda menggunakan IAM untuk mengelola akses ke Audit Manager, pelajari fitur IAM apa yang tersedia untuk digunakan dengan Audit Manager.

Fitur IAM yang dapat Anda gunakan AWS Audit Manager

Fitur IAM	Dukungan Audit Manager
Kebijakan berbasis identitas	Ya
Kebijakan berbasis sumber daya	Tidak
Tindakan kebijakan	Ya
Sumber daya kebijakan	Ya
Kunci persyaratan kebijakan	Parsial
ACL	Tidak
ABAC (tanda dalam kebijakan)	Ya
Kredensial sementara	Ya
Sesi akses teruskan (FAS)	Ya
Peran layanan	Tidak
Peran terkait layanan	Ya

Untuk mendapatkan tampilan tingkat tinggi tentang cara AWS Audit Manager dan AWS layanan lain bekerja dengan sebagian besar fitur IAM, lihat AWS layanan yang bekerja dengan IAM di Panduan Pengguna IAM.

Kebijakan berbasis identitas untuk AWS Audit Manager

Mendukung kebijakan berbasis identitas	Ya

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 pengguna dan peran, di sumber daya mana, dan dengan ketentuan apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat Membuat kebijakan IAM dalam Panduan Pengguna IAM.

Dengan kebijakan berbasis identitas IAM, Anda dapat menentukan tindakan dan sumber daya yang diizinkan atau ditolak, serta ketentuan terkait jenis tindakan yang diizinkan atau ditolak. Anda tidak dapat menentukan pengguna utama dalam kebijakan berbasis identitas karena kebijakan ini berlaku untuk pengguna atau peran yang dilampiri kebijakan. Untuk mempelajari semua elemen yang dapat digunakan dalam kebijakan JSON, lihat Referensi elemen kebijakan JSON IAM dalam Panduan Pengguna IAM.

AWS Audit Manager membuat kebijakan terkelola yang diberi nama `AWSAuditManagerAdministratorAccess` untuk administrator Audit Manager. Kebijakan ini memberikan akses administrasi penuh di Audit Manager. Administrator dapat melampirkan kebijakan ini ke peran atau pengguna yang ada, atau membuat peran baru dengan kebijakan ini.

Kebijakan yang disarankan untuk persona pengguna di AWS Audit Manager

AWS Audit Manager memungkinkan Anda untuk mempertahankan pemisahan tugas di antara pengguna yang berbeda dan untuk audit yang berbeda dengan menggunakan kebijakan IAM yang berbeda. Dua persona di Audit Manager dan kebijakan yang direkomendasikan didefinisikan sebagai berikut.

Persona	Deskripsi dan kebijakan yang direkomendasikan
Pemilik audit	• Persona ini harus memiliki izin yang diperlukan untuk mengelola penilaian di. AWS Audit Manager • Kebijakan yang disarankan untuk digunakan untuk persona ini adalah kebijakan terkelola bernama AWSAuditManagerAdministratorAccess. Anda dapat menggunakan kebijakan ini sebagai titik awal, dan cakupan izin ini sesuai kebutuhan agar sesuai dengan kebutuhan Anda.
Mendelegasikan	• Persona ini dapat mengakses set kontrol yang didelegasikan dalam penilaian. Mereka dapat memperbarui status kontrol, menambahkan komentar, mengirimkan set kontrol untuk ditinjau, dan menambahkan bukti ke laporan penilaian.

Persona	Deskripsi dan kebijakan yang direkomendasikan
	• Kebijakan yang disarankan untuk digunakan untuk persona ini adalah contoh kebijakan berikut:Memungkinkan pengguna akses administrator penuh ke AWS Audit Manager. Anda dapat menggunakan kebijakan ini sebagai titik awal, dan membuat perubahan seperlunya agar sesuai dengan kebutuhan Anda.

Contoh kebijakan berbasis identitas untuk AWS Audit Manager

Untuk melihat contoh kebijakan berbasis identitas Audit Manager, lihat. Contoh kebijakan berbasis identitas untuk AWS Audit Manager

Kebijakan berbasis sumber daya dalam AWS Audit Manager

Mendukung kebijakan berbasis sumber daya	Tidak

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

Untuk mengaktifkan akses lintas akun, Anda dapat menentukan seluruh akun atau entitas IAM di akun lain sebagai pengguna utama dalam kebijakan berbasis sumber daya. Menambahkan pengguna utama lintas akun ke kebijakan berbasis sumber daya bagian dari membangun hubungan kepercayaan. Ketika prinsipal dan sumber daya berbeda Akun AWS, administrator IAM di akun tepercaya juga harus memberikan izin entitas utama (pengguna atau peran) untuk mengakses sumber daya. Izin diberikan dengan melampirkan kebijakan berbasis identitas ke entitas tersebut. Namun, jika kebijakan berbasis sumber daya memberikan akses kepada pengguna utama dalam akun yang sama, kebijakan berbasis identitas lainnya tidak diperlukan. Untuk informasi selengkapnya, lihat Perbedaan peran IAM dengan kebijakan berbasis sumber daya di Panduan Pengguna IAM.

Tindakan kebijakan untuk AWS Audit Manager

Mendukung tindakan kebijakan	Ya

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Yaitu, pengguna utama mana yang dapat melakukan tindakan pada sumber daya apa, dan dalam 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 suatu kebijakan untuk memberikan izin melakukan operasi terkait.

Untuk melihat daftar AWS Audit Manager tindakan, lihat Tindakan yang ditentukan oleh AWS Audit Manager di Referensi Otorisasi Layanan.

Tindakan kebijakan AWS Audit Manager menggunakan awalan berikut sebelum tindakan.

```
auditmanager
```

Untuk menetapkan secara spesifik beberapa tindakan dalam satu pernyataan, pisahkan tindakan-tindakan tersebut dengan koma.

```
"Action": [
      "auditmanager:GetEvidenceDetails",
      "auditmanager:GetEvidenceEventDetails"
         ]
```

Anda juga dapat menentukan beberapa tindakan menggunakan wildcard (*). Misalnya, untuk menentukan semua tindakan yang dimulai dengan kata `Get`, sertakan tindakan berikut.

```
"Action": "auditmanager:Get*"
```

Untuk melihat contoh kebijakan berbasis identitas Audit Manager, lihat. Contoh kebijakan berbasis identitas untuk AWS Audit Manager

Sumber daya kebijakan untuk AWS Audit Manager

Mendukung sumber daya kebijakan	Ya

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Yaitu, pengguna utama mana yang dapat melakukan tindakan pada sumber daya apa, dan dalam kondisi apa.

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

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

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

Untuk melihat daftar jenis AWS Audit Manager sumber daya dan ARNnya, lihat Sumber daya yang ditentukan oleh AWS Audit Manager di Referensi Otorisasi Layanan. Untuk mempelajari tentang tindakan yang dapat digunakan untuk menentukan ARN dari setiap sumber daya, lihat Tindakan yang ditentukan oleh AWS Audit Manager.

Penilaian Audit Manager memiliki format Amazon Resource Name (ARN) berikut:

```
arn:${Partition}:auditmanager:${Region}:${Account}:assessment/${assessmentId}
```

Set kontrol Audit Manager memiliki format ARN berikut:

```
arn:${Partition}:auditmanager:${Region}:${Account}:assessment/
${assessmentId}controlSet/${controlSetId}
```

Kontrol Audit Manager memiliki format ARN berikut:

```
arn:${Partition}:auditmanager:${Region}:${Account}:control/${controlId}
```

Untuk informasi lebih lanjut tentang format ARN, lihat Amazon Resource Name (ARN).

Misalnya, untuk menentukan `i-1234567890abcdef0` penilaian dalam pernyataan Anda, gunakan ARN berikut.

```
"Resource": "arn:aws:auditmanager:us-east-1:123456789012:assessment/
i-1234567890abcdef0"
```

Untuk menentukan semua instance milik akun tertentu, gunakan wildcard (*).

```
"Resource": "arn:aws:auditmanager:us-east-1:123456789012:assessment/*"
```

Beberapa tindakan Audit Manager, seperti untuk membuat sumber daya, tidak dapat dilakukan pada sumber daya tertentu. Dalam kasus tersebut, Anda harus menggunakan wildcard (*).

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

Banyak tindakan API Audit Manager melibatkan banyak sumber daya. Misalnya, `ListAssessments` mengembalikan daftar metadata penilaian yang dapat diakses oleh yang saat ini masuk. Akun AWSOleh karena itu, pengguna harus memiliki izin untuk melihat penilaian. Untuk menentukan beberapa sumber daya dalam satu pernyataan, pisahkan ARN dengan koma.

```
"Resource": [
      "resource1",
      "resource2"
```

Untuk melihat daftar jenis sumber daya Audit Manager dan ARNnya, lihat Sumber Daya yang Ditentukan oleh AWS Audit Manager dalam Panduan Pengguna IAM. Untuk mempelajari tentang tindakan yang dengannya Anda dapat menentukan ARN dari setiap sumber daya, lihat Tindakan yang Ditentukan oleh. AWS Audit Manager

Beberapa tindakan API Audit Manager mendukung beberapa sumber daya. Misalnya, `GetChangeLogs` mengakses,, dan `assessmentID` `controlIDcontrolSetId`, jadi prinsipal harus memiliki izin untuk mengakses masing-masing sumber daya ini. Untuk menentukan beberapa sumber daya dalam satu pernyataan, pisahkan ARN dengan koma.

```
"Resource": [
      "assessmentId",
      "controlId",
      "controlSetId"
```

Kunci kondisi kebijakan untuk AWS Audit Manager

Mendukung kunci kondisi kebijakan spesifik layanan	Parsial

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Yaitu, pengguna utama mana yang dapat melakukan tindakan pada sumber daya apa, dan dalam kondisi apa.

Elemen `Condition` (atau blok `Condition`) memungkinkan Anda menentukan kondisi di mana suatu pernyataan akan diterapkan. Elemen `Condition` bersifat opsional. Anda dapat membuat ekspresi kondisional yang menggunakan operator kondisi, misalnya sama dengan atau kurang dari, untuk mencocokkan kondisi dalam kebijakan dengan nilai-nilai yang diminta.

Jika Anda menentukan beberapa elemen `Condition` dalam satu pernyataan, atau beberapa kunci dalam satu elemen `Condition`, AWS akan mengevaluasinya dengan menggunakan operasi `AND` logis. Jika Anda menentukan beberapa nilai untuk satu kunci kondisi, AWS mengevaluasi kondisi menggunakan `OR` operasi logis. Semua kondisi harus dipenuhi sebelum izin pernyataan diberikan.

Ketika prinsipal dalam pernyataan kebijakan adalah prinsipalAWS layanan, kami sangat menyarankan Anda menggunakan `aws:SourceArn`atau kunci kondisi `aws:SourceAccount`global dalam kebijakan. Anda dapat menggunakan kunci konteks kondisi global ini untuk membantu mencegah skenario deputi yang membingungkan. Kebijakan terdokumentasi berikut menunjukkan bagaimana Anda dapat menggunakan kunci konteks kondisi `aws:SourceAccount` global `aws:SourceArn` dan global di Audit Manager untuk mencegah masalah deputi yang membingungkan.

- Contoh kebijakan untuk topik SNS yang digunakan untuk notifikasi Audit Manager
- Contoh kebijakan untuk kunci KMS yang digunakan dengan topik SNS

Anda juga dapat menggunakan variabel placeholder saat menentukan kondisi. Misalnya, Anda dapat memberikan izin pengguna untuk mengakses sumber daya hanya jika ditandai dengan nama

pengguna mereka. Untuk informasi selengkapnya, silakan lihat Elemen kebijakan IAM: variabel dan tanda di Panduan Pengguna IAM.

Audit Manager tidak menyediakan kunci kondisi khusus layanan apa pun, tetapi mendukung penggunaan beberapa kunci kondisi global. Untuk melihat semua kunci kondisi AWS global, lihat kunci konteks kondisiAWS global di Panduan Pengguna IAM.

Daftar kontrol akses (ACL) di AWS Audit Manager

Mendukung ACL	Tidak

Daftar kontrol akses (ACL) mengontrol pengguna utama (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACL sama dengan kebijakan berbasis sumber daya, meskipun tidak menggunakan format dokumen kebijakan JSON.

Kontrol akses berbasis atribut (ABAC) dengan AWS Audit Manager

Mendukung ABAC (tanda dalam kebijakan)	Ya

Kontrol akses berbasis atribut (ABAC) adalah strategi otorisasi yang menentukan izin berdasarkan atribut. Dalam AWS, atribut ini disebut tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke banyak AWS sumber daya. Pemberian tanda ke entitas dan sumber daya adalah langkah pertama dari ABAC. Kemudian rancanglah kebijakan ABAC untuk mengizinkan operasi-operasi ketika tanda milik pengguna utama cocok dengan tanda yang ada di sumber daya yang ingin diakses.

ABAC sangat berguna di lingkungan yang berkembang dengan cepat dan berguna dalam situasi di mana pengelolaan kebijakan menjadi rumit.

Untuk mengendalikan akses berdasarkan tag, berikan informasi tentang tanda di elemen syarat dari sebuh kebijakan dengan menggunakan kunci-kunci persyaratan `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`, atau `aws:TagKeys`.

Jika sebuah layanan mendukung ketiga kunci kondisi untuk setiap jenis sumber daya, nilainya adalah Ya untuk layanan tersebut. Jika suatu layanan mendukung ketiga kunci kondisi hanya untuk beberapa jenis sumber daya, nilainya adalah Parsial.

Untuk informasi selengkapnya tentang ABAC, lihat Apa itu ABAC? di Panduan Pengguna IAM. Untuk melihat tutorial terkait langkah-langkah penyiapan ABAC, lihat Menggunakan kontrol akses berbasis atribut (ABAC) di Panduan Pengguna IAM.

Untuk informasi selengkapnya tentang menandai AWS Audit Manager sumber daya, lihatPenandaan pada sumber daya AWS Audit Manager.

Menggunakan kredensi sementara dengan AWS Audit Manager

Mendukung kredensial sementara	Ya

Beberapa Layanan AWS tidak berfungsi saat Anda masuk menggunakan kredensil sementara. Untuk informasi tambahan, termasuk yang Layanan AWS bekerja dengan kredensi sementara, lihat Layanan AWS yang bekerja dengan IAM di Panduan Pengguna IAM.

Anda menggunakan kredensyal sementara jika Anda masuk AWS Management Console menggunakan metode apa pun kecuali nama pengguna dan kata sandi. Misalnya, ketika Anda mengakses AWS menggunakan tautan masuk tunggal (SSO) perusahaan Anda, proses tersebut secara otomatis membuat kredensil sementara. Anda juga akan membuat kredensial sementara secara otomatis saat masuk ke konsol sebagai pengguna dan kemudian beralih peran. Untuk informasi selengkapnya tentang cara beralih peran, lihat Beralih peran (konsol) di Panduan Pengguna IAM.

Anda dapat membuat kredensyal sementara secara manual menggunakan API AWS CLI atau AWS . Anda kemudian dapat menggunakan kredensil sementara tersebut untuk mengakses. AWS AWS merekomendasikan agar Anda menghasilkan kredensyal sementara secara dinamis alih-alih menggunakan kunci akses jangka panjang. Untuk informasi selengkapnya, lihat Kredensial keamanan sementara di IAM.

Teruskan sesi akses untuk AWS Audit Manager

Mendukung sesi akses maju (FAS)	Ya

Saat Anda menggunakan pengguna atau peran IAM untuk melakukan tindakan AWS, Anda dianggap sebagai prinsipal. Ketika Anda menggunakan beberapa layanan, Anda mungkin melakukan tindakan yang kemudian memulai 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 Meneruskan sesi akses.

Peran layanan untuk AWS Audit Manager

Mendukung peran layanan	Tidak

Peran layanan adalah sebuah peran IAM yang diambil oleh sebuah layanan untuk melakukan tindakan atas nama Anda. Administrator IAM dapat membuat, mengubah, dan menghapus peran layanan dari dalam IAM. Untuk informasi selengkapnya, lihat Membuat peran untuk mendelegasikan izin ke Layanan AWS dalam Panduan pengguna IAM.

> **Warning**
>
> Mengubah izin untuk peran layanan dapat merusak fungsionalitas AWS Audit Manager . Edit peran layanan hanya jika Audit Manager memberikan panduan untuk melakukannya.

Peran terkait layanan untuk AWS Audit Manager

Mendukung peran yang terkait layanan	Ya

Peran terkait layanan adalah jenis peran layanan yang ditautkan ke. Layanan AWSLayanan tersebut dapat mengambil peran untuk melakukan sebuah 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.

Untuk detail tentang peran terkait layanan AWS Audit Manager, lihat. Menggunakan peran terkait layanan untuk AWS Audit Manager

Contoh kebijakan berbasis identitas untuk AWS Audit Manager

Secara default, pengguna dan peran tidak memiliki izin untuk membuat atau memodifikasi sumber daya Audit Manager. Mereka juga tidak dapat melakukan tugas dengan menggunakan AWS

Management Console, AWS Command Line Interface (AWS CLI), atau AWS API. Untuk memberikan izin kepada pengguna untuk melakukan tindakan pada sumber daya yang mereka perlukan, administrator IAM dapat membuat kebijakan IAM. Administrator kemudian dapat menambahkan kebijakan IAM ke peran, dan pengguna dapat menjalankan peran.

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

Untuk detail tentang tindakan dan jenis sumber daya yang ditentukan oleh AWS Audit Manager, termasuk format ARN untuk setiap jenis sumber daya, lihat Tindakan, sumber daya, dan kunci kondisi untuk AWS Audit Manager di Referensi Otorisasi Layanan.

Topik

Praktik terbaik kebijakan

Kebijakan berbasis identitas menentukan apakah seseorang dapat membuat, mengakses, atau menghapus sumber daya Audit Manager di akun Anda. Tindakan ini dikenai biaya untuk Akun AWSAnda. Ketika Anda membuat atau mengedit kebijakan berbasis identitas, ikuti panduan dan rekomendasi ini:

- Mulailah dengan kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit — Untuk mulai memberikan izin kepada pengguna dan beban kerja Anda, gunakan kebijakanAWS terkelola yang memberikan izin untuk banyak kasus penggunaan umum. Mereka tersedia di Anda Akun AWS. Kami menyarankan Anda mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola AWS pelanggan yang khusus untuk kasus penggunaan Anda. Untuk informasi selengkapnya, lihat kebijakan yang dikelolaAWS atau kebijakan yang dikelolaAWS untuk fungsi pekerjaan di Panduan Pengguna IAM.

- Menerapkan izin dengan hak akses paling rendah – Ketika Anda menetapkan izin dengan kebijakan IAM, hanya berikan izin yang diperlukan untuk melakukan tugas. Anda melakukan ini dengan menentukan tindakan yang dapat diambil pada sumber daya tertentu dalam kondisi tertentu, juga dikenal sebagai izin hak akses paling rendah. Untuk informasi selengkapnya tentang cara menggunakan IAM untuk menerapkan izin, lihat Kebijakan dan izin di IAM di Panduan Pengguna IAM.
- Gunakan kondisi dalam kebijakan IAM untuk membatasi akses lebih lanjut – Anda dapat menambahkan kondisi ke kebijakan Anda untuk membatasi akses ke tindakan dan sumber daya. Misalnya, Anda dapat menulis syarat kebijakan untuk menentukan bahwa semua pengajuan harus dikirim menggunakan SSL. Anda juga dapat menggunakan ketentuan untuk memberikan akses ke tindakan layanan jika digunakan melalui yang spesifik Layanan AWS, seperti AWS CloudFormation. Untuk informasi selengkapnya, lihat Elemen kebijakan JSON IAM: Syarat di Panduan Pengguna IAM.
- Menggunakan IAM Access Analyzer untuk memvalidasi kebijakan IAM Anda guna memastikan izin yang aman dan berfungsi – IAM Access Analyzer memvalidasi kebijakan baru dan yang sudah ada sehingga kebijakan tersebut mematuhi bahasa kebijakan IAM (JSON) dan praktik terbaik IAM. IAM Access Analyzer menyediakan lebih dari 100 pemeriksaan kebijakan dan rekomendasi yang dapat ditindaklanjuti untuk membantu Anda membuat kebijakan yang aman dan fungsional. Untuk informasi selengkapnya, lihat validasi kebijakan Analizer Akses IAM di Panduan Pengguna IAM.
- Memerlukan otentikasi multi-faktor (MFA) - Jika Anda memiliki skenario yang mengharuskan pengguna IAM atau pengguna root di Anda, Akun AWSaktifkan MFA untuk keamanan tambahan. Untuk mewajibkan MFA saat operasi API dipanggil, tambahkan kondisi MFA pada kebijakan Anda. Untuk informasi selengkapnya, lihat Mengonfigurasi akses API yang dilindungi MFA di Panduan Pengguna IAM.

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

Izinkan izin minimum yang diperlukan untuk mengaktifkan Audit Manager

Contoh ini menunjukkan bagaimana Anda mengizinkan akun tanpa peran administrator untuk mengaktifkan AWS Audit Manager.

> **Note**
>
> Apa yang kami sediakan di sini adalah kebijakan dasar yang memberikan izin minimum yang diperlukan untuk mengaktifkan Audit Manager. Semua izin dalam kebijakan berikut

diperlukan. Jika Anda menghilangkan bagian apa pun dari kebijakan ini, Anda tidak akan dapat mengaktifkan Audit Manager.
Kami menyarankan Anda meluangkan waktu untuk menyesuaikan izin Anda sehingga mereka memenuhi kebutuhan spesifik Anda. Jika Anda memerlukan bantuan, hubungi administrator atau AWS Support Anda.

Untuk memberikan akses minimum yang diperlukan untuk mengaktifkan Audit Manager, gunakan izin berikut.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "auditmanager:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "auditmanager.amazonaws.com"
                }
            }
        },
        {
            "Sid": "CreateEventsAccess",
            "Effect": "Allow",
            "Action": [
                "events:PutRule"
            ],
            "Resource": "*",
            "Condition": {
                "ForAllValues:StringEquals": {
                    "events:source": [
                        "aws.securityhub"
                    ]
                }
            }
```

```
        },
        {
            "Sid": "EventsAccess",
            "Effect": "Allow",
            "Action": [
                "events:PutTargets"
            ],
            "Resource": "arn:aws:events:*:*:rule/
AuditManagerSecurityHubFindingsReceiver"
        },
        {
            "Effect": "Allow",
            "Action": "kms:ListAliases",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "auditmanager.amazonaws.com"
                }
            }
        }
    ]
}
```

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.

Memungkinkan pengguna akses administrator penuh ke AWS Audit Manager

Contoh kebijakan berikut memberikan akses administrator penuh ke AWS Audit Manager.

- Contoh 1 (Kebijakan terkelola,`AWSAuditManagerAdministratorAccess`)
- Contoh 2 (Izin tujuan laporan penilaian)
- Contoh 3 (Izin tujuan ekspor)
- Contoh 4 (Izin untuk mengaktifkan pencari bukti)
- Contoh 5 (Izin untuk menonaktifkan pencari bukti)

Contoh 1 (Kebijakan terkelola,**`AWSAuditManagerAdministratorAccess`**)

Kebijakan dalam contoh ini adalah kebijakan terkelola,`AWSAuditManagerAdministratorAccess`. Kebijakan ini mencakup kemampuan untuk mengaktifkan dan menonaktifkan Audit Manager,

kemampuan untuk mengubah pengaturan Audit Manager, dan kemampuan untuk mengelola semua sumber daya Audit Manager seperti penilaian, kerangka kerja, kontrol, dan laporan penilaian.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AuditManagerAccess",
            "Effect": "Allow",
            "Action": [
                "auditmanager:*"
            ],
            "Resource": "*"
        },
        {
            "Sid": "OrganizationsAccess",
            "Effect": "Allow",
            "Action": [
                "organizations:ListAccountsForParent",
                "organizations:ListAccounts",
                "organizations:DescribeOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribeAccount",
                "organizations:ListParents",
                "organizations:ListChildren"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowOnlyAuditManagerIntegration",
            "Effect": "Allow",
            "Action": [
                "organizations:RegisterDelegatedAdministrator",
                "organizations:DeregisterDelegatedAdministrator",
                "organizations:EnableAWSServiceAccess"
            ],
            "Resource": "*",
            "Condition": {
                "StringLikeIfExists": {
                    "organizations:ServicePrincipal": [
                        "auditmanager.amazonaws.com"
                    ]
                }
```

```
            }
        },
        {
            "Sid": "IAMAccess",
            "Effect": "Allow",
            "Action": [
                "iam:GetUser",
                "iam:ListUsers",
                "iam:ListRoles"
            ],
            "Resource": "*"
        },
        {
            "Sid": "IAMAccessCreateSLR",
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/
auditmanager.amazonaws.com/AWSServiceRoleForAuditManager*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "auditmanager.amazonaws.com"
                }
            }
        },
        {
            "Sid": "IAMAccessManageSLR",
            "Effect": "Allow",
            "Action": [
                "iam:DeleteServiceLinkedRole",
                "iam:UpdateRoleDescription",
                "iam:GetServiceLinkedRoleDeletionStatus"
            ],
            "Resource": "arn:aws:iam::*:role/aws-service-role/
auditmanager.amazonaws.com/AWSServiceRoleForAuditManager*"
        },
        {
            "Sid": "S3Access",
            "Effect": "Allow",
            "Action": [
                "s3:ListAllMyBuckets"
            ],
            "Resource": "*"
        },
        {
```

```
            "Sid": "KmsAccess",
            "Effect": "Allow",
            "Action": [
                "kms:DescribeKey",
                "kms:ListKeys",
                "kms:ListAliases"
            ],
            "Resource": "*"
        },
        {
            "Sid": "KmsCreateGrantAccess",
            "Effect": "Allow",
            "Action": [
                "kms:CreateGrant"
            ],
            "Resource": "*",
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": "true"
                },
                "StringLike": {
                    "kms:ViaService": "auditmanager.*.amazonaws.com"
                }
            }
        },
        {
            "Sid": "SNSAccess",
            "Effect": "Allow",
            "Action": [
                "sns:ListTopics"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CreateEventsAccess",
            "Effect": "Allow",
            "Action": [
                "events:PutRule"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "events:detail-type": "Security Hub Findings - Imported"
                },
```

```
                "ForAllValues:StringEquals": {
                    "events:source": [
                        "aws.securityhub"
                    ]
                }
            }
        },
        {
            "Sid": "EventsAccess",
            "Effect": "Allow",
            "Action": [
                "events:DeleteRule",
                "events:DescribeRule",
                "events:EnableRule",
                "events:DisableRule",
                "events:ListTargetsByRule",
                "events:PutTargets",
                "events:RemoveTargets"
            ],
            "Resource": "arn:aws:events:*:*:rule/
AuditManagerSecurityHubFindingsReceiver"
        },
        {
            "Sid": "TagAccess",
            "Effect": "Allow",
            "Action": [
                "tag:GetResources"
            ],
            "Resource": "*"
        }
    ]
}
```

Contoh 2 (Izin tujuan laporan penilaian)

Kebijakan ini memberi Anda izin untuk mengakses bucket S3 tertentu, serta menambahkan file ke serta menghapus file darinya. Hal ini memungkinkan Anda untuk menggunakan bucket yang ditentukan sebagai tujuan laporan penilaian di Audit Manager.

Ganti *`teks placeholder`* dengan informasi Anda sendiri. Sertakan bucket S3 yang Anda gunakan sebagai tujuan laporan penilaian dan kunci KMS yang Anda gunakan untuk mengenkripsi laporan penilaian Anda.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
               "s3:PutObject",
               "s3:GetObject",
               "s3:ListBucket",
               "s3:DeleteObject",
               "s3:GetBucketLocation",
               "s3:PutObjectAcl"
            ],
            "Resource": "arn:aws:s3:::DOC-EXAMPLE-DESTINATION-BUCKET/*"
        }
    ]
},
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt",
                "kms:Encrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ]
}
```

Contoh 3 (Izin tujuan ekspor)

Kebijakan berikut memungkinkan CloudTrail untuk mengirimkan hasil kueri pencari bukti ke bucket S3 yang ditentukan. Sebagai praktik keamanan terbaik, kunci kondisi global IAM `aws:SourceArn` membantu memastikan bahwa CloudTrail menulis ke bucket S3 hanya untuk penyimpanan data peristiwa.

Ganti *`teks placeholder`* dengan informasi Anda sendiri, sebagai berikut:

- Ganti *DOC-EXAMPLE-DESTINATION-BUCKET dengan bucket* S3 yang Anda gunakan sebagai tujuan ekspor.
- Ganti *myQueryRunningWilayah* dengan yang sesuai Wilayah AWS untuk konfigurasi Anda.
- Ganti *myAccountID* dengan Akun AWS ID yang digunakan untuk. CloudTrail Ini mungkin tidak sama dengan Akun AWS ID untuk bucket S3. Jika ini adalah penyimpanan data acara organisasi, Anda harus menggunakan Akun AWS untuk akun manajemen.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action": [
                "s3:PutObject*",
                "s3:Abort*"
            ],
            "Resource": [
                "arn:aws:s3:::DOC-EXAMPLE-DESTINATION-BUCKET",
                "arn:aws:s3:::DOC-EXAMPLE-DESTINATION-BUCKET/*"
            ],
            "Condition": {
                "StringEquals": {
                    "AWS:SourceArn":
 "arn:aws:cloudtrail:myQueryRunningRegion:myAccountID:eventdatastore/*"
                }
            }
        },
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::DOC-EXAMPLE-DESTINATION-BUCKET",
            "Condition": {
                "StringEquals": {
                    "AWS:SourceArn":
 "arn:aws:cloudtrail:myQueryRunningRegion:myAccountID:eventdatastore/*"
```

```
                }
            }
        },
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action": [
                "kms:Decrypt*",
                "kms:GenerateDataKey*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "s3.amazonaws.com"
            },
            "Action": [
                "kms:Decrypt*",
                "kms:GenerateDataKey*"
            ],
            "Resource": "*"
        }
    ]
}
```

Contoh 4 (Izin untuk mengaktifkan pencari bukti)

Kebijakan izin berikut diperlukan jika Anda ingin mengaktifkan dan menggunakan fitur pencari bukti. Pernyataan kebijakan ini memungkinkan Audit Manager untuk membuat penyimpanan data peristiwa CloudTrail Lake dan menjalankan kueri penelusuran.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
           "Sid": "ManageCloudTrailLakeQueryAccess",
           "Effect": "Allow",
           "Action": [
               "cloudtrail:StartQuery",
               "cloudtrail:DescribeQuery",
```

```
                "cloudtrail:GetQueryResults",
                "cloudtrail:CancelQuery"
            ],
            "Resource": "arn:aws:cloudtrail:*:*:eventdatastore/*"
        },
        {
            "Sid": "ManageCloudTrailLakeAccess",
            "Effect": "Allow",
            "Action": [
                 "cloudtrail:CreateEventDataStore"
            ],
            "Resource": "arn:aws:cloudtrail:*:*:eventdatastore/*"
         }
    ]
}
```

Contoh 5 (Izin untuk menonaktifkan pencari bukti)

Contoh kebijakan ini memberikan izin untuk menonaktifkan fitur pencari bukti di Audit Manager. Ini melibatkan penghapusan penyimpanan data acara yang dibuat saat Anda pertama kali mengaktifkan fitur tersebut.

Sebelum Anda menggunakan kebijakan ini, ganti *teks placeholder dengan informasi* Anda sendiri. Anda harus menentukan UUID penyimpanan data peristiwa yang dibuat saat Anda mengaktifkan pencari bukti. Anda dapat mengambil ARN penyimpanan data peristiwa dari pengaturan Audit Manager Anda. Untuk informasi selengkapnya, lihat GetSettings di dalam Referensi APIAWS Audit Manager .

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "cloudtrail:DeleteEventDataStore",
                "cloudtrail:UpdateEventDataStore"
            ],
            "Resource": "arn:aws:cloudtrail:::event-data-store-UUID"
        }
    ]
}
```

Memungkinkan akses manajemen pengguna ke AWS Audit Manager

Contoh ini menunjukkan bagaimana Anda mengizinkan akses manajemen non-administrator. AWS Audit Manager

Kebijakan ini memberikan kemampuan untuk mengelola semua sumber daya Audit Manager (penilaian, kerangka kerja, dan kontrol), tetapi tidak memberikan kemampuan untuk mengaktifkan atau menonaktifkan Audit Manager atau mengubah setelan Audit Manager.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AuditManagerAccess",
            "Effect": "Allow",
            "Action": [
                "auditmanager:GetAccountStatus",
                "auditmanager:ListAssessmentFrameworks",
                "auditmanager:CreateAssessmentFramework",
                "auditmanager:GetAssessmentFramework",
                "auditmanager:UpdateAssessmentFramework",
                "auditmanager:DeleteAssessmentFramework",
                "auditmanager:ListAssessmentReports",
                "auditmanager:ListAssessments",
                "auditmanager:CreateAssessment",
                "auditmanager:ListControls",
                "auditmanager:CreateControl",
                "auditmanager:GetControl",
                "auditmanager:UpdateControl",
                "auditmanager:DeleteControl",
                "auditmanager:ListKeywordsForDataSource",
                "auditmanager:GetDelegations",
                "auditmanager:ValidateAssessmentReportIntegrity",
                "auditmanager:ListNotifications",
                "auditmanager:GetServicesInScope",
                "auditmanager:GetSettings",
                "auditmanager:ListTagsForResource",
                "auditmanager:TagResource",
                "auditmanager:UntagResource"
            ],
            "Resource": "*"
        },
        {
```

```
            "Sid": "OrganizationsAccess",
            "Effect": "Allow",
            "Action": [
                "organizations:ListAccountsForParent",
                "organizations:ListAccounts",
                "organizations:DescribeOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribeAccount",
                "organizations:ListParents",
                "organizations:ListChildren"
            ],
            "Resource": "*"
        },
        {
            "Sid": "IAMAccess",
            "Effect": "Allow",
            "Action": [
                "iam:GetUser",
                "iam:ListUsers",
                "iam:ListRoles"
            ],
            "Resource": "*"
        },
        {
            "Sid": "S3Access",
            "Effect": "Allow",
            "Action": [
                "s3:ListAllMyBuckets"
            ],
            "Resource": "*"
        },
        {
            "Sid": "KmsAccess",
            "Effect": "Allow",
            "Action": [
                "kms:DescribeKey",
                "kms:ListKeys",
                "kms:ListAliases"
            ],
            "Resource": "*"
        },
        {
            "Sid": "SNSAccess",
            "Effect": "Allow",
```

```
            "Action": [
                "sns:ListTopics"
            ],
            "Resource": "*"
        },
        {
            "Sid": "TagAccess",
            "Effect": "Allow",
            "Action": [
                "tag:GetResources"
            ],
            "Resource": "*"
        }
    ]
}
```

Izinkan pengguna akses hanya-baca ke AWS Audit Manager

Kebijakan ini memberikan akses hanya-baca ke AWS Audit Manager sumber daya seperti penilaian, kerangka kerja, dan kontrol.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AuditManagerAccess",
            "Effect": "Allow",
            "Action": [
                "auditmanager:Get*",
                "auditmanager:List*"
            ],
            "Resource": "*"
        }
    ]
}
```

Izinkan pengguna melihat izin mereka sendiri

Contoh ini menunjukkan cara membuat kebijakan yang mengizinkan para 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": "*"
        }
    ]
}
```

Izinkan AWS Audit Manager untuk mengirim pemberitahuan ke topik Amazon SNS

Kebijakan dalam contoh ini memberikan izin Audit Manager untuk mengirim notifikasi ke topik Amazon SNS yang ada.

- Contoh 1 - Jika Anda ingin menerima pemberitahuan dari Audit Manager, gunakan contoh ini untuk menambahkan izin ke kebijakan akses topik SNS Anda.

- Contoh 2 - Jika topik SNS Anda menggunakan AWS Key Management Service (AWS KMS) untuk enkripsi sisi server (SSE), gunakan contoh ini untuk menambahkan izin ke kebijakan akses kunci KMS.

Dalam kebijakan berikut, prinsipal yang mendapatkan izin adalah kepala layanan Audit Manager, yaituauditmanager.amazonaws.com. Ketika prinsipal dalam pernyataan kebijakan adalah prinsipalAWS layanan, kami sangat menyarankan Anda menggunakan aws:SourceArnatau kunci kondisi aws:SourceAccountglobal dalam kebijakan. Anda dapat menggunakan kunci konteks kondisi global ini untuk membantu mencegah skenario deputi yang membingungkan.

Contoh 1 (Izin untuk topik SNS)

Pernyataan kebijakan ini memungkinkan Audit Manager untuk mempublikasikan peristiwa ke topik SNS yang ditentukan. Setiap permintaan untuk mempublikasikan ke topik SNS yang ditentukan harus memenuhi ketentuan kebijakan.

Sebelum menggunakan kebijakan ini, ganti *teks placeholder dengan informasi* Anda sendiri. Perhatikan hal-hal berikut ini:

- Jika Anda menggunakan kunci aws:SourceArn kondisi dalam kebijakan ini, nilainya harus berupa ARN sumber daya Audit Manager tempat notifikasi berasal. Dalam contoh di bawah ini, aws:SourceArn menggunakan wildcard (*) untuk ID sumber daya. Hal ini memungkinkan semua permintaan yang berasal dari Audit Manager pada semua sumber Audit Manager. Dengan kunci kondisi aws:SourceArn global, Anda dapat menggunakan operator StringLike atau ArnLike kondisi. Sebagai praktik terbaik, kami sarankan Anda menggunakannyaArnLike.
- Jika Anda menggunakan tombol aws:SourceAccountkondisi, Anda dapat menggunakan operator StringEquals atau StringLike kondisi. Sebagai praktik terbaik, kami menyarankan Anda menggunakan StringEquals untuk menerapkan hak istimewa paling sedikit.
- Jika Anda menggunakan keduanya aws:SourceAccount danaws:SourceArn, nilai akun harus menunjukkan ID akun yang sama.

```
{
  "Version": "2012-10-17",
  "Statement": {
      "Sid": "AllowAuditManagerToUseSNSTopic",
      "Effect": "Allow",
      "Principal": {
        "Service": "auditmanager.amazonaws.com"
```

```
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:region:accountID:topicName",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "accountID"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:auditmanager:region:accountID:*"
        }
      }
    }
}
```

Contoh alternatif berikut hanya menggunakan kunci `aws:SourceArn` kondisi, dengan operator `StringLike` kondisi:

```
      "Condition": {
        "StringLike": {
          "aws:SourceArn": "arn:aws:auditmanager:region:accountID:*"
        }
      }
```

Contoh alternatif berikut hanya menggunakan kunci `aws:SourceAccount` kondisi, dengan operator `StringLike` kondisi:

```
   "Condition": {
     "StringLike": {
       "aws:SourceAccount": "accountID"
     }
    }
```

Contoh 2 (Izin untuk kunci KMS yang dilampirkan ke topik SNS)

Pernyataan kebijakan ini memungkinkan Audit Manager menggunakan kunci KMS untuk menghasilkan kunci data yang digunakan untuk mengenkripsi topik SNS. Setiap permintaan untuk menggunakan kunci KMS untuk operasi yang ditentukan harus memenuhi ketentuan kebijakan.

Sebelum menggunakan kebijakan ini, ganti *`teks placeholder dengan informasi`* Anda sendiri. Perhatikan hal-hal berikut ini:

- Jika Anda menggunakan kunci `aws:SourceArn` kondisi dalam kebijakan ini, nilainya harus ARN sumber daya yang dienkripsi. Misalnya, dalam hal ini, ini adalah topik SNS di akun Anda. Tetapkan nilai ke ARN atau pola ARN dengan karakter wildcard (). * Anda dapat menggunakan operator `StringLike` atau `ArnLike` kondisi dengan kunci `aws:SourceArn` kondisi. Sebagai praktik terbaik, kami sarankan Anda menggunakannya`ArnLike`.
- Jika Anda menggunakan tombol `aws:SourceAccount` kondisi, Anda dapat menggunakan operator `StringEquals` atau `StringLike` kondisi. Sebagai praktik terbaik, kami menyarankan Anda menggunakan `StringEquals` untuk menerapkan hak istimewa paling sedikit. Anda dapat menggunakan `aws:SourceAccount` jika Anda tidak tahu ARN dari topik SNS.
- Jika Anda menggunakan keduanya `aws:SourceAccount` dan`aws:SourceArn`, nilai akun harus menunjukkan ID akun yang sama.

```
{
     "Version": "2012-10-17",
     "Statement": {
       "Sid": "AllowAuditManagerToUseKMSKey",
       "Effect": "Allow",
       "Principal": {
           "Service": "auditmanager.amazonaws.com"
       },
       "Action": [
           "kms:Decrypt",
           "kms:GenerateDataKey"
       ],
       "Resource": "arn:aws:kms:region:accountID:key/*",
       "Condition": {
           "StringEquals": {
                "aws:SourceAccount": "accountID"
            }
            "ArnLike": {
                 "aws:SourceArn": "arn:aws:sns:region:accountID:topicName"
            }
      }
    }
  ]
}
```

Contoh alternatif berikut hanya menggunakan kunci `aws:SourceArn` kondisi, dengan operator `StringLike` kondisi:

```
      "Condition": {
        "StringLike": {
          "aws:SourceArn": "arn:aws:sns:region:accountID:topicName"
        }
      }
```

Contoh alternatif berikut hanya menggunakan kunci `aws:SourceAccount` kondisi, dengan operator `StringLike` kondisi:

```
   "Condition": {
     "StringLike": {
       "aws:SourceAccount": "accountID"
     }
    }
```

Izinkan pengguna menjalankan kueri penelusuran di pencari bukti

Kebijakan berikut memberikan izin untuk melakukan kueri di penyimpanan data peristiwa CloudTrail Lake. Kebijakan izin ini diperlukan jika Anda ingin menggunakan fitur pencari bukti.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ManageCloudTrailLakeQueryAccess",
            "Effect": "Allow",
            "Action": [
                "cloudtrail:StartQuery",
                "cloudtrail:DescribeQuery",
                "cloudtrail:GetQueryResults",
                "cloudtrail:CancelQuery"
            ],
            "Resource": "*"
        }
    ]
}
```

Pencegahan confused deputy lintas layanan

Masalah confused deputy adalah masalah keamanan saat entitas yang tidak memiliki izin untuk melakukan suatu tindakan dapat memaksa entitas yang lebih berhak untuk melakukan tindakan tersebut. Pada tahun AWS, peniruan lintas layanan dapat mengakibatkan masalah wakil yang membingungkan. Peniruan identitas lintas layanan dapat terjadi ketika satu layanan (layanan pemanggil) memanggil layanan lain (layanan yang dipanggil). Layanan panggilan dapat dimanipulasi untuk menggunakan izinnya untuk bertindak atas sumber daya pelanggan lain ketika tidak memiliki izin untuk melakukannya. Untuk mencegah hal ini, Amazon Web Services menyediakan alat yang membantu Anda melindungi data Anda untuk semua layanan dengan prinsipal layanan yang telah diberikan akses ke sumber daya di akun Anda.

Sebaiknya gunakan kunci konteks kondisi `aws:SourceAccount`global `aws:SourceArn`dan global dalam kebijakan sumber daya untuk membatasi izin yang AWS Audit Manager diberikan ke layanan lain untuk akses ke sumber daya Anda.

- Gunakan `aws:SourceArn` jika Anda hanya ingin satu sumber daya dikaitkan dengan akses lintas layanan. Anda juga dapat menggunakan `aws:SourceArn` dengan wildcard (*) jika Anda ingin menentukan beberapa sumber daya.

  Misalnya, Anda dapat menggunakan topik Amazon SNS untuk menerima pemberitahuan aktivitas dari Audit Manager. Dalam hal ini, dalam kebijakan akses topik SNS Anda, nilai `aws:SourceArn` ARN adalah sumber daya Audit Manager tempat notifikasi berasal. Karena kemungkinan Anda memiliki beberapa sumber daya Audit Manager, sebaiknya gunakan `aws:SourceArn` dengan wildcard. Ini memungkinkan Anda untuk menentukan semua sumber Audit Manager Anda dalam kebijakan akses topik SNS Anda.
- Gunakan `aws:SourceAccount` jika Anda ingin mengizinkan sumber daya apa pun di akun tersebut dikaitkan dengan penggunaan lintas layanan.
- Jika `aws:SourceArn` nilainya tidak berisi ID akun, seperti ARN bucket Amazon S3, Anda harus menggunakan kedua kunci konteks kondisi global untuk membatasi izin.
- Jika Anda menggunakan kedua kondisi, dan jika `aws:SourceArn` nilainya berisi ID akun, `aws:SourceAccount` nilai dan akun dalam `aws:SourceArn` nilai harus menunjukkan ID akun yang sama saat digunakan dalam pernyataan kebijakan yang sama.
- Cara paling efektif untuk melindungi dari masalah confused deputy adalah dengan menggunakan kunci konteks kondisi global `aws:SourceArn` dengan ARN sumber daya penuh. Jika Anda tidak mengetahui Nama Sumber Daya Amazon (ARN) lengkap sumber daya atau jika Anda menentukan beberapa sumber daya, gunakan kunci kondisi konteks `aws:SourceArn`

global dengan karakter wildcard (*) untuk bagian ARN yang tidak diketahui. Misalnya, `arn:aws:servicename:*:123456789012:*`.

Audit Manager bingung dengan dukungan wakil

Audit Manager memberikan dukungan wakil yang membingungkan dalam skenario berikut. Contoh kebijakan ini menunjukkan bagaimana Anda dapat menggunakan kunci `aws:SourceArn` dan `aws:SourceAccount` kondisi untuk mencegah masalah wakil yang membingungkan.

- Contoh kebijakan: Topik SNS yang Anda gunakan untuk menerima notifikasi Audit Manager
- Contoh kebijakan: Kunci KMS yang Anda gunakan untuk mengenkripsi topik SNS Anda

Audit Manager tidak memberikan dukungan deputi yang membingungkan untuk kunci terkelola pelanggan yang Anda berikan di Enkripsi data pengaturan Audit Manager Anda. Jika Anda memberikan kunci terkelola pelanggan Anda sendiri, Anda tidak dapat menggunakan `aws:SourceAccount` atau `aws:SourceArn` ketentuan dalam kebijakan kunci KMS tersebut.

AWS kebijakan terkelola untuk AWS Audit Manager

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, pembaruan 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 Kebijakan yang dikelolaAWS dalam Panduan Pengguna IAM.

Topik

- AWS kebijakan terkelola: AWSAuditManagerAdministratorAccess

- AWS kebijakan terkelola: AWSAuditManagerServiceRolePolicy
- AWS Audit Manager pembaruan kebijakan AWS terkelola

AWS kebijakan terkelola: AWSAuditManagerAdministratorAccess

Anda dapat melampirkan kebijakan `AWSAuditManagerAdministratorAccess` ke identitas IAM Anda.

Kebijakan ini memberikan izin administratif yang memungkinkan akses administrasi penuh. AWS Audit ManagerAkses ini mencakup kemampuan untuk mengaktifkan dan menonaktifkan AWS Audit Manager, mengubah pengaturan AWS Audit Manager, dan mengelola semua sumber daya Audit Manager seperti penilaian, kerangka kerja, kontrol, dan laporan penilaian.

AWS Audit Manager memerlukan izin luas di beberapa AWS layanan. Ini karena AWS Audit Manager terintegrasi dengan beberapa AWS layanan untuk mengumpulkan bukti secara otomatis dari Akun AWS dan layanan dalam lingkup penilaian.

Detail izin

Kebijakan ini mencakup izin berikut:

- `Audit Manager`— Memungkinkan kepala sekolah izin penuh pada sumber daya. AWS Audit Manager
- `Organizations`— Memungkinkan kepala sekolah untuk membuat daftar akun dan unit organisasi, dan untuk mendaftarkan atau membatalkan pendaftaran administrator yang didelegasikan. Ini diperlukan agar Anda dapat mengaktifkan dukungan multi-akun dan memungkinkan AWS Audit Manager untuk menjalankan penilaian melalui beberapa akun dan mengkonsolidasikan bukti ke dalam akun administrator yang didelegasikan.
- `iam`— Memungkinkan prinsipal untuk mendapatkan dan mencantumkan pengguna di IAM dan membuat peran terkait layanan. Ini diperlukan agar Anda dapat menunjuk pemilik audit dan delegasi untuk penilaian. Kebijakan ini juga memungkinkan prinsipal untuk menghapus peran terkait layanan dan mengambil status penghapusan. Hal ini diperlukan agar AWS Audit Manager dapat membersihkan sumber daya dan menghapus peran terkait layanan untuk Anda ketika Anda memilih untuk menonaktifkan layanan di. AWS Management Console
- `s3`— Memungkinkan kepala sekolah untuk mencantumkan bucket Amazon Simple Storage Service (Amazon S3) yang tersedia. Kemampuan ini diperlukan agar Anda dapat menunjuk bucket S3 tempat Anda ingin menyimpan laporan bukti atau mengunggah bukti manual.

- `kms`— Memungkinkan kepala sekolah untuk membuat daftar dan mendeskripsikan kunci, daftar alias, dan membuat hibah. Ini diperlukan agar Anda dapat memilih kunci yang dikelola pelanggan untuk enkripsi data.
- `sns`— Memungkinkan kepala sekolah untuk membuat daftar topik berlangganan di Amazon SNS. Ini diperlukan agar Anda dapat menentukan topik SNS mana yang AWS Audit Manager ingin Anda kirimi notifikasi.
- `events`— Memungkinkan kepala sekolah untuk membuat daftar dan mengelola cek dari. AWS Security HubHal ini diperlukan agar secara otomatis AWS Audit Manager dapat mengumpulkan AWS Security Hub temuan untuk AWS layanan yang dipantau oleh AWS Security Hub. Kemudian dapat mengubah data ini menjadi bukti untuk dimasukkan dalam AWS Audit Manager penilaian Anda.
- `tag`— Memungkinkan kepala sekolah untuk mengambil sumber daya yang ditandai. Ini diperlukan agar Anda dapat menggunakan tag sebagai filter penelusuran saat menjelajahi kerangka kerja, kontrol, dan penilaian. AWS Audit Manager

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AuditManagerAccess",
            "Effect": "Allow",
            "Action": [
                "auditmanager:*"
            ],
            "Resource": "*"
        },
        {
            "Sid": "OrganizationsAccess",
            "Effect": "Allow",
            "Action": [
                "organizations:ListAccountsForParent",
                "organizations:ListAccounts",
                "organizations:DescribeOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribeAccount",
                "organizations:ListParents",
                "organizations:ListChildren"
            ],
            "Resource": "*"
```

```
        },
        {
            "Sid": "AllowOnlyAuditManagerIntegration",
            "Effect": "Allow",
            "Action": [
                "organizations:RegisterDelegatedAdministrator",
                "organizations:DeregisterDelegatedAdministrator",
                "organizations:EnableAWSServiceAccess"
            ],
            "Resource": "*",
            "Condition": {
                "StringLikeIfExists": {
                    "organizations:ServicePrincipal": [
                        "auditmanager.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Sid": "IAMAccess",
            "Effect": "Allow",
            "Action": [
                "iam:GetUser",
                "iam:ListUsers",
                "iam:ListRoles"
            ],
            "Resource": "*"
        },
        {
            "Sid": "IAMAccessCreateSLR",
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/
auditmanager.amazonaws.com/AWSServiceRoleForAuditManager*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "auditmanager.amazonaws.com"
                }
            }
        },
        {
            "Sid": "IAMAccessManageSLR",
            "Effect": "Allow",
            "Action": [
```

```
                "iam:DeleteServiceLinkedRole",
                "iam:UpdateRoleDescription",
                "iam:GetServiceLinkedRoleDeletionStatus"
            ],
            "Resource": "arn:aws:iam::*:role/aws-service-role/
auditmanager.amazonaws.com/AWSServiceRoleForAuditManager*"
        },
        {
            "Sid": "S3Access",
            "Effect": "Allow",
            "Action": [
                "s3:ListAllMyBuckets"
            ],
            "Resource": "*"
        },
        {
            "Sid": "KmsAccess",
            "Effect": "Allow",
            "Action": [
                "kms:DescribeKey",
                "kms:ListKeys",
                "kms:ListAliases"
            ],
            "Resource": "*"
        },
        {
            "Sid": "KmsCreateGrantAccess",
            "Effect": "Allow",
            "Action": [
                "kms:CreateGrant"
            ],
            "Resource": "*",
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": "true"
                },
                "StringLike": {
                    "kms:ViaService": "auditmanager.*.amazonaws.com"
                }
            }
        },
        {
            "Sid": "SNSAccess",
            "Effect": "Allow",
```

```
            "Action": [
                "sns:ListTopics"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CreateEventsAccess",
            "Effect": "Allow",
            "Action": [
                "events:PutRule"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "events:detail-type": "Security Hub Findings - Imported"
                },
                "ForAllValues:StringEquals": {
                    "events:source": [
                        "aws.securityhub"
                    ]
                }
            }
        },
        {
            "Sid": "EventsAccess",
            "Effect": "Allow",
            "Action": [
                "events:DeleteRule",
                "events:DescribeRule",
                "events:EnableRule",
                "events:DisableRule",
                "events:ListTargetsByRule",
                "events:PutTargets",
                "events:RemoveTargets"
            ],
            "Resource": "arn:aws:events:*:*:rule/
AuditManagerSecurityHubFindingsReceiver"
        },
        {
            "Sid": "TagAccess",
            "Effect": "Allow",
            "Action": [
                "tag:GetResources"
            ],
```

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

AWS kebijakan terkelola: AWSAuditManagerServiceRolePolicy

Anda tidak dapat melampirkan `AWSAuditManagerServiceRolePolicy` ke entitas IAM Anda. Kebijakan ini dilampirkan pada peran terkait layanan`AWSServiceRoleForAuditManager`, yang memungkinkan Anda AWS Audit Manager melakukan tindakan atas nama Anda. Untuk informasi selengkapnya, lihat Menggunakan peran terkait layanan untuk. AWS Audit Manager

Kebijakan izin peran,`AWSAuditManagerServiceRolePolicy`, memungkinkan AWS Audit Manager untuk mengumpulkan bukti otomatis dengan melakukan hal berikut atas nama Anda:

- Kumpulkan data dari sumber data berikut:
  - Acara manajemen dari AWS CloudTrail
  - Pemeriksaan kepatuhan dari Aturan AWS Config
  - Pemeriksaan kepatuhan dari AWS Security Hub
- Gunakan panggilan API untuk menjelaskan konfigurasi sumber daya Anda untuk hal-hal berikut Layanan AWS.

  > **Tip**
  >
  > Untuk informasi selengkapnya tentang panggilan API yang digunakan Audit Manager untuk mengumpulkan bukti dari layanan ini, lihat Panggilan API yang didukung untuk sumber data kontrol kustom di panduan ini.

  - AWS Certificate Manager
  - AWS Backup
  - Amazon Bedrock
  - AWS CloudTrail
  - Amazon CloudWatch
  - CloudWatch Log Amazon
  - Kolam pengguna Amazon Cognito

- AWS Config
- AWS Direct Connect
- Amazon DynamoDB
- Amazon EC2
- Amazon Elastic Container Service
- Amazon Elastic File System
- Amazon Elastic Kubernetes Service
- Amazon ElastiCache
- Penyeimbang Beban Elastis
- Amazon EMR
- Amazon EventBridge
- Amazon Data Firehose
- Amazon FSx
- Amazon GuardDuty
- AWS Identity and Access Management (IAM)
- Amazon Kinesis
- AWS KMS
- AWS Lambda
- AWS License Manager
- Amazon Managed Streaming untuk Apache Kafka
- AWS Organizations
- Amazon Relational Database Service
- Amazon Redshift
- Amazon Route 53
- Amazon S3
- AWS Security Hub
- Amazon Simple Notification Service
- Amazon Simple Queue Service
- AWS WAF

Detail izin

`AWSAuditManagerServiceRolePolicy`memungkinkan AWS Audit Manager untuk menyelesaikan tindakan berikut pada sumber daya yang ditentukan:

- `acm:GetAccountConfiguration`
- `acm:ListCertificates`
- `backup:ListRecoveryPointsByResource`
- `bedrock:GetCustomModel`
- `bedrock:GetFoundationModel`
- `bedrock:GetModelCustomizationJob`
- `bedrock:GetModelInvocationLoggingConfiguration`
- `bedrock:ListCustomModels`
- `bedrock:ListFoundationModels`
- `bedrock:ListModelCustomizationJobs`
- `cloudtrail:DescribeTrails`
- `cloudtrail:LookupEvents`
- `cloudwatch:DescribeAlarms`
- `cloudwatch:DescribeAlarmsForMetric`
- `cloudwatch:GetMetricStatistics`
- `cloudwatch:ListMetrics`
- `cognito-idp:DescribeUserPool`
- `config:DescribeConfigRules`
- `config:DescribeDeliveryChannels`
- `config:ListDiscoveredResources`
- `directconnect:DescribeDirectConnectGateways`
- `directconnect:DescribeVirtualGateways`
- `dynamodb:DescribeTable`
- `dynamodb:ListBackups`
- `dynamodb:ListGlobalTables`
- `dynamodb:ListTables`
- `ec2:DescribeAddresses`

- ec2:DescribeCustomerGateways
- ec2:DescribeEgressOnlyInternetGateways
- ec2:DescribeFlowLogs
- ec2:DescribeInstances
- ec2:DescribeInternetGateways
- ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations
- ec2:DescribeLocalGateways
- ec2:DescribeLocalGatewayVirtualInterfaces
- ec2:DescribeNatGateways
- ec2:DescribeNetworkAcls
- ec2:DescribeRouteTables
- ec2:DescribeSecurityGroups
- ec2:DescribeSnapshots
- ec2:DescribeTransitGateways
- ec2:DescribeVolumes
- ec2:DescribeVpcEndpoints
- ec2:DescribeVpcPeeringConnections
- ec2:DescribeVpcs
- ec2:DescribeVpnConnections
- ec2:DescribeVpnGateways
- ec2:GetEbsDefaultKmsKeyId
- ec2:GetEbsEncryptionByDefault
- ecs:DescribeClusters
- eks:DescribeAddonVersions
- elasticache:DescribeCacheClusters
- elasticache:DescribeServiceUpdates
- elasticfilesystem:DescribeAccessPoints
- elasticfilesystem:DescribeFileSystems
- elasticloadbalancing:DescribeLoadBalancers
- elasticloadbalancing:DescribeSslPolicies

- elasticloadbalancing:DescribeTargetGroups
- elasticmapreduce:ListClusters
- elasticmapreduce:ListSecurityConfigurations
- events:DeleteRule
- events:DescribeRule
- events:DisableRule
- events:EnableRule
- events:ListConnections
- events:ListEventBuses
- events:ListEventSources
- events:ListRules
- events:ListTargetsByRule
- events:PutRule
- events:PutTargets
- events:RemoveTargets
- firehose:ListDeliveryStreams
- fsx:DescribeFileSystems
- guardduty:ListDetectors
- iam:GenerateCredentialReport
- iam:GetAccountAuthorizationDetails
- iam:GetAccountPasswordPolicy
- iam:GetAccountSummary
- iam:GetCredentialReport
- iam:ListEntitiesForPolicy
- iam:ListGroupPolicies
- iam:ListGroups
- iam:ListOpenIdConnectProviders
- iam:ListPolicies
- iam:ListRolePolicies
- iam:ListRoles

- iam:ListSamlProviders
- iam:ListUserPolicies
- iam:ListUsers
- iam:ListVirtualMFADevices
- kafka:ListClusters
- kafka:ListKafkaVersions
- kinesis:ListStreams
- kms:DescribeKey
- kms:GetKeyPolicy
- kms:GetKeyRotationStatus
- kms:ListGrants
- kms:ListKeyPolicies
- kms:ListKeys
- lambda:ListFunctions
- license-manager:ListAssociationsForLicenseConfiguration
- license-manager:ListLicenseConfigurations
- license-manager:ListUsageForLicenseConfiguration
- logs:DescribeDestinations
- logs:DescribeExportTasks
- logs:DescribeLogGroups
- logs:DescribeMetricFilters
- logs:DescribeResourcePolicies
- logs:FilterLogEvents
- organizations:DescribeOrganization
- organizations:DescribePolicy
- rds:DescribeCertificates
- rds:DescribeDbClusterEndpoints
- rds:DescribeDbClusterParameterGroups
- rds:DescribeDbClusters
- rds:DescribeDBInstances

- rds:DescribeDbSecurityGroups
- redshift:DescribeClusters
- route53:GetQueryLoggingConfig
- s3:GetBucketPolicy
  - Tindakan API ini beroperasi dalam lingkup di Akun AWS mana service-linked-role tersedia. Itu tidak dapat mengakses kebijakan bucket lintas akun.
- s3:GetBucketPublicAccessBlock
- s3:GetBucketVersioning
- s3:GetEncryptionConfiguration
- s3:GetLifecycleConfiguration
- s3:ListAllMyBuckets
- securityhub:DescribeStandards
- sns:ListTopics
- sqs:ListQueues
- waf-regional:GetLoggingConfiguration
- waf-regional:ListRuleGroups
- waf-regional:ListSubscribedRuleGroups
- waf-regional:ListWebACLs
- waf:ListActivatedRulesInRuleGroup

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "acm:GetAccountConfiguration",
    "acm:ListCertificates",
    "backup:ListRecoveryPointsByResource",
    "bedrock:GetCustomModel",
    "bedrock:GetFoundationModel",
    "bedrock:GetModelCustomizationJob",
    "bedrock:GetModelInvocationLoggingConfiguration",
    "bedrock:ListCustomModels",
    "bedrock:ListFoundationModels",
```

```
    "bedrock:ListModelCustomizationJobs",
    "cloudtrail:DescribeTrails",
    "cloudtrail:LookupEvents",
    "cloudwatch:DescribeAlarms",
    "cloudwatch:DescribeAlarmsForMetric",
    "cloudwatch:GetMetricStatistics",
    "cloudwatch:ListMetrics",
    "cognito-idp:DescribeUserPool",
    "config:DescribeConfigRules",
    "config:DescribeDeliveryChannels",
    "config:ListDiscoveredResources",
    "directconnect:DescribeDirectConnectGateways",
    "directconnect:DescribeVirtualGateways",
    "dynamodb:DescribeTable",
    "dynamodb:ListBackups",
    "dynamodb:ListGlobalTables",
    "dynamodb:ListTables",
    "ec2:DescribeAddresses",
    "ec2:DescribeCustomerGateways",
    "ec2:DescribeEgressOnlyInternetGateways",
    "ec2:DescribeFlowLogs",
    "ec2:DescribeInstances",
    "ec2:DescribeInternetGateways",
    "ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations",
    "ec2:DescribeLocalGateways",
    "ec2:DescribeLocalGatewayVirtualInterfaces",
    "ec2:DescribeNatGateways",
    "ec2:DescribeNetworkAcls",
    "ec2:DescribeRouteTables",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSnapshots",
    "ec2:DescribeTransitGateways",
    "ec2:DescribeVolumes",
    "ec2:DescribeVpcEndpoints",
    "ec2:DescribeVpcPeeringConnections",
    "ec2:DescribeVpcs",
    "ec2:DescribeVpnConnections",
    "ec2:DescribeVpnGateways",
    "ec2:GetEbsDefaultKmsKeyId",
    "ec2:GetEbsEncryptionByDefault",
    "ecs:DescribeClusters",
    "eks:DescribeAddonVersions",
    "elasticache:DescribeCacheClusters",
    "elasticache:DescribeServiceUpdates",
```

```
    "elasticfilesystem:DescribeAccessPoints",
    "elasticfilesystem:DescribeFileSystems",
    "elasticloadbalancing:DescribeLoadBalancers",
    "elasticloadbalancing:DescribeSslPolicies",
    "elasticloadbalancing:DescribeTargetGroups",
    "elasticmapreduce:ListClusters",
    "elasticmapreduce:ListSecurityConfigurations",
    "events:DescribeRule",
    "events:ListConnections",
    "events:ListEventBuses",
    "events:ListEventSources",
    "events:ListRules",
    "firehose:ListDeliveryStreams",
    "fsx:DescribeFileSystems",
    "guardduty:ListDetectors",
    "iam:GenerateCredentialReport",
    "iam:GetAccountAuthorizationDetails",
    "iam:GetAccountPasswordPolicy",
    "iam:GetAccountSummary",
    "iam:GetCredentialReport",
    "iam:ListEntitiesForPolicy",
    "iam:ListGroupPolicies",
    "iam:ListGroups",
    "iam:ListOpenIdConnectProviders",
    "iam:ListPolicies",
    "iam:ListRolePolicies",
    "iam:ListRoles",
    "iam:ListSamlProviders",
    "iam:ListUserPolicies",
    "iam:ListUsers",
    "iam:ListVirtualMFADevices",
    "kafka:ListClusters",
    "kafka:ListKafkaVersions",
    "kinesis:ListStreams",
    "kms:DescribeKey",
    "kms:GetKeyPolicy",
    "kms:GetKeyRotationStatus",
    "kms:ListGrants",
    "kms:ListKeyPolicies",
    "kms:ListKeys",
    "lambda:ListFunctions",
    "license-manager:ListAssociationsForLicenseConfiguration",
    "license-manager:ListLicenseConfigurations",
    "license-manager:ListUsageForLicenseConfiguration",
```

```
    "logs:DescribeDestinations",
    "logs:DescribeExportTasks",
    "logs:DescribeLogGroups",
    "logs:DescribeMetricFilters",
    "logs:DescribeResourcePolicies",
    "logs:FilterLogEvents",
    "organizations:DescribeOrganization",
    "organizations:DescribePolicy",
    "rds:DescribeCertificates",
    "rds:DescribeDbClusterEndpoints",
    "rds:DescribeDbClusterParameterGroups",
    "rds:DescribeDbClusters",
    "rds:DescribeDBInstances",
    "rds:DescribeDbSecurityGroups",
    "redshift:DescribeClusters",
    "route53:GetQueryLoggingConfig",
    "s3:GetBucketPublicAccessBlock",
    "s3:GetBucketVersioning",
    "s3:GetEncryptionConfiguration",
    "s3:GetLifecycleConfiguration",
    "s3:ListAllMyBuckets",
    "securityhub:DescribeStandards",
    "sns:ListTopics",
    "sqs:ListQueues",
    "waf-regional:GetLoggingConfiguration",
    "waf-regional:ListRuleGroups",
    "waf-regional:ListSubscribedRuleGroups",
    "waf-regional:ListWebACLs",
    "waf:ListActivatedRulesInRuleGroup"
   ],
   "Resource": "*",
   "Sid": "AuditManagerAPICallAccess"
  },
  {
   "Sid": "AuditManagerS3GetBucketPolicyAccess",
   "Effect": "Allow",
   "Action": [
    "s3:GetBucketPolicy"
   ],
   "Resource": "*",
   "Condition": {
    "StringEquals": {
     "aws:ResourceAccount": [
      "${aws:PrincipalAccount}"
```

```
      ]
     }
    }
   },
   {
    "Sid": "CreateEventsAccess",
    "Effect": "Allow",
    "Action": [
     "events:PutRule"
    ],
    "Resource": "arn:aws:events:*:*:rule/AuditManagerSecurityHubFindingsReceiver",
    "Condition": {
     "StringEquals": {
      "events:detail-type": "Security Hub Findings - Imported"
     },
     "Null": {
      "events:source": "false"
     },
     "ForAllValues:StringEquals": {
      "events:source": [
       "aws.securityhub"
      ]
     }
    }
   },
   {
    "Sid": "EventsAccess",
    "Effect": "Allow",
    "Action": [
     "events:DeleteRule",
     "events:DescribeRule",
     "events:EnableRule",
     "events:DisableRule",
     "events:ListTargetsByRule",
     "events:PutTargets",
     "events:RemoveTargets"
    ],
    "Resource": "arn:aws:events:*:*:rule/AuditManagerSecurityHubFindingsReceiver"
   }
  ]
}
```

AWS Audit Manager pembaruan kebijakan AWS terkelola

Lihat detail tentang pembaruan kebijakan AWS terkelola AWS Audit Manager sejak layanan ini mulai melacak perubahan ini. Untuk peringatan otomatis tentang perubahan pada halaman ini, berlangganan umpan RSS di halaman Riwayat AWS Audit Manager dokumen.

Perubahan	Deskripsi	Tanggal
AWSAuditManagerServiceRolePolicy — Perbarui ke kebijakan yang ada	Peran terkait layanan sekarang memungkinkan AWS Audit Manager untuk melakukan tindakan. `s3:GetBucketPolicy` Tindakan API ini diperlukan untuk mendukung kerangka kerja praktik terbaik AIAWS generatif v1. Hal ini memungkinkan Audit Manager untuk mengumpulkan bukti otomatis tentang pembatasan kebijakan yang berlaku untuk kumpulan data pelatihan data model AI generatif Anda. `GetBucketPolicy` Tindakan beroperasi dalam lingkup di Akun AWS mana service-linked-role tersedia. Itu tidak dapat mengakses kebijakan bucket lintas akun.	12/06/2023
AWSAuditManagerServiceRolePolicy — Perbarui ke kebijakan yang ada	Kami menambahkan izin berikut ke`AWSAuditManagerServiceRolePolicy` . AWS Audit Manager sekarang dapat melakukan tindakan berikut untuk mengumpulkan bukti otomatis tentang sumber daya di Anda Akun AWS. • `acm:GetAccountConfiguration` • `acm:ListCertificates` • `backup:ListRecoveryPointsByResource` • `bedrock:GetCustomModel` • `bedrock:GetFoundationModel`	11/06/2023

Perubahan	Deskripsi	Tanggal
	• bedrock:GetModelCustomizationJob • bedrock:GetModelInvocationLoggingConfiguration • bedrock:ListCustomModels • bedrock:ListFoundationModels • bedrock:ListModelCustomizationJobs • cloudtrail:LookupEvents • cloudwatch:DescribeAlarmsForMetric • cloudwatch:GetMetricStatistics • cloudwatch:ListMetrics • directconnect:DescribeDirectConnectGateways • directconnect:DescribeVirtualGateways • dynamodb:ListBackups • dynamodb:ListGlobalTables • ec2:DescribeAddresses • ec2:DescribeCustomerGateways • ec2:DescribeEgressOnlyInternetGateways • ec2:DescribeInternetGateways • ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations • ec2:DescribeLocalGateways • ec2:DescribeLocalGatewayVirtualInterfaces • ec2:DescribeNatGateways	

Perubahan	Deskripsi	Tanggal
	• ec2:DescribeTransitGateways • ec2:DescribeVpcPeeringConnections • ec2:DescribeVpnConnections • ec2:DescribeVpnGateways • ec2:GetEbsDefaultKmsKeyId • ec2:GetEbsEncryptionByDefault • ecs:DescribeClusters • eks:DescribeAddonVersions • elasticache:DescribeCacheClusters • elasticache:DescribeServiceUpdates • elasticfilesystem:DescribeAccessPoints • elasticloadbalancing:DescribeLoadBalancers • elasticloadbalancing:DescribeSslPolicies • elasticloadbalancing:DescribeTargetGroups • elasticmapreduce:ListClusters • elasticmapreduce:ListSecurityConfigurations • events:ListConnections • events:ListEventBuses • events:ListEventSources • events:ListRules • firehose:ListDeliveryStreams • fsx:DescribeFileSystems	

Perubahan	Deskripsi	Tanggal
	• iam:GetAccountPasswordPolicy • iam:GetCredentialReport • iam:ListOpenIdConnectProviders • iam:ListSamlProviders • iam:ListVirtualMFADevices • kafka:ListClusters • kafka:ListKafkaVersions • kinesis:ListStreams • lambda:ListFunctions • logs:DescribeDestinations • logs:DescribeExportTasks • logs:DescribeLogGroups • logs:DescribeMetricFilters • logs:DescribeResourcePolicies • logs:FilterLogEvents • rds:DescribeCertificates • rds:DescribeDbClusterEndpoints • rds:DescribeDbClusterParameterGroups • rds:DescribeDbClusters • rds:DescribeDbSecurityGroups • redshift:DescribeClusters • s3:GetBucketPublicAccessBlock • s3:GetBucketVersioning • sns:ListTopics • sqs:ListQueues • waf-regional:GetLoggingConfiguration • waf-regional:ListRuleGroups	

Perubahan	Deskripsi	Tanggal
	• `waf-regional:ListSubscribedRuleGroups` • `waf-regional:ListWebACLs`	
AWSAuditManagerServiceRolePolicy — Perbarui ke kebijakan yang ada	Kami menambahkan izin berikut ke`AWSAuditManagerServiceRolePolicy` : • `dynamodb:DescribeTable` • `dynamodb:ListTables` • `ec2:DescribeVolumes` • `kms:GetKeyPolicy` • `kms:GetKeyRotationStatus` • `kms:ListKeyPolicies` • `rds:DescribeDBInstances` • `redshift:DescribeClusters` • `s3:GetEncryptionConfiguration` • `s3:ListAllMyBuckets`	07/07/2022
AWSAuditManagerServiceRolePolicy – Pembaruan pada kebijakan yang sudah ada	Peran terkait layanan sekarang memungkinkan AWS Audit Manager untuk melakukan tindakan. `organizations:DescribeOrganization` Kami juga mencakup `CreateEventsAccess` sumber daya dari wildcard (`*`) ke jenis sumber daya tertentu (). `arn:aws:events:*:*:rule/AuditManagerSecurityHubFindingsReceiver` Terakhir, kami menambahkan operator `Null` kondisi untuk kunci `events:source` kondisi untuk mengonfirmasi bahwa nilai sumber ada dan nilainya tidak null.	05/20/2022

Perubahan	Deskripsi	Tanggal
AWSAuditManagerAdministratorAccess – Pembaruan pada kebijakan yang sudah ada	Kami memperbarui kebijakan kondisi kunci `events:source` untuk mencerminkan bahwa ini adalah kunci multi-nilai.	04/29/2022
AWSAuditManagerServiceRolePolicy – Pembaruan pada kebijakan yang sudah ada	Kami memperbarui kebijakan kondisi kunci `events:source` untuk mencerminkan bahwa ini adalah kunci multi-nilai.	03/16/2022
AWS Audit Manager mulai melacak perubahan	AWS Audit Manager mulai melacak perubahan untuk kebijakan AWS terkelolanya.	05/06/2021

Memecahkan masalah AWS Audit Manager identitas dan akses

Gunakan informasi berikut untuk membantu Anda mendiagnosis dan memperbaiki masalah umum yang mungkin Anda temui saat bekerja dengan Audit Manager dan IAM.

Topik

- Saya tidak berwenang untuk melakukan tindakan di AWS Audit Manager
- Saya tidak berwenang untuk melakukan iam: PassRole
- Saya ingin mengizinkan orang di luar saya Akun AWS untuk mengakses AWS Audit Manager sumber daya saya

Saya tidak berwenang untuk melakukan tindakan di AWS Audit Manager

`AccessDeniedException`Kesalahan muncul ketika pengguna tidak memiliki izin untuk menggunakan AWS Audit Manager atau operasi Audit Manager API.

Dalam hal ini, administrator Anda harus memperbarui kebijakan untuk memungkinkan Anda mengakses.

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 ke Audit Manager.

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 untuk melakukan tindakan di Audit Manager. Namun, tindakan tersebut memerlukan layanan untuk mendapatkan izin yang diberikan oleh peran layanan. Mary tidak memiliki izin untuk meneruskan peran tersebut pada layanan.

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

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

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

Saya ingin mengizinkan orang di luar saya Akun AWS untuk mengakses AWS Audit Manager sumber daya saya

Anda dapat membuat peran yang dapat digunakan pengguna di akun lain atau pengguna 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 pengguna akses ke sumber daya Anda.

Untuk mempelajari selengkapnya, periksa hal berikut:

- Untuk mengetahui apakah Audit Manager mendukung fitur ini, lihatBagaimana AWS Audit Manager 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 Memberikan akses kepada pengguna eksternal yang sah (federasi identitas) dalam Panduan Pengguna IAM.

- Untuk mempelajari perbedaan antara penggunaan peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Perbedaan antara peran IAM dan kebijakan berbasis sumber daya di Panduan Pengguna IAM.

Menggunakan peran terkait layanan untuk AWS Audit Manager

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

Peran terkait layanan membuat pengaturan AWS Audit Manager lebih mudah karena Anda tidak perlu menambahkan izin yang diperlukan secara manual. Audit Manager mendefinisikan izin peran terkait layanan, dan kecuali ditentukan lain, hanya Audit Manager yang dapat mengambil perannya. Izin yang ditentukan mencakup kebijakan kepercayaan dan kebijakan izin, dan kebijakan izin tersebut tidak dapat dilampirkan ke entitas IAM lainnya.

Untuk informasi tentang layanan lain yang mendukung peran tertaut layanan, lihat LayananAWS yang kompatibel dengan IAM dan cari layanan yang memiliki nilai Ya di dalam kolom Peran Tertaut Layanan. Pilih Ya dengan sebuah tautan untuk melihat dokumentasi peran terkait layanan untuk layanan tersebut.

Izin peran terkait layanan untuk AWS Audit Manager

Audit Manager menggunakan peran terkait layanan bernama**`AWSServiceRoleForAuditManager`**, yang memungkinkan akses ke layanan AWS dan sumber daya yang digunakan atau dikelola oleh. AWS Audit Manager

Peran terkait layanan `AWSServiceRoleForAuditManager` memercayai layanan `auditmanager.amazonaws.com` untuk menjalankan peran.

Kebijakan izin peran `AWSAuditManagerServiceRolePolicy`, memungkinkan Audit Manager mengumpulkan bukti otomatis tentang AWS penggunaan Anda. Lebih khusus lagi, dapat mengambil tindakan berikut atas nama Anda.

- Audit Manager dapat digunakan AWS Security Hub untuk mengumpulkan bukti pemeriksaan kepatuhan. Dalam hal ini, Audit Manager menggunakan izin berikut untuk melaporkan hasil pemeriksaan keamanan langsung dari AWS Security Hub. Kemudian melampirkan hasilnya ke kontrol penilaian Anda yang relevan sebagai bukti.

- `securityhub:DescribeStandards`

> **Note**
>
> Untuk informasi selengkapnya tentang kontrol Security Hub tertentu yang dapat dijelaskan oleh Audit Manager, lihat AWS Security Hub kontrol yang didukung oleh AWS Audit Manager.

- Audit Manager dapat digunakan AWS Config untuk mengumpulkan bukti pemeriksaan kepatuhan. Dalam hal ini, Audit Manager menggunakan izin berikut untuk melaporkan hasil evaluasi AWS Config aturan secara langsung. AWS ConfigKemudian melampirkan hasilnya ke kontrol penilaian Anda yang relevan sebagai bukti.
  - `config:DescribeConfigRules`
  - `config:DescribeDeliveryChannels`
  - `config:ListDiscoveredResources`

> **Note**
>
> Untuk informasi selengkapnya tentang AWS Config aturan spesifik yang dapat dijelaskan oleh Audit Manager, lihat AWS Config Aturan yang didukung oleh AWS Audit Manager.

- Audit Manager dapat digunakan AWS CloudTrail untuk mengumpulkan bukti aktivitas pengguna. Dalam hal ini, Audit Manager menggunakan izin berikut untuk menangkap aktivitas pengguna dari CloudTrail log. Ini kemudian melampirkan aktivitas ke kontrol penilaian Anda yang relevan sebagai bukti.
  - `cloudtrail:DescribeTrails`
  - `cloudtrail:LookupEvents`

> **Note**
>
> Untuk informasi selengkapnya tentang CloudTrail peristiwa tertentu yang dapat dijelaskan oleh Audit Manager, lihat namaAWS CloudTrail acara yang didukung oleh AWS Audit Manager.

- Audit Manager dapat menggunakan panggilan AWS API untuk mengumpulkan bukti konfigurasi sumber daya. Dalam hal ini, Audit Manager menggunakan izin berikut untuk memanggil API hanya-

baca yang menjelaskan konfigurasi sumber daya Anda untuk hal berikut. Layanan AWSKemudian melampirkan respons API ke kontrol penilaian Anda yang relevan sebagai bukti.

- acm:GetAccountConfiguration
- acm:ListCertificates
- backup:ListRecoveryPointsByResource
- bedrock:GetCustomModel
- bedrock:GetFoundationModel
- bedrock:GetModelCustomizationJob
- bedrock:GetModelInvocationLoggingConfiguration
- bedrock:ListCustomModels
- bedrock:ListFoundationModels
- bedrock:ListModelCustomizationJobs
- cloudwatch:DescribeAlarms
- cloudwatch:DescribeAlarmsForMetric
- cloudwatch:GetMetricStatistics
- cloudwatch:ListMetrics
- cognito-idp:DescribeUserPool
- directconnect:DescribeDirectConnectGateways
- directconnect:DescribeVirtualGateways
- dynamodb:DescribeTable
- dynamodb:ListBackups
- dynamodb:ListGlobalTables
- dynamodb:ListTables
- ec2:DescribeAddresses
- ec2:DescribeCustomerGateways
- ec2:DescribeEgressOnlyInternetGateways
- ec2:DescribeFlowLogs
- ec2:DescribeInstances
- ec2:DescribeInternetGateways

- ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations

- ec2:DescribeLocalGateways
- ec2:DescribeLocalGatewayVirtualInterfaces
- ec2:DescribeNatGateways
- ec2:DescribeNetworkAcls
- ec2:DescribeRouteTables
- ec2:DescribeSecurityGroups
- ec2:DescribeSnapshots
- ec2:DescribeTransitGateways
- ec2:DescribeVolumes
- ec2:DescribeVpcEndpoints
- ec2:DescribeVpcPeeringConnections
- ec2:DescribeVpcs
- ec2:DescribeVpnConnections
- ec2:DescribeVpnGateways
- ec2:GetEbsDefaultKmsKeyId
- ec2:GetEbsEncryptionByDefault
- ecs:DescribeClusters
- eks:DescribeAddonVersions
- elasticache:DescribeCacheClusters
- elasticache:DescribeServiceUpdates
- elasticfilesystem:DescribeAccessPoints
- elasticfilesystem:DescribeFileSystems
- elasticloadbalancing:DescribeLoadBalancers
- elasticloadbalancing:DescribeSslPolicies
- elasticloadbalancing:DescribeTargetGroups
- elasticmapreduce:ListClusters
- elasticmapreduce:ListSecurityConfigurations
- events:DeleteRule
- events:DescribeRule
- events:DisableRule

- events:EnableRule
- events:ListConnections
- events:ListEventBuses
- events:ListEventSources
- events:ListRules
- events:ListTargetsByRule
- events:PutRule
- events:PutTargets
- events:RemoveTargets
- firehose:ListDeliveryStreams
- fsx:DescribeFileSystems
- guardduty:ListDetectors
- iam:GenerateCredentialReport
- iam:GetAccountAuthorizationDetails
- iam:GetAccountPasswordPolicy
- iam:GetAccountSummary
- iam:GetCredentialReport
- iam:ListEntitiesForPolicy
- iam:ListGroupPolicies
- iam:ListGroups
- iam:ListOpenIdConnectProviders
- iam:ListPolicies
- iam:ListRolePolicies
- iam:ListRoles
- iam:ListSamlProviders
- iam:ListUserPolicies
- iam:ListUsers
- iam:ListVirtualMFADevices
- kafka:ListClusters
- kafka:ListKafkaVersions

- kinesis:ListStreams
- kms:DescribeKey
- kms:GetKeyPolicy
- kms:GetKeyRotationStatus
- kms:ListGrants
- kms:ListKeyPolicies
- kms:ListKeys
- lambda:ListFunctions
- license-manager:ListAssociationsForLicenseConfiguration
- license-manager:ListLicenseConfigurations
- license-manager:ListUsageForLicenseConfiguration
- logs:DescribeDestinations
- logs:DescribeExportTasks
- logs:DescribeLogGroups
- logs:DescribeMetricFilters
- logs:DescribeResourcePolicies
- logs:FilterLogEvents
- organizations:DescribeOrganization
- organizations:DescribePolicy
- rds:DescribeCertificates
- rds:DescribeDbClusterEndpoints
- rds:DescribeDbClusterParameterGroups
- rds:DescribeDbClusters
- rds:DescribeDBInstances
- rds:DescribeDbSecurityGroups
- redshift:DescribeClusters
- route53:GetQueryLoggingConfig
- s3:GetBucketPolicy

  - Tindakan API ini beroperasi dalam lingkup di Akun AWS mana service-linked-role tersedia. Itu tidak dapat mengakses kebijakan bucket lintas akun.

- `s3:GetBucketPublicAccessBlock`
- `s3:GetBucketVersioning`
- `s3:GetEncryptionConfiguration`
- `s3:GetLifecycleConfiguration`
- `s3:ListAllMyBuckets`
- `sns:ListTopics`
- `sqs:ListQueues`
- `waf-regional:GetLoggingConfiguration`
- `waf-regional:ListRuleGroups`
- `waf-regional:ListSubscribedRuleGroups`
- `waf-regional:ListWebACLs`
- `waf:ListActivatedRulesInRuleGroup`

> **Note**
>
> Untuk informasi selengkapnya tentang panggilan API tertentu yang dapat dijelaskan oleh Audit Manager, lihatPanggilan API yang didukung untuk sumber data kontrol kustom.

Untuk melihat detail izin lengkap dari peran terkait layanan`AWSServiceRoleForAuditManager`, lihat AWSAuditManagerServiceRolePolicydi Panduan Referensi KebijakanAWS Terkelola.

Anda harus mengonfigurasi izin untuk mengizinkan entitas IAM (seperti pengguna, grup, atau peran) untuk membuat, mengedit, atau menghapus peran terkait layanan. Untuk informasi selengkapnya, lihat Izin peran tertaut layanan dalam Panduan Pengguna IAM.

Membuat peran AWS Audit Manager terkait layanan

Anda tidak perlu membuat peran tertaut layanan secara manual. Saat Anda mengaktifkan AWS Audit Manager, layanan akan secara otomatis membuat peran terkait layanan untuk Anda. Anda dapat mengaktifkan Audit Manager dari halaman orientasi AWS Management Console, atau melalui API atau AWS CLI. Untuk informasi selengkapnya, lihat Aktifkan AWS Audit Manager di panduan pengguna ini.

Jika Anda menghapus peran terkait layanan ini, dan ingin membuatnya lagi, Anda dapat mengulangi proses yang sama untuk membuat kembali peran tersebut di akun Anda.

Mengedit peran AWS Audit Manager terkait layanan

AWS Audit Manager tidak memungkinkan Anda untuk mengedit peran `AWSServiceRoleForAuditManager` terkait layanan. Setelah membuat peran terkait layanan, Anda tidak dapat mengubah nama peran karena berbagai entitas mungkin mereferensikan peran tersebut. Namun, Anda dapat menyunting penjelasan peran menggunakan IAM. Untuk informasi selengkapnya, lihat Mengedit peran tertaut layanan dalam Panduan Pengguna IAM.

Untuk mengizinkan entitas IAM mengedit deskripsi peran terkait **`AWSServiceRoleForAuditManager`** layanan

Tambahkan pernyataan berikut ke kebijakan izin untuk entitas IAM yang perlu mengedit deskripsi peran terkait layanan.

```
{
    "Effect": "Allow",
    "Action": [
        "iam:UpdateRoleDescription"
    ],
    "Resource": "arn:aws:iam::*:role/aws-service-role/auditmanager.amazonaws.com/
AWSServiceRoleForAuditManager*",
    "Condition": {"StringLike": {"iam:AWSServiceName": "auditmanager.amazonaws.com"}}
}
```

Menghapus peran terkait AWS Audit Manager layanan

Jika Anda tidak perlu lagi menggunakan Audit Manager, sebaiknya hapus peran `AWSServiceRoleForAuditManager` terkait layanan. Dengan begitu, Anda tidak memiliki entitas yang tidak terpakai yang tidak dipantau atau dipelihara secara aktif. Namun, Anda harus membersihkan peran terkait layanan sebelum dapat menghapusnya.

Membersihkan peran terkait layanan

Sebelum dapat menggunakan IAM untuk menghapus peran terkait layanan Audit Manager, Anda harus terlebih dahulu mengonfirmasi bahwa peran tersebut tidak memiliki sesi aktif dan menghapus sumber daya apa pun yang digunakan oleh peran tersebut. Untuk melakukannya, pastikan bahwa Audit Manager dideregistrasi secara keseluruhan. Wilayah AWSSetelah Anda membatalkan pendaftaran, Audit Manager tidak lagi menggunakan peran terkait layanan.

Untuk petunjuk tentang cara membatalkan pendaftaran Audit Manager, lihat sumber daya berikut:

- Menonaktifkan AWS Audit Manager dalam panduan ini
- DeregisterAccount di Referensi APIAWS Audit Manager
- deregister-account di Referensi untukAWS CLI AWS Audit Manager

Untuk petunjuk tentang cara menghapus sumber daya Audit Manager secara manual, lihat Penghapusan data Audit Manager dalam panduan ini.

Menghapus peran tertaut layanan

Anda dapat menghapus peran terkait layanan menggunakan konsol IAM, AWS Command Line Interface (AWS CLI), atau IAM API.

IAM console

Ikuti langkah-langkah berikut untuk menghapus peran terkait layanan di konsol IAM.

Untuk menghapus peran terkait layanan (konsol)

1. Masuk ke AWS Management Console dan buka konsol IAM di https://console.aws.amazon.com/iam/.
2. Di panel navigasi konsol IAM, pilih Peran. Kemudian pilih kotak centang di sebelah`AWSServiceRoleForAuditManager`, bukan nama atau baris itu sendiri.
3. Di bawah Tindakan peran di bagian atas halaman, pilih Hapus.
4. Di kotak dialog konfirmasi, tinjau informasi yang terakhir diakses, yang menunjukkan kapan masing-masing peran yang dipilih terakhir mengakses file Layanan AWS. Hal ini membantu Anda mengonfirmasi aktif tidaknya peran tersebut saat ini. Jika Anda ingin melanjutkan, masukkan **`AWSServiceRoleForAuditManager`** kolom input teks dan pilih Hapus untuk mengirimkan peran terkait layanan untuk dihapus.
5. Perhatikan notifikasi konsol IAM untuk memantau progres penghapusan peran tertaut layanan. Karena penghapusan peran tertaut layanan IAM bersifat asinkron, setelah Anda mengirimkan peran tersebut untuk penghapusan, tugas penghapusan dapat berhasil atau gagal. Jika tugas berhasil, maka peran dihapus dari daftar dan pesan sukses muncul di bagian atas halaman.

AWS CLI

Anda dapat menggunakan perintah IAM dari AWS CLI untuk menghapus peran terkait layanan.

Untuk menghapus peran terkait layanan (AWS CLI)

1. Masukkan perintah berikut untuk membuat daftar peran di akun Anda:

```
aws iam get-role --role-name AWSServiceRoleForAuditManager
```

2. Karena peran yang terhubung dengan layanan tidak dapat dihapus jika sedang digunakan atau memiliki sumber daya terkait, Anda harus mengirimkan permintaan penghapusan. Permintaan tersebut dapat ditolak jika syarat-syarat ini tidak terpenuhi. Anda harus menangkap `deletion-task-id` dari tanggapan untuk memeriksa status tugas penghapusan.

   Ketik perintah berikut untuk mengirimkan permintaan penghapusan peran yang terhubung dengan layanan:

```
aws iam delete-service-linked-role --role-name AWSServiceRoleForAuditManager
```

3. Gunakan perintah berikut untuk memeriksa status tugas penghapusan:

```
aws iam get-service-linked-role-deletion-status --deletion-task-id deletion-task-id
```

   Kemungkinan status tugas penghapusan dapat berupa `NOT_STARTED`, `IN_PROGRESS`, `SUCCEEDED`, atau `FAILED`. Jika penghapusan gagal, panggilan akan mengembalikan alasan kegagalan panggilan agar Anda dapat memecahkan masalah.

IAM API

Anda dapat menggunakan IAM API untuk menghapus peran terkait layanan.

Untuk menghapus peran terkait layanan (API)

1. Hubungi GetRoleuntuk membuat daftar peran di akun Anda. Dalam permintaan, tentukan `AWSServiceRoleForAuditManager` sebagai`RoleName`.
2. Karena peran yang terhubung dengan layanan tidak dapat dihapus jika sedang digunakan atau memiliki sumber daya terkait, Anda harus mengirimkan permintaan penghapusan. Permintaan tersebut dapat ditolak jika syarat-syarat ini tidak terpenuhi. Anda harus menangkap `DeletionTaskId` dari tanggapan untuk memeriksa status tugas penghapusan.

Untuk mengirimkan permintaan penghapusan untuk peran tertaut layanan, panggil DeleteServiceLinkedRole. Dalam permintaan, tentukan `AWSServiceRoleForAuditManager` sebagai`RoleName`.

3. Untuk memeriksa status penghapusan, panggil GetServiceLinkedRoleDeletionStatus. Di permintaan tersebut, tentukan `DeletionTaskId`.

   Kemungkinan status tugas penghapusan dapat berupa `NOT_STARTED`, `IN_PROGRESS`, `SUCCEEDED`, atau `FAILED`. Jika penghapusan gagal, panggilan akan mengembalikan alasan kegagalan panggilan agar Anda dapat memecahkan masalah.

> **Tip**
>
> Penghapusan gagal jika layanan Audit Manager menggunakan peran atau memiliki sumber daya terkait. Ini hanya terjadi jika Anda masih terdaftar di Audit Manager dalam satu atau lebih Wilayah AWS. Setelah Anda membatalkan pendaftaran, Audit Manager berhenti menggunakan peran terkait layanan.
> Untuk mengatasi masalah penghapusan yang gagal, pertama-tama pastikan bahwa Anda membatalkan pendaftaran Audit Manager Wilayah AWS di semua tempat Anda menggunakan layanan. Kemudian, coba lagi untuk mengikuti langkah-langkah dalam prosedur sebelumnya.

Wilayah yang Didukung untuk AWS Audit Manager peran terkait layanan

AWS Audit Manager mendukung penggunaan peran terkait layanan di semua Wilayah AWS tempat layanan tersedia. Untuk informasi selengkapnya, lihat AWS titik akhir layanan.

Validasi kepatuhan untuk AWS Audit Manager

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

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 DayaAWS — 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 PanduanAWS 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 mengevaluasi sumber daya AWS Anda dan memeriksa kepatuhan Anda terhadap standar industri keamanan dan praktik terbaik. Untuk daftar layanan dan kontrol yang didukung, lihat Referensi kontrol Security Hub.
- 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 Audit Manager

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 InfrastrukturAWS Global.

Keamanan infrastruktur di AWS Audit Manager

Sebagai layanan terkelola, AWS Audit Manager dilindungi oleh keamanan jaringan AWS global. Untuk informasi tentang layanan AWS keamanan dan cara AWS melindungi infrastruktur, lihat KeamananAWS Cloud. Untuk mendesain AWS lingkungan Anda menggunakan praktik terbaik untuk keamanan infrastruktur, lihat Perlindungan Infrastruktur dalam Kerangka Kerja yang AWS Diarsiteksikan dengan Baik Pilar Keamanan.

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

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

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

Anda dapat memanggil operasi API ini dari lokasi jaringan mana pun, AWS Audit Manager tetapi mendukung kebijakan akses berbasis sumber daya, yang dapat mencakup pembatasan berdasarkan

alamat IP sumber. Anda juga dapat menggunakan kebijakan Audit Manager untuk mengontrol akses dari titik akhir Amazon Virtual Private Cloud (Amazon VPC) tertentu atau VPC tertentu. Secara efektif, ini mengisolasi akses jaringan ke sumber daya Audit Manager yang diberikan hanya dari VPC tertentu dalam AWS jaringan.

AWS Audit Manager dan antarmuka titik akhir VPC ()AWS PrivateLink

Anda dapat membuat koneksi pribadi antara VPC Anda dan AWS Audit Manager dengan membuat antarmuka VPC endpoint. Endpoint antarmuka didukung oleh AWS PrivateLink, teknologi yang memungkinkan Anda mengakses API Audit Manager secara pribadi tanpa gateway internet, perangkat NAT, koneksi VPN, atau koneksi Direct AWS Connect. Instans di VPC Anda tidak memerlukan alamat IP publik untuk berkomunikasi dengan Audit Manager API. Lalu lintas antara VPC Anda dan AWS Audit Manager tidak meninggalkan jaringan. AWS

Setiap titik akhir antarmuka diwakili oleh satu atau beberapa Antarmuka Jaringan Elastis di subnet Anda.

Untuk informasi selengkapnya, lihat Antarmuka VPC endpoint (AWS PrivateLink) dalam Panduan Pengguna Amazon VPC.

Pertimbangan untuk titik akhir AWS Audit Manager VPC

Sebelum menyiapkan titik akhir VPC antarmuka AWS Audit Manager, pastikan Anda meninjau properti dan batasan titik akhir Antarmuka di Panduan Pengguna Amazon VPC.

AWS Audit Manager mendukung panggilan ke semua tindakan API-nya dari VPC Anda.

Buat VPC endpoint antarmuka untuk AWS Audit Manager

Anda dapat membuat titik akhir VPC untuk AWS Audit Manager layanan menggunakan konsol VPC Amazon atau (). AWS Command Line Interface AWS CLIUntuk informasi selengkapnya, lihat Membuat titik akhir antarmuka dalam Panduan Pengguna Amazon VPC.

Buat titik akhir VPC untuk AWS Audit Manager menggunakan nama layanan berikut:

- `com.amazonaws.region.auditmanager`

Jika Anda mengaktifkan DNS pribadi untuk titik akhir, Anda dapat membuat permintaan API untuk AWS Audit Manager menggunakan nama DNS default untuk Wilayah, misalnya,. `auditmanager.us-east-1.amazonaws.com`

Untuk informasi selengkapnya, lihat Mengakses layanan melalui titik akhir antarmuka dalam Panduan Pengguna Amazon VPC.

Membuat kebijakan titik akhir VPC untuk AWS Audit Manager

Anda dapat melampirkan kebijakan titik akhir ke VPC endpoint yang mengendalikan akses ke AWS Audit Manager. Kebijakan titik akhir menentukan informasi berikut:

- Prinsipal yang dapat melakukan tindakan.
- Tindakan yang dapat dilakukan.
- Sumber daya yang menjadi target tindakan.

Untuk informasi selengkapnya, lihat Mengontrol akses ke layanan dengan titik akhir VPC dalam Panduan Pengguna Amazon VPC.

Contoh: Kebijakan titik akhir VPC untuk tindakan AWS Audit Manager

Berikut ini adalah contoh kebijakan endpoint untuk AWS Audit Manager. Saat dilampirkan ke titik akhir, kebijakan ini memberikan akses ke tindakan Audit Manager yang terdaftar untuk semua prinsipal di semua sumber daya.

```
{
   "Statement":[
      {
         "Principal":"*",
         "Effect":"Allow",
         "Action":[
            "auditmanager:GetAssessments",
            "auditmanager:GetServicesInScope",
            "auditmanager:ListNotifications"
         ],
         "Resource":"*"
      }
   ]
}
```

Penebangan dan pemantauan di AWS Audit Manager

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

- AWS CloudTrail merekam panggilan API dan kejadian terkait yang dilakukan oleh atau atas Akun AWS Anda dan mengirimkan berkas log ke bucket Amazon S3 yang Anda tentukan. Anda dapat mengidentifikasi pengguna dan akun yang memanggil AWS, alamat IP asal panggilan dilakukan, dan waktu panggilan terjadi. Untuk mengetahui informasi selengkapnya, lihat Panduan PenggunaAWS CloudTrail.
- Amazon EventBridge adalah layanan bus acara tanpa server yang memudahkan untuk menghubungkan aplikasi Anda dengan data dari berbagai sumber. EventBridge memberikan aliran data real-time dari aplikasi Anda sendiri, aplikasi oftware-as-a S-Service (SaaS), dan AWS layanan serta rute data tersebut ke target seperti Lambda. Hal ini memungkinkan Anda memantau kejadian yang terjadi dalam layanan, dan membangun arsitektur yang didorong kejadian. Untuk informasi selengkapnya, lihat Panduan EventBridge Pengguna Amazon.

Pemantauan AWS Audit Manager dengan Amazon EventBridge

Amazon EventBridge membantu Anda mengotomatiskan Layanan AWS dan merespons secara otomatis peristiwa sistem seperti masalah ketersediaan aplikasi atau perubahan sumber daya.

Anda dapat menggunakan EventBridge aturan untuk mendeteksi dan bereaksi terhadap peristiwa Audit Manager. Berdasarkan aturan yang Anda buat, EventBridge memanggil satu atau beberapa tindakan target saat peristiwa cocok dengan nilai yang Anda tentukan dalam aturan. Bergantung pada jenis acara, Anda mungkin ingin mengirim pemberitahuan, menangkap informasi acara, mengambil tindakan korektif, memulai acara, atau mengambil tindakan lain.

Misalnya, Anda dapat mendeteksi setiap kali peristiwa Audit Manager berikut terjadi di akun Anda:

- Pemilik audit membuat, memperbarui, atau menghapus penilaian
- Pemilik audit mendelegasikan set kontrol untuk ditinjau
- Seorang delegasi menyelesaikan peninjauan mereka dan menyerahkan kontrol yang ditinjau kembali ke pemilik audit
- Pemilik audit memperbarui status kontrol penilaian

Tindakan yang dapat dipicu secara otomatis meliputi hal-hal berikut:

- Gunakan AWS Lambda fungsi untuk meneruskan notifikasi ke saluran Slack.
- Dorong data tentang pemeriksaan ke Amazon Kinesis Data Streams untuk mendukung pemantauan status yang komprehensif dan real-time.
- Kirim topik Amazon Simple Notification Service (Amazon SNS) ke email Anda.
- Dapatkan pemberitahuan dengan tindakan CloudWatch alarm Amazon.

> **Note**
>
> Audit Manager memberikan acara secara tahan lama. Ini berarti bahwa Audit Manager akan berhasil mengantarkan acara ke EventBridge setidaknya satu kali. Dalam kasus di mana acara tidak dapat disampaikan karena gangguan EventBridge layanan, mereka akan dicoba lagi nanti oleh Audit Manager hingga 24 jam.

EventBridge format contoh untuk Audit Manager

Kode JSON berikut menunjukkan contoh peristiwa pembuatan penilaian di Audit Manager. Untuk informasi tentang salah satu bidang dalam acara ini, lihat Referensi struktur acara.

```
{
    "version": "0",
    "id": "55c5a6f3-6183-3989-49ec-a3c998857644",
    "detail-type": "Assessment Created",
    "source": "aws.auditmanager",
    "account": "111122223333",
    "time": "2023-07-27T00:38:33Z",
    "region": "us-west-2",
    "resources":
        [
            "arn:aws:auditmanager:us-west-2:111122223333:assessment/a1b2c3d4-e5f6-g7h8-
i9j0-k1l2m3n4o5p6"
        ],
    "detail":
    {
        "eventID": "4e939b2f-9429-3141-beec-d640d83ef68e",
        "author": "arn:aws:sts::111122223333:assumed-role/roleName/role-session-name",
        "assessmentTenantId": "111122223333",
```

```
        "assessmentName": "myAssessment",
        "eventTime": 1690418289068,
        "eventName": "CREATE",
        "eventType": "ASSESSMENT",
        "assessmentID": "a1b2c3d4-e5f6-g7h8-i9j0-k1l2m3n4o5p6"
    }
}
```

Prasyarat untuk membuat aturan EventBridge

Sebelum Anda membuat aturan untuk acara Audit Manager, kami sarankan Anda melakukan 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 SNS sehingga setiap kali tinjauan set kontrol selesai, Anda akan menerima pesan teks atau email. Untuk informasi lebih lanjut, lihat EventBridge target.

Membuat EventBridge aturan untuk Audit Manager

Ikuti langkah-langkah berikut untuk membuat EventBridge aturan yang memicu peristiwa yang dipancarkan oleh Audit Manager. Peristiwa dipancarkan atas dasar upaya terbaik.

Untuk membuat EventBridge aturan untuk Audit Manager

1. Buka EventBridge konsol Amazon di https://console.aws.amazon.com/events/.
2. Di panel navigasi, pilih Aturan.
3. Pilih Buat aturan.
4. Pada halaman Tentukan detail aturan, masukkan nama dan deskripsi untuk aturan tersebut.
5. Simpan nilai default untuk bus Acara dan tipe Aturan, lalu pilih Berikutnya.
6. Pada halaman pola acara Build, untuk sumber acara, pilih AWS acara atau acara EventBridge mitra.
7. Untuk metode Creation, pilih Custom pattern (JSON editor).
8. Di bawah Pola acara, tulis pola acara di JSON dan tentukan bidang yang ingin Anda gunakan untuk pencocokan.

   Untuk mencocokkan acara Audit Manager, Anda dapat menggunakan pola sederhana berikut:

```
{
  "detail-type": ["Event"]
}
```

Ganti *Event* dengan salah satu nilai yang didukung berikut:

a. Masuk `Assessment Created` untuk mendapatkan notifikasi saat penilaian dibuat.

b. Masuk `Assessment Updated` untuk mendapatkan notifikasi saat penilaian diperbarui.

c. Masuk `Assessment Deleted` untuk mendapatkan notifikasi saat penilaian dihapus.

d. Masukkan `Assessment ControlSet Delegation Created` untuk mendapatkan notifikasi saat set kontrol didelegasikan untuk ditinjau.

e. Masuk `Assessment ControlSet Reviewed` untuk mendapatkan notifikasi saat set kontrol penilaian ditinjau.

f. Masuk `Assessment Control Reviewed` untuk mendapatkan pemberitahuan saat kontrol penilaian ditinjau.

> **Tip**
>
> Tambahkan lebih banyak bidang ke pola acara Anda sesuai kebutuhan. Untuk informasi selengkapnya tentang bidang yang tersedia, lihat pola EventBridge acara Amazon.

9. Pilih Berikutnya.

10. Pada halaman 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.

> **Tip**
>
> Bidang yang ditampilkan bervariasi tergantung pada layanan yang dipilih. Untuk informasi selengkapnya tentang target yang tersedia, lihat Target yang tersedia di EventBridge konsol.

11. Untuk banyak jenis target, EventBridge perlu izin untuk mengirim acara ke target. Dalam kasus ini, EventBridge dapat membuat peran IAM yang diperlukan agar aturan Anda berjalan.

a. Untuk membuat IAM role secara otomatis, pilih Buat peran baru untuk sumber daya khusus ini.

b. Untuk menggunakan IAM role yang Anda buat sebelumnya, pilih Gunakan peran yang ada.

12. (Opsional) Pilih Tambahkan target lain untuk menambahkan target lain untuk aturan ini.
13. Pilih Berikutnya.
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 Audit Manager dan kemudian mengirimkannya ke target yang Anda tentukan.

Logging panggilan AWS Audit Manager API dengan CloudTrail

Audit Manager terintegrasi dengan CloudTrail, layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atau Layanan AWS dalam Audit Manager. CloudTrail menangkap semua panggilan API untuk Audit Manager sebagai peristiwa. Panggilan yang diambil mencakup panggilan dari konsol Audit Manager dan panggilan kode ke operasi API Audit Manager.

Jika Anda membuat jejak, Anda dapat mengaktifkan pengiriman CloudTrail peristiwa secara terus menerus ke bucket Amazon S3, termasuk peristiwa untuk Audit Manager. 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 Audit Manager, alamat IP dari mana permintaan dibuat, siapa yang membuat permintaan, kapan dibuat, dan detail tambahan.

Untuk mempelajari selengkapnya CloudTrail, lihat PanduanAWS CloudTrail Pengguna.

Informasi Audit Manager di CloudTrail

CloudTrail diaktifkan pada Akun AWS saat Anda membuat akun. Ketika aktivitas terjadi di Audit Manager, aktivitas tersebut dicatat dalam suatu CloudTrail peristiwa bersama dengan Layanan AWS peristiwa lain dalam riwayat Acara.

Anda dapat melihat, mencari, dan mengunduh acara terbaru di situs Anda Akun AWS. Untuk informasi lain, lihat Melihat Peristiwa dengan Riwayat Peristiwa CloudTrail .

Untuk catatan acara yang sedang berlangsung di Anda Akun AWS, termasuk acara untuk Audit Manager, buat jejak. Jejak memungkinkan CloudTrail untuk mengirimkan file log ke bucket Amazon S3. Secara default, saat Anda membuat jejak di konsol, jejak tersebut berlaku untuk semua Wilayah AWS. Jejak mencatat peristiwa dari semua Wilayah di AWS partisi dan mengirimkan file log ke bucket Amazon S3 yang Anda tentukan.

Selain itu, Anda dapat mengonfigurasi lainnya Layanan AWS 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 tindakan Audit Manager dicatat oleh CloudTrail dan didokumentasikan dalam ReferensiAWS Audit Manager API. Misalnya, panggilan ke`CreateCustomControl`, `DeleteControl` dan operasi `UpdateAssessmentTemplate` API menghasilkan entri dalam file CloudTrail log.

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

- Apakah permintaan dibuat dengan kredensyal pengguna root.
- Apakah permintaan dibuat dengan kredensial keamanan sementara untuk suatu peran atau pengguna gabungan.
- Apakah permintaan tersebut dibuat oleh Layanan AWSlain.

Untuk informasi lain, lihat Elemen userIdentity CloudTrail .

Memahami Entri Berkas Log Audit Manager

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.

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

```
{
      eventVersion:"1.05",
      userIdentity:{
        type:"IAMUser",
        principalId:"principalId",
        arn:"arn:aws:iam::accountId:user/userName",
        accountId:"111122223333",
        accessKeyId:"accessKeyId",
        userName:"userName",
        sessionContext:{
          sessionIssuer:{
          },
          webIdFederationData:{
          },
          attributes:{
            mfaAuthenticated:"false",
            creationDate:"2020-11-19T07:32:06Z"
          }
        }
      },
      eventTime:"2020-11-19T07:32:36Z",
      eventSource:"auditmanager.amazonaws.com",
      eventName:"CreateAssessment",
      awsRegion:"us-west-2",
      sourceIPAddress:"sourceIPAddress",
      userAgent:"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
      requestParameters:{
        frameworkId:"frameworkId",
        assessmentReportsDestination:{
          destination:"***",
          destinationType:"S3"
        },
        clientToken:"***",
        scope:{
          awsServices:[
            {
              serviceName:"license-manager"
            }
```

```
        ],
        awsAccounts:"***"
      },
      roles:"***",
      name:"***",
      description:"***",
      tags:"***"
    },
    responseElements:{
      assessment:"***"
    },
    requestID:"0d950f8c-5211-40db-8c37-2ed38ffcc894",
    eventID:"a782029a-959e-4549-81df-9f6596775cb0",
    readOnly:false,
    eventType:"AwsApiCall",
    recipientAccountId:"recipientAccountId"
  }
```

Analisis konfigurasi dan kerentanan di AWS Audit Manager

Konfigurasi dan kontrol TI adalah tanggung jawab bersama antara AWS dan Anda, pelanggan kami. Untuk informasi selengkapnya, lihat model tanggung jawab AWS bersama.

Penandaan pada sumber daya AWS Audit Manager

Tanda adalah label metadata yang Anda tetapkan atau AWS yang ditetapkan ke sumber daya AWS. Setiap tanda terdiri dari kunci dan nilai. Untuk tanda yang Anda tetapkan, Anda menentukan kunci dan nilai. Misalnya, Anda dapat menentukan kunci sebagai `stage` dan nilai untuk satu sumber daya sebagai `test`.

Tanda membantu Anda melakukan hal berikut:

- Temukan sumber daya Audit Manager Anda dengan mudah. Anda dapat menggunakan tag sebagai kriteria pencarian saat menjelajahi pustaka kerangka kerja dan pustaka kontrol.
- Kaitkan sumber daya Anda dengan jenis kepatuhan. Anda dapat menandai beberapa sumber daya dengan tag khusus kepatuhan untuk mengaitkan sumber daya tersebut dengan kerangka kerja tertentu.
- Mengidentifikasi dan mengorganisir sumber daya AWS Anda. Banyak yangLayanan AWS mendukung penandaan, sehingga Anda dapat menetapkan tanda yang sama ke sumber daya dari layanan yang berbeda untuk menunjukkan bahwa sumber daya tersebut terkait.
- Telusuri biaya AWS Anda. Anda mengaktifkan tag ini pada AWS Billing and Cost Management dasbor.AWS menggunakan tag untuk mengategorikan biaya Anda lalu mengirimkan laporan alokasi biaya bulanan kepada Anda. Untuk informasi selengkapnya, lihat Menggunakan tanda alokasi biaya dalam AWS Billing and Cost ManagementBuku Panduan.

Bagian berikut menyediakan informasi selengkapnya tentang tag untuk AWS Audit Manager.

Sumber daya yang didukung di Audit Manager

Sumber daya Audit Manager berikut mendukung penandaan:

- Penilaian
- Kontrol
- Kerangka

Pembatasan tanda

Pembatasan dasar berikut berlaku untuk tag pada sumber daya Audit Manager:

- Jumlah tanda maksimum yang dapat Anda tetapkan ke sumber daya — 50
- Panjang kunci maksimum — 128 karakter Unicode
- Panjang nilai maksimum — 256 karakter Unicode
- Karakter yang valid untuk kunci dan nilai — a-z, A-Z, 0-9, spasi, dan karakter berikut: _.:/= + - dan @
- Kunci dan nilai peka huruf besar dan kecil
- Jangan gunakan `aws:` sebagai prefiks untuk kunci; ini dicadangkan untuk penggunaan AWS

Mengelola Tanda

Anda dapat menetapkan tag sebagai properti saat membuat penilaian, kerangka kerja, atau kontrol. Anda dapat menambahkan, mengedit, dan menghapus tag melalui konsol Audit Manager,AWS Command Line Interface (AWS CLI), dan Audit Manager API. Untuk informasi selengkapnya, lihat tautan berikut.

- Untuk penilaian:
  - Membuat penilaiandanMengedit penilaian di bagian Penilaian pada panduan ini
  - Tab tagdi bagian Tinjau penilaian dari panduan ini
  - CreateAssessmentdan UpdateAssessmentdalam ReferensiAWS Audit Manager API
  - TagResourcedan UntagResourcedalam ReferensiAWS Audit Manager API
- Untuk kerangka kerja:
  - Membuat kerangka kerja khususdanMengedit kerangka kerja khusus di bagian pustaka Framework dari panduan ini
  - Tab tag di bagian Lihat rincian kerangka kerja pada panduan ini
  - CreateAssessmentFrameworkdan UpdateAssessmentFrameworkdalam ReferensiAWS Audit Manager API
  - TagResourcedan UntagResourcedalam ReferensiAWS Audit Manager API
- Untuk pengendali:
  - Membuat kontrol khususdanMengedit kontrol khusus di bagian Pustaka Kontrol pada panduan ini
  - Tab tag di bagian Lihat rincian kontrol panduan ini
  - CreateControldan UpdateControldalam ReferensiAWS Audit Manager API
  - TagResourcedan UntagResourcedalam ReferensiAWS Audit Manager API

Membuat sumber daya AWS Audit Manager dengan AWS CloudFormation

AWS Audit Manager terintegrasi dengan AWS CloudFormation, yaitu layanan yang membantu Anda membuat model dan mengatur sumber daya AWS agar Anda dapat menghemat waktu untuk membuat dan mengelola sumber daya dan infrastruktur Anda. Anda membuat template yang menjelaskan semuaAWSsumber daya yang Anda inginkan (seperti penilaian), danAWS CloudFormationketentuan dan mengkonfigurasi sumber daya untuk Anda.

Saat Anda menggunakanAWS CloudFormation, Anda dapat menggunakan kembali templat Anda untuk menyiapkan sumber daya Audit Manager secara konsisten dan berulang kali. Jelaskan sumber daya Anda sekali, lalu sediakan sumber daya yang sama berulang-ulang dalam beberapa akun dan Wilayah AWS.

Audit Manager danAWS CloudFormationtemplat

Untuk menyediakan dan mengonfigurasi sumber daya untuk Audit Manager dan layanan terkait, Anda harus memahamiAWS 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.

Audit Manager mendukung pembuatan penilaian diAWS CloudFormation. Untuk informasi selengkapnya, termasuk contoh templat JSON dan YAML untuk penilaian, lihatAWS Audit ManagerReferensi tipe sumber dayadi dalamAWS CloudFormationPanduan Pengguna.

Pelajari selengkapnya tentang AWS CloudFormation

Untuk mempelajari selengkapnya tentang AWS CloudFormation, lihat sumber daya berikut:

- AWS CloudFormation
- AWS CloudFormationPanduan Pengguna
- AWS CloudFormationReferensi API
- AWS CloudFormationPanduan Pengguna Baris Perintah

Riwayat dokumen untuk Panduan AWS Audit Manager Pengguna

Tabel berikut menjelaskan perubahan penting dalam setiap rilis Panduan AWS Audit Manager Pengguna mulai 8 Desember 2020, dan seterusnya.

Perubahan	Deskripsi	Tanggal
Kerangka kerja baru yang didukung: PCI DSS V4.0	Kerangka kerja prebuilt baru sekarang tersedia diAWS Audit Manager. Untuk informasi lebih lanjut, lihat PCI DSS V4.0.	Desember 19, 2023
Support untuk panggilan AWS API tambahan	Sekarang Anda dapat menggunakan panggilan AWS API tambahan sebagai sumber data untuk kontrol kustom Anda di Audit Manager. Untuk informasi selengkapnya, lihat Panggilan API yang didukung untuk sumber data kontrol kustom.	Desember 7, 2023
Kebijakan AWS terkelola yang diperbarui	AWS Audit Managertelah memperbarui AWSAuditManagerServiceRolePolicy. Untuk informasi selengkapnya, lihat kebijakan AWS terkelola untuk AWS Audit Manager.	Desember 6, 2023
Support untuk temuan kontrol AWS Security Hub konsolidasi	Audit Manager sekarang mendukung kontrol terkonsolidasi diAWS Security Hub. Untuk informasi selengkapnya, lihat AWS Security Hubkontro	16 November 2023

	l yang didukung oleh AWS Audit Manager.	
Integrasi dengan MetricStream	Anda sekarang dapat menelan bukti dari Audit Manager ke dalam MetricStream. Untuk informasi selengkapnya, lihat Integrasi dengan produk GRC pihak ketiga.	14 November 2023
Kerangka kerja baru yang didukung: AWS praktik terbaik AI generatif	Kerangka kerja prebuilt baru sekarang tersedia diAWS Audit Manager. Untuk informasi selengkapnya, lihat kerangka kerja praktik terbaik AI AWS generatif v1.	8 November 2023
Kebijakan AWS terkelola yang diperbarui	AWS Audit Managertelah memperbarui AWSAuditManagerServiceRolePolicy. Untuk informasi selengkapnya, lihat kebijakan AWS terkelola untuk AWS Audit Manager.	6 November 2023
Integrasi dengan Amazon EventBridge	Anda sekarang dapat memantau peristiwa yang terjadi AWS Audit Manager dan menggunakan peristiwa ini sebagai bagian dari arsitektur berbasis acara Anda. Untuk informasi selengkapnya, lihat Memantau AWS Audit Manager dengan Amazon EventBridge.	Agustus 18, 2023

Support untuk penilaian risiko dan opsi bukti manual baru	Sekarang Anda dapat menggunakan alur kerja pembuatan kontrol kustom untuk mendukung penilaian risiko. Kontrol sekarang dapat mewakili pertanyaan penilaian risiko, dan Anda dapat memberikan jawaban dengan mengunggah file atau memasukkan teks sebagai bukti manual. Untuk informasi selengkapnya, lihat Membuat kontrol kustom dan Menambahkan bukti manual.	12 Juni 2023
Support untuk ekspor CSV	Anda sekarang dapat mengekspor hasil pencarian pencari bukti Anda dalam format CSV. Untuk informasi selengkapnya, lihat Mengekspor hasil penelusuran Anda.	9 Juni 2023
Kerangka kerja baru yang didukung: Panduan Keamanan Informasi Pusat Keamanan Cyber Australia (ACSC)	Kerangka kerja prebuilt baru sekarang tersedia diAWS Audit Manager. Untuk informasi lebih lanjut, lihat Australian Cyber Security Centre (ACSC) Information Security Manual.	24 Maret 2023

Laporan penilaian yang lebih baik	Kami melakukan perbaikan pada format dan isi laporan penilaian Audit Manager. Untuk informasi selengkapnya tentang cara menavigasi dan memahami laporan penilaian, lihat Laporan penilaian.	Maret 23, 2023
Support untuk panggilan API paginasi	AWS Audit Managersekarang mendukung panggilan API paginasi sebagai sumber data untuk pengumpulan bukti. Untuk informasi selengkapnya, lihat Panggilan API Paginasi.	8 Maret 2023
Kerangka kerja baru yang didukung: HIPAA Final Omnibus Security Rule 2013	Kerangka kerja prebuilt baru sekarang tersedia diAWS Audit Manager. Untuk informasi lebih lanjut, lihat HIPAA Final Omnibus Security Rule 2013. Untuk tujuan diferensiasi, kerangka kerja HIPAA yang sudah ada sebelumnya (sebelumnya bernama HIPAA di perpustakaan kerangka kerja) sekarang bernama HIPAA Security Rule 2003.	8 Maret 2023

Support untuk panggilan AWS API tambahan	Sekarang Anda dapat menggunakan sembilan panggilan AWS API tambahan sebagai sumber data untuk kontrol kustom Anda di Audit Manager. Untuk informasi selengkapnya, lihat Panggilan API yang didukung untuk sumber data kontrol kustom.	3 Maret 2023
Panduan yang diperbarui untuk menyelaraskan dengan praktik terbaik IAM	Panduan yang diperbarui untuk menyelaraskan dengan praktik terbaik IAM. Untuk informasi selengkapnya, lihat Praktik terbaik keamanan di IAM.	Januari 6, 2023
Pengaturan retensi data baru	Sekarang Anda dapat menentukan apakah Anda ingin menghapus semua data saat menonaktifkan Audit Manager. Untuk informasi selengkapnya, lihat Menonaktifkan AWS Audit Manager dan Menghapus data Audit Manager.	Januari 6, 2023
Support untuk pencari bukti	Anda sekarang dapat menggunakan pencari bukti untuk melakukan kueri penelusuran pada data bukti Anda. Untuk informasi selengkapnya, lihat Pencari bukti.	18 November 2022

Kerangka kerja baru yang didukung: Australian Cyber Security Centre (ACSC) Essential Eight	Kerangka kerja prebuilt baru sekarang tersedia diAWS Audit Manager. Untuk informasi lebih lanjut, lihat Australian Cyber Security Centre (ACSC) Essential Eight.	Agustus 24, 2022
Kebijakan AWS terkelola yang diperbarui	AWS Audit Managertelah memperbarui AWSAuditManagerServiceRolePolicy. Untuk informasi selengkapnya, lihat kebijakan AWS terkelola untuk AWS Audit Manager.	Juli 7, 2022
Kebijakan AWS terkelola yang diperbarui	AWS Audit Managertelah memperbarui AWSAuditManagerServiceRolePolicy. Untuk informasi selengkapnya, lihat kebijakan AWS terkelola untuk AWS Audit Manager.	Mei 20, 2022
Kerangka kerja baru yang didukung: Canadian Centre for Cyber Security Medium Cloud Control Profile	Kerangka kerja prebuilt baru sekarang tersedia diAWS Audit Manager. Untuk informasi selengkapnya, lihat Canadian Centre for Cyber Security Medium Cloud Control Profile.	6 Mei 2022
Kebijakan AWS terkelola yang diperbarui	AWS Audit Managertelah memperbarui AWSAuditManagerAdministratorAccesskebijakan. Untuk informasi selengkapnya, lihat kebijakan AWS terkelola untuk AWS Audit Manager.	April 29, 2022

Support untuk aturan AWS Config terkelola tambahan	Sekarang Anda dapat menggunakan 91 aturan AWS Config terkelola tambahan sebagai sumber data untuk kontrol kustom Anda di Audit Manager. Untuk informasi selengkapnya, lihat Menggunakan aturan AWS Config terkelola dengan AWS Audit Manager.	27 April 2022
Support untuk aturan AWS Config kustom	Sekarang Anda dapat menggunakan aturan AWS Config kustom sebagai sumber data untuk kontrol kustom Anda di Audit Manager. Untuk informasi selengkapnya, lihat Menggunakan aturan AWS Config khusus dengan AWS Audit Manager.	27 April 2022
Kerangka kerja baru yang didukung: ISO/IEC 27001:2013 Lampiran A	Kerangka kerja prebuilt baru sekarang tersedia diAWS Audit Manager. Untuk informasi lebih lanjut, lihat ISO/IEC 27001: 2013 Lampiran A.	7 April 2022
Kebijakan AWS terkelola yang diperbarui	AWS Audit Managertelah memperbarui AWSAuditManagerServiceRolePolicy. Untuk informasi selengkapnya, lihat kebijakan AWS terkelola untuk AWS Audit Manager.	16 Maret 2022

Kerangka kerja baru yang didukung: CIS Benchmark untuk CIS Amazon Web Services Foundations Benchmark v1.4	Dua kerangka kerja prebuilt baru sekarang tersedia diAWS Audit Manager: CIS Benchmark untuk CIS Amazon Web Services Foundations Benchmark v1.4, Level 1, dan CIS Benchmark untuk CIS Amazon Web Services Foundations Benchmark v1.4, Level 1 dan 2. Untuk informasi lebih lanjut, lihat CIS Benchmark untuk CIS AWS Audit Manager Foundations Benchmark v1.4.0.	Maret 2, 2022
Kerangka kerja baru yang didukung: Kontrol CIS v8 IG1	Kerangka kerja prebuilt baru sekarang tersedia diAWS Audit Manager. Untuk informasi lebih lanjut, lihat Kontrol CIS v8 IG1.	Maret 2, 2022
AWS Audit Managerdasbor	Sekarang Anda dapat menggunakan dasbor Audit Manager untuk memantau penilaian aktif Anda dan mengidentifikasi bukti yang tidak sesuai dengan cepat. Untuk informasi selengkapnya, lihat Menggunakan dasbor Audit Manager.	18 November 2021

Berbagi kerangka kustom	Anda sekarang dapat membagikan kerangka kerja Audit Manager kustom Anda dengan yang lainAkun AWS, atau mereplikasi mereka ke yang lain Wilayah AWS di bawah akun Anda sendiri. Untuk informasi selengkapnya, lihat Berbagi kerangka kustom.	Oktober 22, 2021
Contoh AWS Audit Manager kontrol baru	Sekarang Anda dapat meninjau contoh kontrol dan mempelajari cara Audit Manager membantu mewujudkan AWS lingkungan Anda sesuai dengan persyarat annya. Untuk informasi selengkapnya, lihat Contoh AWS Audit Manager kontrol.	September 21, 2021
Kerangka kerja baru yang didukung: Gramm-Leach-Bliley Act (GLBA)	Kerangka kerja prebuilt baru sekarang tersedia diAWS Audit Manager. Untuk informasi lebih lanjut, lihat Gramm-Leach-Bliley Act (GLBA).	2 September 2021
Bab pemecahan masalah baru	Bab pemecahan masalah baru sekarang tersedia. Untuk informasi selengkapnya, lihat Pemecahan Masalah di. AWS Audit Manager	23 Agustus 2021

Bab delegasi baru dan tutorial	Kami memperluas dokumentasi delegasi kami ke babak baru. Untuk informasi selengkapnya, lihat Delegasi di AWS Audit Manager. Kami juga menambahkan tutorial baru yang ditujukan untuk delegasi yang meninjau set kontrol untuk pertama kalinya. AWS Audit Manager Untuk informasi selengkapnya, lihat Tutorial untuk Delegasi: Meninjau set kontrol.	25 Juni 2021
Kerangka kerja baru yang didukung: NIST SP 800-171 Rev. 2	Kerangka kerja prebuilt baru sekarang tersedia diAWS Audit Manager. Untuk informasi lebih lanjut, lihat NIST SP 800-171 Rev. 2.	17 Juni 2021
Laporan penilaian yang lebih baik	Kami melakukan perbaikan pada format dan isi laporan AWS Audit Manager penilaian. Untuk informasi selengkapnya tentang cara menavigasi dan memahami laporan penilaian baru, lihat Laporan penilaian.	8 Juni 2021
Halaman kebijakan AWS terkelola baru	AWS Audit Managertelah mulai melacak perubahan untuk kebijakan yang dikelola. Untuk informasi selengkapnya, lihat kebijakan terkelola AWS untuk AWS Audit Manager.	6 Mei 2021

Kerangka kerja baru yang didukung: NIST Cybersecurity Framework versi 1.1	Kerangka kerja prebuilt baru sekarang tersedia diAWS Audit Manager. Untuk informasi selengkapnya, lihat NIST Cybersecurity Framework versi 1.1.	5 Mei 2021
Kerangka kerja baru yang didukung: AWS Well-Arch itected	Kerangka kerja prebuilt baru sekarang tersedia diAWS Audit Manager. Untuk informasi lebih lanjut, lihat AWSWell-Architected.	5 Mei 2021
Kerangka kerja baru yang didukung: AWS Praktik Terbaik Keamanan Dasar	Kerangka kerja prebuilt baru sekarang tersedia diAWS Audit Manager. Untuk informasi selengkapnya, lihat Praktik Terbaik Keamanan AWS Dasar.	5 Mei 2021
Kerangka kerja baru yang didukung: GxP EU Annex 11	Kerangka kerja prebuilt baru sekarang tersedia diAWS Audit Manager. Untuk informasi lebih lanjut, lihat GxP EU Annex 11.	28 April 2021
Kerangka kerja baru yang didukung: NIST 800-53 (Rev. 5) Rendah Sedang-Tinggi	Kerangka kerja prebuilt baru sekarang tersedia diAWS Audit Manager. Untuk informasi lebih lanjut, lihat NIST 800-53 (Rev. 5) Rendah Sedang-Tinggi.	25 Maret 2021

Kerangka kerja baru yang didukung: CIS Benchmark untuk CIS Foundations Benchmark v1.3 AWS Audit Manager	Dua kerangka kerja prebuilt baru sekarang tersedia diAWS Audit Manager: CIS Benchmark untuk CIS AWS Audit Manager Foundations Benchmark v1.3.0, Level 1, dan CIS Benchmark untuk CIS Foundations Benchmark v1.3.0, Level 1 dan 2. AWS Audit Manager Untuk informasi lebih lanjut, lihat CIS Benchmark untuk CIS AWS Audit Manager Foundations Benchmark v1.3.0.	22 Maret 2021
Rilis awal	Rilis awal Panduan AWS Audit Manager Pengguna dan Referensi API.	8 Desember 2020

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.