



Panduan Pengguna

# Amazon Macie



# Amazon Macie: Panduan Pengguna

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

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

---

# Table of Contents

Apa itu Amazon Macie? .....	1
Fitur Amazon Macie .....	2
Mengakses Amazon Macie .....	5
Harga untuk Amazon Macie .....	6
Layanan terkait .....	7
Memulai .....	8
Sebelum Anda memulai .....	8
Langkah 1: Aktifkan Amazon Macie .....	8
Langkah 2: Konfigurasi repositori untuk hasil penemuan data sensitif .....	9
Langkah 3: Jelajahi temuan sampel .....	10
Langkah 4: Buat pekerjaan untuk menemukan data sensitif .....	11
Langkah 5: Tinjau temuan Anda .....	13
Konsep dan terminologi .....	14
akun .....	14
akun administrator .....	14
izinkan daftar .....	15
penemuan data sensitif otomatis .....	15
AWSFormat Pencarian Keamanan (ASFF) .....	15
byte atau ukuran yang dapat diklasifikasikan .....	16
objek yang dapat diklasifikasikan .....	16
pengidentifikasi data kustom .....	16
aturan filter .....	17
temuan .....	17
menemukan acara .....	17
pekerjaan .....	18
pengidentifikasi data terkelola .....	18
akun anggota .....	18
organisasi .....	19
penemuan kebijakan .....	19
temuan sampel .....	19
penemuan data sensitif .....	19
pekerjaan penemuan data sensitif .....	20
Hasil Penemuan Data Sensitif .....	20
akun mandiri .....	21

temuan yang ditekan .....	21
aturan penindasan .....	21
byte atau ukuran yang tidak dapat diklasifikasikan .....	21
objek yang tidak dapat diklasifikasikan .....	22
Memantau keamanan dan privasi data .....	23
Cara Macie memantau keamanan data Amazon S3 .....	24
Komponen kunci .....	25
Penyegaran data .....	28
Pertimbangan tambahan .....	29
Menilai postur keamanan Amazon S3 Anda .....	31
Menampilkan dasbor .....	32
Memahami komponen dasbor .....	32
Memahami statistik keamanan data di dasbor .....	37
Menganalisis postur keamanan Amazon S3 Anda .....	40
Meninjau inventaris bucket S3 Anda .....	41
Memfilter inventaris bucket S3 Anda .....	53
Mengizinkan Macie untuk mengakses bucket S3 dan objek .....	66
Menemukan data sensitif .....	70
Menggunakan pengidentifikasi data terkelola .....	72
Persyaratan kata kunci .....	73
Referensi cepat berdasarkan tipe data sensitif .....	75
Referensi terperinci berdasarkan kategori data sensitif .....	87
Membangun pengidentifikasi data kustom .....	127
Mendefinisikan kriteria deteksi .....	127
Mendefinisikan pengaturan keparahan .....	129
Membuat pengidentifikasi data khusus .....	131
Dukungan Regex .....	133
Mendefinisikan pengecualian data sensitif dengan daftar izinkan .....	134
Izinkan opsi dan persyaratan daftar .....	136
Membuat dan mengelola daftar izinkan .....	148
Melakukan penemuan data sensitif otomatis .....	166
Cara kerja penemuan otomatis .....	167
Mengonfigurasi penemuan otomatis untuk akun Anda .....	175
Mengelola penemuan otomatis untuk bucket S3 individual .....	184
Menilai cakupan penemuan otomatis .....	187
Meninjau statistik dan hasil penemuan otomatis .....	200

Penilaian sensitivitas untuk bucket S3 .....	227
Pengaturan penemuan otomatis default .....	234
Menjalankan tugas penemuan data sensitif .....	245
Opsi ruang lingkup untuk tugas .....	247
Membuat tugas .....	260
Meninjau statistik dan hasil tugas .....	272
Tugas pemantauan .....	277
Mengelola tugas .....	295
Biaya tugas prakiraan dan pemantauan .....	305
Pengidentifikasi data terkelola direkomendasikan untuk pekerjaan .....	308
Menganalisis objek S3 terenkripsi .....	312
Opsi enkripsi untuk objek S3 .....	313
Mengizinkan Macie menggunakan pelanggan yang dikelola AWS KMS key .....	315
Menyimpan dan mempertahankan hasil penemuan data sensitif .....	321
Gambaran Umum .....	323
Langkah 1: Verifikasi izin Anda .....	324
Langkah 2: Konfigurasi AWS KMS key .....	326
Langkah 3: Pilih ember S3 .....	329
Kelas dan format penyimpanan yang didukung .....	338
Kelas penyimpanan yang didukung .....	339
Format file dan penyimpanan yang didukung .....	340
Menganalisis temuan .....	342
Tipe temuan .....	344
Jenis temuan kebijakan .....	345
Jenis temuan data sensitif .....	348
Bekerja dengan temuan sampel .....	349
Membuat temuan sampel .....	350
Meninjau temuan sampel .....	351
Menekan temuan sampel .....	353
Meninjau temuan .....	353
Memfilter temuan .....	357
Hal mendasar filter .....	358
Membuat dan menerapkan filter .....	367
Membuat dan mengelola aturan filter .....	377
Bidang untuk memfilter temuan .....	385
Menyelidiki data sensitif dengan temuan .....	421

Menemukan data sensitif .....	422
Mengambil sampel data sensitif .....	425
Skema untuk lokasi data sensitif .....	468
Menekan temuan .....	479
Membuat aturan penekanan .....	481
Meninjau temuan yang ditekan .....	484
Mengubah aturan penekanan .....	484
Menghapus aturan penekanan .....	487
Penilaian tingkat kepelikan untuk temuan .....	488
Penilaian tingkat kepelikan untuk temuan kebijakan .....	490
Penilaian tingkat kepelikan untuk temuan data sensitif .....	490
Pemantauan dan pemrosesan temuan .....	497
Mengonfigurasi pengaturan publikasi untuk temuan .....	498
Memilih tujuan publikasi .....	499
Menentukan frekuensi publikasi .....	500
Mengubah frekuensi publikasi .....	501
EventBridgeIntegrasi .....	502
Bekerja dengan EventBridge .....	503
Membuat EventBridge aturan untuk temuan .....	503
Integrasi Security Hub .....	508
Bagaimana Macie memublikasikan temuan ke Security Hub .....	509
Contoh temuan Macie di Security Hub .....	514
Mengaktifkan dan mengonfigurasi integrasi Security Hub .....	519
Menghentikan publikasi temuan ke Security Hub .....	520
Integrasi Pemberitahuan Pengguna .....	520
Bekerja dengan Notifikasi Pengguna AWS .....	521
Mengaktifkan dan mengonfigurasi pemberitahuan untuk temuan .....	522
Memetakan bidang notifikasi untuk menemukan bidang .....	524
Mengubah pengaturan pemberitahuan untuk temuan .....	528
Menonaktifkan notifikasi untuk temuan .....	528
EventBridge skema acara untuk temuan .....	528
Skema peristiwa .....	529
Contoh peristiwa untuk temuan kebijakan .....	530
Contoh peristiwa untuk temuan data sensitif .....	534
Prakiraan dan pemantauan biaya .....	541
Memahami cara prakiraan biaya penggunaan dihitung .....	541

Meninjau perkiraan biaya penggunaan .....	545
Meninjau perkiraan biaya penggunaan di konsol .....	545
Melakukan kueri pada perkiraan biaya penggunaan dengan API .....	546
Berpartisipasi dalam uji coba gratis .....	551
Mengelola beberapa akun .....	555
Hubungan akun administrator dan anggota .....	556
Mengelola akun dengan AWS Organizations .....	561
Pertimbangan dan rekomendasi .....	562
Mengintegrasikan dan mengkonfigurasi organisasi .....	565
Meninjau akun organisasi .....	575
Mengelola akun anggota .....	579
Menunjuk akun administrator yang berbeda .....	587
Menonaktifkan integrasi dengan AWS Organizations .....	590
Mengelola akun dengan undangan .....	591
Pertimbangan dan rekomendasi .....	593
Membuat dan mengelola organisasi .....	596
Meninjau akun organisasi .....	608
Menunjuk akun administrator yang berbeda .....	613
Mengelola keanggotaan Anda di organisasi .....	614
Keamanan .....	620
Perlindungan data .....	621
Enkripsi at rest .....	622
Enkripsi dalam transit .....	622
Identity and Access Management .....	622
Audiens .....	623
Mengautentikasi dengan identitas .....	623
Mengelola kebijakan menggunakan akses .....	627
Bagaimana Macie bekerja dengan IAM .....	630
Contoh kebijakan berbasis identitas .....	640
Peran terkait layanan .....	649
Kebijakan yang dikelola AWS .....	653
Pemecahan Masalah .....	660
Pencatatan dan pemantauan .....	661
Validasi kepatuhan .....	661
Ketahanan .....	662
Keamanan infrastruktur .....	663

---

Titik akhir VPC (AWS PrivateLink) .....	663
Pertimbangan untuk titik akhir VPC Macie .....	664
Membuat titik akhir VPC antarmuka untuk Macie .....	665
Mencatat panggilan API .....	666
Informasi Macie di CloudTrail .....	666
Memahami entri berkas log Macie .....	667
Penandaan sumber daya .....	672
Dasar-dasar penandaan .....	672
Menggunakan tag dalam kebijakan IAM .....	674
Menambahkan tag ke sumber daya .....	675
Meninjau tag untuk sumber daya .....	678
Mengedit tag untuk sumber daya .....	681
Menghapus tag dari sumber daya .....	684
Membuat sumber daya dengan AWS CloudFormation .....	687
Macie dan template AWS CloudFormation .....	687
Pelajari selengkapnya tentang AWS CloudFormation .....	688
Menangguhkan atau menonaktifkan Macie .....	689
Menangguhkan Macie .....	689
Menonaktifkan Macie .....	690
Kuota Macie .....	692
Riwayat dokumen .....	696
.....	dccxxi



# Apa itu Amazon Macie?

Amazon Macie adalah layanan keamanan data yang menemukan data sensitif dengan menggunakan pembelajaran mesin dan pencocokan pola, memberikan visibilitas terhadap risiko keamanan data, dan memungkinkan perlindungan otomatis terhadap risiko tersebut.

Untuk membantu Anda mengelola postur keamanan data estate Amazon Simple Storage Service (Amazon S3) organisasi Anda, Macie menyediakan inventaris bucket S3 Anda, dan secara otomatis mengevaluasi dan memantau bucket untuk keamanan dan kontrol akses. Jika Macie mendeteksi potensi masalah dengan keamanan atau privasi data Anda, seperti bucket yang dapat diakses publik, Macie menghasilkan temuan bagi Anda untuk meninjau dan memperbaiki seperlunya.

Macie juga mengotomatiskan penemuan dan pelaporan data sensitif untuk memberi Anda pemahaman yang lebih baik tentang data yang disimpan organisasi Anda di Amazon S3. Untuk mendeteksi data sensitif, Anda dapat menggunakan kriteria dan teknik bawaan yang disediakan Macie, kriteria khusus yang Anda tentukan, atau kombinasi keduanya. Jika Macie mendeteksi data sensitif dalam objek S3, Macie menghasilkan temuan untuk memberi tahu Anda tentang data sensitif yang ditemukan Macie.

Selain temuan, Macie menyediakan statistik dan data lain yang menawarkan wawasan tentang postur keamanan data Amazon S3 Anda, dan di mana data sensitif mungkin berada di data estate Anda. Statistik dan data dapat memandu keputusan Anda untuk melakukan investigasi lebih dalam terhadap bucket dan objek S3 tertentu. Anda dapat meninjau dan menganalisis temuan, statistik, dan data lainnya dengan menggunakan konsol Amazon Macie atau Amazon Macie API. Anda juga dapat memanfaatkan integrasi Macie dengan Amazon EventBridge dan AWS Security Hub untuk memantau, memproses, dan memulihkan temuan dengan menggunakan layanan, aplikasi, dan sistem lain.

## Topik

- [Fitur Amazon Macie](#)
- [Mengakses Amazon Macie](#)
- [Harga untuk Amazon Macie](#)
- [Layanan terkait](#)

## Fitur Amazon Macie

Berikut adalah beberapa cara utama Amazon Macie dapat membantu Anda menemukan, memantau, dan melindungi data sensitif Anda di Amazon S3.

### Mengotomatiskan penemuan data sensitif

Dengan Macie, Anda dapat mengotomatiskan penemuan dan pelaporan data sensitif dengan dua cara: dengan mengonfigurasi Macie [melakukan penemuan data sensitif otomatis](#), dan oleh [membuat dan menjalankan pekerjaan penemuan data sensitif](#). Jika Macie mendeteksi data sensitif dalam objek S3, Macie akan menciptakan temuan data sensitif untuk Anda. Temuan ini memberikan laporan detail tentang data sensitif yang Macie temukan.

Penemuan data sensitif otomatis memberikan visibilitas luas ke tempat data sensitif berada di kawasan data Amazon S3 Anda. Dengan opsi ini, Macie terus mengevaluasi inventaris bucket S3 Anda dan menggunakan teknik pengambilan sampel untuk mengidentifikasi dan memilih objek S3 representatif dari bucket Anda. Macie kemudian mengambil dan menganalisis objek yang dipilih, memeriksa mereka untuk data sensitif.

Pekerjaan penemuan data sensitif memberikan analisis yang lebih dalam dan lebih bertarget. Dengan opsi ini, Anda menentukan luas dan kedalaman analisis—bucket S3 untuk dianalisis, kedalaman pengambilan sampel, dan kriteria khusus yang berasal dari properti objek S3. Anda juga dapat mengonfigurasi pekerjaan untuk dijalankan hanya sekali untuk analisis dan penilaian sesuai permintaan, atau secara berulang untuk analisis, penilaian, dan pemantauan berkala.

Kedua opsi tersebut dapat membantu Anda membangun dan mempertahankan tampilan komprehensif data yang disimpan organisasi Anda di Amazon S3 dan risiko keamanan atau kepatuhan apa pun untuk data tersebut.

### Temukan berbagai tipe data sensitif

Untuk menemukan data sensitif dengan Macie, Anda dapat menggunakan kriteria dan teknik bawaan, seperti pembelajaran mesin dan pencocokan pola, untuk menganalisis objek dalam bucket S3. Kriteria dan teknik ini, disebut sebagai [pengidentifikasi data terkelola](#), dapat mendeteksi daftar tipe data sensitif yang besar dan berkembang untuk banyak negara dan wilayah, termasuk beberapa jenis informasi identitas pribadi (PII), informasi keuangan, dan data kredensial.

Anda juga dapat menggunakan [pengidentifikasi data kustom](#). Pengenal data kustom adalah sekumpulan kriteria yang Anda tetapkan untuk mendeteksi data sensitif—ekspresi reguler (regex)

yang mendefinisikan pola teks untuk mencocokkan dan, opsional, urutan karakter dan aturan kedekatan yang menyempurnakan hasil. Dengan jenis pengenalan ini, Anda dapat mendeteksi data sensitif yang mencerminkan skenario tertentu, kekayaan intelektual, atau data kepemilikan Anda. Anda dapat melengkapi pengidentifikasi data terkelola yang disediakan Macie.

Untuk menyempurnakan analisis, Anda juga dapat menggunakan [izinkan daftar](#). Iizinkan daftar menentukan pola teks dan teks tertentu yang ingin Macie abaikan di objek S3. Ini biasanya merupakan pengecualian data sensitif untuk skenario atau lingkungan tertentu Anda—misalnya, nama perwakilan publik untuk organisasi Anda, nomor telepon publik untuk organisasi Anda, atau data sampel yang digunakan organisasi Anda untuk pengujian.

## Mengevaluasi dan memantau data untuk keamanan dan kontrol akses

Saat Anda mengaktifkan Macie, Macie secara otomatis menghasilkan dan mulai memelihara inventaris lengkap bucket S3 Anda. Macie juga mulai mengevaluasi dan memantau ember untuk keamanan dan kontrol akses. Jika Macie mendeteksi potensi masalah dengan keamanan atau privasi bucket, Macie akan menciptakan [temuan kebijakan](#) untuk Anda.

Selain temuan spesifik, [adasbor](#) memberi Anda snapshot statistik agregat untuk data Amazon S3 Anda. Ini termasuk statistik untuk metrik utama seperti berapa banyak bucket Anda yang dapat diakses publik atau dibagikan dengan yang lain Akun AWS. Anda dapat menelusuri setiap statistik untuk meninjau data pendukung.

Macie juga menyediakan informasi rinci dan statistik untuk masing-masing bucket S3 dalam inventaris Anda. Data mencakup kerusakan akses publik bucket dan pengaturan enkripsi, serta ukuran dan jumlah objek yang dapat dianalisis Macie untuk mendeteksi data sensitif di bucket. Anda dapat [menelusuri inventaris](#), atau mengurutkan dan mem-filter inventaris menurut bidang-bidang tertentu. Bila Anda memilih bucket, panel akan menampilkan detail bucket.

## Meninjau dan menganalisis temuan

Di Macie, temuan adalah laporan terperinci tentang data sensitif yang dideteksi Macie dalam objek S3 atau potensi masalah dengan keamanan atau privasi bucket S3. Setiap temuan menyediakan tingkat kepelikan, informasi tentang sumber daya yang terpengaruh, dan detail tambahan, seperti kapan dan bagaimana Macie menemukan masalah.

Untuk [meninjau, menganalisis, dan mengelola temuan](#), Anda dapat menggunakan halaman Temuan pada konsol Amazon Macie. Halaman ini mencantumkan temuan Anda dan memberikan detail temuan individual. Halaman tersebut juga menyediakan beberapa pilihan untuk pengelompokan, pem-filteran, pemilahan, dan penekanan temuan. Anda juga dapat

menggunakan Amazon Macie API untuk kueri, mengambil, dan penekanan temuan. Jika Anda menggunakan API, Anda dapat mengirimkan data ke aplikasi, layanan, atau sistem lain untuk analisis yang lebih dalam, penyimpanan jangka panjang, atau pelaporan.

## Memantau dan memproses temuan dengan layanan dan sistem lain

Untuk mendukung integrasi dengan layanan dan sistem lain, Macie [menerbitkan temuan ke Amazon EventBridge](#) sebagai menemukan peristiwa. EventBridge adalah layanan bus acara tanpa server yang dapat merutekan data temuan ke target seperti AWS Lambda fungsi dan topik Amazon Simple Notification Service (Amazon SNS). Dengan EventBridge, Anda dapat memantau dan memproses temuan dalam waktu dekat sebagai bagian dari alur kerja keamanan dan kepatuhan yang ada.

Anda juga dapat mengonfigurasi Macie untuk [menerbitkan temuan ke AWS Security Hub](#). Security Hub adalah layanan yang memberikan pandangan menyeluruh tentang postur keamanan Anda di seluruh lingkungan AWS Anda dan membantu memeriksa lingkungan Anda terhadap standar industri keamanan dan praktik terbaik. Dengan Security Hub, Anda dapat dengan lebih mudah memantau dan memproses temuan Anda sebagai bagian dari analisis yang lebih luas mengenai postur keamanan organisasi Anda di AWS. Anda juga dapat mengumpulkan temuan dari beberapa Wilayah AWS, dan kemudian memantau dan memproses data temuan gabungan dari satu Wilayah.

## Kelola beberapa akun Macie secara terpusat

Jika Anda AWS lingkungan memiliki beberapa akun, Anda bisa [mengelola Macie secara terpusat](#) untuk akun di lingkungan Anda. Anda dapat melakukan ini dengan dua cara, dengan mengintegrasikan Macie AWS Organizations atau dengan mengirim dan menerima undangan keanggotaan di Macie.

Dalam konfigurasi multi-akun, administrator Macie yang ditunjuk dapat melakukan tugas tertentu dan mengakses pengaturan Macie, data, dan sumber daya tertentu untuk akun yang merupakan anggota organisasi yang sama. Tugas termasuk meninjau informasi tentang bucket S3 yang dimiliki oleh akun anggota, meninjau temuan kebijakan untuk bucket tersebut, dan memeriksa bucket untuk data sensitif. Jika akun tersebut terkait melalui AWS Organizations, administrator Macie juga dapat mengaktifkan Macie untuk akun anggota di organisasi.

## Mengembangkan dan mengelola sumber daya secara terprogram

Selain konsol Amazon Macie, Anda dapat berinteraksi dengan Macie menggunakan [API Amazon Macie API](#). Amazon Macie API memberi Anda akses terprogram yang komprehensif ke pengaturan, data, dan sumber daya akun Macie Anda.

Untuk berinteraksi dengan Macie secara terprogram, Anda dapat mengirim permintaan HTTPS langsung ke Macie atau menggunakan versi terbaru dari AWS CLI atau AWS SDK. AWS menyediakan alat dan SDK yang terdiri dari pustaka dan kode contoh untuk berbagai bahasa dan platform, seperti PowerShell, Java, Go, Python, C++, dan .NET.

## Mengakses Amazon Macie

Amazon Macie tersedia di sebagian besar Wilayah AWS. Untuk daftar Wilayah tempat Macie saat ini tersedia, lihat [Titik akhir dan kuota Amazon Macie](#) di dalam Referensi Umum AWS. Untuk informasi tentang pengelolaan Wilayah AWS untuk Akun AWS, lihat [Menentukan yang Wilayah AWS Akun Anda dapat menggunakan](#) di dalam AWS Account Management Panduan Referensi.

Di setiap Wilayah, Anda dapat bekerja dengan Macie dengan salah satu cara-cara berikut.

### AWS Management Console

AWS Management Console adalah antarmuka berbasis peramban yang dapat Anda gunakan untuk membuat dan mengelola sumber daya AWS. Sebagai bagian dari konsol itu, konsol Amazon Macie menyediakan akses ke akun, data, dan sumber daya Macie Anda. Anda dapat melakukan tugas Macie apa pun dengan menggunakan konsol Macie—meninjau statistik dan informasi lain tentang bucket S3 Anda, membuat dan menjalankan pekerjaan penemuan data sensitif, meninjau dan menganalisis temuan, dan banyak lagi.

### AWS CLI

Dengan alat baris perintah AWS, Anda dapat mengeluarkan perintah di baris perintah sistem Anda untuk melakukan tugas Macie dan tugas AWS. Menggunakan baris perintah dapat lebih cepat dan lebih nyaman dibandingkan konsol. Alat baris perintah juga berguna jika Anda ingin membangun skrip yang melakukan tugas.

AWS menyediakan dua set alat baris perintah: AWS Command Line Interface (AWS CLI) dan AWS Tools for PowerShell. Untuk informasi tentang menginstal dan menggunakan AWS CLI, lihat [Panduan Pengguna AWS Command Line Interface](#). Untuk informasi tentang menginstal dan menggunakan Alat untuk PowerShell, lihat [AWS Tools for PowerShell Panduan Pengguna](#).

### AWS SDK

AWS menyediakan SDK yang terdiri atas pustaka dan kode sampel untuk berbagai bahasa dan platform pemrograman, misalnya Java, Go, Python, C++, dan .NET. SDK menyediakan akses terprogram yang nyaman ke Macie dan lainnya Layanan AWS. SDK menangani tugas seperti

menandatangani permintaan secara kriptografis, mengelola kesalahan, dan mencoba kembali permintaan secara otomatis. Untuk informasi tentang menginstal dan menggunakan SDK AWS, lihat [Alat untuk Membangun di AWS](#).

## API REST Amazon Macie

Amazon Macie REST API memberi Anda akses terprogram yang komprehensif ke akun, data, dan sumber daya Macie Anda. Dengan API ini, Anda dapat mengirim permintaan HTTPS langsung ke Macie. Namun, tidak seperti alat baris perintah dan SDK AWS, penggunaan API ini memerlukan aplikasi Anda untuk menangani detail tingkat rendah seperti menghasilkan hash untuk menandatangani permintaan. Untuk informasi tentang API ini, lihat [Referensi API Amazon Macie](#).

## Harga untuk Amazon Macie

Seperti produk AWS lainnya, tidak ada kontrak atau komitmen minimum untuk menggunakan Amazon Macie.

Harga Macie didasarkan pada beberapa dimensi—mengevaluasi dan memantau bucket S3 untuk keamanan dan kontrol akses, memantau objek S3 untuk penemuan data sensitif otomatis, dan menganalisis objek S3 untuk menemukan dan melaporkan data sensitif dalam objek. Untuk informasi selengkapnya, lihat [Harga Amazon Macie](#).

Untuk membantu Anda memahami dan memprakiraan biaya penggunaan Macie, Macie menyediakan perkiraan biaya penggunaan untuk akun Anda. Anda bisa [meninjau perkiraan ini](#) di konsol Amazon Macie dan mengaksesnya dengan Amazon Macie API. Tergantung pada bagaimana Anda menggunakan layanan ini, Anda mungkin dikenakan biaya tambahan untuk menggunakan layanan AWS dalam kombinasi dengan fitur Macie tertentu, seperti mengambil data bucket dari Amazon S3 dan menggunakan pelanggan yang dikelola AWS KMS keys untuk mendekripsi objek untuk analisis.

Ketika Anda mengaktifkan Macie untuk pertama kalinya, Anda akan AWS secara otomatis terdaftar dalam uji coba gratis 30 hari Macie. Ini termasuk akun individual yang diaktifkan sebagai bagian dari organisasi di AWS Organizations. Selama uji coba gratis, tidak ada biaya untuk menggunakan Macie dalam hal yang berlaku Wilayah AWS untuk mengevaluasi dan memantau bucket S3 Anda untuk keamanan dan kontrol akses. Bergantung pada pengaturan akun Anda, uji coba gratis juga dapat mencakup melakukan penemuan data sensitif otomatis untuk data Amazon S3 Anda. Uji coba gratis tidak termasuk menjalankan pekerjaan penemuan data sensitif untuk menemukan dan melaporkan data sensitif di objek S3.

Untuk membantu Anda memahami dan memprakiraan biaya penggunaan Macie setelah uji coba gratis berakhir, Macie memberi Anda perkiraan biaya penggunaan berdasarkan penggunaan Macie selama uji coba. Data penggunaan Anda juga menunjukkan jumlah waktu yang tersisa sebelum uji coba gratis berakhir. Anda bisa [meninjau data ini](#) di konsol Amazon Macie dan mengaksesnya dengan Amazon Macie API.

## Layanan terkait

Untuk lebih mengamankan data, beban kerja, dan aplikasi Anda di AWS, pertimbangkan untuk menggunakan Layanan AWS dalam kombinasi dengan Amazon Macie.

### AWS Security Hub

AWS Security Hub memberi Anda pandangan komprehensif tentang status keamanan sumber daya AWS Anda dan membantu memeriksa lingkungan AWS Anda terhadap standar industri keamanan dan praktik terbaik. Hal ini dilakukan sebagian dengan mengonsumsi, menggabungkan, mengatur, dan memprioritaskan temuan keamanan Anda dari beberapa Layanan AWS (termasuk Macie) dan didukung AWS Produk Jaringan Mitra (APN). Security Hub membantu menganalisis tren keamanan Anda dan mengidentifikasi masalah keamanan prioritas tertinggi di lingkungan AWS.

Untuk mempelajari selengkapnya tentang Security Hub, lihat [Panduan Pengguna AWS Security Hub](#). Untuk mempelajari cara menggunakan Macie dan Security Hub secara bersamaan, lihat [Integrasi Amazon Macie dengan AWS Security Hub](#).

### Amazon GuardDuty

Amazon GuardDuty adalah layanan pemantauan keamanan yang menganalisis dan memproses jenis AWS log, seperti AWS CloudTrail log peristiwa data untuk Amazon S3 dan CloudTrail log acara manajemen. Aplikasi ini menggunakan umpan intelijen ancaman, seperti daftar alamat IP dan domain berbahaya, dan machine learning untuk mengidentifikasi aktivitas yang tidak terduga dan berpotensi tidak sah dan berbahaya dalam lingkungan AWS.

Untuk mempelajari lebih lanjut tentang GuardDuty, lihat [Amazon GuardDuty Panduan Pengguna](#).

Untuk mempelajari tentang layanan keamanan AWS tambahan, lihat [Keamanan, Identitas, dan Kepatuhan di AWS](#).

# Memulai dengan Amazon Macie

Tutorial ini memberikan pengantar untuk Amazon Macie. Anda akan belajar cara mengaktifkan Macie untuk Akun AWS. Anda juga akan mempelajari cara menilai postur keamanan Amazon Simple Storage Service (Amazon S3) dan mengonfigurasi pengaturan Macie kunci untuk menemukan dan melaporkan data sensitif di bucket S3 Anda.

## Tugas

- [Sebelum Anda memulai](#)
- [Langkah 1: Aktifkan Amazon Macie](#)
- [Langkah 2: Konfigurasi repositori untuk hasil penemuan data sensitif](#)
- [Langkah 3: Jelajahi temuan sampel](#)
- [Langkah 4: Buat pekerjaan untuk menemukan data sensitif](#)
- [Langkah 5: Tinjau temuan Anda](#)

## Sebelum Anda memulai

Saat Anda mendaftar ke Amazon Web Services (AWS), akun Anda secara otomatis mendaftar untuk semua Layanan AWS, termasuk Amazon Macie. Namun, untuk mengaktifkan dan menggunakan Macie, pertama-tama Anda harus menyiapkan izin yang memungkinkan Anda mengakses konsol Amazon Macie dan operasi API. Anda atau AWS administrator dapat melakukannya dengan menggunakan AWS Identity and Access Management (IAM) untuk melampirkan kebijakan AWS terkelola yang dinamai `AmazonMacieFullAccess` ke identitas IAM Anda. Untuk mempelajari selengkapnya, lihat [Kebijakan terkelola AWS untuk Amazon Macie](#).

## Langkah 1: Aktifkan Amazon Macie

Setelah mengatur izin yang diperlukan, Anda dapat mengaktifkan Amazon Macie untuk Akun AWS. Ikuti langkah-langkah ini untuk mengaktifkan Macie untuk akun Anda.

Untuk mengaktifkan Macie

1. [Buka konsol Amazon Macie di https://console.aws.amazon.com/macie/](https://console.aws.amazon.com/macie/).
2. Dengan menggunakan Wilayah AWS pemilih di sudut kanan atas halaman, pilih Wilayah di mana Anda ingin mengaktifkan dan menggunakan Macie.



3. Di halaman Amazon Macie, pilih Memulai.
4. (Opsional) Saat Anda mengaktifkan Macie, Macie secara otomatis membuat peran terkait layanan yang memberi Macie izin yang diperlukan untuk memanggil sumber daya lain Layanan AWS dan memantau sumber daya atas nama Anda. AWS Untuk meninjau kebijakan izin untuk peran ini, pilih Lihat izin peran di konsol. Untuk mempelajari selengkapnya tentang peran ini, lihat [Peran tertaut layanan untuk Amazon Macie](#).
5. Pilih Aktifkan Macie.

Dalam beberapa menit, Macie secara otomatis menghasilkan dan mulai memelihara inventaris lengkap bucket S3 Anda di Wilayah saat ini. Macie juga mulai mengevaluasi dan memantau ember untuk keamanan dan kontrol akses. Untuk mempelajari selengkapnya, lihat [Cara Macie memantau keamanan data Amazon S3](#).

Bergantung pada pengaturan akun Anda, Macie juga mulai melakukan penemuan data sensitif otomatis untuk bucket S3 Anda. Macie mulai terus-menerus mengidentifikasi, memilih, dan menganalisis objek S3 representatif di ember Anda, memeriksa objek untuk data sensitif. Seiring kemajuan analisis, Macie memberikan statistik dan hasil lain yang dapat Anda tinjau, biasanya dalam waktu 48 jam setelah mengaktifkan Macie untuk akun Anda. Anda dapat menyesuaikan analisis dengan mengonfigurasi pengaturan penemuan data sensitif otomatis untuk akun Anda. Untuk mempelajari selengkapnya, lihat [Cara kerja penemuan data sensitif otomatis](#).

Untuk meninjau statistik agregat, pilih Ringkasan di panel navigasi di konsol. Untuk meninjau detail tentang bucket S3 individual di inventaris Anda, pilih bucket S3 di panel navigasi. Untuk kemudian menampilkan detail ember, pilih ember. Panel detail menampilkan statistik dan informasi lain yang memberikan wawasan tentang keamanan, privasi, dan sensitivitas data bucket. Untuk mempelajari selengkapnya tentang detail ini, lihat [Meninjau inventaris bucket S3 Anda](#).

## Langkah 2: Konfigurasi repositori untuk hasil penemuan data sensitif

Dengan Amazon Macie, Anda dapat menemukan data sensitif di bucket S3 dengan dua cara: dengan mengonfigurasi Macie untuk melakukan penemuan data sensitif otomatis dan dengan menjalankan pekerjaan penemuan data sensitif. Pekerjaan penemuan data sensitif adalah pekerjaan yang Anda buat untuk menganalisis objek di bucket S3 untuk menentukan apakah objek tersebut berisi data sensitif.

Macie membuat catatan untuk setiap objek S3 yang dianalisis saat Anda menjalankan pekerjaan penemuan data sensitif atau melakukan penemuan data sensitif otomatis. Catatan-catatan ini, disebut sebagai hasil penemuan data sensitif, mencatat rincian tentang analisis objek individu. Macie juga menciptakan hasil penemuan data sensitif untuk objek yang tidak dapat dianalisis karena kesalahan atau masalah. Hasil penemuan data sensitif memberi Anda catatan analisis yang dapat membantu audit atau investigasi privasi dan perlindungan data.

Macie menyimpan hasil penemuan data sensitif Anda hanya selama 90 hari. Untuk mengakses hasil dan mengaktifkan penyimpanan dan retensi jangka panjang mereka, konfigurasi Macie untuk menyimpan hasilnya dalam bucket S3. Anda harus melakukan ini dalam waktu 30 hari setelah mengaktifkan Macie. Setelah Anda melakukan ini, bucket dapat berfungsi sebagai repositori jangka panjang definitif untuk semua hasil penemuan data sensitif Anda.

Untuk mempelajari cara mengkonfigurasi repositori ini, lihat [Menyimpan dan mempertahankan hasil penemuan data sensitif](#)

## Langkah 3: Jelajahi temuan sampel

Di Amazon Macie, temuan adalah laporan terperinci tentang potensi pelanggaran kebijakan yang dideteksi Macie untuk bucket S3 atau data sensitif yang dideteksi Macie di objek S3. Macie menyediakan dua kategori temuan, temuan kebijakan dan temuan data sensitif. Macie membuat temuan kebijakan ketika kebijakan atau pengaturan untuk bucket diubah dengan cara yang mengurangi keamanan atau privasi bucket dan objek bucket. Macie membuat temuan data sensitif ketika mendeteksi data sensitif dalam objek S3. Dalam setiap kategori, ada beberapa jenis temuan.

Untuk mengeksplorasi dan mempelajari tentang berbagai kategori dan jenis temuan yang disediakan Macie, secara opsional membuat dan meninjau temuan sampel. Temuan sampel menggunakan data contoh dan nilai placeholder untuk menunjukkan jenis informasi yang mungkin disertakan Macie dalam setiap jenis temuan.

Ikuti langkah-langkah ini untuk membuat dan meninjau temuan sampel.

Untuk membuat dan meninjau temuan sampel

1. [Buka konsol Amazon Macie di https://console.aws.amazon.com/macie/](https://console.aws.amazon.com/macie/).
2. Pada panel navigasi, silakan pilih Pengaturan.
3. Di bawah Temuan sampel, pilih Hasilkan temuan sampel. Macie menghasilkan satu sampel temuan untuk setiap jenis temuan yang didukung Macie.

4. Di panel navigasi, pilih Temuan. Halaman Temuan menampilkan temuan untuk akun Anda saat ini di Wilayah AWS. Ini termasuk temuan sampel yang Anda buat pada langkah sebelumnya.
5. Pada halaman Temuan, temukan temuan yang jenisnya dimulai dengan [SAMPEL].
6. Untuk meninjau detail temuan sampel tertentu, pilih temuannya. Panel detail menampilkan detail temuan.

Untuk mempelajari tentang setiap jenis temuan, lihat [Tipe temuan](#). Untuk mempelajari lebih lanjut tentang membuat dan meninjau temuan sampel, lihat [Bekerja dengan temuan sampel](#).

## Langkah 4: Buat pekerjaan untuk menemukan data sensitif

Untuk menemukan dan melaporkan data sensitif di bucket S3, Anda dapat menjalankan pekerjaan penemuan data sensitif. Pekerjaan penemuan data sensitif adalah pekerjaan yang Anda buat untuk menganalisis objek di bucket S3 untuk menentukan apakah objek tersebut berisi data sensitif. Tidak seperti penemuan data sensitif otomatis, Anda menentukan luas dan kedalaman analisis. Anda juga menentukan seberapa sering menjalankan pekerjaan—sekali atau secara berkala berdasarkan jadwal.

Ikuti langkah-langkah ini untuk membuat pekerjaan yang berjalan sekali, segera setelah Anda membuatnya, dan menggunakan pengaturan default. Untuk mempelajari cara membuat tugas yang berjalan secara berkala atau menggunakan pengaturan kustom, lihat [Membuat tugas penemuan data sensitif](#).

Untuk membuat tugas penemuan data sensitif

1. [Buka konsol Amazon Macie di https://console.aws.amazon.com/macie/](https://console.aws.amazon.com/macie/).
2. Di panel navigasi, pilih Tugas.
3. Pilih Buat tugas.
4. Untuk langkah Pilih bucket S3, pilih Pilih bucket tertentu. Kemudian, di tabel, pilih kotak centang untuk setiap bucket S3 yang ingin Anda analisis pekerjaan.

Tabel ini menyediakan inventaris lengkap bucket S3 Anda saat ini. Wilayah AWS Untuk menemukan bucket tertentu dengan lebih mudah, masukkan kriteria filter di kotak filter di atas tabel. Anda juga dapat mengurutkan tabel dengan memilih judul kolom dalam tabel.

5. Setelah selesai memilih bucket, pilih Selanjutnya.
6. Untuk langkah Review S3 bucket, tinjau dan verifikasi pilihan bucket Anda, lalu pilih Berikutnya.

7. Untuk langkah Perbaiki ruang lingkup, pilih Tugas satu kali, lalu pilih Selanjutnya.
8. Untuk langkah Pilih pengidentifikasi data terkelola, pilih Direkomendasikan. Secara opsional tinjau tabel pengidentifikasi data terkelola yang kami rekomendasikan untuk pekerjaan, lalu pilih Berikutnya.

Pengidentifikasi data terkelola adalah seperangkat kriteria dan teknik bawaan yang dirancang untuk mendeteksi jenis data sensitif tertentu — misalnya, nomor kartu kredit, kunci akses AWS rahasia, atau nomor paspor untuk negara atau wilayah tertentu. Untuk mempelajari selengkapnya, lihat [Menggunakan pengidentifikasi data terkelola](#).

9. Untuk langkah Pilih pengidentifikasi data kustom, pilih Selanjutnya.

Pengidentifikasi data kustom adalah sekumpulan kriteria yang Anda tentukan untuk mendeteksi data sensitif—ekspresi reguler (regex) yang mendefinisikan pola teks agar cocok dan, secara opsional, urutan karakter dan aturan kedekatan yang menyempurnakan hasil. Untuk mempelajari selengkapnya, lihat [Membangun pengidentifikasi data kustom](#).

10. Untuk langkah Pilih izinkan daftar, pilih Berikutnya.

Di Macie, daftar izinkan menentukan teks atau pola teks yang Anda ingin Macie abaikan saat memeriksa objek S3 untuk data sensitif. Ini biasanya pengecualian data sensitif untuk skenario atau lingkungan tertentu. Untuk mempelajari selengkapnya, lihat [Mendefinisikan pengecualian data sensitif dengan daftar izinkan](#).

11. Untuk langkah Masukkan pengaturan umum, masukkan nama dan, secara opsional, deskripsi pekerjaan. Kemudian pilih Selanjutnya.
12. Untuk langkah Tinjau dan buat, tinjau pengaturan konfigurasi tugas dan verifikasi bahwa mereka sudah benar.

Anda juga dapat meninjau total perkiraan biaya (dalam Dolar AS) untuk menjalankan tugas. Perkiraan tersebut dapat membantu Anda menentukan apakah akan menyesuaikan pengaturan pekerjaan sebelum Anda menyimpan pekerjaan. Untuk mempelajari selengkapnya, lihat [Memprakirakan biaya tugas penemuan data sensitif](#).

13. Ketika Anda selesai meninjau dan memverifikasi pengaturan tugas, pilih Kirim.

Macie segera mulai menjalankan tugas. Untuk mempelajari cara memantau pekerjaan, lihat [memeriksa status pekerjaan penemuan data sensitif](#).

## Langkah 5: Tinjau temuan Anda

Amazon Macie secara otomatis memantau bucket S3 Anda untuk keamanan dan kontrol akses, dan membuat temuan kebijakan untuk melaporkan potensi masalah dengan keamanan atau privasi bucket Anda. Jika Anda membuat dan menjalankan pekerjaan penemuan data sensitif atau mengonfigurasi Macie untuk melakukan penemuan data sensitif otomatis, Macie juga membuat temuan data sensitif untuk melaporkan data sensitif yang dideteksi di objek S3. Untuk mempelajari lebih lanjut tentang temuan, lihat [Menganalisis temuan](#).

Ikuti langkah-langkah ini untuk meninjau temuan Anda.

Untuk meninjau temuan Anda

1. [Buka konsol Amazon Macie di https://console.aws.amazon.com/macie/](https://console.aws.amazon.com/macie/).
2. Di panel navigasi, pilih Temuan. Halaman Temuan menampilkan temuan untuk akun Anda saat iniWilayah AWS.
3. (Opsional) Untuk memfilter temuan berdasarkan kriteria tertentu, masukkan kriteria di kotak filter di atas tabel.
4. Untuk meninjau detail temuan tertentu, pilih temuannya. Panel detail menampilkan detail temuan.

Untuk mempelajari lebih lanjut, termasuk cara mengelompokkan dan memfilter temuan, lihat [Meninjau temuan](#).

# Konsep dan terminologi Amazon Macie

Di Amazon Macie, kami membangun [AWSkonsep dan terminologi umum dan](#) menggunakan istilah tambahan ini.

## akun

Standar Akun AWS yang berisi AWS sumber daya Anda dan identitas yang dapat mengakses sumber daya tersebut.

Untuk menggunakan Macie, Anda masuk AWS dengan Akun AWS kredensial Anda, pilih Wilayah AWS di mana Anda ingin menggunakan Macie, dan kemudian mengaktifkan Macie untuk Anda di Wilayah itu. Akun AWS Untuk informasi selengkapnya, lihat [Memulai dengan Amazon Macie](#).

Ada tiga jenis akun di Macie:

- Akun administrator — Jenis akun ini mengelola akun Macie untuk suatu organisasi. Organisasi adalah seperangkat akun Macie yang terkait satu sama lain dan dikelola secara terpusat sebagai sekelompok akun terkait secara spesifik. Wilayah AWS
- Akun anggota — Jenis akun ini dikaitkan dengan dan dikelola oleh akun administrator Macie untuk suatu organisasi.
- Akun mandiri — Jenis akun ini bukan administrator atau akun anggota. Itu bukan bagian dari organisasi.

Anda dapat menambahkan akun Macie ke organisasi dengan dua cara: dengan mengintegrasikan Macie dengan AWS Organizations atau dengan mengirim dan menerima undangan keanggotaan Macie. Untuk informasi selengkapnya, lihat [Mengelola beberapa akun](#).

## akun administrator

Di Macie, akun yang mengelola akun Macie untuk suatu organisasi. Organisasi adalah seperangkat akun Macie yang terkait satu sama lain dan dikelola secara terpusat sebagai sekelompok akun terkait secara spesifik. Wilayah AWS

Pengguna akun administrator Macie memiliki akses ke data inventaris Amazon Simple Storage Service (Amazon S3), [temuan kebijakan](#), dan pengaturan serta sumber daya Macie tertentu untuk

semua akun di organisasinya. Mereka juga dapat melakukan [penemuan data sensitif otomatis](#) dan menjalankan [pekerjaan penemuan data sensitif](#) untuk mendeteksi data sensitif di bucket S3 yang dimiliki akun. Bergantung pada bagaimana akun ditetapkan sebagai akun administrator, mereka mungkin juga dapat melakukan tugas tambahan untuk akun lain di organisasi mereka.

Untuk informasi selengkapnya, lihat [Mengelola beberapa akun](#).

## izinkan daftar

Di Macie, daftar izinkan menentukan teks atau pola teks yang Anda ingin Macie abaikan saat memeriksa objek S3 untuk data sensitif.

Anda dapat membuat dua jenis daftar izinkan di Macie: file teks biasa yang mencantumkan kata-kata tertentu dan jenis urutan karakter lainnya untuk diabaikan, atau ekspresi reguler (regex) yang mendefinisikan pola teks untuk diabaikan. Jika objek berisi teks yang cocok dengan entri atau pola dalam daftar izin, Macie tidak melaporkan teks dalam [temuan data sensitif](#), statistik, dan jenis hasil lainnya, bahkan jika teks tersebut cocok dengan kriteria pengenalan data [terkelola atau pengidentifikasi data kustom](#).

Untuk informasi selengkapnya, lihat [Mendefinisikan pengecualian data sensitif dengan daftar izinkan](#).

## penemuan data sensitif otomatis

Serangkaian aktivitas analisis otomatis yang terus dilakukan Macie untuk mengidentifikasi dan memilih objek representatif dari bucket S3, dan memeriksa objek yang dipilih untuk data sensitif.

Seiring kemajuan analisis, Macie menghasilkan catatan data sensitif yang ditemukannya ([temuan data sensitif](#)) dan analisis yang dilakukannya ([hasil penemuan data sensitif](#)). Macie juga memperbarui statistik dan informasi lain yang diberikannya tentang data Amazon S3.

Untuk informasi selengkapnya, lihat [Melakukan penemuan data sensitif otomatis](#).

## AWSFormat Pencarian Keamanan (ASFF)

Format JSON standar untuk isi [temuan](#) yang dipublikasikan atau dihasilkan oleh. AWS Security Hub ASFF mencakup rincian tentang sumber masalah keamanan, sumber daya yang terpengaruh, dan status temuan.

Untuk informasi tentang ASFF, lihat [AWS Security Finding Format \(ASFF\)](#) di AWS Security Hub. Untuk informasi tentang mempublikasikan temuan Macie ke Security Hub, lihat [Integrasi Amazon Macie dengan AWS Security Hub](#).

## byte atau ukuran yang dapat diklasifikasikan

Dalam statistik bucket S3 yang disediakan Macie, ukuran penyimpanan total semua [objek yang dapat diklasifikasikan](#) dalam bucket S3.

Jika pembuatan versi diaktifkan untuk bucket, nilai ini didasarkan pada ukuran penyimpanan versi terbaru dari setiap objek yang dapat diklasifikasikan dalam bucket. Jika objek adalah file terkompresi, nilai ini tidak mencerminkan ukuran sebenarnya dari konten file setelah file didekompresi.

Untuk informasi selengkapnya, silakan lihat [Meninjau inventaris bucket S3 Anda](#) dan [Menilai postur keamanan Amazon S3 Anda](#).

## objek yang dapat diklasifikasikan

Objek S3 yang dapat dianalisis Macie untuk mendeteksi data sensitif.

Saat menghitung statistik bucket S3, Macie menentukan bahwa suatu objek dapat diklasifikasikan berdasarkan kelas penyimpanan objek dan ekstensi nama file. Objek dapat diklasifikasikan jika menggunakan kelas penyimpanan Amazon S3 yang didukung dan memiliki ekstensi nama file untuk file atau format penyimpanan yang didukung.

Untuk informasi selengkapnya, silakan lihat [Meninjau inventaris bucket S3 Anda](#) dan [Menilai postur keamanan Amazon S3 Anda](#).

Untuk penemuan data sensitif, Macie menentukan bahwa suatu objek dapat diklasifikasikan berdasarkan kelas penyimpanan objek, ekstensi nama file, dan konten. Sebuah objek dapat diklasifikasikan jika: ia menggunakan kelas penyimpanan Amazon S3 yang didukung, ia memiliki ekstensi nama file untuk file atau format penyimpanan yang didukung, dan Macie memverifikasi bahwa ia dapat mengekstrak dan menganalisis data dari objek.

Untuk informasi selengkapnya, silakan lihat [Menemukan data sensitif](#) dan [Prakiraan dan pemantauan biaya](#).

## pengidentifikasi data kustom

Satu set kriteria yang Anda tentukan untuk mendeteksi data sensitif.



Kriteria terdiri dari ekspresi reguler (regex) yang menentukan pola teks untuk dicocokkan dan, opsional, urutan karakter dan aturan jarak yang menyempurnakan hasil. Urutan karakter dapat berupa:

- Kata kunci, yaitu kata atau frasa yang harus berdekatan dengan teks yang cocok dengan regex, atau
- Abaikan kata-kata, yang merupakan kata atau frasa untuk dikecualikan dari hasil.

Selain kriteria deteksi, Anda dapat menentukan pengaturan tingkat keparahan khusus untuk [temuan data sensitif](#) yang dihasilkan oleh pengenal data kustom.

Untuk informasi selengkapnya, lihat [Membangun pengidentifikasi data kustom](#).

## aturan filter

Satu set kriteria filter berbasis atribut yang Anda buat dan simpan untuk menganalisis [temuan](#) di konsol Amazon Macie. Aturan filter dapat membantu Anda melakukan analisis konsisten terhadap temuan yang memiliki karakteristik spesifik, seperti semua temuan tingkat keparahan tinggi yang melaporkan jenis data sensitif tertentu.

Untuk informasi selengkapnya, lihat [Membuat dan mengelola aturan filter untuk temuan](#).

## temuan

Laporan terperinci tentang data sensitif yang ditemukan Macie di objek S3 atau potensi masalah dengan keamanan atau privasi bucket S3. Setiap temuan memberikan detail seperti peringkat keparahan, informasi tentang sumber daya yang terpengaruh, dan kapan Macie menemukan data atau masalah.

Macie menghasilkan dua kategori temuan: [temuan data sensitif](#), untuk data sensitif yang dideteksi Macie di objek S3, dan [temuan kebijakan](#), untuk masalah potensial yang dideteksi Macie dengan pengaturan keamanan dan kontrol akses untuk bucket S3. Dalam setiap kategori, ada jenis temuan tertentu.

Untuk informasi selengkapnya, lihat [Tipe temuan Amazon Macie](#).

## menemukan acara

EventBridge Acara Amazon yang berisi rincian [temuan data sensitif atau temuan kebijakan](#).

Macie secara otomatis menerbitkan temuan data sensitif dan temuan kebijakan ke Amazon EventBridge sebagai peristiwa. Peristiwa adalah objek JSON yang sesuai dengan EventBridge skema untuk acara. AWS Anda dapat menggunakan peristiwa ini untuk memantau, memproses, dan menindaklanjuti temuan dengan menggunakan aplikasi, layanan, dan sistem lain.

Untuk informasi selengkapnya, silakan lihat [Integrasi Amazon Macie dengan Amazon EventBridge](#) dan [Skema EventBridge acara Amazon untuk temuan Amazon Macie](#).

## pekerjaan

Lihat [pekerjaan penemuan data sensitif](#).

## pengidentifikasi data terkelola

Serangkaian kriteria dan teknik bawaan yang dirancang untuk mendeteksi jenis data sensitif tertentu. Contoh data sensitif termasuk nomor kartu kredit, kunci akses AWS rahasia, atau nomor paspor untuk negara atau wilayah tertentu. Pengidentifikasi ini dapat mendeteksi daftar tipe data sensitif yang besar dan terus bertambah untuk banyak negara dan wilayah.

Untuk informasi selengkapnya, lihat [Menggunakan pengidentifikasi data terkelola](#).

## akun anggota

Akun Macie yang dikelola oleh [akun administrator](#) Macie yang ditunjuk untuk organisasi. Organisasi adalah seperangkat akun Macie yang terkait satu sama lain dan dikelola secara terpusat sebagai sekelompok akun terkait secara spesifik. Wilayah AWS

Akun dapat menjadi akun anggota dengan dua cara: dengan mengintegrasikan Macie dengan organisasi akun di AWS Organizations atau dengan menerima undangan keanggotaan Macie.

Jika Anda memiliki akun anggota, administrator Macie Anda memiliki akses ke data inventaris Amazon S3, temuan [kebijakan](#), serta setelan dan sumber daya Macie tertentu untuk akun Anda. Administrator Anda juga dapat melakukan [penemuan data sensitif otomatis](#) dan menjalankan [pekerjaan penemuan data sensitif](#) untuk mendeteksi data sensitif di bucket S3 Anda. Mereka mungkin juga dapat melakukan tugas tambahan untuk akun Anda, tergantung pada bagaimana akun Anda menjadi akun anggota.

Untuk informasi selengkapnya, lihat [Mengelola beberapa akun](#).

## organisasi

Satu set akun Macie yang terkait satu sama lain dan dikelola secara terpusat sebagai sekelompok akun terkait secara spesifik. Wilayah AWS

Setiap organisasi terdiri dari [akun administrator](#) Macie yang ditunjuk dan satu atau lebih [akun anggota](#) terkait. Akun administrator dapat mengakses pengaturan, data, dan sumber daya Macie tertentu untuk akun anggota. Anda dapat membuat organisasi dengan dua cara: dengan mengintegrasikan Macie dengan AWS Organizations atau dengan mengirim dan menerima undangan keanggotaan di Macie.

Untuk informasi selengkapnya, lihat [Mengelola beberapa akun](#).

## penemuan kebijakan

Laporan terperinci tentang potensi pelanggaran kebijakan atau masalah dengan pengaturan keamanan dan kontrol akses untuk bucket S3. Rinciannya mencakup peringkat keparahan, informasi tentang sumber daya yang terpengaruh, dan kapan Macie menemukan masalahnya.

Macie menghasilkan temuan kebijakan ketika kebijakan atau pengaturan untuk bucket S3 diubah dengan cara yang mengurangi keamanan atau privasi bucket dan objek bucket. Macie menghasilkan temuan ini sebagai bagian dari aktivitas pemantauan yang sedang berlangsung untuk data Amazon S3 Anda. Macie dapat menghasilkan beberapa jenis temuan kebijakan.

Untuk informasi selengkapnya, silakan lihat [Tipe temuan Amazon Macie](#) dan [Memantau keamanan dan privasi data](#).

## temuan sampel

[Temuan](#) yang menggunakan contoh data dan nilai placeholder untuk menunjukkan jenis informasi yang mungkin berisi temuan.

Untuk informasi selengkapnya, lihat [Bekerja dengan temuan sampel](#).

## penemuan data sensitif

Laporan rinci data sensitif yang ditemukan Macie di objek S3. Rinciannya mencakup peringkat keparahan, informasi tentang sumber daya yang terpengaruh, jenis dan jumlah kejadian data sensitif yang ditemukan Macie, dan kapan Macie menemukan data sensitif.

Macie menghasilkan temuan data sensitif jika mendeteksi data sensitif di objek S3 yang dianalisis saat Anda menjalankan [pekerjaan penemuan data sensitif atau melakukan penemuan data sensitif otomatis](#). Macie dapat menghasilkan beberapa jenis temuan data sensitif.

Untuk informasi selengkapnya, silakan lihat [Tipe temuan Amazon Macie](#) dan [Menemukan data sensitif](#).

## pekerjaan penemuan data sensitif

Juga disebut sebagai pekerjaan, serangkaian tugas pemrosesan dan analisis otomatis yang dilakukan Macie untuk mendeteksi dan melaporkan data sensitif dalam objek S3. Saat Anda membuat pekerjaan, Anda menentukan seberapa sering Anda ingin pekerjaan dijalankan, dan Anda menentukan ruang lingkup dan sifat analisis pekerjaan.

Ketika pekerjaan berjalan, Macie menghasilkan catatan data sensitif yang ditemukannya ([temuan data sensitif](#)) dan analisis yang dilakukannya ([hasil penemuan data sensitif](#)). Macie juga menerbitkan data logging ke Amazon CloudWatch Logs.

Untuk informasi selengkapnya, lihat [Menjalankan tugas penemuan data sensitif](#).

## Hasil Penemuan Data Sensitif

Catatan yang mencatat detail tentang analisis yang dilakukan Macie pada objek S3 untuk menentukan apakah objek tersebut berisi data sensitif. Macie menghasilkan dan menulis catatan ini ke file JSON Lines (.jsonl), yang dienkrpsi dan disimpan dalam bucket S3 yang Anda tentukan. Catatan mematuhi skema standar.

Saat Anda menjalankan [pekerjaan penemuan data sensitif](#) atau Macie melakukan [penemuan data sensitif otomatis](#), Macie membuat hasil penemuan data sensitif untuk setiap objek yang disertakan dalam lingkup analisis. Hal ini mencakup:

- Objek tempat Macie menemukan data sensitif, dan karenanya juga menghasilkan [temuan data sensitif](#).
- Objek yang Macie tidak menemukan data sensitif, dan karena itu tidak menghasilkan temuan data sensitif.
- Objek yang tidak dapat dianalisis Macie karena kesalahan atau masalah seperti pengaturan izin atau penggunaan file atau format penyimpanan yang tidak didukung.

Untuk informasi selengkapnya, lihat [Menyimpan dan mempertahankan hasil penemuan data sensitif](#).

## akun mandiri

Akun Macie yang bukan administrator atau akun anggota dalam suatu [organisasi](#). Akun tersebut bukan bagian dari organisasi.

## temuan yang ditekan

[Temuan](#) yang diarsipkan secara otomatis oleh aturan [penindasan](#). Artinya, Macie secara otomatis mengubah status temuan menjadi diarsipkan karena temuan tersebut cocok dengan kriteria aturan penekanan ketika Macie menghasilkan temuan.

Untuk informasi selengkapnya, lihat [Menekan temuan](#).

## aturan penindasan

[Satu set kriteria filter berbasis atribut yang Anda buat dan simpan untuk mengarsipkan \(menekan\) temuan secara otomatis](#). Aturan penekanan sangat membantu dalam situasi saat Anda telah meninjau kelas temuan dan tidak ingin diberi tahu lagi.

Jika Anda menekan temuan dengan aturan penekanan, Macie terus menghasilkan temuan yang sesuai dengan kriteria aturan. Namun, Macie secara otomatis mengubah status temuan menjadi diarsipkan. Ini berarti bahwa temuan tidak muncul secara default di konsol Amazon Macie dan Macie tidak mempublikasikannya ke yang lain. Layanan AWS

Untuk informasi selengkapnya, lihat [Menekan temuan](#).

## byte atau ukuran yang tidak dapat diklasifikasikan

Dalam statistik bucket S3 yang disediakan Macie, ukuran penyimpanan total semua [objek yang tidak dapat diklasifikasikan](#) dalam bucket S3.

Jika pembuatan versi diaktifkan untuk bucket, nilai ini didasarkan pada ukuran penyimpanan versi terbaru dari setiap objek yang tidak dapat diklasifikasikan dalam bucket. Jika objek adalah file terkompresi, nilai ini tidak mencerminkan ukuran sebenarnya dari konten file setelah file didekompresi.

Untuk informasi selengkapnya, silakan lihat [Meninjau inventaris bucket S3 Anda](#) dan [Menilai postur keamanan Amazon S3 Anda](#).

## objek yang tidak dapat diklasifikasikan

Objek S3 yang tidak dapat dianalisis Macie untuk mendeteksi data sensitif.

Saat menghitung statistik bucket S3, Macie menentukan bahwa suatu objek tidak dapat diklasifikasikan berdasarkan kelas penyimpanan objek dan ekstensi nama file. Objek tidak dapat diklasifikasikan jika tidak menggunakan kelas penyimpanan Amazon S3 yang didukung atau tidak memiliki ekstensi nama file untuk file atau format penyimpanan yang didukung.

Untuk informasi selengkapnya, silakan lihat [Meninjau inventaris bucket S3 Anda](#) dan [Menilai postur keamanan Amazon S3 Anda](#).

Untuk penemuan data sensitif, Macie menentukan bahwa suatu objek tidak dapat diklasifikasikan berdasarkan kelas penyimpanan objek, ekstensi nama file, dan konten. Objek tidak dapat diklasifikasikan jika: tidak menggunakan kelas penyimpanan Amazon S3 yang didukung, tidak memiliki ekstensi nama file untuk file atau format penyimpanan yang didukung, atau Macie tidak dapat mengekstrak dan menganalisis data dari objek. Misalnya, objek adalah file yang salah format.

Selengkapnya, lihat [Menemukan data sensitif](#) dan [Prakiraan dan pemantauan biaya](#).

# Memantau keamanan dan privasi data dengan Amazon Macie

Ketika Anda mengaktifkan Amazon Macie untuk Akun AWS, Macie secara otomatis membuat dan mulai mempertahankan inventaris lengkap dari bucket Amazon Simple Storage Service (Amazon S3) Anda di bucket Amazon Simple Storage Service (Amazon S3) Anda saat ini. Wilayah AWS Macie juga mulai mengevaluasi dan memantau bucket untuk kontrol keamanan dan akses. Jika Macie mendeteksi peristiwa yang mengurangi keamanan atau privasi dari bucket S3, Macie akan membuat [Temuan kebijakan](#) untuk Anda tinjau dan perbaiki seperlunya.

Untuk mengevaluasi dan memantau bucket S3 untuk mengetahui adanya data sensitif, Anda dapat membuat dan menjalankan tugas penemuan data sensitif. Tugas penemuan data sensitif dapat melakukan analisis tambahan terhadap objek bucket secara harian, mingguan, atau bulanan. Bergantung pada pengaturan akun, Anda juga dapat mengonfigurasi Macie untuk melakukan penemuan data sensitif otomatis untuk bucket Anda. Penemuan data sensitif otomatis menggunakan teknik pengambilan sampel untuk terus mengidentifikasi, memilih, dan menganalisis objek representatif dalam bucket Anda. Jika Macie mendeteksi data sensitif dalam objek S3, Macie membuat [Temuan data sensitif untuk memberitahu Anda tentang data sensitif](#) yang ditemukan oleh Macie. Untuk informasi selengkapnya, lihat [Menemukan data sensitif](#).

Selain temuan, Macie memberikan visibilitas konstan ke dalam data keamanan dan privasi Amazon S3 Anda. Untuk menilai postur keamanan data Anda dan menentukan di mana harus mengambil tindakan, Anda dapat menggunakan dasbor Ringkasan pada konsol. Dasbor menyediakan snapshot statistik yang digabungkan untuk data Amazon S3 Anda. Statistik mencakup data untuk metrik keamanan utama seperti jumlah bucket yang dapat diakses oleh publik atau dapat dibagikan dengan yang lain. Akun AWS Dasbor juga menampilkan kelompok dari temuan data gabungan untuk akun Anda—misalnya, nama dari 1-5 bucket yang memiliki temuan terbanyak selama tujuh hari sebelumnya. Anda dapat menelusuri setiap statistik untuk meninjau data pendukungnya. Jika Anda lebih memilih untuk kueri statistik secara terprogram, Anda dapat menggunakan [GetBucketStatistics](#) pengoperasian API Amazon Macie.

Untuk analisis dan evaluasi yang lebih dalam, Macie juga menyediakan informasi dan statistik terperinci untuk setiap bucket S3 dalam inventaris Anda. Hal ini mencakup kerusakan setiap akses pengaturan dan enkripsi publik setiap bucket, serta ukuran dan jumlah objek yang dapat dianalisis Macie untuk mendeteksi data sensitif dalam bucket. Inventaris juga menunjukkan apakah Anda mengonfigurasi tugas penemuan data sensitif untuk menganalisis objek dalam

bucket dan, jika demikian, ketika salah satu tugas yang terakhir berjalan. Anda dapat menelusuri, menyortir, dan mem-filter persediaan dengan menggunakan konsol Amazon Macie atau [DescribeBuckets](#) pengoperasian API Amazon Macie.

Jika Anda seorang administrator Macie untuk organisasi, Anda dapat mengakses data statistik dan data lain tentang bucket S3 yang dimiliki oleh akun anggota Anda. Anda juga dapat mengakses temuan kebijakan yang dibuat Macie untuk bucket, dan memeriksa bucket untuk data sensitif. Sebagai administrator Macie, Anda dapat menggunakan Macie untuk menilai dan memantau postur keamanan keseluruhan data estate Amazon S3 organisasi Anda. Untuk informasi selengkapnya, lihat [Mengelola beberapa akun](#).

#### Topik

- [Cara Amazon Macie memantau keamanan data Amazon S3](#)
- [Menilai postur keamanan Amazon S3 Anda dengan Amazon Macie](#)
- [Menganalisis postur keamanan Amazon S3 Anda dengan Amazon Macie](#)
- [Mengizinkan Amazon Macie untuk mengakses bucket S3 dan objek](#)

## Cara Amazon Macie memantau keamanan data Amazon S3

Jika Anda mengaktifkan Amazon Macie untuk akun Anda, Macie membuat [peran terkait layanan AWS Identity and Access Management](#) (IAM) untuk akun Anda saat ini. Wilayah AWS Kebijakan izin untuk peran ini memungkinkan Macie untuk memanggil sumber daya lainnya Layanan AWS dan memantau AWS sumber daya atas nama Anda. Dengan menggunakan peran ini, Macie menghasilkan dan memelihara inventaris lengkap dari bucket Amazon Simple Storage Service (Amazon S3) Anda di Wilayah, dan Macie memantau dan mengevaluasi bucket untuk keamanan dan kontrol akses.

Jika Anda adalah administrator Macie untuk organisasi, inventaris mencakup data statistik dan data lain tentang bucket S3 yang dimiliki oleh akun Anda dan akun anggota di organisasi Anda. Dengan data ini, Anda dapat menggunakan Macie untuk memantau dan mengevaluasi postur keamanan organisasi Anda di lingkungan Amazon S3. Untuk informasi selengkapnya, lihat [Mengelola beberapa akun](#).

#### Topik

- [Komponen utama](#)
- [Penyegaran data](#)



- [Pertimbangan tambahan](#)

## Komponen utama

Amazon Macie menggunakan kombinasi fitur dan teknik untuk menyediakan dan memelihara data tentang bucket S3 Anda, serta untuk memantau serta mengevaluasi bucket untuk keamanan dan kontrol akses.

### Mengumpulkan metadata dan menghitung statistik

Untuk menghasilkan dan memelihara metadata dan statistik untuk inventaris bucket Anda, Macie mengambil metadata bucket dan objek langsung dari Amazon S3. Untuk setiap bucket, metadata meliputi:

- Informasi umum tentang bucket, misalnya nama bucket, Amazon Resource Name (ARN), tanggal pembuatan, pengaturan enkripsi, tag, dan ID akun untuk bucket Akun AWS yang memiliki bucket.
- Pengaturan izin tingkat akun yang berlaku untuk bucket, misalnya memblokir pengaturan akses publik untuk akun.
- Pengaturan izin tingkat bucket untuk bucket, misalnya memblokir pengaturan akses publik untuk bucket dan pengaturan yang berasal dari kebijakan bucket atau daftar kontrol akses (ACL).
- Pengaturan akses bersama dan replikasi untuk bucket, termasuk apakah data bucket direplikasi atau dibagikan dengan Akun AWS yang bukan bagian dari organisasi Anda.
- Jumlah objek dan pengaturan untuk objek dalam bucket, misalnya jumlah objek di dalam bucket dan rincian jumlah objek berdasarkan tipe enkripsi, tipe file, dan kelas penyimpanan.

Macie memberikan informasi ini kepada Anda secara langsung. Macie juga menggunakan informasi untuk menghitung statistik dan memberikan penilaian tentang keamanan dan privasi inventaris bucket Anda secara keseluruhan dan bucket secara individual dalam inventaris Anda. Misalnya, Anda dapat menemukan ukuran penyimpanan total dan jumlah bucket dalam inventaris Anda, ukuran penyimpanan total dan jumlah objek dalam bucket tersebut, serta ukuran penyimpanan total dan jumlah objek yang dapat dianalisis Macie untuk mendeteksi data sensitif pada bucket.

Secara default, metadata dan statistik menyertakan data untuk setiap bagian objek yang ada karena unggahan multibagian yang tidak lengkap. Jika Anda menyegarkan metadata objek




 Tip

Untuk memantau kejadian tingkat objek, sebaiknya gunakan fitur perlindungan Amazon S3 Amazon GuardDuty. Fitur ini memantau peristiwa data tingkat objek, Amazon S3 dan menganalisisnya untuk aktivitas berbahaya dan mencurigakan. Untuk informasi selengkapnya, lihat [Perlindungan Amazon S3 di Amazon GuardDuty](#) dalam Amazon GuardDuty Panduan Pengguna.

## Mengevaluasi keamanan dan kontrol akses bucket

Untuk mengevaluasi keamanan dan kontrol akses tingkat bucket, Macie menggunakan penalaran berbasis logika otomatis untuk menganalisis kebijakan berbasis sumber daya yang berlaku untuk bucket. Macie juga menganalisis pengaturan izin tingkat akun dan tingkat bucket yang berlaku untuk bucket. Analisis ini memfaktorkan kebijakan bucket, ACL tingkat bucket, dan memblokir pengaturan akses publik untuk akun dan bucket.

Untuk kebijakan berbasis sumber daya, Macie menggunakan [Zelkova](#). Zelkova adalah mesin peng analisis otomatis yang menerjemahkan kebijakan AWS Identity and Access Management (IAM) ke dalam pernyataan logis dan menjalankan serangkaian pemecah logika khusus dan untuk tujuan umum (teori modulo satisfiability) terhadap masalah keputusan. Macie menerapkan Zelkova berulang kali pada kebijakan dengan kueri yang semakin spesifik untuk mencirikan kelas perilaku yang dimungkinkan oleh kebijakan. Untuk mempelajari selengkapnya tentang sifat pemecah yang digunakan Zelkova, lihat [Teori Modulo Satisfiability](#).

 Important

Untuk melakukan tugas-tugas sebelumnya untuk bucket, Macie harus diizinkan untuk mengakses bucket. Jika setelah izin bucket mencegah Macie mengambil metadata untuk bucket atau objek bucket, Macie hanya dapat memberikan subset informasi tentang bucket, seperti nama bucket dan tanggal pembuatan. Macie tidak dapat melakukan tugas tambahan apa pun untuk bucket. Untuk informasi selengkapnya, lihat [Mengizinkan Macie untuk mengakses bucket S3 dan objek](#).

## Penyegaran data

Jika Anda mengaktifkan Amazon Macie untuk AndaAkun AWS, Macie akan mengambil metadata untuk bucket S3 dan objek langsung dari Amazon S3. Setelah itu, Macie secara otomatis mengambil metadata bucket dan objek secara langsung dari Amazon S3 setiap hari sebagai bagian dari siklus penyegaran harian.

Macie juga mengambil metadata bucket langsung dari Amazon S3 jika terjadi salah satu hal berikut:

- Anda menyegarkan data inventaris dengan memilih segarkan



pada konsol Amazon Macie. Anda dapat menyegarkan data setiap lima menit.

- Anda mengirimkan [DescribeBuckets](#) permintaan ke API Amazon Macie secara terprogram dan Anda belum mengirimkan DescribeBuckets permintaan dalam lima menit sebelumnya.
- Macie mendeteksi kejadian AWS CloudTrail yang relevan.

Macie juga dapat mengambil metadata objek terbaru untuk bucket tertentu jika Anda memilih untuk menyegarkan data tersebut secara manual. Hal ini dapat membantu jika Anda baru saja membuat bucket atau membuat perubahan signifikan pada objek bucket selama 24 jam terakhir. Untuk me-refresh metadata objek secara manual untuk bucket, pilih refresh



di bagian Object statistics pada [panel detail bucket](#) pada halaman bucket S3 konsol. Fitur ini tersedia untuk bucket dengan objek sebanyak 30.000 atau kurang.

Setiap kali Macie mengambil metadata bucket atau objek, Macie secara otomatis memperbarui semua data yang relevan dalam inventaris Anda. Jika Macie mendeteksi perbedaan yang memengaruhi keamanan atau privasi bucket, Macie akan segera mulai mengevaluasi dan menganalisis perubahan. Ketika analisis selesai, Macie memperbarui data yang relevan dalam inventaris Anda. Jika ada perbedaan yang menurunkan keamanan atau privasi bucket, Macie juga akan membuat [temuan kebijakan](#) yang sesuai yang dapat ditinjau dan dipulihkan jika diperlukan.

Untuk menentukan waktu terbaru Macie mengambil bucket atau metadata objek untuk akun Anda, Anda dapat merujuk ke bidang Terakhir diperbarui pada konsol. Bidang ini muncul di dasbor Ringkasan dan halaman bucket S3, dan di [panel detail bucket](#) pada halaman bucket S3. (Jika Anda menggunakan API Amazon Macie untuk meminta data inventaris, bidang `lastUpdated` menyediakan informasi ini.) Jika Anda adalah administrator Macie untuk organisasi, bidang Terakhir

diperbarui menunjukkan tanggal dan waktu paling awal saat Macie mengambil data untuk akun di organisasi Anda.


Pada kesempatan langka dalam kondisi tertentu, latensi dan permasalahan lain dapat mencegah Macie mengambil metadata bucket dan objek. Hal ini juga dapat menunda notifikasi bahwa Macie menerima perubahan pada inventaris bucket Anda atau pengaturan izin dan kebijakan untuk setiap bucket. Misalnya, masalah pengiriman dengan CloudTrail kejadian dapat menyebabkan penundaan. Jika ini terjadi, Macie menganalisis data baru dan yang diperbarui pada kesempatan berikutnya saat melakukan penyegaran harian, yaitu dalam waktu 24 jam.

## Pertimbangan tambahan

Ketika Anda gunakan Amazon Macie untuk memantau dan menilai postur keamanan data Amazon S3, ingat hal-hal berikut:

- Data inventaris hanya berlaku untuk bucket S3 di saat ini. Wilayah AWS Untuk mengakses data untuk Wilayah tambahan, aktifkan dan gunakan Macie di setiap Wilayah tambahan.
- Jika Anda adalah administrator Macie untuk organisasi, Anda dapat mengakses data inventaris untuk akun anggota hanya jika Macie diaktifkan untuk akun tersebut di Wilayah saat ini.
- Jika pengaturan izin bucket mencegah Macie mengambil informasi tentang bucket atau objek bucket, Macie tidak dapat mengevaluasi dan memantau keamanan dan privasi data bucket atau memberikan informasi rinci tentang bucket.

Untuk membantu Anda mengidentifikasi ember di mana hal ini terjadi, Macie melakukan hal berikut:

- Dalam inventaris bucket Anda, Macie menampilkan ikon peringatan  untuk bucket. Untuk detail bucket, Macie hanya menampilkan subset bidang dan data: ID akun untuk Akun AWS yang memiliki bucket; nama bucket, Amazon Resource Name (ARN), tanggal pembuatan, dan Wilayah; dan, tanggal dan waktu ketika Macie baru-baru ini mengambil metadata bucket dan objek untuk bucket sebagai bagian dari siklus penyegaran harian. Jika Anda menggunakan API Amazon Macie untuk meminta data inventaris, Macie menyediakan kode kesalahan dan pesan untuk bucket dan nilai untuk sebagian besar properti bucket adalah nol.
- Pada dasbor Ringkasan, bucket memiliki nilai Tidak Dikenal untuk akses Publik, Enkripsi, dan statistik Berbagi. (Jika Anda menggunakan Amazon Macie API untuk melakukan kueri statistik, bucket memiliki nilai unknown untuk statistik ini.) Selain itu, Macie mengecualikan bucket saat menghitung data untuk statistik Storage dan Objects.

Untuk menyelidiki masalah, tinjau pengaturan kebijakan dan izin bucket di Amazon S3. Misalnya, bucket mungkin memiliki kebijakan bucket yang membatasi. Untuk informasi selengkapnya, lihat [Mengizinkan Macie untuk mengakses bucket S3 dan objek](#).

- Data tentang akses dan izin terbatas pada pengaturan tingkat akun dan tingkat bucket. Ini tidak mencerminkan pengaturan tingkat objek yang menentukan akses ke objek tertentu dalam bucket. Misalnya, jika akses publik diaktifkan untuk objek tertentu dalam bucket, Macie tidak melaporkan bahwa bucket atau objek bucket tersebut dapat diakses secara publik.

Untuk memantau operasi tingkat objek dan mengidentifikasi risiko keamanan potens, sebaiknya gunakan fitur perlindungan Amazon S3 Amazon GuardDuty. Fitur ini memantau peristiwa data tingkat objek, Amazon S3 dan menganalisanya untuk aktivitas berbahaya dan mencurigakan. Untuk informasi selengkapnya, lihat [Perlindungan Amazon S3 di Amazon GuardDuty](#) dalam Amazon GuardDuty Panduan Pengguna.

- Jika Anda menyegarkan metadata objek untuk bucket tertentu secara manual, untuk sementara Macie melaporkan sebagai Tidak Diketahui untuk statistik enkripsi yang berlaku untuk objek. Pada kesempatan lain saat Macie melakukan penyegaran data harian (dalam waktu 24 jam), Macie mengevaluasi ulang metadata enkripsi untuk objek dan melaporkan data kuantitatif untuk statistik lagi.
- Jika Anda menyegarkan metadata objek untuk bucket tertentu secara manual, untuk sementara Macie mengecualikan data untuk bagian objek apa pun yang dikandung bucket sebagai hasil dari unggahan multibagian yang tidak lengkap. Pada kesempatan lain saat Macie melakukan penyegaran data harian (dalam waktu 24 jam), Macie menghitung ulang jumlah dan nilai ukuran penyimpanan untuk objek bucket dan menyertakan data untuk bagian-bagian dalam perhitungan tersebut.
- Dalam kasus yang jarang terjadi, Macie mungkin tidak dapat menentukan apakah bucket dapat diakses secara publik atau dibagikan, atau memerlukan enkripsi sisi server dari objek baru. Misalnya, masalah sementara dapat mencegah Macie mengambil dan menganalisis data yang diperlukan. Atau Macie mungkin tidak dapat sepenuhnya menentukan apakah satu atau beberapa pernyataan kebijakan memberikan akses ke entitas eksternal. Dalam kasus ini, Macie melaporkan sebagai Tidak Diketahui untuk statistik dan bidang yang relevan dalam inventaris. Untuk menyelidiki kasus ini, tinjau pengaturan kebijakan dan izin bucket di Amazon S3.

Perhatikan juga bahwa Macie menghasilkan temuan kebijakan hanya jika keamanan atau privasi bucket berkurang setelah Anda mengaktifkan Macie untuk akun Anda. Misalnya, jika Anda menonaktifkan pengaturan blokir akses publik untuk bucket setelah Anda mengaktifkan

Macie, Macie menghasilkan temuan `BlockPublicAccessDisabledPolicy:IAMUser/S3` untuk bucket. Namun, jika memblokir pengaturan akses publik dinonaktifkan untuk bucket saat Anda mengaktifkan Macie dan tetap terus dinonaktifkan, Macie tidak menghasilkan temuan `BlockPublicAccessDisabledPolicy:IAMUser/S3` untuk bucket.

Selain itu, ketika Macie menilai keamanan dan privasi bucket, Macie tidak memeriksa log akses atau menganalisis pengguna, peran, dan konfigurasi lain yang relevan untuk akun. Sebaliknya, Macie menganalisis dan melaporkan data untuk pengaturan kunci yang menunjukkan potensi risiko keamanan. Misalnya, jika temuan kebijakan menunjukkan bahwa bucket dapat diakses secara publik, tidak berarti bahwa entitas eksternal mengakses bucket. Demikian halnya jika temuan kebijakan menunjukkan bahwa bucket dibagikan dengan Akun AWS di luar organisasi, Macie tidak berusaha menentukan apakah akses ini ditujukan dan aman. Sebaliknya, temuan ini menunjukkan bahwa entitas eksternal berpotensi mengakses data bucket, yang mungkin menjadi risiko keamanan yang tidak diinginkan.

## Menilai postur keamanan Amazon S3 Anda dengan Amazon Macie

Untuk menilai keseluruhan postur keamanan data Amazon Simple Storage Service (Amazon S3) Anda dan menentukan lokasi untuk mengambil tindakan, Anda dapat menggunakan opsi dasbor Ringkasan pada konsol Amazon Macie.

Dasbor Ringkasan menyediakan snapshot statistik agregat untuk data Amazon S3 Anda saat ini. Wilayah AWS Statistik mencakup data untuk metrik keamanan utama seperti jumlah bucket yang dapat diakses publik atau dibagikan dengan yang lain. Akun AWS Dasbor juga menampilkan kelompok data temuan gabungan untuk akun Anda—misalnya, tipe temuan yang memiliki jumlah kejadian tertinggi selama tujuh hari sebelumnya. Jika Anda administrator Macie untuk suatu organisasi, dasbor menyediakan statistik dan data gabungan untuk semua akun di organisasi Anda. Anda dapat secara opsional memfilter data berdasarkan akun.

Untuk melakukan analisis yang lebih dalam, Anda dapat menelusuri dan meninjau data pendukung untuk masing-masing item di dasbor. Anda juga dapat [meninjau dan menganalisis inventaris bucket S3](#) menggunakan konsol Amazon Macie, atau membuat kueri dan menganalisis data inventaris secara terprogram menggunakan [DescribeBuckets](#) pengoperasian Amazon Macie API.

### Topik

- [Menampilkan dasbor Ringkasan](#)
- [Memahami komponen dasbor Ringkasan](#)
- [Memahami statistik keamanan data di dasbor Ringkasan](#)

## Menampilkan dasbor Ringkasan

Di konsol Amazon Macie, dasbor Ringkasan menyediakan snapshot statistik agregat dan data temuan untuk data Amazon S3 Anda saat ini. Wilayah AWS Jika Anda lebih suka menanyakan statistik secara terprogram, Anda dapat menggunakan [GetBucketStatistics](#) pengoperasian Amazon Macie API.

Untuk menampilkan dasbor Ringkasan

1. [Buka konsol Amazon Macie di https://console.aws.amazon.com/macie/](https://console.aws.amazon.com/macie/).
2. Di panel navigasi, pilih Ringkasan. Macie menampilkan dasbor Ringkasan.
3. Untuk menentukan kapan Macie baru-baru ini mengambil bucket atau metadata objek dari Amazon S3 untuk akun Anda, lihat bidang Terakhir diperbarui di bagian atas dasbor. Untuk informasi selengkapnya, lihat [Penyegaran data](#).
4. Untuk menelusuri dan meninjau data pendukung untuk item di dasbor, pilih item tersebut.

Jika Anda adalah administrator Macie untuk organisasi, dasbor menampilkan statistik dan data agregat untuk akun dan akun anggota di organisasi Anda. Untuk mem-filter dasbor dan menampilkan data hanya untuk akun tertentu, masukkan ID akun di kotak Akun di atas dasbor.

## Memahami komponen dasbor Ringkasan

Di dasbor Ringkasan, statistik dan data disusun menjadi beberapa bagian. Di bagian atas dasbor, Anda akan menemukan statistik agregat yang menunjukkan berapa banyak data yang Anda simpan di Amazon S3, dan berapa banyak data yang dapat dianalisis Amazon Macie untuk mendeteksi data sensitif. Anda juga dapat merujuk ke bidang Terakhir diperbarui untuk menentukan kapan Macie baru-baru ini mengambil bucket atau metadata objek dari Amazon S3 untuk akun Anda. Bagian tambahan menyediakan statistik dan data temuan terbaru yang dapat membantu Anda menilai keamanan, privasi, dan sensitivitas data Amazon S3 Anda saat ini. Wilayah AWS

Statistik dan data diatur ke dalam bagian-bagian berikut:

[Penyimpanan dan penemuan data sensitif](#) | [Masalah penemuan & cakupan otomatis](#) | [Keamanan data](#) | [Bucket S3 teratas](#) | [Jenis temuan teratas](#) | [Temuan kebijakan](#)

Saat Anda meninjau setiap bagian, secara opsional pilih item untuk ditelusuri dan tinjau data pendukung.



## Penyimpanan dan penemuan data sensitif

Statistik di bagian atas dasbor menunjukkan berapa banyak data yang Anda simpan di Amazon S3, dan berapa banyak data yang dapat dianalisis Macie untuk mendeteksi data sensitif. Sebagai contoh:

Total accounts	Storage (classifiable/total)	Objects (classifiable/total)
7	307.4 GB / 313.1 GB	514.0 k / 520.7 k

Di bagian ini:

- **Total akun** — Bidang ini muncul jika Anda adalah administrator Macie untuk organisasi atau Anda memiliki akun Macie mandiri. Ini menunjukkan jumlah total ember Akun AWS itu sendiri dalam inventaris bucket S3 Anda. Jika Anda seorang administrator Macie, ini adalah jumlah total akun Macie yang Anda kelola untuk organisasi Anda. Jika Anda memiliki akun Macie mandiri, nilai ini adalah 1.

**Total bucket S3** — Bidang ini muncul jika akun Macie Anda adalah anggota organisasi. Ini menunjukkan jumlah total ember dalam inventaris Anda, termasuk ember yang tidak berisi objek apa pun.

- **Penyimpanan** — Metrik ini memberikan informasi tentang ukuran penyimpanan objek dalam inventaris bucket Anda:
  - **Dapat Diklasifikasikan** — Ukuran total penyimpanan dari semua objek yang dapat dianalisis oleh Macie di dalam bucket.
  - **Total** — Ukuran total penyimpanan semua objek dalam bucket, termasuk objek yang tidak dapat dianalisis oleh Macie.

Jika salah satu objek adalah file kompresi, nilai-nilai ini tidak mencerminkan ukuran asli dari file-file tersebut setelah mereka diekstrak. Jika versioning diaktifkan untuk salah satu bucket, nilai-nilai ini didasarkan pada ukuran penyimpanan versi terbaru dari setiap objek dalam bucket tersebut.

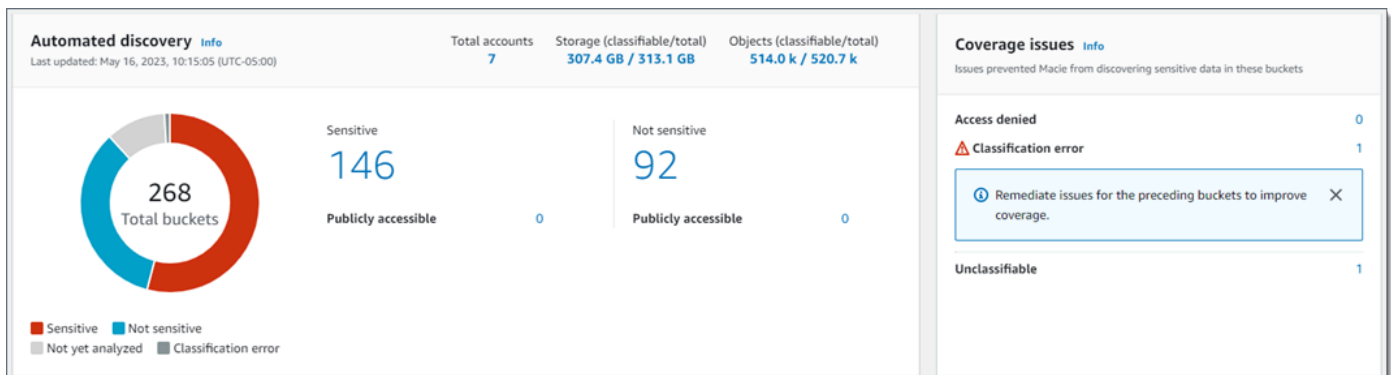
- **Objek** — Metrik ini memberikan informasi tentang jumlah objek dalam inventaris bucket Anda:
  - **Dapat Diklasifikasikan** — Jumlah total dari objek yang dapat dianalisis oleh Macie di dalam bucket.
  - **Total** — Jumlah total dari objek di dalam bucket, termasuk objek yang tidak dapat dianalisis oleh Macie.

Dalam statistik sebelumnya, data dan objek dapat diklasifikasikan jika mereka menggunakan kelas penyimpanan Amazon S3 yang didukung dan mereka memiliki ekstensi nama file untuk file atau format penyimpanan yang didukung. Anda dapat mendeteksi data sensitif dalam objek dengan menggunakan Macie. Untuk informasi selengkapnya, lihat [Kelas dan format penyimpanan yang didukung](#).

Perhatikan bahwa statistik Penyimpanan dan Objek tidak menyertakan data tentang objek dalam bucket yang tidak diizinkan diakses oleh Macie. Misalnya, objek dalam bucket yang memiliki kebijakan bucket yang membatasi. Untuk mengidentifikasi bucket di mana hal ini terjadi, Anda dapat [meninjau inventaris bucket Anda](#) dengan menggunakan tabel bucket S3. Jika ikon peringatan (⚠) muncul di sebelah nama bucket, Macie tidak diizinkan mengakses bucket.

## Masalah Penemuan & Cakupan Otomatis

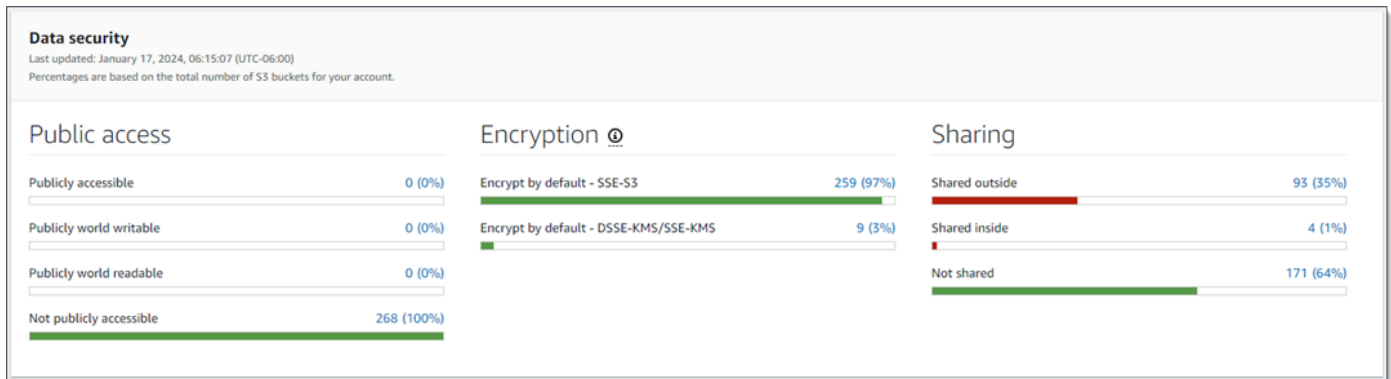
Jika penemuan data sensitif otomatis diaktifkan untuk akun Anda, bagian ini akan muncul di dasbor. Statistik di bagian ini menangkap status dan hasil aktivitas penemuan data sensitif otomatis yang telah dilakukan Macie sejauh ini untuk data Amazon S3 Anda. Sebagai contoh:



Untuk detail tentang statistik ini, lihat [Meninjau statistik sensitivitas data agregat di dasbor Ringkasan](#).

## Keamanan data

Bagian ini memberikan statistik yang menunjukkan potensi risiko keamanan dan privasi untuk data Amazon S3 Anda. Sebagai contoh:



Untuk detail tentang statistik ini, lihat [Memahami statistik keamanan data di dasbor Ringkasan](#).

## Bucket S3 teratas

Bagian ini mencantumkan ember S3 yang menghasilkan temuan terbanyak dari jenis apa pun selama tujuh hari sebelumnya, sebanyak lima ember. Hal ini juga menunjukkan jumlah temuan yang dibuat oleh Macie untuk setiap bucket. Sebagai contoh:

<b>Top S3 buckets</b> Past 7 days	
S3 Bucket	Total findings
DOC-EXAMPLE-BUCKET1	28
DOC-EXAMPLE-BUCKET2	10
DOC-EXAMPLE-BUCKET3	8
DOC-EXAMPLE-BUCKET4	2
DOC-EXAMPLE-BUCKET5	2

[View all findings by bucket](#)

Untuk menampilkan dan secara opsional menelusuri semua temuan untuk bucket selama tujuh hari sebelumnya, pilih nilai dalam bidang Total temuan. Untuk menampilkan semua temuan terkini untuk semua bucket, dikelompokkan menurut bucket, pilih Melihat semua temuan berdasarkan bucket.

Bagian ini kosong jika Macie tidak membuat temuan apa pun selama tujuh hari ke belakang. [Atau semua temuan yang dibuat selama tujuh hari sebelumnya ditekan oleh aturan penindasan.](#)

## Jenis temuan teratas

Bagian ini berisi daftar [tipe temuan](#) yang memiliki jumlah kejadian tertinggi selama tujuh hari sebelumnya, sebanyak lima tipe temuan. Hal ini juga menunjukkan jumlah temuan yang dibuat oleh Macie untuk setiap tipe. Sebagai contoh:

Top finding types	
Past 7 days	
Finding type	Total findings
SensitiveData:S3Object/Multiple	32
SensitiveData:S3Object/Personal	13
Policy:IAMUser/S3BucketSharedExternally	2
Policy:IAMUser/S3BlockPublicAccessDisabled	1
Policy:IAMUser/S3BucketEncryptionDisabled	1

[View all findings by type](#)

Untuk menampilkan dan secara opsional menelusuri semua temuan dari tipe tertentu selama tujuh hari sebelumnya, pilih nilai dalam bidang Total temuan. Untuk menampilkan semua temuan saat ini, dikelompokkan berdasarkan tipe temuan, pilih [Melihat semua temuan berdasarkan tipe](#).

Bagian ini kosong jika Macie tidak membuat temuan apa pun selama tujuh hari ke belakang. [Atau semua temuan yang dibuat selama tujuh hari sebelumnya ditekan oleh aturan penindasan.](#)

## Temuan kebijakan

Bagian ini berisi daftar [temuan kebijakan](#) yang baru-baru ini dibuat atau diperbarui oleh Macie, sebanyak sepuluh temuan. Sebagai contoh:

Policy findings		
Most recent policy findings		
<span style="color: red;">High</span>	Policy:IAMUser/S3BucketReplicatedExternally	9 hours ago
<span style="color: red;">High</span>	Policy:IAMUser/S3BucketSharedExternally	9 hours ago
<span style="color: orange;">Medium</span>	Policy:IAMUser/S3BucketSharedWithCloudFront	9 hours ago
<span style="color: red;">High</span>	Policy:IAMUser/S3BucketPublic	9 hours ago
<span style="color: red;">High</span>	Policy:IAMUser/S3BlockPublicAccessDisabled	9 hours ago
<span style="color: green;">Low</span>	Policy:IAMUser/S3BucketEncryptionDisabled	9 hours ago

Untuk menampilkan detail temuan tertentu, pilih temuan.

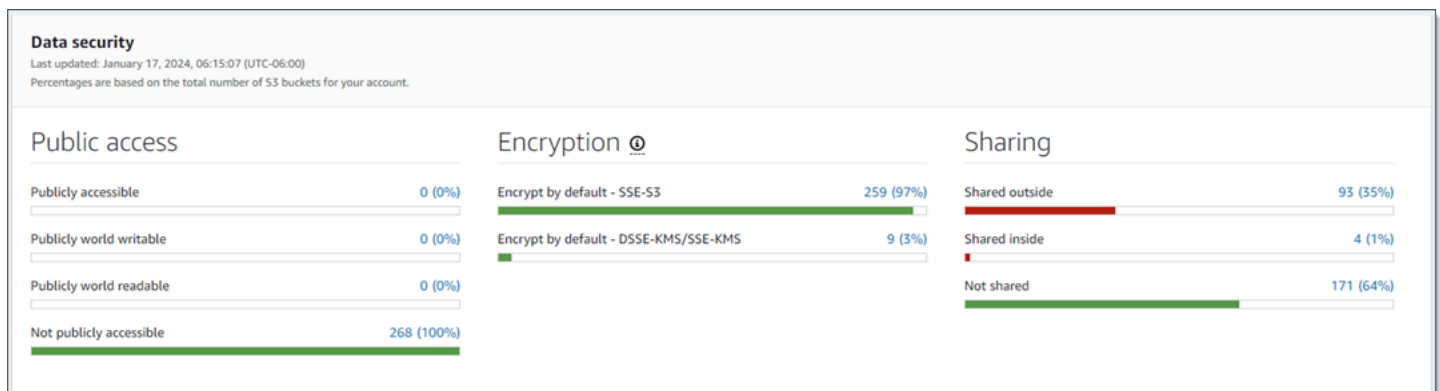
Bagian ini kosong jika Macie tidak membuat ataupun memperbarui kebijakan temuan apa pun selama tujuh hari ke belakang. [Atau semua temuan kebijakan yang dibuat atau diperbarui selama tujuh hari sebelumnya ditekan oleh aturan penindasan.](#)

## Memahami statistik keamanan data di dasbor Ringkasan

Bagian keamanan data pada dasbor Ringkasan menyediakan statistik yang dapat membantu Anda mengidentifikasi dan menyelidiki potensi risiko keamanan dan privasi untuk data Amazon S3 Anda saat ini. Wilayah AWS Misalnya, Anda dapat menggunakan data ini untuk mengidentifikasi bucket S3 yang dapat diakses publik atau dibagikan dengan yang lain. Akun AWS

Jika akun Macie Anda adalah anggota organisasi, [penyimpanan dan statistik penemuan data sensitif](#) di bagian atas bagian ini menunjukkan berapa banyak data yang Anda simpan di Amazon S3, dan berapa banyak data yang dapat dianalisis Macie untuk mendeteksi data sensitif.

Untuk semua jenis akun Macie, statistik tambahan disusun menjadi tiga area, seperti yang ditunjukkan pada gambar berikut.



Statistik individu di setiap area adalah sebagai berikut.

### Akses publik

Statistik ini menunjukkan berapa banyak bucket S3 yang atau tidak dapat diakses publik:

- Dapat diakses publik — Jumlah dan persentase bucket yang mengizinkan masyarakat umum untuk mendapat akses membaca atau menulis ke bucket.
- Dapat ditulis oleh publik — Jumlah dan persentase bucket yang mengizinkan masyarakat umum untuk mendapat akses menulis ke bucket.

- Dapat dibaca oleh publik — Jumlah dan persentase bucket yang mengizinkan masyarakat umum untuk mendapat akses membaca ke bucket.
- Tidak dapat diakses publik — Jumlah dan persentase bucket yang tidak mengizinkan masyarakat umum untuk mendapat akses membaca atau menulis ke bucket.

Untuk menghitung setiap persentase, Macie membagi jumlah bucket yang sesuai dengan jumlah total bucket dalam inventaris bucket Anda.

Untuk menentukan nilai di bagian ini, Macie menganalisis kombinasi pengaturan tingkat akun dan ember untuk setiap bucket: pengaturan blokir akses publik untuk akun; pengaturan blokir akses publik untuk bucket; kebijakan bucket untuk bucket; dan, daftar kontrol akses (ACL) untuk bucket. Untuk informasi tentang pengaturan ini, lihat [Identity and access management di Amazon S3](#) dan [Melakukan blokir akses publik ke penyimpanan Amazon S3 Anda](#) di Panduan Pengguna Amazon Simple Storage Service.

Dalam kasus tertentu, bagian Akses publik juga menampilkan nilai untuk Tidak Dikenal. Jika nilai ini muncul, Macie tidak dapat mengevaluasi pengaturan akses publik untuk jumlah dan persentase bucket yang telah ditentukan. Misalnya, masalah sementara atau pengaturan izin ember mencegah Macie mengambil data yang diperlukan. Atau Macie tidak dapat sepenuhnya menentukan apakah satu atau beberapa pernyataan kebijakan mengizinkan entitas eksternal untuk mengakses bucket.

## Enkripsi

Statistik ini menunjukkan berapa banyak bucket S3 yang dikonfigurasi untuk menerapkan jenis enkripsi sisi server tertentu ke objek yang ditambahkan ke bucket:

- Enkripsi secara default — SSE-S3 — Jumlah dan persentase bucket yang pengaturan enkripsi defaultnya dikonfigurasi untuk mengenkripsi objek baru dengan kunci terkelola Amazon S3. Untuk bucket ini, objek baru dienkripsi secara otomatis menggunakan enkripsi SSE-S3.
- Enkripsi secara default — DSSE-KMS/SSE-KMS — Jumlah dan persentase bucket yang pengaturan enkripsi defaultnya dikonfigurasi untuk mengenkripsi objek baru dengan, baik kunci yang dikelola pelanggan atau pelanggan. AWS KMS key Kunci yang dikelola AWS Untuk bucket ini, objek baru dienkripsi secara otomatis menggunakan enkripsi DSSE-KMS atau SSE-KMS.

Untuk menghitung setiap persentase, Macie membagi jumlah bucket yang sesuai dengan jumlah total bucket dalam inventaris bucket Anda.

Untuk menentukan nilai di bagian ini, Macie menganalisis pengaturan enkripsi default untuk setiap bucket. Mulai 5 Januari 2023, Amazon S3 secara otomatis menerapkan enkripsi sisi server dengan kunci terkelola Amazon S3 (SSE-S3) sebagai tingkat dasar enkripsi untuk objek yang ditambahkan ke bucket. Anda dapat mengonfigurasi pengaturan enkripsi default bucket untuk menggunakan enkripsi sisi server dengan AWS KMS kunci (SSE-KMS) atau enkripsi sisi server dua lapis dengan kunci (DSSE-KMS). Untuk informasi tentang setelan dan opsi enkripsi [default](#), lihat [Menyetel perilaku enkripsi sisi server default untuk bucket S3 di Panduan Pengguna](#) Layanan Penyimpanan Sederhana Amazon.

Dalam kasus tertentu, bagian Enkripsi juga menampilkan nilai untuk Tidak Dikenal. Jika nilai ini muncul, Macie tidak dapat mengevaluasi pengaturan enkripsi default untuk jumlah dan persentase bucket yang ditentukan. Misalnya, masalah sementara atau pengaturan izin ember mencegah Macie mengambil data yang diperlukan.

## Berbagi

Statistik ini menunjukkan berapa banyak bucket S3 yang atau tidak dibagikan dengan yang lain, identitas akses CloudFront asal Akun AWS Amazon (OAI), atau kontrol akses CloudFront asal (OAC):

- Dibagikan di luar — Jumlah dan persentase bucket yang dibagikan dengan satu atau beberapa hal berikut atau kombinasi berikut ini: CloudFront OAI, CloudFront OAC, atau akun yang tidak berada di organisasi yang sama.
- Dibagikan di dalam — Jumlah dan persentase bucket yang dibagikan dengan satu atau beberapa akun di organisasi yang sama. Ember ini tidak dibagikan dengan CloudFront OAI atau OAC.
- Tidak dibagikan — Jumlah dan persentase bucket yang tidak dibagikan dengan akun lain, CloudFront OAI, atau CloudFront OAC.

Untuk menghitung setiap persentase, Macie membagi jumlah bucket yang sesuai dengan jumlah total bucket dalam inventaris bucket Anda.

Untuk menentukan apakah bucket dibagikan dengan yang lain Akun AWS, Macie menganalisis kebijakan bucket dan ACL untuk setiap bucket. Selain itu, suatu Organisasi merupakan set akun Macie yang terkelola secara terpusat sebagai grup dari akun-akun terkait melalui AWS Organizations atau dengan undangan Macie. Untuk informasi tentang opsi Amazon S3 untuk berbagi bucket, lihat [Manajemen identitas dan akses di Amazon S3](#) di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.





Anda dapat meninjau data estate Amazon S3 Anda dengan menggunakan inventaris ini, dan memeriksa detail dan statistik untuk pengaturan keamanan kunci dan metrik yang berlaku untuk masing-masing bucket S3. Misalnya, Anda dapat mengakses rincian pengaturan akses dan enkripsi publik setiap bucket, serta ukuran dan jumlah objek yang dapat dianalisis Macie untuk mendeteksi data sensitif di setiap bucket. Anda juga dapat menentukan apakah Anda mengonfigurasi tugas penemuan data sensitif untuk menganalisis objek dalam bucket dan, jika demikian, ketika salah satu tugas yang terakhir berjalan. Jika penemuan data sensitif otomatis diaktifkan untuk akun Anda, Anda juga dapat menggunakan inventaris untuk meninjau hasil aktivitas penemuan data sensitif otomatis yang telah dilakukan Macie sejauh ini untuk akun atau organisasi Anda. Untuk informasi selengkapnya, lihat [Menemukan data sensitif](#).

Anda dapat menelusuri dan memfilter data inventaris dengan menggunakan halaman Bucket S3 pada konsol Amazon Macie. Anda juga dapat mengakses data inventaris Anda secara terprogram dengan menggunakan [DescribeBuckets](#) operasi Amazon Macie.

Topik

- [Meninjau inventaris bucket S3 Anda dengan Amazon Macie](#)
- [Memfilter inventaris bucket S3 Anda dengan Amazon Macie](#)

## Meninjau inventaris bucket S3 Anda dengan Amazon Macie

Di konsol Amazon Macie, halaman bucket S3 memberikan wawasan terperinci tentang keamanan dan privasi data Amazon Simple Storage Service (Amazon S3) saat ini. Wilayah AWS Anda dapat meninjau dan menganalisis inventaris lengkap dari bucket S3 Anda di Wilayah saat ini dengan halaman ini, dan meninjau informasi dan statistik detail untuk masing-masing bucket. Jika Anda administrator Macie untuk suatu organisasi, inventaris Anda mencakup detail dan statistik untuk bucket S3 yang dimiliki oleh akun anggota di organisasi Anda.

Halaman bucket S3 juga menunjukkan kapan Macie baru-baru ini mengambil bucket atau metadata objek dari Amazon S3 untuk akun Anda. Anda dapat menemukan informasi ini di bidang Terakhir diperbarui di bagian atas halaman. Jika Anda administrator Macie untuk suatu organisasi, bidang ini menunjukkan tanggal dan waktu paling awal saat Macie mengambil data untuk akun di organisasi Anda. Untuk informasi selengkapnya, lihat [Penyegaran data](#).

Perhatikan bahwa sebagian besar data inventaris terbatas pada bucket yang diizinkan diakses Macie untuk akun Anda. Jika setelah izin bucket mencegah Macie mengambil informasi tentang bucket atau objek bucket, Macie hanya dapat memberikan subset informasi

tentang bucket. Jika hal ini terjadi pada bucket tertentu, Macie menampilkan icon peringatan



dan pesan untuk bucket di inventaris bucket Anda. Untuk detail bucket, Macie hanya menampilkan subset bidang dan data: ID akun untuk pemilik bucket; nama bucket, Nama Sumber Daya Amazon (ARN), tanggal pembuatan, dan Wilayah; dan, saat Macie baru-baru ini mengambil metadata bucket dan objek untuk bucket sebagai bagian dari siklus penyegaran harian. Akun AWS Untuk menyelidiki masalah ini, tinjau setelan kebijakan dan izin bucket di Amazon S3. Misalnya, bucket mungkin memiliki kebijakan bucket yang membatasi. Untuk informasi selengkapnya, lihat [Mengizinkan Macie untuk mengakses bucket S3 dan objek](#).

Jika Anda lebih suka mengakses dan menanyakan data inventaris Anda secara terprogram, Anda dapat menggunakan [DescribeBuckets](#) pengoperasian Amazon Macie API.

Topik

- [Meninjau inventaris bucket S3 Anda](#)
- [Meninjau detail ember S3](#)

## Meninjau inventaris bucket S3 Anda

Halaman bucket S3 di konsol Amazon Macie memberikan informasi tentang bucket S3 Anda saat ini. Wilayah AWS Tabel menampilkan informasi ringkasan di halaman ini untuk setiap bucket dalam inventaris Anda. Untuk menyesuaikan tampilan Anda, Anda dapat mengurutkan dan memfilter tabel. Jika Anda memilih bucket dalam tabel, panel detail menampilkan informasi tambahan tentang bucket. Ini mencakup detail dan statistik untuk pengaturan dan metrik yang memberikan wawasan tentang keamanan dan privasi data bucket. Anda dapat secara opsional mengeksport data dari tabel ke file nilai yang dipisahkan koma (CSV).

Jika penemuan data sensitif otomatis diaktifkan untuk akun Anda, Anda juga memiliki opsi untuk meninjau inventaris Anda dengan menggunakan peta panas interaktif. Peta ini memberikan representasi visual sensitivitas data di seluruh kawasan data Amazon S3 Anda. Ini menangkap hasil aktivitas penemuan data sensitif otomatis yang telah dilakukan Macie untuk akun atau organisasi Anda. Untuk mempelajari peta ini, lihat [Memvisualisasikan sensitivitas data dengan peta bucket S3](#).

Untuk meninjau inventaris bucket S3 Anda

1. [Buka konsol Amazon Macie di https://console.aws.amazon.com/macie/](https://console.aws.amazon.com/macie/).
2. Di panel navigasi, pilih Bucket S3. Halaman bucket S3 menampilkan inventaris bucket Anda.

Jika halaman menampilkan peta interaktif inventaris bucket Anda, pilih table



di bagian atas halaman. Macie kemudian menampilkan jumlah ember di inventaris Anda dan tabel ember.

3. Di bagian atas halaman, pilih segarkan



secara opsional untuk mengambil metadata bucket terbaru dari Amazon S3.

Jika ikon informasi



muncul di samping nama bucket, kami merekomendasikan Anda untuk melakukan hal ini. Ikon ini menunjukkan bahwa bucket dibuat selama 24 jam terakhir, mungkin setelah Macie terakhir mengambil bucket dan metadata objek dari Amazon S3 sebagai bagian dari [siklus penyegaran harian](#).

4. Di halaman Bucket S3, gunakan tabel untuk meninjau subset informasi tentang setiap bucket di inventaris Anda:

- Sensitivitas — Skor sensitivitas bucket saat ini. Kolom ini hanya muncul jika penemuan data sensitif otomatis diaktifkan untuk akun Anda. Untuk informasi tentang kisaran skor sensitivitas yang didefinisikan Macie, lihat. [Penilaian sensitivitas untuk bucket S3](#)
- Bucket – Nama bucket.
- Akun — ID akun untuk pemilik bucket. Akun AWS
- Objek yang dapat diklasifikasikan – Jumlah total objek yang dapat dianalisis Macie untuk mendeteksi data sensitif dalam bucket.
- Ukuran yang dapat diklasifikasikan – Ukuran penyimpanan total semua objek yang dapat dianalisis Macie untuk mendeteksi data sensitif dalam bucket.

Perhatikan jika nilai ini tidak mencerminkan ukuran sebenarnya dari setiap objek terkompresi setelah objek didekompresi. Selain itu, jika versioning diaktifkan untuk bucket, nilai ini didasarkan pada ukuran penyimpanan versi terbaru dari setiap objek dalam bucket.

- Dipantau berdasarkan pekerjaan — Apakah ada pekerjaan penemuan data sensitif yang dikonfigurasi untuk menganalisis objek secara berkala dalam ember setiap hari, mingguan, atau bulanan.

Jika nilai untuk bidang ini Ya, bucket secara eksplisit disertakan dalam tugas berkala atau bucket yang sesuai dengan kriteria untuk tugas berkala dalam 24 jam terakhir. Selain itu, status dari setidaknya salah satu tugas tersebut tidak Dibatalkan. Macie memperbarui data ini setiap hari.

- Pekerjaan terbaru — Jika ada pekerjaan penemuan data sensitif satu kali atau berkala yang dikonfigurasi untuk menganalisis objek dalam bucket, nilai untuk bidang ini menunjukkan tanggal dan waktu terbaru ketika salah satu pekerjaan tersebut mulai berjalan. Jika tidak, bidang ini akan kosong.

Dalam data sebelumnya, objek dapat diklasifikasikan jika mereka menggunakan kelas penyimpanan Amazon S3 yang didukung dan mereka memiliki ekstensi nama file untuk file atau format penyimpanan yang didukung. Anda dapat mendeteksi data sensitif dalam objek dengan menggunakan Macie. Untuk informasi selengkapnya, lihat [Kelas dan format penyimpanan yang didukung](#).

5. Untuk menganalisis inventaris Anda dengan menggunakan tabel, lakukan salah satu hal berikut ini:
  - Untuk mengurutkan tabel dengan bidang tertentu, klik judul kolom untuk bidang. Untuk mengubah urutan pengurutan, klik judul kolom lagi.
  - Untuk memfilter tabel dan hanya menampilkan bucket yang memiliki nilai spesifik untuk bidang, letakkan kursor Anda di kotak filter, lalu tambahkan kondisi filter untuk bidang tersebut. Untuk lebih menyempurnakan hasilnya, tambahkan syarat filter untuk bidang tambahan. Untuk informasi selengkapnya, lihat [Memfilter inventaris bucket S3 Anda](#).
6. Untuk meninjau detail dan statistik untuk bucket tertentu, pilih nama bucket dalam tabel, lalu merujuk ke panel detail.

#### Tip

Anda dapat memutar dan menelusuri banyak bidang di panel detail ember. Untuk menampilkan bucket yang memiliki nilai yang sama untuk bidang, pilih



di bidang tersebut. Untuk menampilkan bucket yang memiliki nilai lain untuk bidang, pilih



di bidang tersebut.

7. Untuk mengekspor data dari tabel ke file CSV, pilih kotak centang untuk setiap baris yang ingin Anda ekspor, atau pilih kotak centang di judul kolom pilihan untuk memilih semua baris. Kemudian pilih Ekspor ke CSV di bagian atas halaman. Anda dapat mengekspor hingga 50.000 baris dari tabel.


## Meninjau detail ember S3

Di konsol Amazon Macie, Anda dapat menggunakan panel detail pada halaman Bucket S3 untuk meninjau statistik dan informasi lainnya tentang bucket S3 individu dalam inventaris bucket Anda. Ini mencakup detail dan statistik untuk pengaturan dan metrik yang memberikan wawasan tentang keamanan dan privasi data bucket.

Misalnya, Anda dapat meninjau rincian setelan akses publik bucket S3, dan menentukan apakah bucket dikonfigurasi untuk mereplikasi objek atau dibagikan dengan yang lain. Akun AWS Anda juga dapat menentukan tugas penemuan data sensitif yang dikonfigurasi untuk memeriksa bucket untuk data sensitif. Jika ada, Anda dapat mengakses detail tentang pekerjaan yang berjalan paling baru, dan secara opsional menampilkan temuan apa pun yang dihasilkan oleh pekerjaan tersebut.

Jika penemuan data sensitif otomatis diaktifkan untuk akun Anda, Anda juga dapat menggunakan panel detail untuk meninjau statistik penemuan data sensitif dan informasi lainnya tentang bucket S3 individual. Panel menangkap hasil aktivitas penemuan data sensitif otomatis yang telah dilakukan Macie sejauh ini untuk sebuah ember. Untuk mempelajari detail ini, lihat [Meninjau detail sensitivitas data untuk masing-masing bucket S3](#).

Untuk meninjau detail ember S3

1. [Buka konsol Amazon Macie di https://console.aws.amazon.com/macie/](https://console.aws.amazon.com/macie/).
2. Di panel navigasi, pilih Bucket S3. Halaman bucket S3 menampilkan inventaris bucket Anda.
3. Di bagian atas halaman, pilih segarkan  secara opsional untuk mengambil metadata bucket terbaru dari Amazon S3.
4. Di tabel atau peta bucket S3, pilih bucket yang detailnya ingin Anda tinjau. Panel detail menampilkan statistik dan informasi lainnya tentang bucket.

Di panel detail, statistik dan informasi bucket disusun ke dalam bagian utama berikut:

[Ikhtisar](#) | [Statistik objek](#) | [Enkripsi sisi server](#) | [Penemuan data sensitif](#) | [Akses publik](#) | [Replikasi](#) | [Tag](#)

Ketika Anda meninjau informasi di setiap bagian, Anda secara opsional dapat beralih dan menelusuri bidang tertentu. Untuk menampilkan bucket yang memiliki nilai yang sama untuk bidang, pilih



di bidang tersebut. Untuk menampilkan bucket yang memiliki nilai lain untuk bidang, pilih



di bidang tersebut.

## Ikhtisar

Bagian ini memberikan informasi umum tentang bucket, seperti nama bucket, kapan bucket dibuat, dan ID akun untuk Akun AWS yang memiliki bucket. Sebagai catatan khusus, bidang Terakhir diperbarui menunjukkan kapan Macie baru-baru ini mengambil metadata dari Amazon S3 untuk bucket atau objek bucket.

Kolom Akses bersama menunjukkan apakah bucket dibagikan dengan yang lain Akun AWS, identitas akses CloudFront asal Amazon (OAI), atau kontrol akses CloudFront asal (OAC):

- Eksternal — Bucket dibagikan dengan satu atau beberapa hal berikut atau kombinasi berikut ini: CloudFront OAI, CloudFront OAC, atau akun yang berada di luar (bukan bagian dari) organisasi Anda.
- Internal — Bucket dibagikan dengan satu atau beberapa akun yang bersifat internal (bagian dari) organisasi Anda. Itu tidak dibagikan dengan CloudFront OAI atau OAC.
- Tidak dibagikan - Bucket tidak dibagikan dengan akun lain, CloudFront OAI, atau CloudFront OAC.
- Tidak diketahui - Macie tidak dapat mengevaluasi pengaturan akses bersama untuk bucket.

Untuk menentukan apakah bucket dibagikan dengan yang lain Akun AWS, Macie menganalisis kebijakan bucket dan daftar kontrol akses (ACL) untuk bucket tersebut. Analisis ini terbatas pada pengaturan tingkat ember. Itu tidak mencerminkan pengaturan tingkat objek apa pun untuk berbagi objek tertentu di ember. Selain itu, suatu Organisasi merupakan set akun Macie yang dikelola secara terpusat sebagai grup dari akun-akun terkait melalui AWS Organizations atau dengan undangan Macie. Untuk mempelajari tentang opsi Amazon S3 untuk berbagi bucket, lihat [Manajemen identitas dan akses di Amazon S3](#) di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

### Note

Dalam kasus tertentu, Macie mungkin salah menunjukkan bahwa bucket dibagikan dengan Akun AWS yang eksternal (bukan bagian dari) organisasi Anda. Hal ini dapat



- Jika pembuatan versi diaktifkan untuk bucket, nilai ukuran didasarkan pada ukuran penyimpanan versi terbaru dari setiap objek di bucket.
- Jika bucket berisi objek terkompresi, nilai ukuran tidak mencerminkan ukuran sebenarnya dari objek tersebut setelah didekompresi.
- Jika Anda menyegarkan metadata objek untuk bucket, Macie untuk sementara melaporkan Tidak Diketahui untuk statistik enkripsi yang berlaku untuk objek. Macie akan mengevaluasi kembali dan memperbarui data untuk statistik ini ketika melakukan [penyegaran harian](#) berikutnya dari bucket dan metadata objek, yaitu dalam waktu 24 jam.
- Secara default, jumlah objek dan nilai ukuran menyertakan data untuk setiap bagian objek yang berisi bucket sebagai akibat dari unggahan multibagian yang tidak lengkap. Jika Anda me-refresh metadata objek untuk bucket, Macie mengecualikan data untuk bagian objek dari nilai yang dihitung ulang. Saat Macie melakukan penyegaran harian berikutnya dari bucket dan metadata objek (dalam 24 jam), Macie menghitung ulang dan memperbarui nilai untuk statistik ini dan menyertakan data untuk bagian objek dalam nilai lagi.

Perhatikan bahwa Macie tidak dapat menganalisis bagian objek untuk mendeteksi data sensitif. Amazon S3 pertama-tama harus menyelesaikan perakitan bagian-bagian menjadi satu atau lebih objek untuk dianalisis oleh Macie. Untuk informasi tentang unggahan multibagian dan bagian objek, termasuk cara menghapus bagian secara otomatis dengan aturan siklus hidup, lihat [Mengunggah dan menyalin objek menggunakan unggahan multibagian di Panduan Pengguna Layanan Penyimpanan](#) Sederhana Amazon. Untuk mengidentifikasi bucket yang berisi bagian objek, Anda dapat merujuk ke metrik unggahan multibagian yang tidak lengkap di Amazon S3 Storage Lens. Untuk informasi selengkapnya, lihat [Menilai aktivitas dan penggunaan penyimpanan Anda](#) di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

Statistik objek diatur sebagai berikut.

Objek yang dapat diklasifikasikan

Bagian ini menunjukkan jumlah total objek yang dapat dianalisis Macie untuk mendeteksi data sensitif dan ukuran penyimpanan total objek tersebut. Objek ini menggunakan kelas penyimpanan Amazon S3 yang didukung dan memiliki ekstensi nama file untuk file atau format penyimpanan yang didukung. Anda dapat mendeteksi data sensitif dalam objek dengan menggunakan Macie. Untuk informasi selengkapnya, lihat [Kelas dan format penyimpanan yang didukung](#).



## Objek yang tidak dapat diklasifikasikan

Bagian ini menunjukkan jumlah objek yang tidak dapat dianalisis Macie untuk mendeteksi data sensitif dan ukuran penyimpanan total objek tersebut. Objek ini tidak menggunakan kelas penyimpanan Amazon S3 yang didukung atau mereka tidak memiliki ekstensi nama file untuk file atau format penyimpanan yang didukung.

### Objek yang tidak dapat diklasifikasikan: Kelas penyimpanan

Bagian ini menyediakan rincian jumlah dan ukuran penyimpanan objek yang tidak dapat dianalisis Macie karena objek tidak menggunakan kelas penyimpanan Amazon S3 yang didukung.

### Objek yang tidak dapat diklasifikasikan: Jenis file

Bagian ini menyediakan rincian jumlah dan ukuran penyimpanan objek yang tidak dapat dianalisis Macie karena objek tidak memiliki ekstensi nama file untuk file atau format penyimpanan yang didukung.

### Objek berdasarkan jenis enkripsi

Bagian ini menyediakan rincian jumlah objek yang menggunakan setiap tipe enkripsi yang didukung Amazon S3:

- Customer provided — Jumlah objek yang dienkripsi dengan kunci yang disediakan pelanggan. Objek ini menggunakan enkripsi SSE-C.
- AWS KMSManaged — Jumlah objek yang dienkripsi dengan AWS KMS key, baik kunci yang dikelola pelanggan Kunci yang dikelola AWS atau pelanggan. Objek ini menggunakan enkripsi DSSE-KMS atau SSE-KMS.
- Amazon S3 dikelola - Jumlah objek yang dienkripsi dengan kunci terkelola Amazon S3. Objek ini menggunakan enkripsi SSE-S3.
- Tidak ada enkripsi – Jumlah objek yang tidak dienkripsi atau menggunakan enkripsi di sisi klien. (Jika objek dienkripsi menggunakan enkripsi di sisi klien, Macie tidak dapat mengakses dan melaporkan data enkripsi untuk objek.)
- Tidak Diketahui – Jumlah objek yang tidak dimiliki Macie untuk metadata enkripsi saat ini. Hal ini biasanya terjadi jika Anda baru-baru ini memilih untuk secara manual menyegarkan metadata untuk objek bucket. Macie akan memperbarui statistik enkripsi ketika melakukan penyegaran harian berikutnya bucket dan metadata objek, dalam waktu 24 jam.

Untuk informasi tentang setiap jenis enkripsi yang didukung, lihat [Melindungi data dengan enkripsi](#) di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

## Enkripsi sisi server

Bagian ini menyediakan wawasan ke pengaturan enkripsi di sisi server untuk bucket.

Bidang Enkripsi yang diperlukan oleh kebijakan bucket menunjukkan apakah kebijakan bucket memerlukan enkripsi objek di sisi server saat objek ditambahkan ke bucket:

- Tidak – Bucket tidak memiliki kebijakan bucket atau kebijakan bucket tidak memerlukan enkripsi di sisi server objek baru. Jika kebijakan bucket ada, tidak memerlukan [PutObject](#) permintaan untuk menyertakan header enkripsi sisi server yang valid.
- Ya — Kebijakan bucket memerlukan enkripsi objek baru di sisi server. [PutObject](#) permintaan untuk bucket harus menyertakan header enkripsi sisi server yang valid. Jika tidak, maka Amazon S3 akan menolak permintaan tersebut.
- Tidak diketahui — Macie tidak dapat mengevaluasi kebijakan bucket untuk menentukan apakah itu memerlukan enkripsi sisi server dari objek baru.

Untuk penilaian ini, header enkripsi sisi server yang valid adalah: `x-amz-server-side-encryption` dengan nilai `AES256` atau `aws:kms`, dan `x-amz-server-side-encryption-customer-algorithm` dengan nilai `AES256`. Untuk informasi tentang penggunaan kebijakan bucket agar memerlukan enkripsi objek baru di sisi server, lihat [Melindungi data dengan enkripsi sisi server](#) di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

Bidang enkripsi default menunjukkan algoritme enkripsi sisi server mana yang dikonfigurasi bucket untuk diterapkan secara default ke objek yang ditambahkan ke bucket:

- AES256 - Pengaturan enkripsi default bucket dikonfigurasi untuk mengenkripsi objek baru dengan kunci terkelola Amazon S3. Objek baru dienkripsi secara otomatis menggunakan enkripsi SSE-S3.
- `aws:kms` - Pengaturan enkripsi default bucket dikonfigurasi untuk mengenkripsi objek baru dengan AWS KMS key, baik kunci terkelola Kunci yang dikelola AWS atau pelanggan. Objek baru dienkripsi secara otomatis menggunakan enkripsi SSE-KMS. AWS KMS key Bidang menunjukkan Nama Sumber Daya Amazon (ARN) atau pengenal unik (ID kunci) untuk kunci yang digunakan.
- `aws:kms:dsse` — Pengaturan enkripsi default bucket dikonfigurasi untuk mengenkripsi objek baru dengan AWS KMS key, baik kunci terkelola atau pelanggan. Kunci yang dikelola AWS Objek baru dienkripsi secara otomatis menggunakan enkripsi DSSE-KMS. AWS KMS key Bidang menunjukkan ARN atau ID kunci untuk kunci yang digunakan.
- Tidak ada - Pengaturan enkripsi default bucket tidak menentukan perilaku enkripsi sisi server untuk objek baru.

Mulai 5 Januari 2023, Amazon S3 secara otomatis menerapkan enkripsi sisi server dengan kunci terkelola Amazon S3 (SSE-S3) sebagai tingkat dasar enkripsi untuk objek yang ditambahkan ke bucket. Anda dapat mengonfigurasi pengaturan enkripsi default bucket untuk menggunakan enkripsi sisi server dengan AWS KMS kunci (SSE-KMS) atau enkripsi sisi server dua lapis dengan kunci (DSSE-KMS). AWS KMS Untuk informasi tentang setelan dan opsi enkripsi [default, lihat Menyetel perilaku enkripsi sisi server default untuk bucket S3 di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon](#).

## Penemuan data sensitif

Bagian ini menunjukkan apakah ada pekerjaan penemuan data sensitif yang dikonfigurasi untuk menganalisis objek secara berkala dalam ember setiap hari, mingguan, atau bulanan. Jika nilai untuk bidang Dipantau secara aktif oleh tugas adalah Ya, bucket secara eksplisit disertakan dalam tugas berkala atau bucket sesuai dengan kriteria untuk tugas berkala dalam 24 jam terakhir. Selain itu, status setidaknya satu dari tugas-tugas itu tidak Dibatalkan. Macie memperbarui data ini setiap hari.

Jika setiap tipe tugas penemuan data sensitif (tugas berkala atau tugas satu kali) dikonfigurasi untuk memeriksa bucket, bidang Tugas terbaru menyediakan pengenalan unik untuk tugas yang baru-baru ini mulai berjalan. Bidang Tugas terbaru berjalan menunjukkan ketika tugas itu mulai berjalan.

### Tip

Untuk menampilkan semua temuan data sensitif yang dihasilkan tugas, pilih tautan di bidang Tugas terbaru. Di panel detail tugas yang muncul, pilih Tampilkan hasil di bagian atas panel, lalu pilih Tampilkan temuan.

## Akses publik

Bagian ini menunjukkan apakah bucket dapat diakses publik. Ini juga memberikan rincian berbagai pengaturan tingkat akun dan ember yang menentukan apakah ini masalahnya. Bidang Izin efektif menunjukkan hasil kumulatif dari pengaturan ini:

- Tidak publik – Bucket tidak dapat diakses secara publik.
- Publik – Bucket dapat diakses secara publik.
- Tidak Diketahui – Macie tidak mampu mengevaluasi semua pengaturan akses publik untuk bucket.

Perhatikan jika data ini terbatas untuk pengaturan tingkat akun dan bucket. Ini tidak mencerminkan pengaturan tingkat objek yang memungkinkan akses publik ke objek tertentu dalam bucket.

Untuk mempelajari tentang pengaturan Amazon S3 untuk mengelola akses publik ke bucket dan data bucket, lihat [Identity and access management di Amazon S3](#) dan [Memblokir akses publik ke penyimpanan Amazon S3 Anda](#) di Panduan Pengguna Amazon Simple Storage Service.

## Replikasi

Di bagian ini, bidang Replicated menunjukkan apakah bucket dikonfigurasi untuk mereplikasi objek ke bucket lain. Jika nilai untuk bidang ini adalah Ya, satu atau beberapa aturan replikasi dikonfigurasi dan diaktifkan untuk bucket. Bagian ini kemudian juga mencantumkan ID akun untuk masing-masing Akun AWS yang memiliki bucket tujuan.

Kolom eksternal yang direplikasi menunjukkan apakah bucket dikonfigurasi untuk mereplikasi objek ke bucket Akun AWS yang berada di luar (bukan bagian dari) organisasi Anda. Organisasi adalah kumpulan akun Macie yang dikelola secara terpusat sebagai sekelompok akun terkait melalui AWS Organizations atau dengan undangan Macie. Jika nilai untuk bidang ini adalah Ya, aturan replikasi dikonfigurasi dan diaktifkan untuk bucket, dan aturan dikonfigurasi untuk mereplikasi objek ke bucket yang dimiliki oleh eksternal. Akun AWS

### Note

Dalam kondisi tertentu, Macie mungkin salah menunjukkan bahwa bucket dikonfigurasi untuk mereplikasi objek ke bucket yang dimiliki oleh eksternal. Akun AWS [Hal ini dapat terjadi jika bucket tujuan dibuat berbeda Wilayah AWS selama 24 jam sebelumnya, setelah Macie mengambil bucket dan metadata objek dari Amazon S3 sebagai bagian dari siklus penyegaran harian.](#)

Untuk menyelidiki masalah dengan menggunakan Macie, pilih refresh



)  
untuk mengambil metadata bucket terbaru dari Amazon S3. Kemudian tinjau daftar ID akun di bagian ini. Untuk penyelidikan lebih dalam, gunakan Amazon S3 untuk meninjau aturan replikasi bucket.

Untuk mempelajari tentang opsi Amazon S3 dan pengaturan untuk mereplikasi objek bucket, lihat [Mereplikasi objek](#) di Panduan Pengguna Amazon Simple Storage Service.

## Tag

Jika tag dikaitkan dengan bucket, bagian ini muncul di panel dan mencantumkan tag tersebut. Tag adalah label yang dapat Anda tentukan dan tetapkan ke jenis AWS sumber daya tertentu, termasuk bucket S3. Setiap tanda terdiri dari kunci tanda yang diperlukan dan nilai tanda opsional.

Untuk mempelajari tentang penandaan bucket, lihat [Menggunakan tanda bucket S3 alokasi biaya](#) di Panduan Pengguna Amazon Simple Storage Service.

## Memfilter inventaris bucket S3 Anda dengan Amazon Macie

Untuk mengidentifikasi dan memfokuskan pada bucket yang memiliki karakteristik tertentu, Anda dapat memfilter inventaris bucket S3 Anda di konsol Amazon Macie dan kueri yang Anda kirimkan secara terprogram menggunakan API Amazon Macie. Ketika Anda membuat filter, Anda menggunakan atribut bucket tertentu untuk menentukan kriteria untuk menyertakan atau mengecualikan bucket dari tampilan atau dari hasil kueri. Atribut bucket adalah bidang yang menyimpan metadata tertentu untuk bucket.

Di Macie, filter terdiri atas syarat berjumlah satu atau lebih. Setiap syarat, juga disebut sebagai Kriteria, terdiri dari tiga bagian:

- Bidang berbasis atribut, seperti Nama bucket, Kunci tanda, atau Ditetapkan dalam tugas.
- Operator, seperti sama dengan atau tidak sama dengan.
- Satu atau beberapa nilai. Tipe dan jumlah nilai tergantung pada bidang dan operator yang Anda pilih.

Cara Anda menentukan dan menerapkan syarat filter tergantung pada Anda yang menggunakan konsol Amazon Macie atau API Amazon Macie.

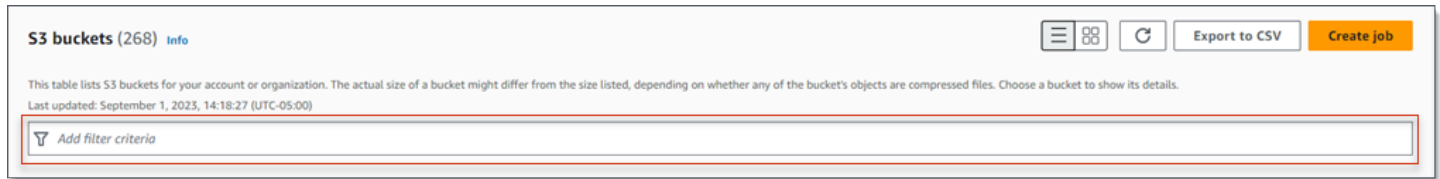
### Topik

- [Memfilter inventaris Anda di konsol Amazon Macie](#)
- [Memfilter inventaris Anda secara terprogram dengan API Amazon Macie](#)

## Memfilter inventaris Anda di konsol Amazon Macie

Jika Anda menggunakan konsol Amazon Macie untuk memfilter inventaris bucket S3, Macie menyediakan opsi untuk membantu Anda memilih bidang, operator, dan nilai untuk kondisi individual.

Anda mengakses opsi ini dengan menggunakan kotak filter pada halaman bucket S3, seperti yang ditunjukkan pada gambar berikut.

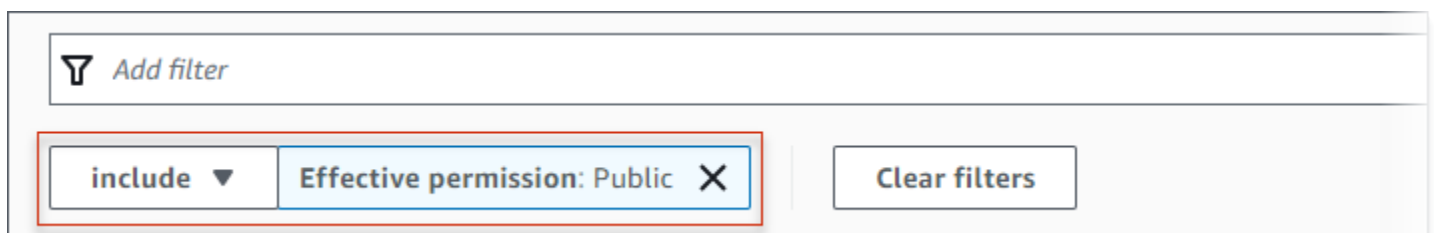


Saat Anda menempatkan kursor di kotak filter, Macie menampilkan daftar bidang yang dapat Anda gunakan dalam kondisi filter. Bidang disusun berdasarkan kategori logis. Misalnya, kategori Common fields mencakup bidang yang menyimpan informasi umum tentang bucket S3. Kategori akses publik mencakup bidang yang menyimpan data tentang berbagai jenis pengaturan akses publik yang dapat diterapkan ke bucket. Bidang diurutkan menurut abjad dalam setiap kategori.

Untuk menambahkan syarat, mulailah dengan memilih bidang dari daftar. Untuk menemukan bidang, jelajahi daftar lengkap, atau memasukkan bagian dari nama bidang untuk mempersempit daftar bidang.

Tergantung pada bidang yang Anda pilih, Macie menampilkan opsi yang berbeda. Opsi mencerminkan tipe dan sifat bidang yang Anda pilih. Misalnya, jika Anda memilih bidang Akses bersama, Macie menampilkan daftar nilai untuk dipilih. Jika Anda memilih bidang nama Bucket, Macie menampilkan kotak teks di mana Anda dapat memasukkan nama bucket S3. Bidang mana pun yang Anda pilih, Macie memandu Anda melalui langkah-langkah untuk menambahkan syarat yang menyertakan pengaturan yang diperlukan untuk bidang tersebut.

Setelah Anda menambahkan kondisi, Macie menerapkan kriteria untuk kondisi dan menampilkan kondisi dalam token filter di bawah kotak filter, seperti yang ditunjukkan pada gambar berikut.




Di dalam contoh ini, syarat dikonfigurasi untuk menyertakan semua bucket yang dapat diakses secara publik, dan untuk mengecualikan semua bucket lainnya. Ini mengembalikan bucket di mana nilai untuk bidang izin Efektif sama dengan Publik.

Saat Anda menambahkan lebih banyak kondisi, Macie menerapkan kriteria mereka dan menampilkannya di bawah kotak filter. Jika Anda menambahkan beberapa syarat, Macie

menggunakan logika AND untuk bergabung dengan syarat dan mengevaluasi kriteria filter. Ini berarti bahwa bucket S3 cocok dengan kriteria filter hanya jika cocok dengan semua kondisi dalam filter. Anda dapat merujuk ke area di bawah kotak filter kapan saja untuk menentukan kriteria mana yang telah Anda terapkan.

Untuk memfilter inventaris Anda dengan menggunakan konsol tersebut

1. [Buka konsol Amazon Macie di https://console.aws.amazon.com/macie/.](https://console.aws.amazon.com/macie/)
2. Di panel navigasi, pilih Bucket S3. Halaman bucket S3 menampilkan inventaris bucket Anda.
3. Di bagian atas halaman, pilih segarkan  secara opsional untuk mengambil metadata bucket terbaru dari Amazon S3.
4. Tempatkan kursor Anda di kotak filter, lalu pilih bidang yang akan digunakan untuk kondisi tersebut.
5. Pilih atau masukkan tipe nilai yang sesuai untuk bidang, simpan tips berikut dalam pikiran.

Tanggal, waktu, dan rentang waktu

Untuk tanggal dan waktu, gunakan kotak Dari dan Kepada untuk menentukan rentang waktu inklusif:

- Untuk menentukan rentang waktu tetap, gunakan kotak Dari dan Kepada untuk menentukan tanggal pertama dan waktu serta tanggal terakhir dan waktu dalam rentang, masing-masing.
- Untuk menentukan rentang waktu relatif yang dimulai pada tanggal dan waktu tertentu dan berakhir pada waktu saat ini, masukkan tanggal dan waktu mulai di kotak Dari, dan menghapus teks apa pun di kotak Untuk.
- Untuk menentukan rentang waktu relatif yang berakhir pada tanggal dan waktu tertentu, masukkan tanggal dan waktu akhir di kotak Untuk, dan menghapus teks apa pun di kotak Dari.

Perhatikan bahwa nilai waktu menggunakan notasi 24 jam. Jika Anda menggunakan pemilih tanggal untuk memilih tanggal, Anda dapat menyempurnakan nilai dengan memasukkan teks secara langsung di kotak Dari dan Kepada.

## Angka dan rentang numerik

Untuk nilai numerik, gunakan kotak Dari dan Kepada untuk memasukkan integer yang menentukan rentang numerik inklusif:

- Untuk menentukan rentang numerik tetap, gunakan kotak Dari dan Kepada untuk menentukan angka terendah dan tertinggi dalam rentang, masing-masing.
- Untuk menentukan rentang numerik tetap yang terbatas pada satu nilai tertentu, masukkan nilai di kedua kotak Dari dan Kepada. Misalnya, untuk memasukkan hanya bucket S3 yang berisi tepat 15 objek, masukkan kotak **15** Dari dan Ke.
- Untuk menentukan rentang numerik relatif yang dimulai pada angka tertentu, masukkan angka dalam kotak Dari, dan jangan memasukkan teks apa pun di kotak Kepada.
- Untuk menentukan rentang numerik relatif yang berakhir pada angka tertentu, masukkan angka dalam kotak Kepada, dan jangan memasukkan teks apa pun di kotak Dari.

## Nilai teks (string)

Untuk tipe nilai ini, masukkan nilai lengkap dan valid untuk bidang. Nilai peka terhadap huruf besar dan kecil.

Perhatikan jika Anda tidak dapat menggunakan nilai parsial atau karakter wildcard dalam tipe nilai ini. Satu-satunya pengecualian adalah bidang Nama bucket. Untuk bidang tersebut, Anda dapat menentukan prefiks daripada nama bucket lengkap. Misalnya, untuk menemukan semua bucket S3 yang namanya dimulai dengan my-S3, masukkan **my-S3** sebagai nilai filter untuk bidang Nama bucket. Jika Anda memasukkan nilai lain, seperti **My-s3** atau **my\***, Macie tidak akan mengembalikan bucket.

6. Setelah Anda selesai menambahkan nilai untuk bidang, pilih Terapkan. Macie menerapkan kriteria filter dan menampilkan kondisi dalam token filter di bawah kotak filter.
7. Ulangi langkah 4 hingga 6 untuk setiap syarat tambahan yang ingin Anda tambahkan.
8. Untuk menghapus kondisi, pilih X di token filter untuk kondisi tersebut.
9. Untuk mengubah kondisi, hapus kondisi dengan memilih X di token filter untuk kondisi tersebut. Lalu ulangi langkah 4 hingga 6 untuk menambahkan syarat dengan pengaturan yang benar.

## Memfilter inventaris Anda secara terprogram dengan API Amazon Macie

Untuk memfilter inventaris bucket S3 Anda secara terprogram, tentukan kriteria filter dalam kueri yang Anda kirimkan menggunakan [DescribeBuckets](#) pengoperasian Amazon Macie API. Operasi ini



mengembalikan susunan objek. Setiap objek berisi data statistik dan informasi lain tentang bucket yang cocok dengan kriteria filter.

Untuk menentukan kriteria filter dalam kueri, sertakan peta syarat filter dalam permintaan Anda. Untuk setiap syarat, tentukan bidang, operator, dan satu atau beberapa nilai untuk bidang tersebut. Tipe dan jumlah nilai tergantung pada bidang dan operator yang Anda pilih. Untuk informasi tentang bidang, operator, dan jenis nilai yang dapat Anda gunakan dalam suatu kondisi, lihat [Sumber Data Amazon S3](#) di Referensi API Amazon Macie.

Contoh berikut menunjukkan kepada Anda cara menentukan kriteria filter dalam kueri yang Anda kirimkan menggunakan [AWS Command Line Interface\(AWS CLI\)](#). Anda juga dapat melakukan ini dengan menggunakan versi terbaru dari alat baris AWS perintah lain atau AWS SDK, atau dengan mengirim permintaan HTTPS langsung ke Macie. Untuk informasi tentang alat AWS dan SDK, lihat [Alat untuk Membangun di AWS](#).

Contoh

- [Contoh 1: Temukan bucket berdasarkan nama bucket](#)
- [Contoh 2: Temukan bucket yang dapat diakses secara publik](#)
- [Contoh 3: Temukan bucket yang berisi objek yang tidak terenkripsi](#)
- [Contoh 4: Temukan bucket yang tidak dipantau oleh tugas](#)
- [Contoh 5: Temukan bucket yang mereplikasi data ke akun eksternal](#)
- [Contoh 6: Temukan bucket berdasarkan beberapa kriteria](#)

Contoh menggunakan perintah [describe-buckets](#). Jika contoh berhasil berjalan, Macie mengembalikan susunan `buckets`. Array berisi objek untuk setiap bucket yang ada di saat ini Wilayah AWS dan cocok dengan kriteria filter. Untuk contoh output ini, perluas bagian berikut.

Contoh dari susunan **buckets**

Dalam contoh ini, `buckets` array memberikan rincian tentang dua bucket yang cocok dengan kriteria filter yang ditentukan dalam kueri.

```
{
  "buckets": [
    {
      "accountId": "123456789012",
      "allowsUnencryptedObjectUploads": "FALSE",
      "bucketArn": "arn:aws:s3:::DOC-EXAMPLE-BUCKET1",
```

```

"bucketCreatedAt": "2020-05-18T19:54:00+00:00",
"bucketName": "DOC-EXAMPLE-BUCKET1",
"classifiableObjectCount": 13,
"classifiableSizeInBytes": 1592088,
"jobDetails": {
  "isDefinedInJob": "TRUE",
  "isMonitoredByJob": "TRUE",
  "lastJobId": "08c81dc4a2f3377fae45c9ddaexample",
  "lastJobRunTime": "2021-04-26T14:55:30.270000+00:00"
},
"lastAutomatedDiscoveryTime": "2022-12-10T19:11:25.364000+00:00",
"lastUpdated": "2022-12-13T07:33:06.337000+00:00",
"objectCount": 13,
"objectCountByEncryptionType": {
  "customerManaged": 0,
  "kmsManaged": 2,
  "s3Managed": 7,
  "unencrypted": 4,
  "unknown": 0
},
"publicAccess": {
  "effectivePermission": "NOT_PUBLIC",
  "permissionConfiguration": {
    "accountLevelPermissions": {
      "blockPublicAccess": {
        "blockPublicAcls": true,
        "blockPublicPolicy": true,
        "ignorePublicAcls": true,
        "restrictPublicBuckets": true
      }
    },
    "bucketLevelPermissions": {
      "accessControlList": {
        "allowsPublicReadAccess": false,
        "allowsPublicWriteAccess": false
      },
      "blockPublicAccess": {
        "blockPublicAcls": true,
        "blockPublicPolicy": true,
        "ignorePublicAcls": true,
        "restrictPublicBuckets": true
      },
      "bucketPolicy": {
        "allowsPublicReadAccess": false,

```

```
        "allowsPublicWriteAccess": false
      }
    }
  },
  "region": "us-east-1",
  "replicationDetails": {
    "replicated": false,
    "replicatedExternally": false,
    "replicationAccounts": []
  },
  "sensitivityScore": 78,
  "serverSideEncryption": {
    "kmsMasterKeyId": null,
    "type": "NONE"
  },
  "sharedAccess": "NOT_SHARED",
  "sizeInBytes": 4549746,
  "sizeInBytesCompressed": 0,
  "tags": [
    {
      "key": "Division",
      "value": "HR"
    },
    {
      "key": "Team",
      "value": "Recruiting"
    }
  ],
  "unclassifiableObjectCount": {
    "fileType": 0,
    "storageClass": 0,
    "total": 0
  },
  "unclassifiableObjectSizeInBytes": {
    "fileType": 0,
    "storageClass": 0,
    "total": 0
  },
  "versioning": true
},
{
  "accountId": "123456789012",
  "allowsUnencryptedObjectUploads": "TRUE",
```

```
"bucketArn": "arn:aws:s3:::DOC-EXAMPLE-BUCKET2",
"bucketCreatedAt": "2020-11-25T18:24:38+00:00",
"bucketName": "DOC-EXAMPLE-BUCKET2",
"classifiableObjectCount": 8,
"classifiableSizeInBytes": 133810,
"jobDetails": {
  "isDefinedInJob": "TRUE",
  "isMonitoredByJob": "FALSE",
  "lastJobId": "188d4f6044d621771ef7d65f2example",
  "lastJobRunTime": "2021-04-09T19:37:11.511000+00:00"
},
"lastAutomatedDiscoveryTime": "2022-12-12T19:11:25.364000+00:00",
"lastUpdated": "2022-12-13T07:33:06.337000+00:00",
"objectCount": 8,
"objectCountByEncryptionType": {
  "customerManaged": 0,
  "kmsManaged": 0,
  "s3Managed": 8,
  "unencrypted": 0,
  "unknown": 0
},
"publicAccess": {
  "effectivePermission": "NOT_PUBLIC",
  "permissionConfiguration": {
    "accountLevelPermissions": {
      "blockPublicAccess": {
        "blockPublicAcls": true,
        "blockPublicPolicy": true,
        "ignorePublicAcls": true,
        "restrictPublicBuckets": true
      }
    },
    "bucketLevelPermissions": {
      "accessControlList": {
        "allowsPublicReadAccess": false,
        "allowsPublicWriteAccess": false
      },
      "blockPublicAccess": {
        "blockPublicAcls": true,
        "blockPublicPolicy": true,
        "ignorePublicAcls": true,
        "restrictPublicBuckets": true
      },
      "bucketPolicy": {
```

```
        "allowsPublicReadAccess": false,
        "allowsPublicWriteAccess": false
    }
}
},
"region": "us-east-1",
"replicationDetails": {
    "replicated": false,
    "replicatedExternally": false,
    "replicationAccounts": []
},
"sensitivityScore": 95,
"serverSideEncryption": {
    "kmsMasterKeyId": null,
    "type": "AES256"
},
"sharedAccess": "EXTERNAL",
"sizeInBytes": 175978,
"sizeInBytesCompressed": 0,
"tags": [
    {
        "key": "Division",
        "value": "HR"
    },
    {
        "key": "Team",
        "value": "Recruiting"
    }
],
"unclassifiableObjectCount": {
    "fileType": 3,
    "storageClass": 0,
    "total": 3
},
"unclassifiableObjectSizeInBytes": {
    "fileType": 2999826,
    "storageClass": 0,
    "total": 2999826
},
"versioning": true
}
]
```

```
}
```

Jika tidak ada bucket yang cocok dengan kriteria filter, Macie mengembalikan array kosong `buckets`.

```
{  
  "buckets": []  
}
```

Contoh 1: Temukan bucket berdasarkan nama bucket

Contoh ini menggunakan perintah [deskripsi-buckets](#) untuk menanyakan metadata untuk semua bucket yang namanya dimulai dengan `my-S3` dan berada di saat ini. Wilayah AWS

Untuk Linux, macOS, atau Unix:

```
$ aws macie2 describe-buckets --criteria '{"bucketName":{"prefix":"my-S3"}}'
```

Untuk Microsoft Windows:

```
C:\> aws macie2 describe-buckets --criteria="{\"bucketName\":{\"prefix\": \"my-S3\"}}"
```

Dengan:

- `bucketName` menentukan nama JSON dari bidang Nama bucket.
- `prefiks` menentukan operator prefiks.
- `my-S3` adalah nilai untuk bidang Nama bucket.

Contoh 2: Temukan bucket yang dapat diakses secara publik

Contoh ini menggunakan [perintah deskripsi-buckets](#) untuk menanyakan metadata untuk bucket yang ada saat ini Wilayah AWS dan, berdasarkan kombinasi setelan izin, dapat diakses publik.

Untuk Linux, macOS, atau Unix:

```
$ aws macie2 describe-buckets --criteria '{"publicAccess.effectivePermission":{"eq":["PUBLIC"]}}'
```

Untuk Microsoft Windows:

```
C:\> aws macie2 describe-buckets --criteria={"publicAccess.effectivePermission": {"eq":["PUBLIC"]}}
```

Dengan:

- *publicAccess.effectivePermission* menentukan nama JSON dari bidang Izin efektif.
- *eq* menentukan operator yang sama.
- *PUBLIK* adalah nilai enumerasi untuk bidang Izin efektif.

Contoh 3: Temukan bucket yang berisi objek yang tidak terenkripsi

Contoh ini menggunakan perintah [deskripsi-buckets](#) untuk menanyakan metadata untuk bucket yang ada di saat ini dan berisi objek yang tidak terenkripsi. Wilayah AWS

Untuk Linux, macOS, atau Unix:

```
$ aws macie2 describe-buckets --criteria '{"objectCountByEncryptionType.unencrypted":{"gte":1}}'
```

Untuk Microsoft Windows:

```
C:\> aws macie2 describe-buckets --criteria={"objectCountByEncryptionType.unencrypted":{"gte":1}}
```

Dengan:

- *objectCountByEncryptionType.unencrypted* menentukan nama JSON dari bidang No encryption.
- *gte* menentukan operator Lebih besar dari atau sama.
- *1* adalah nilai terendah dalam inklusif, rentang numerik relatif untuk bidang Tidak ada enkripsi.

Contoh 4: Temukan bucket yang tidak dipantau oleh tugas

Contoh ini menggunakan [perintah deskripsi-buckets](#) untuk menanyakan metadata untuk bucket yang ada saat ini Wilayah AWS dan tidak terkait dengan pekerjaan penemuan data sensitif berkala.

Untuk Linux, macOS, atau Unix:

```
$ aws macie2 describe-buckets --criteria '{"jobDetails.isMonitoredByJob":{"eq":["FALSE"]}}'
```

Untuk Microsoft Windows:

```
C:\> aws macie2 describe-buckets --criteria="{\"jobDetails.isMonitoredByJob\":{\"eq\":[\"FALSE\"]}}"
```

Dengan:

- *Rincian Pekerjaan. isMonitoredByJob* menentukan nama JSON dari Active monitored by job field.
- *eq* menentukan operator yang sama.
- *SALAH* adalah nilai enumerasi untuk bidang Dipantau secara aktif oleh tugas.

Contoh 5: Temukan bucket yang mereplikasi data ke akun eksternal

Contoh ini menggunakan perintah [describe-buckets](#) untuk menanyakan metadata untuk bucket yang ada saat ini Wilayah AWS dan dikonfigurasi untuk mereplikasi objek ke objek yang bukan bagian dari organisasi Akun AWS Anda.

Untuk Linux, macOS, atau Unix:

```
$ aws macie2 describe-buckets --criteria '{"replicationDetails.replicatedExternally":{"eq":["true"]}}'
```

Untuk Microsoft Windows:

```
C:\> aws macie2 describe-buckets --criteria="{\"replicationDetails.replicatedExternally\":{\"eq\":[\"true\"]}}"
```

Dengan:

- *replicationDetails.replicatedExternally* menentukan nama JSON dari bidang Direplikasi secara eksternal.
- *eq* menentukan operator yang sama.
- *benar* menentukan nilai Boolean untuk bidang Direplikasi secara eksternal.



## Contoh 6: Temukan bucket berdasarkan beberapa kriteria

Contoh ini menggunakan [perintah deskripsi-buckets](#) untuk menanyakan metadata untuk bucket yang ada saat ini Wilayah AWS dan sesuai dengan kriteria berikut: dapat diakses publik berdasarkan kombinasi setelan izin; berisi objek yang tidak terenkripsi; dan tidak terkait dengan pekerjaan penemuan data sensitif berkala.

Untuk Linux, macOS, atau Unix, menggunakan karakter garis miring terbalik (\) untuk meningkatkan keterbacaan:

```
$ aws macie2 describe-buckets \
--criteria '{"publicAccess.effectivePermission":{"eq":
["PUBLIC"]},"objectCountByEncryptionType.unencrypted":
{"gte":1},"jobDetails.isMonitoredByJob":{"eq":["FALSE"]}}'
```

Untuk Microsoft Windows, menggunakan karakter kelanjutan baris tanda sisipan (^) untuk meningkatkan keterbacaan:

```
C:\> aws macie2 describe-buckets ^
--criteria={"publicAccess.effectivePermission\":{"eq\":
["PUBLIC\"]},"objectCountByEncryptionType.unencrypted\":{"gte\":1},
\jobDetails.isMonitoredByJob\":{"eq\":["FALSE\"]}}
```

Dengan:

- *publicAccess.effectivePermission* menentukan nama JSON dari bidang Izin efektif, dan:
  - *eq* menentukan operator yang sama.
  - *PUBLIK* adalah nilai enumerasi untuk bidang Izin efektif.
- *objectCountByEncryptionType.unencrypted* menentukan nama JSON dari bidang No encryption, dan:
  - *gte* menentukan operator Lebih besar dari atau sama.
  - *1* adalah nilai terendah dalam inklusif, rentang numerik relatif untuk bidang Tidak ada enkripsi.
- *Rincian Pekerjaan. isMonitoredByJob* menentukan nama JSON dari Active monitored by job field, dan:
  - *eq* menentukan operator yang sama.
  - *SALAH* adalah nilai enumerasi untuk bidang Dipantau secara aktif oleh tugas.

## Mengizinkan Amazon Macie untuk mengakses bucket S3 dan objek

Saat Anda mengaktifkan Amazon Macie untuk Akun AWS, Macie membuat [peran tertaut layanan](#) yang memberikan Macie izin yang diperlukan untuk memanggil Amazon Simple Storage Service (Amazon S3) dan lainnya atas nama Anda. Layanan AWS Peran tertaut layanan menyederhanakan proses penyiapan Layanan AWS karena Anda tidak perlu menambahkan izin layanan secara manual agar layanan dapat menyelesaikan tindakan atas nama Anda. Untuk mempelajari lebih lanjut tentang jenis peran ini, lihat [Menggunakan peran tertaut layanan](#) di AWS Identity and Access Management Panduan Pengguna.

Kebijakan izin untuk peran tertaut layanan Macie melakukan tindakan yang mencakup pengambilan informasi tentang bucket `AWSServiceRoleForAmazonMacie` S3 dan objek Anda, dan mengambil objek dari bucket S3 Anda, dan mengambil objek dari bucket Anda. Jika Anda adalah administrator Macie untuk organisasi, kebijakan tersebut juga memungkinkan Macie melakukan tindakan ini atas nama Anda untuk akun anggota di organisasi Anda.

Macie menggunakan izin ini untuk melakukan tugas seperti:

- Buat dan pertahankan inventaris bucket S3 Anda
- Menyediakan data statistik dan lainnya tentang ember dan objek dalam ember
- Pantau dan evaluasi bucket untuk kontrol keamanan dan akses
- Analisis objek dalam bucket untuk mendeteksi data sensitif

Dalam kebanyakan kasus, Macie memiliki izin yang dibutuhkan untuk melakukan tugas-tugas ini. Namun, jika bucket S3 memiliki kebijakan bucket yang membatasi, kebijakan mungkin mencegah Macie melakukan beberapa atau semua tugas ini.

Kebijakan bucket adalah berbasis sumber daya AWS Identity and Access Management (kebijakan IAM) yang menentukan tindakan prinsipiel (pengguna, akun, akun, layanan, atau entitas lain) dapat dilakukan pada bucket S3, dan syarat di tempat prinsipiel dapat melakukan tindakan tersebut. Tindakan dan syarat dapat diterapkan pada operasi tingkat bucket, seperti mengambil informasi tentang bucket, dan operasi tingkat objek, seperti mengambil objek dari bucket.

Kebijakan bucket biasanya memberikan atau membatasi akses dengan menggunakan pernyataan `Allow` eksplisit atau pernyataan `Deny` beserta syarat. Misalnya, kebijakan bucket mungkin berisi pernyataan `Allow` atau `Deny` yang menolak akses ke bucket kecuali alamat IP sumber tertentu, Amazon Virtual Private Cloud (Amazon VPC) endpoint, atau VPC yang digunakan untuk mengakses

bucket. Untuk informasi tentang cara menggunakan kebijakan bucket untuk memberikan atau membatasi akses ke bucket, lihat [Kebijakan bucket dan kebijakan pengguna](#) dan [Cara Amazon S3 mengotorisasi permintaan](#) di Panduan Pengguna Amazon Simple Storage Service.

Jika kebijakan bucket menggunakan pernyataan Allow eksplisit, kebijakan tidak mencegah Macie mengambil informasi tentang bucket dan objek bucket, atau mengambil objek dari bucket. Hal ini karena pernyataan Allow di dalam kebijakan izin untuk peran tertaut layanan Macie memberikan izin tersebut.

Namun, jika kebijakan bucket menggunakan Deny pernyataan eksplisit dengan satu atau beberapa syarat, Macie mungkin tidak diizinkan untuk mengambil informasi tentang bucket atau objek bucket, atau mengambil objek bucket. Misalnya, jika kebijakan bucket secara eksplisit menolak akses dari semua sumber kecuali alamat IP tertentu, Macie tidak akan diizinkan untuk menganalisis objek bucket saat Anda menjalankan tugas penemuan data sensitif. Hal ini karena kebijakan bucket yang dibatasi lebih diutamakan dibandingkan pernyataan Allow di dalam kebijakan izin untuk peran tertaut layanan Macie.

Untuk mengizinkan Macie mengakses bucket S3 yang memiliki kebijakan bucket S3 yang memiliki kebijakan bucket S3, Anda dapat menambahkan syarat untuk peran tertaut layanan Macie ke kebijakan bucket S3 yang memiliki kebijakan bucket AWSServiceRoleForAmazonMacie S3. Syarat ini dapat mengecualikan peran tertaut layanan Macie dari pencocokan pembatasan Deny dalam kebijakan. Hal ini dapat dilakukan dengan menggunakan [kunci konteks syarat `aws:PrincipalArn global`](#) dan Amazon Resource Name (ARN) peran tertaut layanan Macie.

Prosedur berikut memandu Anda melalui proses ini dan memberikan contoh.

Untuk menambahkan peran tertaut layanan Macie ke kebijakan bucket

1. Masuk ke AWS Management Console dan buka konsol Amazon S3 di <https://console.aws.amazon.com/s3/>.
2. Di panel navigasi, pilih Bucket.
3. Pilih bucket S3 yang ingin Anda izinkan Macie untuk mengakses.
4. Di tab Izin, di dalam Kebijakan bucket, pilih Edit.
5. Di editor Kebijakan bucket, identifikasi setiap pernyataan Deny yang membatasi akses dan mencegah Macie mengakses bucket atau objek bucket.
6. Dalam setiap Deny pernyataan, tambahkan syarat yang menggunakan kunci konteks syarat `aws:PrincipalArn global` dan tentukan ARN dari peran tertaut layanan Macie untuk Anda.  
Akun AWS

Nilai untuk kunci syarat harus `arn:aws:iam::123456789012:role/aws-service-role/macie.amazonaws.com/AWSServiceRoleForAmazonMacie`, dengan **123456789012** adalah ID akun untuk Akun AWS Anda.

Tempat Anda menambahkan ini ke kebijakan bucket tergantung pada struktur, elemen, dan syarat yang saat ini berisi kebijakan. Untuk mempelajari tentang struktur dan elemen yang didukung, lihat [Kebijakan dan izin di Amazon S3](#) di Panduan Pengguna Amazon Simple Storage Service.

Berikut ini adalah contoh kebijakan bucket yang menggunakan *Deny* pernyataan eksplisit untuk membatasi akses ke bucket S3 bernama DOC-EXAMPLE-BUCKET. Dengan kebijakan saat ini, bucket dapat diakses hanya dari VPC endpoint dengan ID adalah `vpce-1a2b3c4d`. Akses dari semua VPC endpoints lainnya ditolak, termasuk akses dari dan Macie. AWS Management Console

```
{
  "Version": "2012-10-17",
  "Id": "Policy1415115example",
  "Statement": [
    {
      "Sid": "Access from specific VPCE only",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::DOC-EXAMPLE-BUCKET",
        "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
      ],
      "Condition": {
        "StringNotEquals": {
          "aws:SourceVpce": "vpce-1a2b3c4d"
        }
      }
    }
  ]
}
```

Untuk mengubah kebijakan ini dan memungkinkan Macie mengakses bucket S3 dan objek bucket S3, kita dapat menambahkan syarat yang menggunakan [operator StringNotLike syarat](#) dan kunci [konteks syarat `aws:PrincipalArn global`](#). Syarat tambahan ini tidak termasuk peran tertaut layanan Macie dari pencocokan pembatasan Deny.

```

{
  "Version": "2012-10-17",
  "Id": " Policy1415115example ",
  "Statement": [
    {
      "Sid": "Access from specific VPCE and Macie only",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::DOC-EXAMPLE-BUCKET",
        "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
      ],
      "Condition": {
        "StringNotEquals": {
          "aws:SourceVpce": "vpce-1a2b3c4d"
        },
        "StringNotLike": {
          "aws:PrincipalArn": "arn:aws:iam::123456789012:role/aws-service-role/
macie.amazonaws.com/AWSServiceRoleForAmazonMacie"
        }
      }
    }
  ]
}

```

Pada contoh sebelumnya, operator `StringNotLike` syarat menggunakan kunci konteks `aws:PrincipalArn` syarat untuk menentukan ARN dari peran tertaut layanan Macie, di tempat:

- `123456789012` adalah ID akun untuk Akun AWS yang diizinkan untuk menggunakan Macie untuk mengambil informasi tentang bucket dan objek bucket, dan mengambil objek dari bucket.
- `macie.amazonaws.com` adalah pengidentifikasi untuk prinsipiel layanan Macie.
- `AWSServiceRoleForAmazonMacie` ini adalah nama peran tertaut layanan Macie.

Kami menggunakan operator `StringNotLike` karena kebijakan sudah menggunakan operator `StringNotEquals`. Kebijakan dapat menggunakan operator `StringNotEquals` hanya sekali.

Untuk contoh kebijakan tambahan dan informasi detail tentang mengelola akses ke sumber daya Amazon S3, lihat [Identity and access management di Amazon S3](#) di Panduan Pengguna Amazon Simple Storage Service.

# Menemukan data sensitif dengan Amazon Macie

Dengan Amazon Macie, Anda dapat mengotomatiskan penemuan, pencatatan, dan pelaporan data sensitif di data estate Amazon Simple Storage Service (Amazon S3) Anda. Anda dapat melakukannya dengan dua cara: dengan mengonfigurasi Macie untuk melakukan penemuan data sensitif otomatis untuk akun atau organisasi Anda, dan dengan membuat dan menjalankan pekerjaan penemuan data sensitif untuk akun atau organisasi Anda.

## Penemuan data sensitif otomatis

Penemuan data sensitif otomatis memberikan visibilitas luas ke tempat data sensitif berada di kawasan data Amazon S3 Anda. Dengan opsi ini, Macie mengevaluasi inventaris bucket S3 Anda setiap hari dan menggunakan teknik pengambilan sampel untuk mengidentifikasi dan memilih objek S3 representatif dari bucket Anda. Macie kemudian mengambil dan menganalisis objek yang dipilih, memeriksa mereka untuk data sensitif. Untuk informasi selengkapnya, lihat [Melakukan penemuan data sensitif otomatis](#).

## Lowongan kerja penemuan data sensitif

Pekerjaan penemuan data sensitif memberikan analisis yang lebih dalam dan lebih bertarget. Dengan opsi ini, Anda menentukan luas dan kedalaman analisis—bucket S3 spesifik yang Anda pilih atau bucket yang sesuai dengan kriteria tertentu. Anda juga dapat memperbaiki cakupan analisis dengan memilih opsi seperti kriteria khusus yang berasal dari properti objek S3. Selain itu, Anda dapat mengonfigurasi pekerjaan untuk dijalankan hanya sekali untuk analisis dan penilaian sesuai permintaan, atau secara berulang untuk analisis, penilaian, dan pemantauan berkala. Untuk informasi selengkapnya, lihat [Menjalankan tugas penemuan data sensitif](#).

Dengan opsi, penemuan data sensitif otomatis, atau pekerjaan penemuan data sensitif, Anda dapat menganalisis objek S3 dengan menggunakan pengidentifikasi data terkelola yang disediakan Macie, pengidentifikasi data kustom yang Anda tentukan, atau kombinasi keduanya. Anda juga dapat menyempurnakan analisis dengan menggunakan daftar izinkan.

## Pengidentifikasi data terkelola

Pengidentifikasi data terkelola adalah kriteria dan teknik bawaan yang dirancang untuk mendeteksi jenis data sensitif tertentu—misalnya, nomor kartu kredit, AWS kunci akses rahasia, atau nomor paspor untuk negara atau wilayah tertentu. Mereka dapat mendeteksi daftar tipe data sensitif yang besar dan berkembang untuk banyak negara dan wilayah, termasuk beberapa

jenis data kredensial, informasi keuangan, dan informasi identitas pribadi (PII). Untuk informasi selengkapnya, lihat [Menggunakan pengidentifikasi data terkelola](#).

## Pengidentifikasi data khusus

Pengidentifikasi data khusus menentukan kriteria khusus untuk mendeteksi data sensitif. Setiap pengenalan data kustom menentukan ekspresi reguler (regex) yang mendefinisikan pola teks untuk mencocokkan dan, opsional, urutan karakter dan aturan kedekatan yang menyempurnakan hasil. Anda dapat menggunakannya untuk mendeteksi data sensitif yang mencerminkan skenario tertentu, kekayaan intelektual, atau data kepemilikan Anda—misalnya, ID karyawan, nomor akun pelanggan, atau klasifikasi data internal. Untuk informasi selengkapnya, lihat [Membangun pengidentifikasi data kustom](#).

## Izinkan daftar

Di Macie, izinkan daftar menentukan pola teks dan teks untuk diabaikan di objek S3, biasanya pengecualian data sensitif untuk skenario atau lingkungan tertentu Anda—misalnya, nama publik atau nomor telepon untuk organisasi Anda, atau data sampel yang digunakan organisasi Anda untuk pengujian. Jika Macie menemukan teks yang cocok dengan entri atau pola dalam daftar izinkan, Macie tidak melaporkan kejadian teks tersebut, meskipun teks tersebut cocok dengan kriteria pengenalan data terkelola atau pengenalan data kustom. Untuk informasi selengkapnya, lihat [Mendefinisikan pengecualian data sensitif dengan daftar izinkan](#).

Ketika Macie menganalisis objek S3, Macie mengambil versi terbaru objek dari Amazon S3, dan kemudian memeriksa konten objek untuk data sensitif. Macie dapat menganalisis objek jika berikut ini benar:

- Objek menggunakan file atau format penyimpanan yang didukung dan disimpan langsung di Amazon S3 menggunakan kelas penyimpanan yang didukung. Untuk informasi selengkapnya, lihat [Kelas dan format penyimpanan yang didukung](#).
- Jika objek dienkripsi, itu dienkripsi dengan kunci yang dapat diakses Macie dan diizinkan untuk digunakan. Untuk informasi selengkapnya, lihat [Menganalisis objek S3 terenkripsi](#).
- Jika objek disimpan dalam bucket yang memiliki kebijakan bucket yang membatasi, kebijakan memungkinkan Macie untuk mengakses objek dalam bucket. Untuk informasi selengkapnya, lihat [Mengizinkan Macie untuk mengakses bucket S3 dan objek](#).

Untuk membantu Anda memenuhi dan menjaga kepatuhan terhadap persyaratan keamanan dan privasi data Anda, Macie menghasilkan catatan data sensitif yang ditemukannya dan analisis

yang dilakukannya—temuan data sensitif dan hasil penemuan data sensitif. SEBUAH temuan data sensitif adalah laporan rinci dari data sensitif yang Macie ditemukan di objek S3. Hasil temuan data sensitif adalah catatan yang mencatat detail tentang analisis terhadap suatu objek. Setiap jenis rekaman mematuhi skema standar, yang dapat membantu Anda query, memantau, dan memproses mereka dengan menggunakan aplikasi lain, layanan, dan sistem yang diperlukan.

### Tip

Meskipun Macie dioptimalkan untuk Amazon S3, Anda dapat menggunakannya untuk menemukan data sensitif dalam sumber daya yang saat ini Anda simpan di tempat lain. Anda dapat melakukan ini dengan memindahkan data ke Amazon S3 sementara atau permanen. Misalnya, ekspor Amazon Relational Database Service atau snapshot Amazon Aurora ke Amazon S3 dalam format Apache Parquet. Atau ekspor tabel Amazon DynamoDB ke Amazon S3. Kemudian Anda dapat membuat tugas untuk menganalisis data di Amazon S3.

## Topik

- [Menggunakan pengidentifikasi data terkelola di Amazon Macie](#)
- [Membangun pengidentifikasi data kustom di Amazon Macie](#)
- [Mendefinisikan pengecualian data sensitif dengan Amazon Macie memungkinkan daftar](#)
- [Melakukan penemuan data sensitif otomatis dengan Amazon Macie](#)
- [Menjalankan tugas penemuan data sensitif di Amazon Macie](#)
- [Menganalisis objek Amazon S3 terenkripsi dengan Amazon Macie](#)
- [Menyimpan dan mempertahankan hasil penemuan data sensitif dengan Amazon Macie](#)
- [Kelas dan format penyimpanan yang didukung oleh Amazon Macie](#)

## Menggunakan pengidentifikasi data terkelola di Amazon Macie

Amazon Macie menggunakan kombinasi kriteria dan teknik, termasuk pembelajaran mesin dan pencocokan pola, untuk mendeteksi data sensitif di objek Amazon Simple Storage Service (Amazon S3). Kriteria dan teknik ini, secara kolektif disebut sebagai pengidentifikasi data terkelola, dapat mendeteksi daftar besar dan berkembang jenis data sensitif untuk banyak negara dan wilayah, termasuk beberapa jenis data kredensial, informasi keuangan, informasi kesehatan pribadi (PHI), dan informasi pribadi (PII). Setiap pengidentifikasi data terkelola dirancang untuk mendeteksi jenis data



sensitif tertentu—misalnya, AWS kunci akses rahasia, nomor kartu kredit, atau nomor paspor untuk negara atau wilayah tertentu.

Macie dapat mendeteksi kategori data sensitif berikut dengan menggunakan pengidentifikasi data terkelola:

- Kredensial, untuk data kredensial seperti kunci pribadi dan AWS kunci akses rahasia.
- Informasi keuangan, untuk data keuangan seperti nomor kartu kredit dan nomor rekening bank.
- Informasi pribadi, untuk PHI seperti asuransi kesehatan dan nomor identifikasi medis, dan PII seperti nomor identifikasi SIM dan nomor paspor.

Dalam setiap kategori, Macie dapat mendeteksi beberapa jenis data sensitif. Topik dalam daftar bagian ini dan menjelaskan setiap jenis dan persyaratan yang relevan untuk mendeteksi itu. Untuk setiap jenis, mereka juga menunjukkan pengenal unik (ID) untuk pengenal data terkelola yang dirancang untuk mendeteksi data. Ketika Anda [membuat pekerjaan penemuan data sensitif](#) atau [mengkonfigurasi pengaturan penemuan data sensitif otomatis](#), Anda dapat menggunakan ID ini untuk menentukan pengidentifikasi data terkelola yang ingin digunakan Macie saat menganalisis objek S3.

Untuk daftar pengidentifikasi data terkelola yang kami rekomendasikan untuk pekerjaan, lihat [Pengidentifikasi data terkelola direkomendasikan untuk pekerjaan penemuan data sensitif](#). Untuk daftar pengidentifikasi data terkelola yang kami rekomendasikan dan digunakan secara default untuk penemuan data sensitif otomatis, lihat [Pengaturan default untuk penemuan data sensitif otomatis](#).

Topik

- [Persyaratan kata kunci untuk pengidentifikasi data terkelola Amazon Macie](#)
- [Referensi cepat: Pengidentifikasi data terkelola Amazon Macie](#)
- [Referensi terperinci: Pengidentifikasi data terkelola Amazon Macie](#)

## Persyaratan kata kunci untuk pengidentifikasi data terkelola Amazon Macie

Untuk mendeteksi jenis data sensitif tertentu dengan menggunakan pengenal data terkelola, Amazon Macie mengharuskan kata kunci berada di dekat data. Jika ini adalah kasus untuk jenis data tertentu, topik selanjutnya di bagian ini menunjukkan persyaratan kata kunci untuk data tersebut.

Jika kata kunci harus berada di dekat tipe data tertentu, kata kunci biasanya harus berada dalam 30 karakter (inklusif) dari data tersebut. Persyaratan kedekatan tambahan bervariasi berdasarkan jenis file atau format penyimpanan objek Amazon Simple Storage Service (Amazon S3).

### Terstruktur, data kolumnar

Untuk data kolumnar, kata kunci harus menjadi bagian dari nilai yang sama atau dalam nama kolom atau bidang yang menyimpan nilai. Hal ini berlaku untuk buku kerja Microsoft Excel, file CSV, dan file TSV.

Misalnya, jika nilai untuk bidang berisi kedua SSN dan angka sembilan digit yang menggunakan sintaks Nomor Jaminan Sosial (SSN) US, Macie dapat mendeteksi SSN di bidang. Demikian pula, jika nama kolom berisi SSN, Macie dapat mendeteksi setiap SSN di kolom. Macie memperlakukan nilai-nilai dalam kolom yang berada di dekat kata kunci SSN.

### Terstruktur, data berbasis catatan

Untuk data berbasis catatan, kata kunci harus menjadi bagian dari nilai yang sama atau dalam nama elemen di dalam jalur ke bidang atau susunan yang menyimpan nilai. Hal ini berlaku untuk kontainer objek Apache Avro, file Apache Parquet, file JSON, dan file JSON Lines.

Misalnya, jika nilai untuk bidang berisi keduanyakredensial dan urutan karakter yang menggunakan sintaks AWS kunci akses rahasia, Macie dapat mendeteksi kunci di lapangan. Demikian pula, jika path ke field adalah `$.credentials.aws.key`, Macie dapat mendeteksi AWS kunci akses rahasia di lapangan. Macie memperlakukan nilai di lapangan sebagai berada di dekat kata kunci kredensial.

### Data tidak terstruktur

Tidak ada persyaratan kedekatan tambahan untuk file Adobe Portable Document Format, dokumen Microsoft Word, pesan email, dan file teks non-biner selain file CSV, JSON, JSON Lines, dan TSV. Kata kunci biasanya harus berada dalam 30 karakter (inklusif) dari data tersebut. Hal ini termasuk data terstruktur apa pun, seperti tabel, dalam tipe file ini.

Kata kunci tidak sensitif terhadap kasus. Selain itu, jika kata kunci berisi spasi, Macie secara otomatis mencocokkan variasi kata kunci yang tidak berisi spasi atau mengandung garis bawah (`_`) atau tanda hubung (`-`), bukan spasi. Dalam kasus tertentu, Macie juga memperluas atau menyingkat kata kunci untuk mengatasi variasi umum kata kunci.

Untuk demonstrasi tentang cara kata kunci menyediakan konteks dan membantu Macie mendeteksi jenis data sensitif tertentu, tonton video berikut: [Cara Amazon Macie menggunakan kata kunci untuk menemukan data sensitif](#).

## Referensi cepat: Pengidentifikasi data terkelola Amazon Macie

Di Amazon Macie, pengenalan data terkelola adalah seperangkat kriteria dan teknik bawaan yang dirancang untuk mendeteksi jenis data sensitif tertentu—misalnya, nomor kartu kredit, kunci akses AWS rahasia, atau nomor paspor untuk negara atau wilayah tertentu. Pengidentifikasi ini dapat mendeteksi daftar tipe data sensitif yang besar dan terus bertambah untuk banyak negara dan wilayah, termasuk berbagai jenis data kredensial, informasi keuangan, informasi kesehatan pribadi (PHI), dan informasi identitas pribadi (PII).

Tabel berikut mencantumkan semua pengidentifikasi data terkelola yang saat ini disediakan Macie, yang diatur berdasarkan tipe data sensitif. Untuk setiap jenis, ini memberikan informasi berikut:

- **Kategori data sensitif** — Menentukan kategori umum data sensitif yang mencakup jenis: Kredensial, untuk data kredensial seperti kunci pribadi; Informasi keuangan, untuk data keuangan seperti nomor kartu kredit dan nomor rekening bank; Informasi pribadi: PHI untuk informasi kesehatan pribadi seperti asuransi kesehatan dan nomor identifikasi medis; dan, Informasi pribadi: PII untuk informasi pribadi seperti nomor identifikasi SIM dan nomor paspor.
- **ID pengenalan data terkelola** - Menentukan pengenalan unik (ID) untuk satu atau beberapa pengidentifikasi data terkelola yang dirancang untuk mendeteksi data. Saat membuat pekerjaan penemuan data sensitif atau mengonfigurasi setelan penemuan data sensitif otomatis, Anda dapat menggunakan ID ini untuk menentukan pengidentifikasi data terkelola mana yang ingin digunakan Macie saat menganalisis data. Untuk daftar pengidentifikasi data terkelola yang kami rekomendasikan untuk pekerjaan, lihat [Pengidentifikasi data terkelola direkomendasikan untuk pekerjaan penemuan data sensitif](#). Untuk daftar pengidentifikasi data terkelola yang kami rekomendasikan untuk penemuan data sensitif otomatis, lihat [Pengaturan default untuk penemuan data sensitif otomatis](#).
- **Kata kunci diperlukan** - Menentukan apakah deteksi memerlukan kata kunci untuk berada di dekat data. Untuk informasi tentang bagaimana Macie menggunakan kata kunci saat menganalisis data, lihat [Persyaratan kata kunci](#).
- **Negara dan wilayah** - Menentukan negara atau wilayah mana pengidentifikasi data terkelola yang berlaku dirancang untuk. Jika pengidentifikasi data terkelola tidak dirancang untuk negara atau wilayah tertentu, nilai ini adalah Any.

Untuk meninjau detail tambahan tentang pengidentifikasi data terkelola untuk jenis data sensitif tertentu, pilih jenisnya.

Tipe data sensitif	Kategori data sensitif	ID pengenal data terkelola	Diperlukan kata kunci	Negara dan wilayah
<a href="#">AWS secret access key</a>	Kredensial	AWS_CREDENTIALS	Ya	Setiap
<a href="#">Nomor rekening bank</a>	Informasi keuangan	BANK_ACCOUNT_NUMBER(untuk Kanada dan AS)	Ya	Kanada, AS
<a href="#">Nomor Rekening Bank Dasar (BBAN)</a>	Informasi keuangan	Tergantung pada negara atau wilayah: FRANCE_BANK_ACCOUNT_NUMBER, GERMANY_BANK_ACCOUNT_NUMBER, ITALY_BANK_ACCOUNT_NUMBER, SPAIN_BANK_ACCOUNT_NUMBER, UK_BANK_ACCOUNT_NUMBER	Ya	Prancis, Jerman, Italia, Spanyol, Inggris
<a href="#">Tanggal lahir</a>	Informasi pribadi: PII	DATE_OF_BIRTH	Ya	Setiap
<a href="#">Tanggal kedaluwarsa kartu kredit</a>	Informasi keuangan	CREDIT_CARD_EXPIRATION	Ya	Setiap
<a href="#">Data strip magnetik kartu kredit</a>	Informasi keuangan	CREDIT_CARD_MAGNETIC_STRIPE	Ya	Setiap
<a href="#">Nomor kartu kredit</a>	Informasi keuangan	CREDIT_CARD_NUMBER(untuk nomor kartu kredit yang berdekatan dengan kata kunci), CREDIT_CARD_NUMBER	Bervariasi	Setiap

Tipe data sensitif	Kategori data sensitif	ID pengenal data terkelola	Diperlukan kata kunci	Negara dan wilayah
		_(NO_KEYWORD) (untuk nomor kartu kredit yang tidak berdekatan dengan kata kunci)		
<a href="#">Kode verifikasi kartu kredit</a>	Informasi keuangan	CREDIT_CARD_SECURITY_CODE	Ya	Setiap

Tipe data sensitif	Kategori data sensitif	ID pengenal data terkelola	Diperlukan kata kunci	Negara dan wilayah
<a href="#">Nomor identifikasi lisensi</a>	Informasi pribadi: PII	Tergantung pada negara atau wilayah:  AUSTRALIA_DRIVERS_LICENSE, AUSTRIA_DRIVERS_LICENSE, BELGIUM_DRIVERS_LICENSE, BULGARIA_DRIVERS_LICENSE, CANADA_DRIVERS_LICENSE, CROATIA_DRIVERS_LICENSE, CYPRUS_DRIVERS_LICENSE, CZECHIA_DRIVERS_LICENSE, DENMARK_DRIVERS_LICENSE, DRIVERS_LICENSE (for the US), ESTONIA_DRIVERS_LICENSE, FINLAND_DRIVERS_LICENSE, FRANCE_DRIVERS_LICENSE, GERMANY_DRIVERS_LICENSE, GREECE_DRIVERS_LICENSE, HUNGARY_DRIVERS_LICENSE, INDIA_DRIVERS_LICENSE, IRELAND_DRIVERS_LICENSE, ITALY_DRIVERS_LICENSE, LATVIA_DRIVERS_LICENSE, LITHUANIA_DRIVERS_LICENSE, LUXEMBOURG_DRIVERS_LICENSE, MALTA_DRIVERS_LICENSE, NETHERLANDS_DRIVERS_LICENSE, POLAND_DRIVERS_LICENSE, PORTUGAL_DRIVERS_LICENSE, ROMANIA_DRIVERS_LICENSE, SLOVAKIA_DRIVERS_LICENSE, SLOVENIA_DRIVERS_LICENSE, SPAIN_DRIVERS_LICENSE	Ya	Australia, Austria, Belgia, Bulgaria, Kanada, Kroasia, Siprus, Republik Ceko, Denmark, Estonia, Finlandia, Prancis, Jerman, Yunani, Hongaria, India, Irlandia, Italia, Latvia, Lituania, Luksemburg, Malta, Belanda, Polandia, Portugal, Rumania, Slovakia, Slovenia, Spanyol, Swedia, Inggris, AS

Tipe data sensitif	Kategori data sensitif	ID pengenalan data terkelola	Diperlukan kata kunci	Negara dan wilayah
		NSE, SWEDEN_DRIVERS_LICENSE, UK_DRIVERS_LICENSE		
<a href="#">Nomor Registrasi Badan Penegakan Narkoba (DEA)</a>	Informasi pribadi: PHI	US_DRUG_ENFORCEMENT_AGENCY_NUMBER	Ya	AS
<a href="#">Nomor Roll Pemilu</a>	Informasi pribadi: PII	UK_ELECTORAL_ROLL_NUMBER	Ya	UK
<a href="#">Nama lengkap</a>	Informasi pribadi: PII	NAME	Tidak	Apa saja, jika nama menggunakan set karakter Latin
<a href="#">Koordinat Sistem Pemosisian Global (GPS)</a>	Informasi pribadi: PII	LATITUDE_LONGITUDE	Ya	Apa saja, jika koordinat berada di dekat kata kunci bahasa Inggris
<a href="#">Kunci API Google Cloud</a>	Kredensial	GCP_API_KEY	Ya	Setiap

Tipe data sensitif	Kategori data sensitif	ID pengenalan data terkelola	Diperlukan kata kunci	Negara dan wilayah
<a href="#">Nomor Klaim Asuransi Kesehatan (HICN)</a>	Informasi pribadi: PHI	USA_HEALTH_INSURANCE_CLAIM_NUMBER	Ya	AS
<a href="#">Nomor asuransi atau identifikasi medis</a>	Informasi pribadi: PHI	Tergantung pada negara atau wilayah: CANADA_HEALTH_NUMBER, EUROPEAN_HEALTH_INSURANCE_CARD_NUMBER, FINLAND_EUROPEAN_HEALTH_INSURANCE_NUMBER, FRANCE_HEALTH_INSURANCE_NUMBER, UK_NHS_NUMBER, USA_MEDICARE_BENEFICIARY_IDENTIFIER	Ya	Canada, EU, Finland, France, UK, US
<a href="#">Kode Sistem Pengkodean Prosedur Umum Kesehatan (HCPCS)</a>	Informasi pribadi: PHI	USA_HEALTHCARE_PROCEDURE_CODE	Ya	AS
<a href="#">Header Otorisasi Dasar HTTP</a>	Kredensial	HTTP_BASIC_AUTH_HEADER	Tidak	Setiap
<a href="#">HTTP cookie</a>	Informasi pribadi: PII	HTTP_COOKIE	Tidak	Setiap



Tipe data sensitif	Kategori data sensitif	ID pengenalan data terkelola	Diperlukan kata kunci	Negara dan wilayah
<a href="#">Nomor Rekening Bank Internasional (IBAN)</a>	Informasi keuangan	Tergantung pada negara atau wilayah: ALBANIA_BANK_ACCOUNT_NUMBER, ANDORRA_BANK_ACCOUNT_NUMBER, BOSNIA_AND_HERZEGOVINA_BANK_ACCOUNT_NUMBER, BRAZIL_BANK_ACCOUNT_NUMBER, BULGARIA_BANK_ACCOUNT_NUMBER, COSTA_RICA_BANK_ACCOUNT_NUMBER, CROATIA_BANK_ACCOUNT_NUMBER, CYPRUS_BANK_ACCOUNT_NUMBER, CZECH_REPUBLIC_BANK_ACCOUNT_NUMBER, DENMARK_BANK_ACCOUNT_NUMBER, DOMINICAN_REPUBLIC_BANK_ACCOUNT_NUMBER, EGYPT_BANK_ACCOUNT_NUMBER, ESTONIA_BANK_ACCOUNT_NUMBER, FAROE_ISLANDS_BANK_ACCOUNT_NUMBER, FINLAND_BANK_ACCOUNT_NUMBER, FRANCE_BANK_ACCOUNT_NUMBER, GEORGIA_BANK_ACCOUNT_NUMBER, GERMANY_BANK_ACCOUNT_NUMBER, GREECE_BANK_ACCOUNT_NUMBER, GREENLAND_BANK_ACCOUNT_NUMBER, HUNGARY_BANK_ACCOUNT_NUMBER, ICELAND_BANK_ACCOUNT_NUMBER, IRELAND_BANK_ACCOUNT_NUMBER	Tidak	Albania, Andorra, Bosnia-Herzegovina, Brasil, Bulgaria, Kosta Rika, Kroasia, Siprus, Republik Ceko, Denmark, Republik Dominika, Mesir, Estonia, Kepulauan Faroe, Finlandia, Prancis, Georgia, Jerman, Yunani, Greenland, Hongaria, Islandia, Irlandia, Italia, Yordania, Kosovo, Liechtenstein,

Tipe data sensitif	Kategori data sensitif	ID pengenalan data terkelola	Diperlukan kata kunci	Negara dan wilayah
		, ITALY_BANK_ACCOUNT_NUMBER, JORDAN_BANK_ACCOUNT_NUMBER, KOSOVO_BANK_ACCOUNT_NUMBER, LIECHTENSTEIN_BANK_ACCOUNT_NUMBER, LITHUANIA_BANK_ACCOUNT_NUMBER, MALTA_BANK_ACCOUNT_NUMBER, MAURITANIA_BANK_ACCOUNT_NUMBER, MAURITIUS_BANK_ACCOUNT_NUMBER, MONACO_BANK_ACCOUNT_NUMBER, MONTENEGRO_BANK_ACCOUNT_NUMBER, NETHERLANDS_BANK_ACCOUNT_NUMBER, NORTH_MACEDONIA_BANK_ACCOUNT_NUMBER, POLAND_BANK_ACCOUNT_NUMBER, PORTUGAL_BANK_ACCOUNT_NUMBER, SAN_MARINO_BANK_ACCOUNT_NUMBER, SENEGAL_BANK_ACCOUNT_NUMBER, SERBIA_BANK_ACCOUNT_NUMBER, SLOVAKIA_BANK_ACCOUNT_NUMBER, SLOVENIA_BANK_ACCOUNT_NUMBER, SPAIN_BANK_ACCOUNT_NUMBER, SWEDEN_BANK_ACCOUNT_NUMBER, SWITZERLAND_BANK_ACCOUNT_NUMBER, TIMOR_LESTE_BANK_ACCOUNT_NUMBER, TUNISIA_BANK_ACCOUNT_NUMBER, TURKIYE_BANK_ACCOUNT_NUMBER, UK_BANK_ACCOUNT_NUMBER,		Lithuania, Malta, Mauritania, Mauritius, Monako, Montenegro, Belanda, Makedonia Utara, Polandia, Portugal, San Marino, Senegal, Serbia, Slovakia, Slovenia, Spanyol, Swedia, Swiss, Timor-Leste, Tunisia, Türkiye, Inggris, Ukraina, Uni Emirat Arab, Kepulauan Virgin (Inggris)

Tipe data sensitif	Kategori data sensitif	ID pengenal data terkelola	Diperlukan kata kunci	Negara dan wilayah
		UKRAINE_BANK_ACCOUNT_NUMBER, UNITED_ARAB_EMIRATES_BANK_ACCOUNT_NUMBER, VIRGIN_ISLANDS_BANK_ACCOUNT_NUMBER (untuk Kepulauan Virgin Britania Raya)		
<a href="#">Token Web JSON (JWT)</a>	Kredensial	JSON_WEB_TOKEN	Tidak	Setiap
<a href="#">Alamat surat-menyurat</a>	Informasi pribadi: PII	ADDRESS, BRAZIL_CEP_CODE (untuk Pos Código de Endereçamento Brasil)	Bervariasi	Australia, Brasil, Kanada, Prancis, Jerman, Italia, Spanyol, Inggris, AS
<a href="#">Kode Obat Nasional (NDC)</a>	Informasi pribadi: PHI	USA_NATIONAL_DRUG_CODE	Ya	AS
<a href="#">Nomor identifikasi nasional</a>	Informasi pribadi: PII	Tergantung pada negara atau wilayah: BRAZIL_RG_NUMBER, FRANCE_NATIONAL_IDENTIFICATION_NUMBER, GERMANY_NATIONAL_IDENTIFICATION_NUMBER, INDIA_AADHAAR_NUMBER, ITALY_NATIONAL_IDENTIFICATION_NUMBER, SPAIN_DNI_NUMBER	Ya	Brasil, Prancis, Jerman, India, Italia, Spanyol

Tipe data sensitif	Kategori data sensitif	ID pengenalan data terkelola	Diperlukan kata kunci	Negara dan wilayah
<a href="#">Nomor Asuransi Nasional (NINO)</a>	Informasi pribadi: PII	UK_NATIONAL_INSURANCE_NUMBER	Ya	UK
<a href="#">Pengenalan Penyedia Nasional (NPI)</a>	Informasi pribadi: PHI	USA_NATIONAL_PROVIDER_IDENTIFIER	Ya	AS
<a href="#">Kunci pribadi OpenSSH</a>	Kredensial	OPENSSSH_PRIVATE_KEY	Tidak	Setiap
<a href="#">Nomor paspor</a>	Informasi pribadi: PII	Tergantung pada negara atau wilayah: CANADA_PASSPORT_NUMBER, FRANCE_PASSPORT_NUMBER, GERMANY_PASSPORT_NUMBER, ITALY_PASSPORT_NUMBER, SPAIN_PASSPORT_NUMBER, UK_PASSPORT_NUMBER, USA_PASSPORT_NUMBER	Ya	Canada, France, Germany, Italy, Spain, UK, US
<a href="#">Nomor tempat tinggal permanen</a>	Informasi pribadi: PII	CANADA_NATIONAL_IDENTIFICATION_NUMBER	Ya	Kanada
<a href="#">Kunci pribadi PGP</a>	Kredensial	PGP_PRIVATE_KEY	Tidak	Setiap

Tipe data sensitif	Kategori data sensitif	ID pengenalan data terkelola	Diperlukan kata kunci	Negara dan wilayah
<a href="#">Nomor telepon</a>	Informasi pribadi: PII	Tergantung pada negara atau wilayah: BRAZIL_PHONE_NUMBER, FRANCE_PHONE_NUMBER, GERMANY_PHONE_NUMBER, ITALY_PHONE_NUMBER, PHONE_NUMBER (for Canada and the US), SPAIN_PHONE_NUMBER, UK_PHONE_NUMBER	Bervariasi	Brazil, Canada, France, Germany, Italy, Spain, UK, US
<a href="#">Kunci pribadi Standar Kriptografi Kunci Publik (PKCS)</a>	Kredensial	PKCS	Tidak	Setiap
<a href="#">Kunci pribadi PuTTY</a>	Kredensial	PUTTY_PRIVATE_KEY	Tidak	Setiap
<a href="#">Nomor Asuransi Sosial (SIN)</a>	Informasi pribadi: PII	CANADA_SOCIAL_INSURANCE_NUMBER	Ya	Kanada
<a href="#">Nomor Jaminan Sosial (SSN)</a>	Informasi pribadi: PII	Tergantung pada negara atau wilayah: SPAIN_SOCIAL_SECURITY_NUMBER, USA_SOCIAL_SECURITY_NUMBER	Ya	Spain, US

Tipe data sensitif	Kategori data sensitif	ID pengenalan data terkelola	Diperlukan kata kunci	Negara dan wilayah
<a href="#">the section called “Kunci API Stripe”</a>	Kredensial	STRIPE_CREDENTIALS	Tidak	Setiap
<a href="#">Nomor identifikasi wajib pajak atau referensi</a>	Informasi pribadi: PII	Tergantung pada negara atau wilayah:  AUSTRALIA_TAX_FILE_NUMBER, BRAZIL_CNPJ_NUMBER, BRAZIL_CPF_NUMBER, FRANCE_TAX_IDENTIFICATION_NUMBER, GERMANY_TAX_IDENTIFICATION_NUMBER, INDIA_PERMANENT_ACCOUNT_NUMBER, ITALY_NATIONAL_IDENTIFICATION_NUMBER, SPAIN_NIE_NUMBER, SPAIN_NIF_NUMBER, SPAIN_TAX_IDENTIFICATION_NUMBER, UK_TAX_IDENTIFICATION_NUMBER, USA_INDIVIDUAL_TAX_IDENTIFICATION_NUMBER	Ya	Australia, Brasil, Prancis, Jerman, India, Italia, Spanyol, Inggris, AS
<a href="#">Pengidentifikasi perangkat unik (UDI)</a>	Informasi pribadi: PHI	MEDICAL_DEVICE_UDI	Ya	AS

Tipe data sensitif	Kategori data sensitif	ID pengenal data terkelola	Diperlukan kata kunci	Negara dan wilayah
<a href="#">Nomor identifikasi kendaraan (VIN)</a>	Informasi pribadi: PII	VEHICLE_IDENTIFICATION_NUMBER	Ya	Setiap, jika VIN berada di dekat kata kunci dalam salah satu bahasa berikut: English, French, German, Lithuania n, Polish, Portuguese, Romanian, or Spanish

## Referensi terperinci: Pengidentifikasi data terkelola Amazon Macie

Di Amazon Macie, pengidentifikasi data terkelola adalah kriteria dan teknik bawaan yang dirancang untuk mendeteksi jenis data sensitif tertentu. Mereka dapat mendeteksi daftar tipe data sensitif yang besar dan terus bertambah untuk banyak negara dan wilayah, termasuk berbagai jenis data kredensial, informasi keuangan, dan informasi pribadi. Setiap pengidentifikasi data terkelola dirancang untuk mendeteksi jenis data sensitif tertentu — misalnya, kunci akses AWS rahasia, nomor kartu kredit, atau nomor paspor untuk negara atau wilayah tertentu.

Macie dapat mendeteksi beberapa kategori data sensitif dengan menggunakan pengidentifikasi data terkelola. Dalam setiap kategori, Macie dapat mendeteksi beberapa jenis data sensitif. Topik di bagian ini mencantumkan dan menjelaskan setiap jenis dan persyaratan yang relevan untuk mendeteksi data. Untuk detail tentang pengidentifikasi data terkelola untuk jenis data sensitif tertentu, Anda dapat menelusuri topik berdasarkan kategori:

- [Kredensial](#) — Untuk data kredensial seperti kunci pribadi dan AWS kunci akses rahasia.
- [Informasi keuangan](#) — Untuk data keuangan seperti nomor kartu kredit dan nomor rekening bank.
- [Informasi pribadi: PHI](#) — Untuk informasi kesehatan pribadi (PHI) seperti asuransi kesehatan dan nomor identifikasi medis.
- [Informasi pribadi: PII](#) — Untuk informasi identitas pribadi (PII) seperti nomor identifikasi SIM dan nomor paspor.

Atau Anda dapat memilih jenis data sensitif tertentu dari tabel berikut. Tabel mencantumkan semua pengidentifikasi data terkelola yang saat ini disediakan Macie, yang diatur berdasarkan tipe data sensitif. Tabel ini juga merangkum persyaratan yang relevan untuk mendeteksi setiap jenis.

Tipe data sensitif	Kategori data sensitif	ID pengenalan data terkelola	Diperlukan kata kunci	Negara dan wilayah
<a href="#">AWS secret access key</a>	Kredensial	AWS_CREDENTIALS	Ya	Setiap
<a href="#">Nomor rekening bank</a>	Informasi keuangan	BANK_ACCOUNT_NUMBER(untuk Kanada dan AS)	Ya	Kanada, AS
<a href="#">Nomor Rekening Bank Dasar (BBAN)</a>	Informasi keuangan	Tergantung pada negara atau wilayah: FRANCE_BANK_ACCOUNT_NUMBER, GERMANY_BANK_ACCOUNT_NUMBER, ITALY_BANK_ACCOUNT_NUMBER, SPAIN_BANK_ACCOUNT_NUMBER, UK_BANK_ACCOUNT_NUMBER	Ya	Prancis, Jerman, Italia, Spanyol, Inggris
<a href="#">Tanggal lahir</a>	Informasi pribadi: PII	DATE_OF_BIRTH	Ya	Setiap
<a href="#">Tanggal kedaluwarsa</a>	Informasi keuangan	CREDIT_CARD_EXPIRATION	Ya	Setiap



Tipe data sensitif	Kategori data sensitif	ID pengenalan data terkelola	Diperlukan kata kunci	Negara dan wilayah
<a href="#">sa kartu kredit</a>				
<a href="#">Data strip magnetik kartu kredit</a>	Informasi keuangan	CREDIT_CARD_MAGNETIC_STRIPE	Ya	Setiap
<a href="#">Nomor kartu kredit</a>	Informasi keuangan	CREDIT_CARD_NUMBER(untuk nomor kartu kredit yang berdekatan dengan kata kunci), CREDIT_CARD_NUMBER_(NO_KEYWORD) (untuk nomor kartu kredit yang tidak berdekatan dengan kata kunci)	Bervariasi	Setiap
<a href="#">Kode verifikasi kartu kredit</a>	Informasi keuangan	CREDIT_CARD_SECURITY_CODE	Ya	Setiap

Tipe data sensitif	Kategori data sensitif	ID pengenal data terkelola	Diperlukan kata kunci	Negara dan wilayah
<a href="#">Nomor identifikasi lisensi</a>	Informasi pribadi: PII	Tergantung pada negara atau wilayah: AUSTRALIA_DRIVERS_LICENSE, AUSTRIA_DRIVERS_LICENSE, BELGIUM_DRIVERS_LICENSE, BULGARIA_DRIVERS_LICENSE, CANADA_DRIVERS_LICENSE, CROATIA_DRIVERS_LICENSE, CYPRUS_DRIVERS_LICENSE, CZECHIA_DRIVERS_LICENSE, DENMARK_DRIVERS_LICENSE, DRIVERS_LICENSE (for the US), ESTONIA_DRIVERS_LICENSE, FINLAND_DRIVERS_LICENSE, FRANCE_DRIVERS_LICENSE, GERMANY_DRIVERS_LICENSE, GREECE_DRIVERS_LICENSE, HUNGARY_DRIVERS_LICENSE, INDIA_DRIVERS_LICENSE, IRELAND_DRIVERS_LICENSE, ITALY_DRIVERS_LICENSE, LATVIA_DRIVERS_LICENSE, LITHUANIA_DRIVERS_LICENSE, LUXEMBOURG_DRIVERS_LICENSE, MALTA_DRIVERS_LICENSE, NETHERLANDS_DRIVERS_LICENSE, POLAND_DRIVERS_LICENSE, PORTUGAL_DRIVERS_LICENSE, ROMANIA_DRIVERS_LICENSE, SLOVAKIA_DRIVERS_LICENSE, SLOVENIA_DRIVERS_LICENSE, SPAIN_DRIVERS_LICENSE	Ya	Australia, Austria, Belgia, Bulgaria, Kanada, Kroasia, Siprus, Republik Ceko, Denmark, Estonia, Finlandia, Prancis, Jerman, Yunani, Hongaria, India, Irlandia, Italia, Latvia, Lituania, Luksemburg, Malta, Belanda, Polandia, Portugal, Rumania, Slovakia, Slovenia, Spanyol, Swedia, Inggris, AS

Tipe data sensitif	Kategori data sensitif	ID pengenalan data terkelola	Diperlukan kata kunci	Negara dan wilayah
		NSE, SWEDEN_DRIVERS_LICENSE, UK_DRIVERS_LICENSE		
<a href="#">Nomor Registrasi Badan Penegakan Narkoba (DEA)</a>	Informasi pribadi: PHI	US_DRUG_ENFORCEMENT_AGENCY_NUMBER	Ya	AS
<a href="#">Nomor Roll Pemilu</a>	Informasi pribadi: PII	UK_ELECTORAL_ROLL_NUMBER	Ya	UK
<a href="#">Nama lengkap</a>	Informasi pribadi: PII	NAME	Tidak	Apa saja, jika nama menggunakan set karakter Latin
<a href="#">Koordinat Sistem Pemosisia n Global (GPS)</a>	Informasi pribadi: PII	LATITUDE_LONGITUDE	Ya	Apa saja, jika koordinat berada di dekat kata kunci bahasa Inggris
<a href="#">Kunci API Google Cloud</a>	Kredensial	GCP_API_KEY	Ya	Setiap

Tipe data sensitif	Kategori data sensitif	ID pengenalan data terkelola	Diperlukan kata kunci	Negara dan wilayah
<a href="#">Nomor Klaim Asuransi Kesehatan (HICN)</a>	Informasi pribadi: PHI	USA_HEALTH_INSURANCE_CLAIM_NUMBER	Ya	AS
<a href="#">Nomor asuransi atau identifikasi medis</a>	Informasi pribadi: PHI	Tergantung pada negara atau wilayah: CANADA_HEALTH_NUMBER, EUROPEAN_HEALTH_INSURANCE_CARD_NUMBER, FINLAND_EUROPEAN_HEALTH_INSURANCE_NUMBER, FRANCE_HEALTH_INSURANCE_NUMBER, UK_NHS_NUMBER, USA_MEDICARE_BENEFICIARY_IDENTIFIER	Ya	Canada, EU, Finland, France, UK, US
<a href="#">Kode Sistem Pengkodean Prosedur Umum Kesehatan (HCPCS)</a>	Informasi pribadi: PHI	USA_HEALTHCARE_PROCEDURE_CODE	Ya	AS
<a href="#">Header Otorisasi Dasar HTTP</a>	Kredensial	HTTP_BASIC_AUTH_HEADER	Tidak	Setiap
<a href="#">HTTP cookie</a>	Informasi pribadi: PII	HTTP_COOKIE	Tidak	Setiap

Tipe data sensitif	Kategori data sensitif	ID pengenalan data terkelola	Diperlukan kata kunci	Negara dan wilayah
<a href="#">Nomor Rekening Bank Internasional (IBAN)</a>	Informasi keuangan	Tergantung pada negara atau wilayah:  ALBANIA_BANK_ACCOUNT_NUMBER , ANDORRA_BANK_ACCOUNT_NUMBER, BOSNIA_AND_HERZEGOVINA_BANK_ACCOUNT_NUMBER, BRAZIL_BANK_ACCOUNT_NUMBER, BULGARIA_BANK_ACCOUNT_NUMBER, COSTA_RICA_BANK_ACCOUNT_NUMBER, CROATIA_BANK_ACCOUNT_NUMBER , CYPRUS_BANK_ACCOUNT_NUMBER, CZECH_REPUBLIC_BANK_ACCOUNT_NUMBER, DENMARK_BANK_ACCOUNT_NUMBER, DOMINICAN_REPUBLIC_BANK_ACCOUNT_NUMBER, EGYPT_BANK_ACCOUNT_NUMBER, ESTONIA_BANK_ACCOUNT_NUMBER, FAROE_ISLANDS_BANK_ACCOUNT_NUMBER, FINLAND_BANK_ACCOUNT_NUMBER, FRANCE_BANK_ACCOUNT_NUMBER, GEORGIA_BANK_ACCOUNT_NUMBER, GERMANY_BANK_ACCOUNT_NUMBER , GREECE_BANK_ACCOUNT_NUMBER, GREENLAND_BANK_ACCOUNT_NUMBER, HUNGARY_BANK_ACCOUNT_NUMBER, ICELAND_BANK_ACCOUNT_NUMBER, IRELAND_BANK_ACCOUNT_NUMBER	Tidak	Albania, Andorra, Bosnia-Herzegovina , Brasil, Bulgaria, Kosta Rika, Kroasia, Siprus, Republik Ceko, Denmark, Republik Dominika, Mesir, Estonia, Kepulauan Faroe, Finlandia , Prancis, Georgia, Jerman, Yunani, Greenland , Hongaria, Islandia, Irlandia, Italia, Yordania, Kosovo, Liechtenstein,

Tipe data sensitif	Kategori data sensitif	ID pengenalan data terkelola	Diperlukan kata kunci	Negara dan wilayah
		, ITALY_BANK_ACCOUNT_NUMBER, JORDAN_BANK_ACCOUNT_NUMBER, KOSOVO_BANK_ACCOUNT_NUMBER, LIECHTENSTEIN_BANK_ACCOUNT_NUMBER, LITHUANIA_BANK_ACCOUNT_NUMBER, MALTA_BANK_ACCOUNT_NUMBER, MAURITANIA_BANK_ACCOUNT_NUMBER, MAURITIUS_BANK_ACCOUNT_NUMBER, MONACO_BANK_ACCOUNT_NUMBER, MONTENEGRO_BANK_ACCOUNT_NUMBER, NETHERLANDS_BANK_ACCOUNT_NUMBER, NORTH_MACEDONIA_BANK_ACCOUNT_NUMBER, POLAND_BANK_ACCOUNT_NUMBER, PORTUGAL_BANK_ACCOUNT_NUMBER, SAN_MARINO_BANK_ACCOUNT_NUMBER, SENEGAL_BANK_ACCOUNT_NUMBER, SERBIA_BANK_ACCOUNT_NUMBER, SLOVAKIA_BANK_ACCOUNT_NUMBER, SLOVENIA_BANK_ACCOUNT_NUMBER, SPAIN_BANK_ACCOUNT_NUMBER, SWEDEN_BANK_ACCOUNT_NUMBER, SWITZERLAND_BANK_ACCOUNT_NUMBER, TIMOR_LESTE_BANK_ACCOUNT_NUMBER, TUNISIA_BANK_ACCOUNT_NUMBER, TURKIYE_BANK_ACCOUNT_NUMBER, UK_BANK_ACCOUNT_NUMBER,		Lithuania, Malta, Mauritania, Mauritius, Monako, Montenegro, Belanda, Makedonia Utara, Polandia, Portugal, San Marino, Senegal, Serbia, Slovakia, Slovenia, Spanyol, Swedia, Swiss, Timor-Leste, Tunisia, Türkiye, Inggris, Ukraina, Uni Emirat Arab, Kepulauan Virgin (Inggris)

Tipe data sensitif	Kategori data sensitif	ID pengenal data terkelola	Diperlukan kata kunci	Negara dan wilayah
		UKRAINE_BANK_ACCOUNT_NUMBER, UNITED_ARAB_EMIRATES_BANK_ACCOUNT_NUMBER, VIRGIN_ISLANDS_BANK_ACCOUNT_NUMBER (untuk Kepulauan Virgin Britania Raya)		
<a href="#">Token Web JSON (JWT)</a>	Kredensial	JSON_WEB_TOKEN	Tidak	Setiap
<a href="#">Alamat surat-menyurat</a>	Informasi pribadi: PII	ADDRESS, BRAZIL_CEP_CODE (untuk Pos Código de Endereçamento Brasil)	Bervariasi	Australia, Brasil, Kanada, Prancis, Jerman, Italia, Spanyol, Inggris, AS
<a href="#">Kode Obat Nasional (NDC)</a>	Informasi pribadi: PHI	USA_NATIONAL_DRUG_CODE	Ya	AS
<a href="#">Nomor identifikasi nasional</a>	Informasi pribadi: PII	Tergantung pada negara atau wilayah: BRAZIL_RG_NUMBER, FRANCE_NATIONAL_IDENTIFICATION_NUMBER, GERMANY_NATIONAL_IDENTIFICATION_NUMBER, INDIA_AADHAAR_NUMBER, ITALY_NATIONAL_IDENTIFICATION_NUMBER, SPAIN_DNI_NUMBER	Ya	Brasil, Prancis, Jerman, India, Italia, Spanyol

Tipe data sensitif	Kategori data sensitif	ID pengenal data terkelola	Diperlukan kata kunci	Negara dan wilayah
<a href="#">Nomor Asuransi Nasional (NINO)</a>	Informasi pribadi: PII	UK_NATIONAL_INSURANCE_NUMBER	Ya	UK
<a href="#">Pengenal Penyedia Nasional (NPI)</a>	Informasi pribadi: PHI	USA_NATIONAL_PROVIDER_IDENTIFIER	Ya	AS
<a href="#">Kunci pribadi OpenSSH</a>	Kredensial	OPENSSSH_PRIVATE_KEY	Tidak	Setiap
<a href="#">Nomor paspor</a>	Informasi pribadi: PII	Tergantung pada negara atau wilayah: CANADA_PASSPORT_NUMBER, FRANCE_PASSPORT_NUMBER, GERMANY_PASSPORT_NUMBER, ITALY_PASSPORT_NUMBER, SPAIN_PASSPORT_NUMBER, UK_PASSPORT_NUMBER, USA_PASSPORT_NUMBER	Ya	Canada, France, Germany, Italy, Spain, UK, US
<a href="#">Nomor tempat tinggal permanen</a>	Informasi pribadi: PII	CANADA_NATIONAL_IDENTIFICATION_NUMBER	Ya	Kanada
<a href="#">Kunci pribadi PGP</a>	Kredensial	PGP_PRIVATE_KEY	Tidak	Setiap



Tipe data sensitif	Kategori data sensitif	ID pengenal data terkelola	Diperlukan kata kunci	Negara dan wilayah
<a href="#">Nomor telepon</a>	Informasi pribadi: PII	Tergantung pada negara atau wilayah: BRAZIL_PHONE_NUMBER, FRANCE_PHONE_NUMBER, GERMANY_PHONE_NUMBER, ITALY_PHONE_NUMBER, PHONE_NUMBER (for Canada and the US), SPAIN_PHONE_NUMBER, UK_PHONE_NUMBER	Bervariasi	Brazil, Canada, France, Germany, Italy, Spain, UK, US
<a href="#">Kunci pribadi Standar Kriptografi Kunci Publik (PKCS)</a>	Kredensial	PKCS	Tidak	Setiap
<a href="#">Kunci pribadi PuTTY</a>	Kredensial	PUTTY_PRIVATE_KEY	Tidak	Setiap
<a href="#">Nomor Asuransi Sosial (SIN)</a>	Informasi pribadi: PII	CANADA_SOCIAL_INSURANCE_NUMBER	Ya	Kanada
<a href="#">Nomor Jaminan Sosial (SSN)</a>	Informasi pribadi: PII	Tergantung pada negara atau wilayah: SPAIN_SOCIAL_SECURITY_NUMBER, USA_SOCIAL_SECURITY_NUMBER	Ya	Spain, US

Tipe data sensitif	Kategori data sensitif	ID pengenalan data terkelola	Diperlukan kata kunci	Negara dan wilayah
<a href="#">the section called “Kunci API Stripe”</a>	Kredensial	STRIPE_CREDENTIALS	Tidak	Setiap
<a href="#">Nomor identifikasi wajib pajak atau referensi</a>	Informasi pribadi: PII	Tergantung pada negara atau wilayah:  AUSTRALIA_TAX_FILE_NUMBER, BRAZIL_CNPJ_NUMBER, BRAZIL_CPF_NUMBER, FRANCE_TAX_IDENTIFICATION_NUMBER, GERMANY_TAX_IDENTIFICATION_NUMBER, INDIA_PERMANENT_ACCOUNT_NUMBER, ITALY_NATIONAL_IDENTIFICATION_NUMBER, SPAIN_NIE_NUMBER, SPAIN_NIF_NUMBER, SPAIN_TAX_IDENTIFICATION_NUMBER, UK_TAX_IDENTIFICATION_NUMBER, USA_INDIVIDUAL_TAX_IDENTIFICATION_NUMBER	Ya	Australia, Brasil, Prancis, Jerman, India, Italia, Spanyol, Inggris, AS
<a href="#">Pengidentifikasi perangkat unik (UDI)</a>	Informasi pribadi: PHI	MEDICAL_DEVICE_UDI	Ya	AS

Tipe data sensitif	Kategori data sensitif	ID pengenalan data terkelola	Diperlukan kata kunci	Negara dan wilayah
<a href="#">Nomor identifikasi kendaraan (VIN)</a>	Informasi pribadi: PII	VEHICLE_IDENTIFICATION_NUMBER	Ya	Setiap, jika VIN berada di dekat kata kunci dalam salah satu bahasa berikut: English, French, German, Lithuania n, Polish, Portuguese, Romanian, or Spanish

## Pengidentifikasi data terkelola untuk data kredensial

Amazon Macie dapat mendeteksi beberapa jenis data kredensial sensitif dengan menggunakan pengidentifikasi data terkelola. Topik di halaman ini menentukan setiap jenis dan memberikan informasi tentang pengenalan data terkelola yang dirancang untuk mendeteksi data. Setiap topik memberikan informasi berikut:

- ID pengenalan data terkelola - Menentukan pengenalan unik (ID) untuk pengenalan data terkelola yang dirancang untuk mendeteksi data. Saat Anda [membuat pekerjaan penemuan data sensitif](#) atau [mengonfigurasi setelah penemuan data sensitif otomatis](#), Anda dapat menggunakan ID ini untuk menentukan apakah Anda ingin Macie menggunakan pengenalan data terkelola saat menganalisis data.

- Negara dan wilayah yang didukung - Menunjukkan negara atau wilayah mana yang dirancang untuk pengenalan data terkelola yang berlaku. Jika pengenalan data terkelola tidak dirancang untuk negara atau wilayah tertentu, nilai ini adalah Any.
- Kata kunci diperlukan - Menentukan apakah deteksi memerlukan kata kunci untuk berada di dekat data. Jika kata kunci diperlukan, topik juga memberikan contoh kata kunci yang diperlukan. Untuk informasi tentang bagaimana Macie menggunakan kata kunci saat menganalisis data, lihat [Persyaratan kata kunci](#)
- Komentar - Memberikan detail relevan yang dapat memengaruhi pilihan pengenalan data terkelola atau penyelidikan Anda terhadap kejadian data sensitif yang dilaporkan. Detailnya mencakup informasi seperti standar yang didukung, persyaratan sintaks, dan pengecualian.

Topik tercantum dalam urutan abjad berdasarkan tipe data sensitif.

Tipe data sensitif

- [AWS secret access key](#)
- [Kunci API Google Cloud](#)
- [Header Otorisasi Dasar HTTP](#)
- [Token Web JSON \(JWT\)](#)
- [Kunci pribadi OpenSSH](#)
- [Kunci pribadi PGP](#)
- [Kunci pribadi Standar Kriptografi Kunci Publik \(PKCS\)](#)
- [Kunci pribadi PuTTY](#)
- [Kunci API Stripe](#)

AWS secret access key

ID pengenalan data terkelola: AWS\_CREDENTIALS

Negara dan wilayah yang didukung: Apa saja

Kata kunci yang dibutuhkan: Ya. Kata kunci meliputi: aws\_secret\_access\_key, credentials, secret access key, secret key, set-awscredential

Komentar: Macie tidak melaporkan kemunculan urutan karakter berikut, yang biasanya digunakan sebagai contoh fiktif: dan. je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY wJa1rXUtnFEMI/K7MDENG/bPxrFiCYEXAMPLEKEY

## Kunci API Google Cloud

ID pengenalan data terkelola: GCP\_API\_KEY

Negara dan wilayah yang didukung: Apa saja

Kata kunci yang dibutuhkan: Ya. Kata kunci meliputi: G\_PLACES\_KEY, GCP api key, GCP key, google cloud key, google-api-key, google-cloud-apikeys, GOOGLEKEY, X-goog-api-key

Komentar: Macie hanya dapat mendeteksi komponen string (`keyString`) dari kunci Google Cloud API. Support tidak menyertakan deteksi ID atau komponen nama tampilan kunci Google Cloud API.

## Header Otorisasi Dasar HTTP

ID pengenalan data terkelola: HTTP\_BASIC\_AUTH\_HEADER

Negara dan wilayah yang didukung: Apa saja

Kata kunci yang dibutuhkan: Tidak

Komentar: Deteksi memerlukan header lengkap, termasuk nama bidang dan arahan skema otentikasi, seperti yang ditentukan oleh [RFC 7617](#). Misalnya: `Authorization: Basic QWxhZGRpbjpvGVuIHNIc2FtZQ==` dan `Proxy-Authorization: Basic dGVzdDoxMjPCow==`.

## Token Web JSON (JWT)

ID pengenalan data terkelola: JSON\_WEB\_TOKEN

Negara dan wilayah yang didukung: Apa saja

Kata kunci yang dibutuhkan: Tidak

Komentar: Macie dapat mendeteksi JSON Web Tokens (JWTs) yang memenuhi persyaratan yang ditentukan oleh [RFC 7519](#) untuk struktur JSON Web Signature (JWS). Token dapat ditandatangani atau tidak ditandatangani.

## Kunci pribadi OpenSSH

ID pengenalan data terkelola: OPENSSH\_PRIVATE\_KEY

Negara dan wilayah yang didukung: Apa saja

Kata kunci yang dibutuhkan: Tidak

Komentar: Tidak ada

Kunci pribadi PGP

ID pengenalan data terkelola: PGP\_PRIVATE\_KEY

Negara dan wilayah yang didukung: Apa saja

Kata kunci yang dibutuhkan: Tidak

Komentar: Tidak ada

Kunci pribadi Standar Kriptografi Kunci Publik (PKCS)

ID pengenalan data terkelola: PKCS

Negara dan wilayah yang didukung: Apa saja

Kata kunci yang dibutuhkan: Tidak

Komentar: Tidak ada

Kunci pribadi PuTTY

ID pengenalan data terkelola: PUTTY\_PRIVATE\_KEY

Negara dan wilayah yang didukung: Apa saja

Kata kunci yang dibutuhkan: Tidak

Komentar: Macie dapat mendeteksi kunci pribadi PuTTY yang menggunakan header standar dan urutan header berikut `PuTTY-User-Key-File:Encryption,,,, CommentPublic-Lines, Private-Lines` dan `Private-MAC`. Nilai header dapat berisi karakter alfanumerik, tanda hubung (-), dan karakter baris baru (atau) `\n \r`. `Public-Lines` dan `Private-Lines` nilai juga dapat berisi garis miring ke depan (/), ditambah tanda (+), dan tanda sama dengan (=). `Private-MAC` nilai juga dapat berisi tanda plus (+). Support tidak menyertakan deteksi kunci pribadi dengan nilai header yang berisi karakter lain, seperti spasi atau garis bawah (\_). Support juga tidak menyertakan deteksi kunci pribadi yang menyertakan header khusus.

Kunci API Stripe

ID pengenalan data terkelola: STRIPE\_CREDENTIALS

Negara dan wilayah yang didukung: Apa saja

Kata kunci yang dibutuhkan: Tidak

Komentar: Macie tidak melaporkan kemunculan urutan karakter berikut, yang biasanya digunakan dalam contoh kode Stripe: `dan. sk_test_4eC39HqLyjWDarjtT1zdp7dc pk_test_TYooMQauvdEDq54NiTphI7jx`

## Pengidentifikasi data terkelola untuk informasi keuangan

Amazon Macie dapat mendeteksi berbagai jenis informasi keuangan sensitif dengan menggunakan pengidentifikasi data terkelola. Topik pada halaman ini mencantumkan setiap jenis dan memberikan informasi tentang pengidentifikasi data terkelola yang dirancang untuk mendeteksi data. Setiap topik memberikan informasi berikut:

- ID pengenalan data terkelola - Menentukan pengenalan unik (ID) untuk satu atau beberapa pengidentifikasi data terkelola yang dirancang untuk mendeteksi data. Saat [membuat pekerjaan penemuan data sensitif](#) atau [mengonfigurasi setelan penemuan data sensitif otomatis](#), Anda dapat menggunakan ID ini untuk menentukan pengidentifikasi data terkelola mana yang ingin digunakan Macie saat menganalisis data.
- Negara dan wilayah yang didukung - Menunjukkan negara atau wilayah mana pengidentifikasi data terkelola yang berlaku dirancang untuk. Jika pengidentifikasi data terkelola tidak dirancang untuk negara atau wilayah tertentu, nilai ini adalah Any.
- Kata kunci diperlukan - Menentukan apakah deteksi memerlukan kata kunci untuk berada di dekat data. Jika kata kunci diperlukan, topik juga memberikan contoh kata kunci yang diperlukan. Untuk informasi tentang bagaimana Macie menggunakan kata kunci saat menganalisis data, lihat [Persyaratan kata kunci](#).
- Komentar - Memberikan detail relevan yang dapat memengaruhi pilihan pengenalan data terkelola atau penyelidikan Anda terhadap kejadian data sensitif yang dilaporkan. Detailnya mencakup informasi seperti standar yang didukung, persyaratan sintaks, dan pengecualian.

Topik tercantum dalam urutan abjad berdasarkan tipe data sensitif.

Tipe data sensitif

- [Nomor rekening bank](#)
- [Nomor Rekening Bank Dasar \(BBAN\)](#)
- [Tanggal kedaluwarsa kartu kredit](#)

- [Data strip magnetik kartu kredit](#)
- [Nomor kartu kredit](#)
- [Kode verifikasi kartu kredit](#)
- [Nomor Rekening Bank Internasional \(IBAN\)](#)

## Nomor rekening bank

Macie dapat mendeteksi nomor rekening bank Kanada dan AS yang terdiri dari 9-17 digit urutan dan tidak mengandung spasi apa pun.

ID pengidentifikasi data terkelola: BANK\_ACCOUNT\_NUMBER

Negara dan wilayah yang didukung: Kanada, AS

Kata kunci yang dibutuhkan: Ya. Kata kunci meliputi: bank account, bank acct, checking account, checking acct, deposit account, deposit acct, savings account, savings acct, chequing account, chequing acct

Komentar: Pengidentifikasi data terkelola ini secara eksplisit dirancang untuk mendeteksi nomor rekening bank untuk Kanada dan AS. [Negara-negara ini tidak menggunakan format Nomor Rekening Bank Dasar \(BBAN\) atau Nomor Rekening Bank Internasional \(IBAN\) yang ditentukan oleh standar internasional ISO untuk penomoran rekening bank, sebagaimana ditentukan oleh ISO 13616.](#)

Untuk mendeteksi nomor rekening bank untuk negara dan wilayah lain, gunakan pengidentifikasi data terkelola yang dirancang untuk format tersebut. Lihat informasi yang lebih lengkap di [Nomor Rekening Bank Dasar \(BBAN\)](#) dan [Nomor Rekening Bank Internasional \(IBAN\)](#).

## Nomor Rekening Bank Dasar (BBAN)

[Macie dapat mendeteksi Nomor Rekening Bank Dasar \(BBANs\) yang sesuai dengan struktur BBAN yang ditentukan oleh standar internasional ISO untuk penomoran rekening bank, sebagaimana ditentukan oleh ISO 13616.](#) Ini termasuk BBAN yang tidak berisi spasi, atau menggunakan pemisah spasi atau tanda hubung — misalnya,, dan. NWBK60161331926819 NWBK 6016 1331 9268 19 NWBK-6016-1331-9268-19

ID pengenalan data terkelola: Tergantung pada negara atau wilayah, FRANCE\_BANK\_ACCOUNT\_NUMBER, GERMANY\_BANK\_ACCOUNT\_NUMBER, ITALY\_BANK\_ACCOUNT\_NUMBER, SPAIN\_BANK\_ACCOUNT\_NUMBER, UK\_BANK\_ACCOUNT\_NUMBER



Negara dan wilayah yang didukung: Prancis, Jerman, Italia, Spanyol, Inggris

Kata kunci yang dibutuhkan: Ya. Tabel berikut mencantumkan kata kunci yang Macie kenali untuk negara dan wilayah tertentu.

Negara atau wilayah	Kata kunci
France	account code, account number, accountno#, accountnumber#, bban, code bancaire, compte bancaire, customer account id, customer account number, customer bank account id, iban, numéro de compte
Germany	account code, account number, accountno #, accountnumber#, bankleitzahl, bban, customer account id, customer account number, customer bank account id, geheimzahl, iban, kartennummer, kontonummer, kreditkartennummer, sepa
Italy	account code, account number, accountno #, accountnumber#, bban, codice bancario, conto bancario, customer account id, customer account number, customer bank account id, iban, numero di conto
Spain	account code, account number, accountno #, accountnumber#, bban, código cuenta, código cuenta bancaria, cuenta cliente id, customer account ID, customer account number, customer bank account id, iban, número cuenta bancaria cliente, número cuenta cliente
UK	account code, account number, accountno #, accountnumber#, bban, customer account id, customer account number, customer bank account id, iban, sepa

Komentar: Pengidentifikasi data terkelola ini juga dapat mendeteksi Nomor Rekening Bank Internasional (IBAN) yang sesuai dengan standar ISO 13616. Untuk informasi selengkapnya, lihat [Nomor Rekening Bank Internasional \(IBAN\)](#). Pengidentifikasi data terkelola untuk Inggris (UK\_BANK\_ACCOUNT\_NUMBER) juga dapat mendeteksi nomor rekening bank domestik untuk Inggris — misalnya, . 60-16-13 31926819

Tanggal kedaluwarsa kartu kredit

ID pengidentifikasi data terkelola: CREDIT\_CARD\_EXPIRATION

Negara dan wilayah yang didukung: Apa saja

Kata kunci yang dibutuhkan: Ya. Kata kunci meliputi: exp d, exp m, exp y, expiration, expiry

Komentar: Support mencakup sebagian besar format tanggal, seperti semua digit dan kombinasi digit dan nama bulan. Komponen tanggal dapat dipisahkan dengan garis miring (/), tanda hubung (-), atau kata kunci yang berlaku. Misalnya, Macie dapat mendeteksi tanggal seperti 02/26, 02/2026, Feb 202626-Feb, dan expY=2026, expM=02.

Data strip magnetik kartu kredit

ID pengidentifikasi data terkelola: CREDIT\_CARD\_MAGNETIC\_STRIPE

Negara dan wilayah yang didukung: Apa saja

Kata kunci yang dibutuhkan: Ya. Kata kunci meliputi: card data, iso7813, mag, magstripe, stripe, swipe

Komentar: Support termasuk trek 1 dan 2.

Nomor kartu kredit

ID pengenalan data terkelola: CREDIT\_CARD\_NUMBER untuk nomor kartu kredit yang berdekatan dengan kata kunci, CREDIT\_CARD\_NUMBER\_(NO\_KEYWORD) untuk nomor kartu kredit yang tidak berdekatan dengan kata kunci

Negara dan wilayah yang didukung: Apa saja

Kata kunci yang dibutuhkan: Bervariasi. Kata kunci diperlukan oleh pengidentifikasi data CREDIT\_CARD\_NUMBER terkelola. Kata kunci meliputi: account number, american express, amex,

bank card, card, card num, card number, cc #, ccn, check card, credit, credit card#, dankort, debit, debit card, diners club, discover, electron, japanese card bureau, jcb, mastercard, mc, pan, payment account number, payment card number, pcn, union pay, visa. Kata kunci tidak diperlukan oleh pengidentifikasi data CREDIT\_CARD\_NUMBER\_(NO\_KEYWORD) terkelola.

Komentar: Deteksi mengharuskan data menjadi urutan 13-19 digit yang mematuhi rumus pemeriksaan Luhn dan menggunakan awalan nomor kartu standar untuk salah satu jenis kartu kredit berikut: American Express, Dankort, Diner's Club, Discover, Electron, Japanese Card Bureau (JCB), Mastercard, dan Visa. UnionPay

Macie tidak melaporkan kemunculan urutan berikut, yang telah disediakan oleh penerbit kartu kredit untuk pengujian

publik:122000000000003,,2222405343248877,2222990905257051,2223007648726984,222357712042222222222224444333322221111,4462030000000000,4484070000000000,4911830000000,49175111010030175156 5185540810000019 5200828282828210 5204230080000017 5204740009900014,,,5420923878724339,,5454545454545454,,5455330760000018,,55069004900076009244561

Kode verifikasi kartu kredit

ID pengidentifikasi data terkelola: CREDIT\_CARD\_SECURITY\_CODE

Negara dan wilayah yang didukung: Apa saja

Kata kunci yang dibutuhkan: Ya. Kata kunci meliputi: card id, card identification code, card identification number, card security code, card validation code, card validation number, card verification data, card verification value, cvc, cvc2, cvv, cvv2, elo verification code

Komentar: Tidak ada

Nomor Rekening Bank Internasional (IBAN)

Macie dapat mendeteksi Nomor Rekening Bank Internasional (IBAN) yang terdiri dari hingga 34 karakter alfanumerik, termasuk elemen seperti kode negara. [Lebih khusus lagi, Macie dapat mendeteksi IBAN yang sesuai dengan standar internasional ISO untuk penomoran rekening bank, sebagaimana ditentukan oleh ISO 13616.](#) Ini termasuk IBAN yang tidak berisi spasi, atau menggunakan pemisah spasi atau tanda hubung — misalnya,,, dan. GB29NWBK60161331926819 GB29 NWBK 6016 1331 9268 19 GB29-NWBK-6016-1331-9268-19 Deteksi mencakup pemeriksaan validasi berdasarkan skema Modulus 97.

ID pengenal data terkelola: Tergantung pada negara atau wilayah, ALBANIA\_BANK\_ACCOUNT\_NUMBER, ANDORRA\_BANK\_ACCOUNT\_NUMBER, BOSNIA\_AND\_HERZEGOVINA\_BANK\_ACCOUNT\_NUMBER, BRAZIL\_BANK\_ACCOUNT\_NUMBER, BULGARIA\_BANK\_ACCOUNT\_NUMBER, COSTA\_RICA\_BANK\_ACCOUNT\_NUMBER, CROATIA\_BANK\_ACCOUNT\_NUMBER, CYPRUS\_BANK\_ACCOUNT\_NUMBER, CZECH\_REPUBLIC\_BANK\_ACCOUNT\_NUMBER, DENMARK\_BANK\_ACCOUNT\_NUMBER, DOMINICAN\_REPUBLIC\_BANK\_ACCOUNT\_NUMBER, EGYPT\_BANK\_ACCOUNT\_NUMBER, ESTONIA\_BANK\_ACCOUNT\_NUMBER, FAROE\_ISLANDS\_BANK\_ACCOUNT\_NUMBER, FINLAND\_BANK\_ACCOUNT\_NUMBER, FRANCE\_BANK\_ACCOUNT\_NUMBER, GEORGIA\_BANK\_ACCOUNT\_NUMBER, GERMANY\_BANK\_ACCOUNT\_NUMBER, GREECE\_BANK\_ACCOUNT\_NUMBER, GREENLAND\_BANK\_ACCOUNT\_NUMBER, HUNGARY\_BANK\_ACCOUNT\_NUMBER, ICELAND\_BANK\_ACCOUNT\_NUMBER, IRELAND\_BANK\_ACCOUNT\_NUMBER, ITALY\_BANK\_ACCOUNT\_NUMBER, JORDAN\_BANK\_ACCOUNT\_NUMBER, KOSOVO\_BANK\_ACCOUNT\_NUMBER, LIECHTENSTEIN\_BANK\_ACCOUNT\_NUMBER, LITHUANIA\_BANK\_ACCOUNT\_NUMBER, MALTA\_BANK\_ACCOUNT\_NUMBER, MAURITANIA\_BANK\_ACCOUNT\_NUMBER, MAURITIUS\_BANK\_ACCOUNT\_NUMBER, MONACO\_BANK\_ACCOUNT\_NUMBER, MONTENEGRO\_BANK\_ACCOUNT\_NUMBER, NETHERLANDS\_BANK\_ACCOUNT\_NUMBER, NORTH\_MACEDONIA\_BANK\_ACCOUNT\_NUMBER, POLAND\_BANK\_ACCOUNT\_NUMBER, PORTUGAL\_BANK\_ACCOUNT\_NUMBER, SAN\_MARINO\_BANK\_ACCOUNT\_NUMBER, SENEGAL\_BANK\_ACCOUNT\_NUMBER, SERBIA\_BANK\_ACCOUNT\_NUMBER, SLOVAKIA\_BANK\_ACCOUNT\_NUMBER, SLOVENIA\_BANK\_ACCOUNT\_NUMBER, SPAIN\_BANK\_ACCOUNT\_NUMBER, SWEDEN\_BANK\_ACCOUNT\_NUMBER, SWITZERLAND\_BANK\_ACCOUNT\_NUMBER, TIMOR\_LESTE\_BANK\_ACCOUNT\_NUMBER, TUNISIA\_BANK\_ACCOUNT\_NUMBER, TURKIYE\_BANK\_ACCOUNT\_NUMBER, UK\_BANK\_ACCOUNT\_NUMBER, UKRAINE\_BANK\_ACCOUNT\_NUMBER, UNITED\_ARAB\_EMIRATES\_BANK\_ACCOUNT\_NUMBER, VIRGIN\_ISLANDS\_BANK\_ACCOUNT\_NUMBER (untuk Kepulauan Virgin Inggris)

Negara dan wilayah yang didukung: Albania, Andorra, Bosnia-Herzegovina, Brasil, Bulgaria, Kosta Rika, Kroasia, Siprus, Republik Ceko, Denmark, Republik Dominika, Mesir, Estonia, Kepulauan Faroe, Finlandia, Prancis, Georgia, Jerman, Yunani, Greenland, Hongaria, Islandia, Irlandia, Italia, Yordania, Kosovo, Liechtenstein, Lithuania, Malta, Mauritania, Mauritius, Monako, Montenegro, Belanda, Makedonia Utara, Polandia, Portugal, San Marino, Senegal, Serbia, Slovakia, Slovenia, Spanyol, Swedia, Swiss, Timor-Leste, Tunisia, Türkiye, Inggris, Ukraina, United Arab Emirates, Kepulauan Virgin (Inggris)

Kata kunci yang dibutuhkan: Tidak

Komentar: Pengidentifikasi data terkelola untuk Prancis, Jerman, Italia, Spanyol, dan Inggris juga dapat mendeteksi Nomor Rekening Bank Dasar (BBANs) yang sesuai dengan struktur BBAN yang ditentukan oleh standar ISO 13616, jika urutan karakter berada di dekat kata kunci. Untuk informasi selengkapnya, lihat [Nomor Rekening Bank Dasar \(BBAN\)](#).

## Pengidentifikasi data terkelola untuk informasi kesehatan pribadi (PHI)

Amazon Macie dapat mendeteksi berbagai jenis informasi kesehatan pribadi (PHI) yang sensitif dengan menggunakan pengidentifikasi data terkelola. Topik di halaman ini menentukan setiap jenis dan memberikan informasi tentang pengenal data terkelola yang dirancang untuk mendeteksi data. Setiap topik memberikan informasi berikut:

- ID pengenal data terkelola - Menentukan pengenal unik (ID) untuk pengenal data terkelola yang dirancang untuk mendeteksi data. Saat Anda [membuat pekerjaan penemuan data sensitif](#) atau [mengonfigurasi setelah penemuan data sensitif otomatis](#), Anda dapat menggunakan ID ini untuk menentukan apakah Anda ingin Macie menggunakan pengenal data terkelola saat menganalisis data.
- Negara dan wilayah yang didukung - Menunjukkan negara atau wilayah mana yang dirancang untuk pengenal data terkelola yang berlaku. Jika pengenal data terkelola tidak dirancang untuk negara atau wilayah tertentu, nilai ini adalah Any.
- Kata kunci diperlukan - Menentukan apakah deteksi memerlukan kata kunci untuk berada di dekat data. Jika kata kunci diperlukan, topik juga memberikan contoh kata kunci yang diperlukan. Untuk informasi tentang bagaimana Macie menggunakan kata kunci saat menganalisis data, lihat [Persyaratan kata kunci](#)
- Komentar - Memberikan detail relevan yang dapat memengaruhi pilihan pengenal data terkelola atau penyelidikan Anda terhadap kejadian data sensitif yang dilaporkan. Detailnya mencakup informasi seperti standar yang didukung, persyaratan sintaks, dan pengecualian.

Topik tercantum dalam urutan abjad berdasarkan tipe data sensitif.

Tipe data sensitif

- [Nomor Registrasi Badan Penegakan Narkoba \(DEA\)](#)
- [Nomor Klaim Asuransi Kesehatan \(HICN\)](#)
- [Nomor asuransi atau identifikasi medis](#)

- [Kode Sistem Pengkodean Prosedur Umum Kesehatan \(HCPCS\)](#)
- [Kode Obat Nasional \(NDC\)](#)
- [Pengenal Penyedia Nasional \(NPI\)](#)
- [Pengidentifikasi perangkat unik \(UDI\)](#)

Nomor Registrasi Badan Penegakan Narkoba (DEA)

ID pengenalan data terkelola: US\_DRUG\_ENFORCEMENT\_AGENCY\_NUMBER

Negara dan wilayah yang didukung: AS

Kata kunci yang dibutuhkan: Ya. Kata kunci meliputi: dea number, dea registration

Komentar: Tidak ada

Nomor Klaim Asuransi Kesehatan (HICN)

ID pengenalan data terkelola: USA\_HEALTH\_INSURANCE\_CLAIM\_NUMBER

Negara dan wilayah yang didukung: AS

Kata kunci yang dibutuhkan: Ya. Kata kunci meliputi: health insurance claim number, hic no, hic no., hic number, hic#, hicn, hicn#., hico#

Komentar: Tidak ada

Nomor asuransi atau identifikasi medis

Support mencakup nomor Kartu Asuransi Kesehatan Eropa untuk UE dan Finlandia, nomor asuransi kesehatan untuk Prancis, Pengidentifikasi Penerima Medicare untuk AS, nomor NHS untuk Inggris, dan Nomor Kesehatan Pribadi untuk Kanada.

ID pengenalan data terkelola: Tergantung pada negara atau wilayah, CANADA\_HEALTH\_NUMBER, EUROPEAN\_HEALTH\_INSURANCE\_CARD\_NUMBER, FINLAND\_EUROPEAN\_HEALTH\_INSURANCE\_NUMBER, FRANCE\_HEALTH\_INSURANCE\_NUMBER, UK\_NHS\_NUMBER, USA\_MEDICARE\_BENEFICIARY\_IDENTIFIER

Negara dan wilayah yang didukung: Kanada, UE, Finlandia, Prancis, Inggris, AS

Kata kunci yang dibutuhkan: Ya. Tabel berikut mencantumkan kata kunci yang Macie kenali untuk negara dan wilayah tertentu.

Negara atau wilayah	Kata kunci
Canada	canada healthcare number, msp number, personal healthcare number, phn, soins de santé
EU	assicurazione sanitaria numero, carta assicurazione numero, carte d'assurance maladie, carte européenne d'assurance maladie, ceam, ehic, ehic#, finlandehicnumber#, gesundheitskarte, hälsokort, health card, health card number, health insurance card, health insurance number, insurance card number, krankenversicherungskarte, krankenversicherungsnummer, medical account number, numero conto medico, numéro d'assurance maladie, numéro de carte d'assurance, numéro de compte medical, número de cuenta médica, número de seguro de salud, número de tarjeta de seguro, sairaanhoitokortin, sairausvaakuuskortti, sairausvakuutusnumero, sjukförsäkring nummer, sjukförsäkringskort, suomi ehic-numero, tarjeta de salud, terveyskortti, tessera sanitaria assicurazione numero, versicherungsnummer
Finland	ehic, ehic#, finland health insurance card, finlandehicnumber#, finska sjukförsäkringskort, hälsokort, health card, health card number, health insurance card, health insurance number, sairaanhoitokortin, sairaanhoitokortin, sairausvakuuskortti, sairausvakuutusnumero, sjukförsäkring nummer, sjukförsäkringskort

Negara atau wilayah	Kata kunci
	t, suomen sairausvakuutuskortti, suomi ehic-numero, terveyskortti
France	carte d'assuré social, carte vitale, insurance card
UK	national health service, NHS
US	mbi, medicare beneficiary

Komentar: Tidak ada

Kode Sistem Pengkodean Prosedur Umum Kesehatan (HCPCS)

ID pengenalan data terkelola: USA\_HEALTHCARE\_PROCEDURE\_CODE

Negara dan wilayah yang didukung: AS

Kata kunci yang dibutuhkan: Ya. Kata kunci meliputi: current procedural terminology, hcpcs, healthcare common procedure coding system

Komentar: Tidak ada

Kode Obat Nasional (NDC)

ID pengenalan data terkelola: USA\_NATIONAL\_DRUG\_CODE

Negara dan wilayah yang didukung: AS

Kata kunci yang dibutuhkan: Ya. Kata kunci meliputi: national drug code, ndc

Komentar: Tidak ada

Pengenalan Penyedia Nasional (NPI)

ID pengenalan data terkelola: USA\_NATIONAL\_PROVIDER\_IDENTIFIER

Negara dan wilayah yang didukung: AS

Kata kunci yang dibutuhkan: Ya. Kata kunci meliputi: hipaa, n.p.i, national provider, npi

Komentar: Tidak ada



## Pengidentifikasi perangkat unik (UDI)

ID pengenalan data terkelola: MEDICAL\_DEVICE\_UDI

Negara dan wilayah yang didukung: AS

Kata kunci yang dibutuhkan: Ya. Kata kunci meliputi: blood, blood bag, dev id, device id, device identifier, gs1, hibcc, iccbba, med, udi, unique device id, unique device identifier

Komentar: Macie dapat mendeteksi pengidentifikasi perangkat unik (UDI) yang sesuai dengan format yang disetujui oleh Badan Pengawas Obat dan Makanan AS. Ini termasuk format standar yang ditentukan oleh GS1, HIBCC, dan ICCBBA. Dukungan ICCBBA adalah untuk standar ISBT.

## Pengidentifikasi data terkelola untuk informasi identitas pribadi (PII)

Amazon Macie dapat mendeteksi berbagai jenis informasi sensitif dan dapat diidentifikasi secara pribadi (PII) dengan menggunakan pengidentifikasi data terkelola. Topik pada halaman ini mencantumkan setiap jenis dan memberikan informasi tentang pengidentifikasi data terkelola yang dirancang untuk mendeteksi data. Setiap topik memberikan informasi berikut:

- ID pengenalan data terkelola - Menentukan pengenalan unik (ID) untuk satu atau beberapa pengidentifikasi data terkelola yang dirancang untuk mendeteksi data. Saat [membuat pekerjaan penemuan data sensitif](#) atau [mengonfigurasi setelah penemuan data sensitif otomatis](#), Anda dapat menggunakan ID ini untuk menentukan pengidentifikasi data terkelola mana yang ingin digunakan Macie saat menganalisis data.
- Negara dan wilayah yang didukung - Menunjukkan negara atau wilayah mana pengidentifikasi data terkelola yang berlaku dirancang untuk. Jika pengidentifikasi data terkelola tidak dirancang untuk negara atau wilayah tertentu, nilai ini adalah Any.
- Kata kunci diperlukan - Menentukan apakah deteksi memerlukan kata kunci untuk berada di dekat data. Jika kata kunci diperlukan, topik juga memberikan contoh kata kunci yang diperlukan. Untuk informasi tentang bagaimana Macie menggunakan kata kunci saat menganalisis data, lihat [Persyaratan kata kunci](#)
- Komentar - Memberikan detail relevan yang dapat memengaruhi pilihan pengenalan data terkelola atau penyelidikan Anda terhadap kejadian data sensitif yang dilaporkan. Detailnya mencakup informasi seperti standar yang didukung, persyaratan sintaks, dan pengecualian.

Topik tercantum dalam urutan abjad berdasarkan tipe data sensitif.

### Tipe data sensitif

- [Tanggal lahir](#)
- [Nomor identifikasi lisensi](#)
- [Nomor Roll Pemilu](#)
- [Nama lengkap](#)
- [Koordinat Sistem Pemosisian Global \(GPS\)](#)
- [HTTP cookie](#)
- [Alamat surat-menyurat](#)
- [Nomor identifikasi nasional](#)
- [Nomor Asuransi Nasional \(NINO\)](#)
- [Nomor paspor](#)
- [Nomor tempat tinggal permanen](#)
- [Nomor telepon](#)
- [Nomor Asuransi Sosial \(SIN\)](#)
- [Nomor Jaminan Sosial \(SSN\)](#)
- [Nomor identifikasi wajib pajak atau referensi](#)
- [Nomor identifikasi kendaraan \(VIN\)](#)

## Tanggal lahir

ID pengenalan data terkelola: DATE\_OF\_BIRTH

Negara dan wilayah yang didukung: Apa saja

Kata kunci yang dibutuhkan: Ya. Kata kunci meliputi: bday, b-day, birth date, birthday, date of birth, dob

Komentar: Support mencakup sebagian besar format tanggal, seperti semua digit dan kombinasi digit dan nama bulan. Komponen tanggal dapat dipisahkan oleh spasi, garis miring (/), atau tanda hubung (-).

## Nomor identifikasi lisensi

ID pengenalan data terkelola: Tergantung pada negara atau wilayah, AUSTRALIA\_DRIVERS\_LICENSE, AUSTRIA\_DRIVERS\_LICENSE, BELGIUM\_DRIVERS\_LICENSE, BULGARIA\_DRIVERS\_LICENSE, CANADA\_DRIVERS\_LICENSE, CROATIA\_DRIVERS\_LICENSE, CYPRUS\_DRIVERS\_LICENSE, CZECHIA\_DRIVERS\_LICENSE,

DENMARK\_DRIVERS\_LICENSE, DRIVERS\_LICENSE (for the US), ESTONIA\_DRIVERS\_LICENSE, FINLAND\_DRIVERS\_LICENSE, FRANCE\_DRIVERS\_LICENSE, GERMANY\_DRIVERS\_LICENSE, GREECE\_DRIVERS\_LICENSE, HUNGARY\_DRIVERS\_LICENSE, INDIA\_DRIVERS\_LICENSE, IRELAND\_DRIVERS\_LICENSE, ITALY\_DRIVERS\_LICENSE, LATVIA\_DRIVERS\_LICENSE, LITHUANIA\_DRIVERS\_LICENSE, LUXEMBOURG\_DRIVERS\_LICENSE, MALTA\_DRIVERS\_LICENSE, NETHERLANDS\_DRIVERS\_LICENSE, POLAND\_DRIVERS\_LICENSE, PORTUGAL\_DRIVERS\_LICENSE, ROMANIA\_DRIVERS\_LICENSE, SLOVAKIA\_DRIVERS\_LICENSE, SLOVENIA\_DRIVERS\_LICENSE, SPAIN\_DRIVERS\_LICENSE, SWEDEN\_DRIVERS\_LICENSE, UK\_DRIVERS\_LICENSE

Negara dan wilayah yang didukung: Australia, Austria, Belgia, Bulgaria, Kanada, Kroasia, Siprus, Republik Ceko, Denmark, Estonia, Finlandia, Prancis, Jerman, Yunani, Hongaria, India, Irlandia, Italia, Latvia, Lithuania, Luksemburg, Malta, Belanda, Polandia, Portugal, Rumania, Slovakia, Slovenia, Spanyol, Swedia, Inggris, AS

Kata kunci yang dibutuhkan: Ya. Tabel berikut mencantumkan kata kunci yang Macie kenali untuk negara dan wilayah tertentu.

Negara atau wilayah	Kata kunci
Australia	dl#, dl:, dlno#, driver licence, driver license, driver permit, drivers lic., drivers licence, driver's licence, drivers license, driver's license, drivers permit, driver's permit, drivers permit number, driving licence, driving license, driving permit
Austria	führerschein, fuhrerschein, führerschein republik österreich, fuhrerschein republik osterreich
Belgium	fuehrerschein, fuehrerschein- nr, fuehrersc heinnummer, fuhrerschein, führerschein, fuhrerschein- nr, führerschein- nr, fuhrersch einnummer, führerscheinnummer, numéro permis conduire, permis de conduire, rijbewijs, rijbewijsnummer

Negara atau wilayah	Kata kunci
Bulgaria	превозно средство, свидетелство за управление на моторно, свидетелство за управление на мпс, сумпс, шофьорска книжка
Canada	dl#, dl., dlno#, driver licence, driver licences, driver license, driver licenses, driver permit, drivers lic., drivers licence, driver's licence, drivers licences, driver's licences, drivers license, driver's license, drivers licenses, driver's licenses, drivers permit, driver's permit, drivers permit number, driving licence, driving license, driving permit, permis de conduire
Croatia	vozačka dozvola
Cyprus	άδεια οδήγησης
Czech Republic	číslo licence, číslo licence řidiče, číslo řidičskéh o průkazu, ovladače lic., povolení k jízdě, povolení řidiče, řidiči povolení, řidičský průkaz, řidičský průkaz
Denmark	kørekort, kørekortnummer
Estonia	juhi litsentsi number, juhiloa number, juhiluba, juhiluba number
Finland	ajokortin numero, ajokortti, förare lic., körkort, körkort nummer, kuljettaja lic., permis de conduire
France	permis de conduire

Negara atau wilayah	Kata kunci
Germany	fuehrerschein, fuehrerschein- nr, fuehrerscheinnummer, fuhrerschein, f"uhrierschein, fuhrerschein- nr, f"uhrierschein- nr, fuhrerscheinnummer, f"uhrierscheinnummer
Greece	δεια οδηγησης, adeia odigisis
Hungary	illeszt"oprogramok lic, jogositv"any, jogs'i, licencszám, vezet"o enged"ely, vezet"oi enged"ely
India	driver licence, driver licences, driver license, driver licenses, drivers lic., drivers licence, driver's licence, drivers licences, driver's licences, drivers license, driver's license, drivers licenses, driver's licenses, driving licence, driving license
Ireland	cead"unas tiom"ana
Italy	patente di guida, patente di guida numero, patente guida, patente guida numero
Latvia	autovad"it"aja apliec"iba, licences numurs, vad"it"aja apliec"iba, vad"it"aja apliec"ibas numurs, vad"it"aja at"lauja, vad"it"aja licences numurs, vad"it"aji lic.
Lithuania	vairuotojo pa"zym"ejimas
Luxembourg	fahrerlaubnis, f"uhriersch"ain
Malta	licenzja tas-sewqan
Netherlands	permis de conduire, rijbewijs, rijbewijsnummer
Poland	numer licencyjny, prawo jazdy, zezwolenie na prowadzenie

Negara atau wilayah	Kata kunci
Portugal	carta de condução, carteira de habilitação, carteira de motorist, carteira habilitação, carteira motorist, licença condução, licença de condução, número de licença, número licença, permissão condução, permissão de condução
Romania	numărul permisului de conducere, permis de conducere
Slovakia	číslo licencie, číslo vodičského preukazu, ovládače lic., povolenia vodičov, povolenie jazdu, povolenie na jazdu, povolenie vodiča, vodičský preukaz
Slovenia	vozniško dovoljenje
Spain	carnet conductor, el carnet de conductor, licencia conductor, licencia de manejo, número carnet conductor, número de carnet de conductor, número de permiso conductor, número de permiso de conductor, número licencia conductor, número permiso conductor, permiso conducción, permiso conductor, permiso de conducción
Sweden	ajokortin numero, dlno# ajokortti, drivere lic., förare lic., körkort, körkort nummer, körkortsnummer, kuljettajat lic.

Negara atau wilayah	Kata kunci
UK	dl#, dl:, dlno#, driver licence, driver licences, driver license, driver licenses, driver permit, drivers lic., drivers licence, driver's licence, drivers licences, driver's licences, drivers license, driver's license, drivers licenses, driver's licenses, drivers permit, driver's permit, drivers permit number, driving licence, driving license, driving permit
US	dl#, dl:, dlno#, driver licence, driver licences, driver license, driver licenses, driver permit, drivers lic., drivers licence, driver's licence, drivers licences, driver's licences, drivers license, driver's license, drivers licenses, driver's licenses, drivers permit, driver's permit, drivers permit number, driving licence, driving license, driving permit

Komentar: Tidak ada

Nomor Roll Pemilu

ID pengenalan data terkelola: UK\_ELECTORAL\_ROLL\_NUMBER

Negara dan wilayah yang didukung: Inggris

Kata kunci yang dibutuhkan: Ya. Kata kunci meliputi: electoral #, electoral number, electoral roll #, electoral roll no., electoral roll number, electoralrollno

Komentar: Tidak ada

Nama lengkap

ID pengenalan data terkelola: NAME

Negara dan wilayah yang didukung: Apa saja

Kata kunci yang dibutuhkan: Tidak

Komentar: Macie hanya dapat mendeteksi nama lengkap. Dukungan terbatas pada set karakter Latin.

### Koordinat Sistem Pemosisian Global (GPS)

ID pengidentifikasi data terkelola: LATITUDE\_LONGITUDE

Negara dan wilayah yang didukung: Apa saja, jika koordinat berada di dekat kata kunci bahasa Inggris.

Kata kunci yang dibutuhkan: Ya. Kata kunci meliputi: coordinate, coordinates, lat long, latitude longitude, position

Komentar: Macie dapat mendeteksi koordinat GPS jika koordinat lintang dan bujur disimpan sebagai pasangan dan mereka dalam format Derajat Desimal (DD), misalnya. 41.948614, -87.655311

Support tidak menyertakan deteksi koordinat dalam format: Degrees Decimal Minutes (DDM), misalnya 41°56.9168'N 87°39.3187'W; atau format Degrees, Minutes, Seconds (DMS), misalnya. 41°56'55.0104"N 87°39'19.1196"W

### HTTP cookie

ID pengidentifikasi data terkelola: HTTP\_COOKIE

Negara dan wilayah yang didukung: Apa saja

Kata kunci yang dibutuhkan: Tidak

Komentar: Deteksi membutuhkan lengkap Cookie atau Set-Cookie header. Header dapat menyertakan satu atau lebih pasangan nama-nilai, misalnya: Set-Cookie: id=TW1rZQ dan. Cookie: session=3948; lang=en

### Alamat surat-menyurat

ID pengenalan data terkelola: ADDRESS (untuk Australia, Kanada, Prancis, Jerman, Italia, Spanyol, Inggris, dan AS), BRAZIL\_CEP\_CODE (untuk Pos Código de Endereçamento Brasil)

Negara dan wilayah yang didukung: Australia, Brasil, Kanada, Prancis, Jerman, Italia, Spanyol, Inggris, AS

Kata kunci yang dibutuhkan: Bervariasi. Kata kunci tidak diperlukan oleh pengidentifikasi data ADDRESS terkelola. Kata kunci diperlukan oleh pengidentifikasi data BRAZIL\_CEP\_CODE terkelola. Kata kunci meliputi: cep, código de endereçamento postal, codigo de endereçamento postal, código postal, codigo postal



Komentar: Meskipun kata kunci tidak diperlukan oleh pengenal data ADDRESS terkelola, deteksi memerlukan alamat untuk menyertakan nama kota atau tempat dan ZIP atau Kode Pos yang sesuai di negara atau wilayah yang didukung. Pengidentifikasi data BRAZIL\_CEP\_CODE terkelola hanya dapat mendeteksi bagian Código de Endereçamento Postal (CEP) dari suatu alamat.

#### Nomor identifikasi nasional

Support termasuk nomor Aadhaar untuk India, nomor Codice Fiscale untuk Italia, pengidentifikasi Documento Nacional de Identidad (DNI) untuk Spanyol, kode Institut Nasional Prancis untuk Statistik dan Studi Ekonomi (INSEE), nomor Kartu Identitas Nasional Jerman, dan nomor Registro Geral (RG) untuk Brasil.

ID pengenal data terkelola: Tergantung pada negara atau wilayah, BRAZIL\_RG\_NUMBER, FRANCE\_NATIONAL\_IDENTIFICATION\_NUMBER, GERMANY\_NATIONAL\_IDENTIFICATION\_NUMBER, INDIA\_AADHAAR\_NUMBER, ITALY\_NATIONAL\_IDENTIFICATION\_NUMBER, SPAIN\_DNI\_NUMBER

Negara dan wilayah yang didukung: Brasil, Prancis, Jerman, India, Italia, Spanyol

Kata kunci yang dibutuhkan: Ya. Tabel berikut mencantumkan kata kunci yang Macie kenali untuk negara dan wilayah tertentu.

Negara atau wilayah	Kata kunci
Brazil	registro geral, rg
France	assurance sociale, carte nationale d'identité, cni, code sécurité sociale, French social security number, fssn#, insee, insurance number, national id number, nationalid#, numéro d'assurance, sécurité sociale, sécurité sociale non., sécurité sociale numéro, social, social security, social security number, socialsecuritynumber, ss#, ssn, ssn#
Germany	ausweisnummer, id number, identification number, identity number, insurance number, personal id, personalausweis
India	aadhaar, aadhar, adhaar, uidai

Negara atau wilayah	Kata kunci
Italy	codice fiscal, dati anagrafici, ehic, health card, health insurance card, p. iva, partita i.v.a., personal data, tax code, tessera sanitaria
Spain	dni, dni#, dninúmero#, documento nacional de identidad, identidad único, identidadúnico#, insurance number, national identification number, national identity, nationalid#, nationali dno#, número nacional identidad, personal identification number, personal identity no, unique identity number, uniqueid#

Komentar: Tidak ada

Nomor Asuransi Nasional (NINO)

ID pengidentifikasi data terkelola: UK\_NATIONAL\_INSURANCE\_NUMBER

Negara dan wilayah yang didukung: Inggris

Kata kunci yang dibutuhkan: Ya. Kata kunci meliputi: insurance no., insurance number, insurance#, national insurance number, nationalinsurance#, nationalinsurancenumber, nin, nino

Komentar: Tidak ada

Nomor paspor

ID pengenalan data terkelola: Tergantung pada negara atau wilayah, CANADA\_PASSPORT\_NUMBER, FRANCE\_PASSPORT\_NUMBER, GERMANY\_PASSPORT\_NUMBER, ITALY\_PASSPORT\_NUMBER, SPAIN\_PASSPORT\_NUMBER, UK\_PASSPORT\_NUMBER, USA\_PASSPORT\_NUMBER

Negara dan wilayah yang didukung: Kanada, Prancis, Jerman, Italia, Spanyol, Inggris, AS

Kata kunci yang dibutuhkan: Ya. Tabel berikut mencantumkan kata kunci yang Macie kenali untuk negara dan wilayah tertentu.

Negara atau wilayah	Kata kunci
Canada	pasport, pasport#, passport, passport#, passportno, passportno#
France	numéro de pasport, pasport, pasport #, pasport n °, pasport non
Germany	ausstellungsdatum, ausstellungsort, geburtsdatum, passport, passports, reiseepass, reiseepassnr, reiseepassnummer
Italy	italian passport number, numéro pasport, numéro pasport italien, passaporto, passaporto italiana, passaporto numero, passport number, repubblica italiana passaporto
Spain	españa pasaporte, libreta pasaporte, número pasaporte, pasaporte, passport, passport book, passport no, passport number, spain passport
UK	pasport #, pasport n °, pasport non, pasportn °, passport #, passport no, passport number, passport#, passportid
US	passport, travel document

Komentar: Tidak ada

Nomor tempat tinggal permanen

ID pengidentifikasi data terkelola: CANADA\_NATIONAL\_IDENTIFICATION\_NUMBER

Negara dan wilayah yang didukung: Kanada

Kata kunci yang dibutuhkan: Ya. Kata kunci meliputi: carte résident permanent, numéro carte résident permanent, numéro résident permanent, permanent resident card, permanent resident card number,

permanent resident no, permanent resident no., permanent resident number, pr no, pr no., pr non, pr number, résident permanent no., résident permanent non

Komentar: Tidak ada

Nomor telepon

ID pengenalan data terkelola: Tergantung pada negara atau wilayah, BRAZIL\_PHONE\_NUMBER, FRANCE\_PHONE\_NUMBER, GERMANY\_PHONE\_NUMBER, ITALY\_PHONE\_NUMBER, PHONE\_NUMBER (for Canada and the US), SPAIN\_PHONE\_NUMBER, UK\_PHONE\_NUMBER

Negara dan wilayah yang didukung: Brasil, Kanada, Prancis, Jerman, Italia, Spanyol, Inggris, AS

Kata kunci yang dibutuhkan: Bervariasi. Jika kata kunci berada di dekat data, nomor tersebut tidak harus menyertakan kode negara. Kata kunci meliputi: cell, contact, fax, fax number, mobile, phone, phone number, tel, telephone, telephone number. Untuk Brasil, kata kunci juga mencakup: cel, celular, fone, móvel, número residencial, numero residencial, telefone. Jika kata kunci tidak dekat dengan data, nomor tersebut harus menyertakan kode negara.

Komentar: Untuk AS, dukungan termasuk nomor bebas pulsa.

Nomor Asuransi Sosial (SIN)

ID pengidentifikasi data terkelola: CANADA\_SOCIAL\_INSURANCE\_NUMBER

Negara dan wilayah yang didukung: Kanada

Kata kunci yang dibutuhkan: Ya. Kata kunci meliputi: canadian id, numéro d'assurance sociale, sin, social insurance number

Komentar: Tidak ada

Nomor Jaminan Sosial (SSN)

ID pengenalan data terkelola: Tergantung pada negara atau wilayah,, SPAIN\_SOCIAL\_SECURITY\_NUMBER USA\_SOCIAL\_SECURITY\_NUMBER

Negara dan wilayah yang didukung: Spanyol, AS

Kata kunci yang dibutuhkan: Ya. Untuk Spanyol, kata kunci meliputi: número de la seguridad social, social security no., social security number, socialsecurityno#, ssn, ssn#. Untuk AS, kata kunci meliputi: social security, ss#, ssn.

Komentar: Tidak ada

## Nomor identifikasi wajib pajak atau referensi

Support meliputi: Nomor CIF, NIE, dan NIF untuk Spanyol; Nomor CNPJ dan CPF untuk Brasil; Nomor Codice Fiscale untuk Italia; ITIN untuk AS; PAN untuk India; Nomor Steueridentifikationsnummer untuk Jerman; TFN untuk Australia; TIN untuk Prancis; dan, nomor TRN dan UTR untuk Inggris.

ID pengenalan data terkelola: Tergantung pada negara atau wilayah, AUSTRALIA\_TAX\_FILE\_NUMBER, BRAZIL\_CNPJ\_NUMBER, BRAZIL\_CPF\_NUMBER, FRANCE\_TAX\_IDENTIFICATION\_NUMBER, GERMANY\_TAX\_IDENTIFICATION\_NUMBER, INDIA\_PERMANENT\_ACCOUNT\_NUMBER, ITALY\_NATIONAL\_IDENTIFICATION\_NUMBER, SPAIN\_NIE\_NUMBER, SPAIN\_NIF\_NUMBER, SPAIN\_TAX\_IDENTIFICATION\_NUMBER, UK\_TAX\_IDENTIFICATION\_NUMBER, USA\_INDIVIDUAL\_TAX\_IDENTIFICATION\_NUMBER

Negara dan wilayah yang didukung: Australia, Brasil, Prancis, Jerman, India, Italia, Spanyol, Inggris, AS

Kata kunci yang dibutuhkan: Ya. Tabel berikut mencantumkan kata kunci yang Macie kenali untuk negara dan wilayah tertentu.

Negara atau wilayah	Kata kunci
Australia	tax file number, tfn
Brazil	cadastro de pessoa física, cadastro de pessoa física, cadastro de pessoas físicas, cadastro de pessoas físicas, cadastro nacional da pessoa jurídica, cadastro nacional da pessoa jurídica, cnpj, cpf
France	numéro d'identification fiscal, tax id, tax identification number, tax number, tin, tin#
Germany	identifikationsnummer, steuer id, steueridentifikationsnummer, steuernummer, tax id, tax identification number, tax number
India	e-pan, pan card, pan number, permanent account number

Negara atau wilayah	Kata kunci
Italy	codice fiscal, dati anagrafici, ehic, health card, health insurance card, p. iva, partita i.v.a., personal data, tax code, tessera sanitaria
Spain	cif, cif número, cifnúmero#, nie, nif, número de contribuyente, número de identidad de extranjero, número de identificación fiscal, número de impuesto corporativo, personal tax number, tax id, tax identification number, tax number, tin, tin#
UK	paye, tax id, tax id no., tax id number, tax identification, tax identification#, tax no., tax number, tax reference, tax#, taxid#, temporary reference number, tin, trn, unique tax reference, unique taxpayer reference, utr
US	i.t.i.n., nomor pokok wajib pajak individu, itin

Komentar: Tidak ada

Nomor identifikasi kendaraan (VIN)

ID pengidentifikasi data terkelola: VEHICLE\_IDENTIFICATION\_NUMBER

Negara dan wilayah yang didukung: Apa saja, jika VIN berada di dekat kata kunci dalam salah satu bahasa berikut: Inggris, Prancis, Jerman, Lituania, Polandia, Portugis, Rumania, atau Spanyol.

Kata kunci yang dibutuhkan: Ya. Kata kunci meliputi: Fahrgestellnummer, niv, numarul de identificare, numarul seriei de sasiu, numer VIN, Número de Identificação do Veículo, Número de Identificación de Automóviles, numéro d'identification du véhicule, vehicle identification number, vin, VIN numeris

Komentar: Macie dapat mendeteksi VIN yang terdiri dari urutan 17 karakter dan mematuhi standar ISO 3779 dan 3780. Standar ini dirancang untuk penggunaan di seluruh dunia.

# Membangun pengidentifikasi data kustom di Amazon Macie

SEBUAH pengenalan data kustom adalah sekumpulan kriteria yang Anda tetapkan untuk mendeteksi data sensitif di objek Amazon Simple Storage Service (Amazon S3). Kriteria terdiri dari ekspresi reguler (regex) yang menentukan pola teks untuk dicocokkan dan, opsional, urutan karakter dan aturan jarak yang menyempurnakan hasil.

Dengan pengidentifikasi data kustom, Anda dapat menentukan kriteria deteksi yang mencerminkan skenario tertentu, kekayaan intelektual, atau data kepemilikan organisasi Anda—misalnya, ID karyawan, nomor akun pelanggan, atau klasifikasi data internal. Jika Anda mengkonfigurasi [lowongan kerja penemuan data sensitif](#) atau [penemuan data sensitif otomatis](#) untuk menggunakan pengidentifikasi ini, Anda dapat menganalisis objek S3 dengan cara yang melengkapi [pengidentifikasi data terkelola](#) yang disediakan Amazon Macie.

Selain kriteria deteksi, Anda dapat menentukan pengaturan tingkat keparahan khusus untuk temuan data sensitif yang dihasilkan oleh pengenalan data kustom. Secara default, Macie menetapkan [Sedang](#) tingkat keparahan pada semua temuan yang dihasilkan oleh pengenalan data kustom—tingkat keparahan tidak berubah berdasarkan jumlah kemunculan teks yang cocok dengan kriteria deteksi pengenalan data kustom. Dengan menentukan pengaturan tingkat keparahan khusus, Anda dapat menentukan tingkat keparahan mana yang akan ditetapkan berdasarkan jumlah kemunculan teks yang cocok dengan kriteria.

## Topik

- [Mendefinisikan kriteria deteksi untuk pengidentifikasi data kustom](#)
- [Mendefinisikan pengaturan tingkat keparahan temuan untuk pengidentifikasi data kustom](#)
- [Membuat pengidentifikasi data khusus](#)
- [Dukungan Regex dalam pengidentifikasi data kustom](#)

## Mendefinisikan kriteria deteksi untuk pengidentifikasi data kustom

Saat Anda membuat pengidentifikasi data kustom, Anda menentukan ekspresi reguler (regex) yang mendefinisikan pola teks untuk mencocokkan dalam objek S3. Macie mendukung subset dari sintaks pola regex yang disediakan oleh [Pustaka Perl Compatible Regular Expressions \(PCRE\)](#). Untuk informasi lebih lanjut, lihat [Dukungan Regex](#) nanti di bagian ini.

Anda juga dapat menentukan urutan karakter, seperti kata dan frasa, dan aturan kedekatan untuk menyempurnakan hasil.

## Kata kunci

Ini adalah urutan karakter tertentu yang harus berada di dekat teks yang cocok dengan pola regex. Persyaratan jarak bervariasi berdasarkan format penyimpanan objek S3 atau tipe file:

- Untuk terstruktur, data kolumnar, Macie menyertakan hasil jika teks cocok dengan pola regex dan kata kunci dalam nama bidang atau kolom yang menyimpan teks, atau teks didahului oleh dan dalam jarak pertandingan maksimum kata kunci di bidang atau nilai sel yang sama. Hal ini berlaku untuk buku kerja Microsoft Excel, file CSV, dan file TSV.
- Untuk data terstruktur dan berbasis rekaman, Macie menyertakan hasil jika teks cocok dengan pola regex dan teks berada dalam jarak pencocokan maksimum kata kunci. Kata kunci dapat dalam nama elemen di jalan ke bidang atau array yang menyimpan teks, atau dapat mendahului dan menjadi bagian dari nilai yang sama di bidang atau array yang menyimpan teks. Hal ini berlaku untuk kontainer objek Apache Avro, file Apache Parquet, file JSON, dan file JSON Lines.
- Untuk data tidak terstruktur, Macie menyertakan hasil jika teks cocok dengan pola regex dan teks didahului oleh dan dalam jarak pencocokan maksimum kata kunci. Hal ini berlaku untuk file Adobe Portable Document Format, dokumen Microsoft Word, pesan email, dan file teks non-biner selain file CSV, JSON, JSON Lines, dan TSV. Termasuk data terstruktur, seperti tabel, dalam tipe file ini.

Anda dapat menentukan sebanyak 50 kata kunci. Setiap kata kunci dapat berisi 3-90 karakter UTF-8. Kata kunci tidak peka huruf besar atau kecil.

### Jarak pertandingan maksimum

Ini adalah aturan kedekatan berbasis karakter untuk kata kunci. Macie menggunakan pengaturan ini untuk menentukan apakah kata kunci mendahului teks yang cocok dengan pola regex. Pengaturan mendefinisikan jumlah maksimum karakter yang dapat ada antara akhir kata kunci lengkap dan akhir teks yang cocok dengan pola regex. Jika teks cocok dengan pola regex, terjadi setelah setidaknya satu kata kunci lengkap, dan terjadi dalam jarak yang ditentukan dari kata kunci, Macie termasuk dalam hasil. Jika tidak, Macie mengecualikannya dari hasil.

Anda dapat menentukan jarak sebanyak 1–300 karakter. Jarak default adalah 50 karakter. Untuk hasil terbaik, jarak ini harus lebih besar dari jumlah minimum karakter teks yang dirancang untuk dideteksi oleh regex. Jika hanya sebagian teks yang berada dalam jarak pencocokan maksimum kata kunci, Macie tidak memasukkannya ke dalam hasil.



## Abaikan kata-kata

Kata yang diabaikan adalah urutan karakter tertentu yang dikecualikan dari hasil pencarian. Jika teks cocok dengan pola regex tetapi berisi kata abaikan, Macie tidak memasukkannya ke dalam hasil.

Anda dapat menentukan sebanyak 10 kata yang diabaikan. Setiap kata abaikan dapat berisi 4-90 karakter UTF-8. Kata yang diabaikan peka huruf besar kecil.

Misalnya, banyak perusahaan memiliki sintaks khusus untuk ID karyawan. Salah satu sintaks tersebut mungkin: huruf kapital yang menunjukkan apakah karyawan adalah penuh-waktu (F) atau paruh waktu (P) karyawan, diikuti oleh tanda hubung (-), diikuti oleh urutan delapan digit yang mengidentifikasi karyawan. Contohnya adalah:F-12345678, untuk karyawan penuh waktu, danP-87654321, untuk karyawan paruh waktu.

Jika Anda membuat pengidentifikasi data kustom untuk mendeteksi ID karyawan yang menggunakan sintaks ini, Anda mungkin dapat menggunakan regex berikut: `[A-Z]-\d{8}`. Untuk menyempurnakan analisis dan menghindari positif palsu, Anda mungkin juga mengonfigurasi pengenalan data khusus untuk menggunakan kata kunci karyawan dan ID karyawan jarak pertandingan maksimum 20 karakter. Dengan kriteria ini, hasilnya mencakup teks yang cocok dengan regex hanya jika teks terjadi setelah kata kunci karyawan atau ID karyawan dan semua teks terjadi dalam 20 karakter dari salah satu kata kunci tersebut.

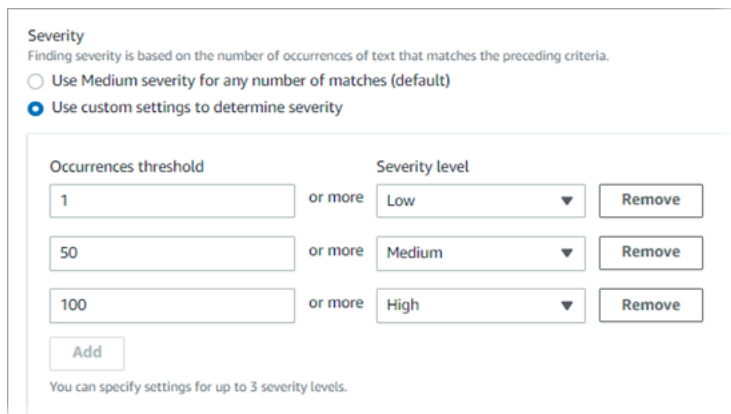
Untuk demonstrasi bagaimana kata kunci dapat membantu Anda menemukan data sensitif dan menghindari positif palsu, tonton video berikut: [Cara Amazon Macie menggunakan kata kunci untuk menemukan data sensitif](#).

## Mendefinisikan pengaturan tingkat keparahan temuan untuk pengidentifikasi data kustom

Saat membuat pengenalan data kustom, Anda juga dapat menentukan pengaturan tingkat keparahan khusus untuk temuan data sensitif yang dihasilkan pengenalan. Secara default, Macie menetapkan `Sedang` tingkat keparahan pada semua temuan yang dihasilkan oleh pengenalan data kustom—jika objek S3 berisi setidaknya satu kejadian teks yang cocok dengan kriteria deteksi pengenalan data kustom, Macie secara otomatis menetapkan `Sedang` keparahan temuan yang dihasilkan.

Dengan pengaturan tingkat keparahan khusus, Anda dapat menentukan tingkat keparahan mana yang akan ditetapkan berdasarkan jumlah kemunculan teks yang cocok dengan kriteria deteksi pengidentifikasi data kustom. Untuk melakukan ini, Anda mendefinisikan ambang kejadian untuk sebanyak tiga tingkat keparahan: Rendah (paling parah), Sedang, dan Tinggi (paling parah). Sebuah ambang kejadian adalah jumlah minimum kecocokan yang harus ada dalam objek S3 untuk menghasilkan temuan dengan tingkat keparahan yang ditentukan. Jika Anda menentukan lebih dari satu ambang batas, ambang batas harus dalam urutan menaik berdasarkan tingkat keparahan, bergerak dari Rendah kepada Tinggi.

Misalnya, gambar berikut menunjukkan pengaturan tingkat keparahan untuk pengenalan data kustom yang menentukan tiga ambang kejadian, satu untuk setiap tingkat keparahan yang didukung Macie.



Tabel berikut menunjukkan tingkat keparahan temuan yang dihasilkan oleh pengenalan data kustom.

Ambang kejadian	Tingkat keparahan	Hasil
1	Rendah	Jika objek S3 berisi 1—49 kejadian teks yang cocok dengan kriteria deteksi, tingkat keparahan temuan yang dihasilkan adalah Rendah.
50	Sedang	Jika objek S3 berisi 50-99 kejadian teks yang sesuai dengan kriteria deteksi, tingkat keparahan temuan yang dihasilkan adalah Sedang.

Ambang kejadian	Tingkat kepelikan	Hasil
100	Tinggi	Jika objek S3 berisi 100 atau lebih kejadian teks yang cocok dengan kriteria deteksi, tingkat keparahan temuan yang dihasilkan adalah Tinggi.

Anda juga dapat menggunakan pengaturan tingkat keparahan untuk menentukan apakah akan membuat temuan sama sekali. Jika objek S3 mengandung lebih sedikit kejadian daripada ambang batas kejadian terendah, Macie tidak membuat temuan.

## Membuat pengidentifikasi data khusus

Ikuti langkah-langkah ini untuk membuat pengenalan data khusus dengan menggunakan konsol Amazon Macie. Untuk membuat pengenalan data khusus secara terprogram, gunakan [CreateCustomDataIdentifier](#) pengoperasian Amazon Macie API.

Untuk membuat pengenalan data kustom

1. Buka konsol Amazon Macie di <https://console.aws.amazon.com/macie/>.
2. Di panel navigasi, di bawah Pengaturan, pilih Pengidentifikasi data kustom.
3. Pilih Create (Buat).
4. Untuk Nama, masukkan nama untuk pengidentifikasi data kustom. Nama dapat berisi sebanyak 128 karakter.

Hindari memasukkan data sensitif apa pun dalam nama. Pengguna lain dari akun Anda mungkin dapat melihat namanya, tergantung pada tindakan yang diizinkan mereka lakukan di Macie.

5. (Opsional) Untuk Deskripsi, masukkan deskripsi singkat tentang pengidentifikasi data kustom. Deskripsi dapat berisi sebanyak 512 karakter.

Hindari memasukkan data sensitif apa pun dalam deskripsi. Pengguna lain dari akun Anda mungkin dapat melihat deskripsi, tergantung pada tindakan yang diizinkan mereka lakukan di Macie.

6. Untuk Ekspresi reguler, masukkan ekspresi reguler (regex) yang mendefinisikan pola teks untuk mencocokkan. Regex dapat berisi sebanyak 512 karakter. Untuk mempelajari tentang sintaks dan batasan yang didukung, lihat [Dukungan Regex](#) pada bagian ini.

7. (Opsional) Untuk Kata kunci, masukkan sebanyak 50 urutan karakter (dipisahkan dengan koma) untuk menentukan teks tertentu yang harus berada di dekat teks yang cocok dengan pola regex. Setiap kata kunci dapat berisi 3-90 karakter UTF-8. Kata kunci tidak peka huruf besar atau kecil.

Macie menyertakan kejadian dalam hasil hanya jika teks cocok dengan pola regex dan teks berada dalam jarak pertandingan maksimum salah satu kata kunci ini, seperti yang dijelaskan dalam [topik sebelumnya](#).

8. (Opsional) Untuk Abaikan kata-kata, masukkan sebanyak 10 urutan karakter (dipisahkan dengan koma) yang menentukan teks tertentu untuk dikecualikan dari hasil. Setiap kata abaikan dapat berisi 4-90 karakter UTF-8. Abaikan kata peka akan huruf besar kecil.

Macie mengecualikan kejadian dari hasil jika teks cocok dengan pola regex tetapi berisi salah satu dari kata-kata mengabaikan ini.

9. (Opsional) Untuk Jarak pertandingan maksimum, masukkan jumlah maksimum karakter yang dapat ada antara akhir kata kunci dan akhir teks yang cocok dengan pola regex. Jaraknya bisa 1-300 karakter. Jarak default adalah 50 karakter.

Macie menyertakan kejadian dalam hasil hanya jika teks cocok dengan pola regex dan teks berada dalam jarak ini dari kata kunci lengkap, seperti yang dijelaskan dalam [topik sebelumnya](#).

10. Untuk Keparahan, pilih bagaimana Anda ingin Macie menetapkan tingkat keparahan ke temuan data sensitif yang dihasilkan oleh pengenalan data kustom:
  - Untuk secara otomatis menetapkan Sedang keparahan untuk semua temuan, pilih Gunakan Tingkat keparahan sedang untuk sejumlah kecocokan (default). Dengan opsi ini, Macie secara otomatis menetapkan Sedang keparahan temuan jika objek S3 yang terpengaruh berisi satu atau lebih kejadian teks yang cocok dengan kriteria deteksi.
  - Untuk menetapkan tingkat keparahan berdasarkan ambang kejadian yang Anda tentukan, pilih Gunakan pengaturan khusus untuk menentukan tingkat keparahan. Kemudian gunakan Ambang kejadian dan Tingkat keparahan pilihan untuk menentukan jumlah minimum kecocokan yang harus ada dalam objek S3 untuk menghasilkan temuan dengan tingkat keparahan yang dipilih.

Misalnya, untuk menetapkan Tinggi keparahan temuan yang melaporkan 100 atau lebih kejadian teks yang cocok dengan kriteria deteksi, masukkan **100** di dalam Ambang kejadian kotak dan kemudian pilih Tinggi dari Tingkat keparahan daftar.

Anda dapat menentukan sebanyak tiga ambang kejadian, satu untuk setiap tingkat keparahan yang didukung Macie: Rendah (paling tidak parah), Sedang, atau Tinggi (untuk yang

paling parah). Jika Anda menentukan lebih dari satu, ambang batas harus dalam urutan menaik berdasarkan tingkat keparahan, bergerak dari Rendah kepada Tinggi. Jika objek S3 mengandung lebih sedikit kejadian daripada ambang batas terendah yang ditentukan, Macie tidak membuat temuan.

11. (Opsional) Untuk Tag, pilih Tambahkan tag, dan kemudian masukkan sebanyak 50 tag untuk ditetapkan ke pengidentifikasi data kustom.

SEBUAH menandai adalah label yang Anda tentukan dan tetapkan untuk jenis tertentu AWS sumber daya. Setiap tanda terdiri dari kunci tanda yang diperlukan dan nilai tanda opsional. Tag dapat membantu Anda mengidentifikasi, mengkategorikan, dan mengelola sumber daya dengan cara yang berbeda, seperti dengan tujuan, pemilik, lingkungan, atau kriteria lainnya. Untuk mempelajari selengkapnya, lihat [Menandai sumber daya Amazon Macie](#).

12. (Opsional) Untuk Evaluasi, masukkan hingga 1.000 karakter di Data sampel kotak, dan kemudian pilih Tes untuk menguji kriteria deteksi. Macie mengevaluasi data sampel dan melaporkan jumlah kejadian teks yang sesuai dengan kriteria. Anda dapat mengulangi langkah ini sebanyak yang Anda inginkan untuk memperbaiki dan mengoptimalkan kriteria.

#### Note

Kami sangat menyarankan agar Anda menguji dan menyempurnakan kriteria deteksi sebelum Anda menyimpan pengenalan data kustom. Karena pengidentifikasi data kustom digunakan oleh tugas penemuan data sensitif, Anda tidak dapat mengedit pengidentifikasi data kustom setelah menyimpannya. Hal ini membantu untuk memastikan bahwa Anda memiliki riwayat tetap temuan dan hasil penemuan data sensitif untuk audit privasi dan perlindungan data atau investigasi yang Anda lakukan.

13. Setelah selesai, pilih Kirim.

Macie menguji pengaturan dan memverifikasi bahwa ia dapat mengkompilasi regex. Jika ada masalah dengan salah satu pengaturan atau regex, kesalahan terjadi dan menunjukkan sifat masalah. Setelah mengatasi masalah apa pun, Anda dapat menyimpan pengidentifikasi data khusus.

## Dukungan Regex dalam pengidentifikasi data kustom

Macie mendukung subset dari sintaks pola regex yang disediakan oleh [Pustaka Perl Compatible Regular Expressions \(PCRE\)](#). Dari konstruksi yang disediakan oleh pustaka PCRE, Macie tidak mendukung elemen pola berikut:

- Backreferences
- Mengambil grup
- Pola bersyarat
- Kode sematan
- Pola bendera global, seperti `/i`, `/m`, dan `/x`
- Pola rekursif
- Asersi lebar nol lookbehind dan lookahead positif dan negatif, seperti `?=`, `?!`, `?<=`, dan `?<!`

Untuk membuat pola regex yang efektif untuk pengidentifikasi data kustom, perhatikan juga tips dan rekomendasi berikut:

- Jangkar- Gunakan jangkar (`^` atau `$`) hanya jika Anda mengharapkan pola muncul di awal atau akhir file, bukan awal atau akhir baris.
- Bounded repeat — Untuk alasan performa, Macie membatasi ukuran grup bounded repeat. Misalnya, `\d{100,1000}` tidak akan dikompilasi di Macie. Untuk memperkirakan fungsionalitas ini, Anda dapat menggunakan open ended repeat seperti `\d{100,}`.
- Ketidakpekaan huruf besar kecil — Untuk membuat bagian pola menjadu tidak peka huruf besar kecil, Anda dapat menggunakan construct `(?i)` bukan bendera `/i`.
- Performa — Prefiks atau pergantian tidak perlu dioptimalkan secara manual. Misalnya, mengubah `/hello|hi|hey/` menjadi `/h(?:ello|i|ey)/` tidak akan meningkatkan performa.
- Wildcard — Untuk alasan performa, Macie membatasi jumlah wildcard berulang. Misalnya, `a*b*a*` tidak akan dikompilasi di Macie.

Untuk melindungi dari ekspresi cacat atau jangka panjang, Macie secara otomatis menguji pola regex terhadap kumpulan teks sampel.

## Mendefinisikan pengecualian data sensitif dengan Amazon Macie memungkinkan daftar

Dengan daftar allow di Amazon Macie, Anda dapat menentukan pola teks dan teks tertentu yang Anda ingin Macie abaikan saat memeriksa objek Simple Storage Service (Amazon S3) untuk data sensitif. Ini biasanya pengecualian data sensitif untuk skenario atau lingkungan tertentu Anda. Jika data cocok dengan teks atau pola teks dalam daftar izinkan, Macie tidak melaporkan data,

meskipun data tersebut sesuai dengan kriteria [pengenal data terkelola atau pengenal data kustom](#). Dengan menggunakan daftar izinkan, Anda dapat menyempurnakan analisis data Amazon S3 dan mengurangi noise.

Anda dapat membuat dan menggunakan dua jenis daftar izinkan di Macie:

- Teks yang telah ditetapkan — Untuk jenis daftar ini, Anda menentukan urutan karakter tertentu yang akan diabaikan, misalnya, nama perwakilan publik untuk organisasi Anda, nomor telepon tertentu, atau data sampel tertentu yang digunakan organisasi Anda untuk pengujian. Jika Anda menggunakan jenis daftar ini, Macie mengabaikan teks yang sama persis dengan entri dalam daftar.

Jenis daftar izinkan ini sangat membantu jika Anda ingin menentukan kata, frasa, dan jenis urutan karakter lainnya yang tidak sensitif, tidak mungkin berubah, dan tidak selalu mematuhi pola umum.

- Ekspresi reguler — Untuk jenis daftar ini, Anda menentukan ekspresi reguler (regex) yang mendefinisikan pola teks yang akan diabaikan—misalnya, nomor telepon publik untuk organisasi Anda, alamat e-mail untuk domain organisasi Anda, atau data sampel berpola yang digunakan organisasi Anda untuk pengujian. Jika Anda menggunakan jenis daftar ini, Macie mengabaikan teks yang benar-benar cocok dengan pola yang ditentukan oleh daftar.

Jenis daftar izinkan ini sangat membantu jika Anda ingin menentukan teks yang tidak sensitif tetapi bervariasi atau kemungkinan akan berubah sementara juga mengikuti pola umum.

Setelah membuat daftar izinkan, Anda dapat [membuat dan mengonfigurasi pekerjaan penemuan data sensitif](#) untuk menggunakannya, atau [menambahkannya ke setelan penemuan data sensitif otomatis](#). Macie kemudian menggunakan daftar ketika menganalisis data. Jika Macie menemukan teks yang cocok dengan entri atau pola dalam daftar izinkan, Macie tidak melaporkan terjadinya teks dalam temuan data sensitif, statistik, dan jenis hasil lainnya.

Anda dapat membuat dan menggunakan daftar izinkan di semua Wilayah AWS tempat Macie saat ini tersedia kecuali Wilayah Asia Pacific (Osaka).

## Topik

- [Izinkan opsi dan persyaratan daftar di Amazon Macie](#)
- [Membuat dan mengelola daftar izinkan di Amazon Macie](#)

## Izinkan opsi dan persyaratan daftar di Amazon Macie

Di Amazon Macie, Anda dapat menggunakan daftar izinkan untuk menentukan pola teks atau teks yang ingin diabaikan Macie saat memeriksa objek Amazon Simple Storage Service (Amazon S3) untuk data sensitif. Macie menyediakan opsi untuk dua jenis daftar izinkan, teks yang telah ditentukan dan ekspresi reguler.

Daftar teks yang telah ditentukan sangat membantu jika Anda ingin Macie mengabaikan kata, frasa, dan jenis urutan karakter tertentu yang Anda anggap tidak sensitif. Contohnya adalah nama perwakilan publik untuk organisasi Anda, nomor telepon tertentu, atau data sampel spesifik yang digunakan organisasi Anda untuk pengujian. Jika Macie menemukan teks yang cocok dengan kriteria pengenalan data terkelola atau pengidentifikasi data kustom dan teks juga cocok dengan entri dalam daftar izin, Macie tidak melaporkan terjadinya teks tersebut dalam temuan data sensitif, statistik, dan jenis hasil lainnya.

Ekspresi reguler (regex) sangat membantu jika Anda ingin Macie mengabaikan teks yang bervariasi atau cenderung berubah sambil juga mengikuti pola umum. Regex menentukan pola teks untuk diabaikan. Contohnya adalah nomor telepon publik untuk organisasi Anda, alamat email untuk domain organisasi Anda, atau data sampel berpola yang digunakan organisasi Anda untuk pengujian. Jika Macie menemukan teks yang cocok dengan kriteria pengenalan data terkelola atau pengidentifikasi data kustom dan teks juga cocok dengan pola regex dalam daftar izin, Macie tidak melaporkan terjadinya teks tersebut dalam temuan data sensitif, statistik, dan jenis hasil lainnya.

Anda dapat membuat dan menggunakan kedua jenis daftar izin di semua Wilayah AWS tempat Macie saat ini tersedia kecuali Wilayah Asia Pasifik (Osaka). Saat Anda membuat dan mengelola daftar izin, ingatlah opsi dan persyaratan berikut. Perhatikan juga bahwa mengizinkan entri daftar dan pola regex untuk alamat surat tidak didukung.

### Topik

- [Pilihan dan persyaratan untuk daftar teks yang telah ditentukan](#)
  - [Persyaratan sintaks](#)
  - [Persyaratan penyimpanan](#)
  - [Persyaratan enkripsi/Dekripsi](#)
  - [Pertimbangan dan rekomendasi desain](#)
- [Opsi dan persyaratan untuk ekspresi reguler dalam daftar izinkan](#)
  - [Dukungan dan rekomendasi sintaks](#)
  - [Contoh-contoh](#)



## Pilihan dan persyaratan untuk daftar teks yang telah ditentukan

Untuk jenis daftar izinkan ini, Anda menyediakan file teks biasa yang dibatasi baris yang mencantumkan urutan karakter tertentu untuk diabaikan. Entri daftar biasanya kata-kata, frasa, dan jenis urutan karakter lainnya yang Anda anggap tidak sensitif, tidak mungkin berubah, dan tidak harus mematuhi pola tertentu. Jika Anda menggunakan jenis daftar ini, Amazon Macie tidak melaporkan kemunculan teks yang sama persis dengan entri dalam daftar. Macie memperlakukan setiap entri daftar sebagai nilai literal string.

Untuk menggunakan jenis daftar izinkan ini, mulailah dengan membuat daftar di editor teks dan menyimpannya sebagai file teks biasa. Kemudian unggah daftar ke bucket S3 dan pastikan bahwa pengaturan penyimpanan dan enkripsi untuk bucket dan objek memungkinkan Macie untuk mengambil dan mendekripsi daftar. Kemudian [buat dan konfigurasi pengaturan untuk daftar di Macie](#).

Setelah Anda mengonfigurasi pengaturan di Macie, kami sarankan Anda menguji daftar izinkan dengan kumpulan data kecil yang representatif untuk akun atau organisasi Anda. Untuk menguji daftar, Anda dapat [membuat pekerjaan satu kali](#) dan mengonfigurasi pekerjaan untuk menggunakan daftar selain pengidentifikasi data terkelola dan pengidentifikasi data khusus yang biasanya Anda gunakan untuk menganalisis data. Anda kemudian dapat meninjau hasil pekerjaan—temuan data sensitif, hasil penemuan data sensitif, atau keduanya. Jika hasil pekerjaan berbeda dari yang Anda harapkan, Anda dapat mengubah dan menguji daftar sampai hasilnya sesuai dengan yang Anda harapkan.

Setelah selesai mengonfigurasi dan menguji daftar izin, Anda dapat membuat dan mengonfigurasi pekerjaan tambahan untuk menggunakannya, atau menambahkannya ke pengaturan penemuan data sensitif otomatis untuk akun Anda. Ketika pekerjaan tersebut mulai berjalan atau siklus analisis penemuan otomatis berikutnya dimulai, Macie mengambil versi terbaru dari daftar dari Amazon S3 dan menyimpannya dalam memori sementara. Macie kemudian menggunakan salinan sementara daftar ini ketika memeriksa objek S3 untuk data sensitif. Ketika pekerjaan selesai berjalan atau siklus analisis selesai, Macie secara permanen menghapus salinan daftarnya dari memori. Daftar ini tidak bertahan di Macie. Hanya pengaturan daftar yang bertahan di Macie.

### Important

Karena daftar teks yang telah ditentukan tidak bertahan di Macie, penting untuk [memeriksa status daftar izin Anda secara berkala](#). Jika Macie tidak dapat mengambil atau mengurai daftar yang Anda konfigurasi pekerjaan atau penemuan otomatis untuk digunakan, Macie

tidak menggunakan daftar tersebut. Ini mungkin menghasilkan hasil yang tidak terduga, seperti temuan data sensitif untuk teks yang Anda tentukan dalam daftar.

## Topik

- [Persyaratan sintaks](#)
- [Persyaratan penyimpanan](#)
- [Persyaratan enkripsi/Dekripsi](#)
- [Pertimbangan dan rekomendasi desain](#)

## Persyaratan sintaks

Saat Anda membuat daftar izinkan jenis ini, perhatikan persyaratan berikut untuk file daftar:

- Daftar harus disimpan sebagai file plaintext (`text/plain`), seperti `file.txt`, `.text`, atau `.plain`.
- Daftar harus menggunakan jeda baris untuk memisahkan entri individu. Sebagai contoh:

```
Akua Mansa  
John Doe  
Martha Rivera  
425-555-0100  
425-555-0101  
425-555-0102
```

Macie memperlakukan setiap baris sebagai entri tunggal yang berbeda dalam daftar. File ini juga dapat berisi baris kosong untuk meningkatkan keterbacaan. Macie melewati baris kosong saat mem-parsing file.

- Setiap entri dapat berisi 1-90 UTF—8 karakter.
- Setiap entri harus lengkap dan sama persis agar teks diabaikan. Macie tidak mendukung penggunaan karakter wildcard atau nilai parsial untuk entri. Macie memperlakukan setiap entri sebagai nilai literal string. Pertandingan tidak peka huruf besar/kecil.
- File dapat berisi 1-100.000 entri.
- Ukuran penyimpanan total file tidak boleh melebihi 35 MB.

## Persyaratan penyimpanan

Saat Anda menambahkan dan mengelola daftar izin di Amazon S3, perhatikan persyaratan dan rekomendasi penyimpanan berikut:

- Dukungan regional — Daftar izin harus disimpan dalam bucket S3 yang Wilayah AWS sama dengan akun Macie Anda. Macie tidak dapat mengakses daftar izin jika disimpan di Wilayah yang berbeda.
- Kepemilikan Bucket — Daftar izin harus disimpan dalam bucket S3 yang dimiliki oleh AndaAkun AWS. Jika Anda ingin akun lain menggunakan daftar izin yang sama, pertimbangkan untuk membuat aturan replikasi Amazon S3 untuk mereplikasi daftar ke bucket yang dimiliki oleh akun tersebut. Untuk informasi tentang mereplikasi objek S3, lihat [Mereplikasi objek di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon](#).

Selain itu, identitas AWS Identity and Access Management (IAM) Anda harus memiliki akses baca ke bucket S3 dan objek yang menyimpan daftar. Jika tidak, Anda tidak akan diizinkan untuk membuat atau memperbarui pengaturan daftar atau memeriksa status daftar dengan menggunakan Macie.

- Kebijakan bucket — Jika Anda menyimpan daftar izin di bucket S3 yang memiliki kebijakan bucket terbatas, pastikan kebijakan tersebut mengizinkan Macie untuk mengambil daftar tersebut. Untuk melakukannya, Anda dapat menambahkan kondisi untuk peran terkait layanan Macie ke kebijakan bucket. Untuk informasi selengkapnya, lihat [Mengizinkan Macie untuk mengakses bucket S3 dan objek](#).

Pastikan juga bahwa kebijakan tersebut memungkinkan identitas IAM Anda memiliki akses baca ke bucket. Jika tidak, Anda tidak akan diizinkan untuk membuat atau memperbarui pengaturan daftar atau memeriksa status daftar dengan menggunakan Macie.

- Jalur objek - Jika Anda menyimpan lebih dari satu daftar izin di Amazon S3, jalur objek untuk setiap daftar harus unik. Dengan kata lain, setiap daftar izinkan harus disimpan secara terpisah sebagai objek S3 miliknya sendiri.
- Kelas penyimpanan - Daftar izin harus disimpan langsung di Amazon S3 menggunakan salah satu kelas penyimpanan berikut: Reduced Redundancy (RRS), S3 Glacier Instant Retrieval, S3 Intelligent-Tiering, S3 One Zone-IA, S3 Standard, atau S3 Standard-IA.
- Pembuatan Versi — Saat menambahkan daftar izin ke bucket S3, sebaiknya Anda juga mengaktifkan pembuatan versi untuk bucket. Anda kemudian dapat menggunakan nilai tanggal dan waktu untuk mengkorelasikan versi daftar dengan hasil pekerjaan penemuan data sensitif

dan siklus penemuan data sensitif otomatis yang menggunakan daftar. Ini dapat membantu audit privasi dan perlindungan data atau investigasi yang Anda lakukan.

- **Kunci Objek** — Untuk mencegah daftar izin dihapus atau ditimpa untuk jangka waktu tertentu atau tanpa batas waktu, Anda dapat mengaktifkan Object Lock untuk bucket S3 yang menyimpan daftar. Mengaktifkan pengaturan ini tidak mencegah Macie mengakses daftar. Untuk informasi tentang pengaturan ini, lihat [Menggunakan Lock Object S3](#) di Panduan Pengguna Amazon Simple Storage Service.

## Persyaratan enkripsi/Dekripsi

Jika Anda mengenkripsi daftar izin di Amazon S3, kebijakan izin untuk peran [terkait layanan Macie biasanya memberi Macie](#) izin yang diperlukan untuk mendekripsi daftar. Namun, ini tergantung pada jenis enkripsi yang digunakan:

- Jika daftar dienkripsi menggunakan enkripsi sisi server dengan kunci terkelola Amazon S3 (SSE-S3), Macie dapat mendekripsi daftar tersebut. Peran terkait layanan untuk akun Macie Anda memberi Macie izin yang dibutuhkan.
- Jika daftar dienkripsi menggunakan enkripsi sisi server dengan AWS terkelola AWS KMS key (DSSE-KMS atau SSE-KMS), Macie dapat mendekripsi daftar tersebut. Peran terkait layanan untuk akun Macie Anda memberi Macie izin yang dibutuhkan.
- Jika daftar dienkripsi menggunakan enkripsi sisi server dengan pelanggan yang dikelola AWS KMS key (DSSE-KMS atau SSE-KMS), Macie dapat mendekripsi daftar hanya jika Anda mengizinkan Macie untuk menggunakan kunci. Untuk mempelajari cara melakukannya, lihat [Mengizinkan Macie menggunakan pelanggan yang dikelola AWS KMS key](#).

### Note

Anda dapat mengenkripsi daftar dengan pelanggan yang dikelola AWS KMS key di toko kunci eksternal. Namun, kuncinya mungkin lebih lambat dan kurang dapat diandalkan daripada kunci yang dikelola sepenuhnya di dalamnya AWS KMS. Jika latensi atau masalah ketersediaan mencegah Macie mendekripsi daftar, Macie tidak menggunakan daftar saat menganalisis objek S3. Ini mungkin menghasilkan hasil yang tidak terduga, seperti temuan data sensitif untuk teks yang Anda tentukan dalam daftar. Untuk mengurangi risiko ini, pertimbangkan untuk menyimpan daftar dalam bucket S3 yang dikonfigurasi untuk menggunakan kunci sebagai Kunci Bucket S3.

Untuk informasi tentang penggunaan kunci KMS di penyimpanan kunci eksternal, lihat [Penyimpanan kunci eksternal](#) di Panduan AWS Key Management Service Pengembang.

Untuk informasi tentang menggunakan Kunci Bucket S3, lihat [Mengurangi biaya SSE-KMS dengan Kunci Bucket Amazon S3 di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon](#).

- Jika daftar dienkripsi menggunakan enkripsi sisi server dengan kunci yang disediakan pelanggan (SSE-C) atau enkripsi sisi klien, Macie tidak dapat mendekripsi daftar tersebut. Pertimbangkan untuk menggunakan enkripsi SSE-S3, DSSE-KMS, atau SSE-KMS sebagai gantinya.

Jika daftar dienkripsi dengan kunci KMS AWS terkelola atau kunci KMS yang dikelola pelanggan, identitas AWS Identity and Access Management (IAM) Anda juga harus diizinkan untuk menggunakan kunci tersebut. Jika tidak, Anda tidak akan diizinkan untuk membuat atau memperbarui pengaturan daftar atau memeriksa status daftar dengan menggunakan Macie. Untuk mempelajari cara memeriksa atau mengubah izin untuk kunci KMS, lihat [Kebijakan kunci AWS KMS di Panduan AWS Key Management Service](#) Pengembang.

Untuk informasi terperinci tentang opsi enkripsi untuk data Amazon S3, lihat [Melindungi data dengan enkripsi](#) di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

Pertimbangan dan rekomendasi desain

Secara umum, Macie memperlakukan setiap entri dalam daftar izinkan sebagai nilai literal string. Artinya, Macie mengabaikan setiap kemunculan teks yang sama persis dengan entri lengkap dalam daftar izinkan. Pertandingan tidak peka huruf besar/kecil.

Namun, Macie menggunakan entri sebagai bagian dari ekstraksi data dan kerangka analisis yang lebih besar. Kerangka kerja ini mencakup pembelajaran mesin dan fungsi pencocokan pola yang faktor dimensi seperti variasi tata bahasa dan sintaksis dan, dalam banyak kasus, kedekatan kata kunci. Kerangka kerja juga memfaktorkan jenis file atau format penyimpanan objek S3. Oleh karena itu, ingatlah pertimbangan dan rekomendasi berikut saat Anda menambahkan dan mengelola entri dalam daftar izin.

Bersiaplah untuk berbagai jenis file dan format penyimpanan

Untuk data yang tidak terstruktur, seperti teks dalam file Adobe Portable Document Format (.pdf), Macie mengabaikan teks yang sama persis dengan entri lengkap dalam daftar izin, termasuk teks yang mencakup beberapa baris atau halaman.

Untuk data terstruktur, seperti data kolumnar dalam file CSV atau data berbasis rekaman dalam file JSON, Macie mengabaikan teks yang sama persis dengan entri lengkap dalam daftar izin jika

semua teks disimpan dalam satu bidang, sel, atau array. Persyaratan ini tidak berlaku untuk data terstruktur yang disimpan dalam file yang tidak terstruktur, seperti tabel dalam file.pdf.

Misalnya, pertimbangkan konten berikut dalam file CSV:

```
Name,Account ID
Akua Mansa,111111111111
John Doe,222222222222
```

Jika Akua Mansa dan John Doe merupakan entri dalam daftar izinkan, Macie mengabaikan nama-nama itu di file CSV. Teks lengkap dari setiap entri daftar disimpan dalam satu Name bidang.

Sebaliknya, pertimbangkan file CSV yang berisi kolom dan bidang berikut:

```
First Name,Last Name,Account ID
Akua,Mansa,111111111111
John,Doe,222222222222
```

Jika Akua Mansa dan John Doe merupakan entri dalam daftar izinkan, Macie tidak mengabaikan nama-nama itu di file CSV. Tak satu pun bidang dalam file CSV berisi teks lengkap entri dalam daftar izinkan.

## Sertakan variasi umum

Tambahkan entri untuk variasi umum data numerik, kata benda yang tepat, istilah, dan urutan karakter alfanumerik. Misalnya, jika Anda menambahkan nama atau frasa yang hanya berisi satu spasi di antara kata-kata, tambahkan juga variasi yang mencakup dua spasi di antara kata. Demikian pula, tambahkan kata dan frasa yang mengandung dan tidak mengandung karakter khusus, dan pertimbangkan untuk menyertakan variasi sintaksis dan semantik yang umum.

Untuk nomor telepon AS 425-555-0100, misalnya, Anda dapat menambahkan entri ini ke daftar izin:

```
425-555-0100
425.555.0100
(425) 555-0100
+1-425-555-0100
```

Untuk tanggal 1 Februari 2022 dalam konteks multinasional, Anda dapat menambahkan entri yang menyertakan variasi sintaksis umum untuk bahasa Inggris dan Prancis, termasuk variasi yang menyertakan dan tidak menyertakan karakter khusus:

```
February 1, 2022
1 février 2022
1 fevrier 2022
Feb 01, 2022
1 fév 2022
1 fev 2022
02/01/2022
01/02/2022
```

Untuk nama orang, sertakan entri untuk berbagai bentuk nama yang Anda anggap tidak sensitif. Misalnya, sertakan: nama depan diikuti dengan nama belakang; nama belakang diikuti dengan nama depan, nama depan dan belakang dipisahkan oleh satu spasi; nama depan dan belakang dipisahkan oleh dua spasi; dan nama panggilan.

Untuk nama Martha Rivera, misalnya, Anda dapat menambahkan:

```
Martha Rivera
Martha Rivera
Rivera, Martha
Rivera, Martha
Rivera Martha
Rivera Martha
```

Jika Anda ingin mengabaikan variasi nama tertentu yang berisi banyak bagian, buat daftar izinkan yang menggunakan ekspresi reguler sebagai gantinya. Misalnya, untuk nama Dr. Martha Lyda Rivera, PhD, Anda dapat menggunakan ekspresi reguler berikut: `^(Dr . )?Martha\s(Lyda |L \.)?\s?Rivera,?( PhD)?$`

## Opsi dan persyaratan untuk ekspresi reguler dalam daftar izinkan

Untuk jenis daftar izinkan ini, Anda menentukan ekspresi reguler (regex) yang mendefinisikan pola teks yang akan diabaikan — misalnya, nomor telepon publik untuk organisasi Anda, alamat email untuk domain organisasi Anda, atau data sampel berpola yang digunakan organisasi Anda untuk pengujian. Regex mendefinisikan pola umum untuk jenis data tertentu yang Anda anggap tidak sensitif. Jika Anda menggunakan jenis daftar izinkan ini, Amazon Macie tidak melaporkan

kemunculan teks yang benar-benar cocok dengan pola yang ditentukan. Tidak seperti daftar izinkan yang menentukan teks yang telah ditentukan untuk diabaikan, Anda membuat dan menyimpan regex dan semua pengaturan daftar lainnya di Macie.

Saat membuat atau memperbarui jenis daftar izin ini, Anda dapat menguji regex daftar dengan data sampel sebelum menyimpan daftar. Kami menyarankan Anda melakukan ini dengan beberapa set data sampel. Jika Anda membuat regex yang terlalu umum, Macie mungkin mengabaikan kemunculan teks yang Anda anggap sensitif. Jika regex terlalu spesifik, Macie mungkin tidak mengabaikan kemunculan teks yang Anda anggap tidak sensitif. Untuk melindungi dari ekspresi yang salah bentuk atau berjalan lama, Macie juga mengkompilasi dan menguji regex terhadap kumpulan teks sampel secara otomatis, dan memberi tahu Anda tentang masalah yang harus diatasi.

Untuk pengujian tambahan, sebaiknya Anda juga menguji regex daftar dengan kumpulan data kecil yang representatif untuk akun atau organisasi Anda. Untuk melakukan ini, Anda dapat [membuat pekerjaan satu kali](#) dan mengonfigurasi pekerjaan untuk menggunakan daftar selain pengidentifikasi data terkelola dan pengidentifikasi data khusus yang biasanya Anda gunakan untuk menganalisis data. Anda kemudian dapat meninjau hasil pekerjaan—temuan data sensitif, hasil penemuan data sensitif, atau keduanya. Jika hasil pekerjaan berbeda dari yang Anda harapkan, Anda dapat mengubah dan menguji regex hingga hasilnya sesuai dengan yang Anda harapkan.

Setelah mengonfigurasi dan menguji daftar izin, Anda dapat membuat dan mengonfigurasi pekerjaan tambahan untuk menggunakannya, atau menambahkannya ke pengaturan penemuan data sensitif otomatis untuk akun Anda. Saat pekerjaan tersebut dijalankan atau Macie melakukan penemuan otomatis untuk akun Anda, Macie menggunakan versi terbaru dari daftar regex untuk menganalisis data.

## Topik

- [Dukungan dan rekomendasi sintaks](#)
- [Contoh-contoh](#)

## Dukungan dan rekomendasi sintaks

Daftar allow dapat menentukan ekspresi reguler (regex) yang berisi sebanyak 512 karakter. Macie mendukung subset dari sintaks pola regex yang disediakan oleh [Pustaka Perl Compatible Regular Expressions \(PCRE\)](#). Dari konstruksi yang disediakan oleh pustaka PCRE, Macie tidak mendukung elemen pola berikut:

- Backreferences



- Mengambil grup
- Pola bersyarat
- Kode sematan
- Pola bendera global, seperti `/i`, `/m`, dan `/x`
- Pola rekursif
- Asersi lebar nol lookbehind dan lookahead positif dan negatif, seperti `?=`, `?!`, `?<=`, dan `?<!`

Untuk membuat pola regex yang efektif untuk daftar izinkan, perhatikan juga tips dan rekomendasi berikut:

- Jangkar — Gunakan jangkar (`^` atau `$`) hanya jika Anda mengharapkan pola muncul di awal atau akhir file, bukan awal atau akhir baris.
- Bounded repeat — Untuk alasan performa, Macie membatasi ukuran grup bounded repeat. Misalnya, `\d{100,1000}` tidak akan dikompilasi di Macie. Untuk memperkirakan fungsionalitas ini, Anda dapat menggunakan open ended repeat seperti `\d{100,}`.
- Ketidakpekaan huruf besar kecil — Untuk membuat bagian pola menjadu tidak peka huruf besar kecil, Anda dapat menggunakan construct `(?i)` bukan bendera `/i`.
- Performa — Prefiks atau pergantian tidak perlu dioptimalkan secara manual. Misalnya, mengubah `/hello|hi|hey/` menjadi `/h(?:ello|i|ey)/` tidak akan meningkatkan performa.
- Wildcard — Untuk alasan performa, Macie membatasi jumlah wildcard berulang. Misalnya, `a*b*a*` tidak akan dikompilasi di Macie.
- Alternasi — Untuk menentukan lebih dari satu pola dalam satu daftar izinkan, Anda dapat menggunakan operator alternasi (`|`) untuk menggabungkan pola. Jika Anda melakukan ini, Macie menggunakan logika OR untuk menggabungkan pola dan membentuk pola baru. Misalnya, jika Anda menentukan `(apple|orange)`, Macie mengenali apel dan oranye sebagai kecocokan dan mengabaikan kemunculan kedua kata tersebut. Jika Anda menggabungkan pola, pastikan untuk membatasi panjang keseluruhan ekspresi gabungan menjadi 512 karakter atau lebih sedikit.

Terakhir, saat Anda mengembangkan regex, rancang untuk mengakomodasi berbagai jenis file dan format penyimpanan. Macie menggunakan regex sebagai bagian dari kerangka ekstraksi dan analisis data yang lebih besar. Framework faktor jenis file objek S3 atau format penyimpanan. Untuk data terstruktur, seperti data kolumnar dalam file CSV atau data berbasis rekaman dalam file JSON, Macie mengabaikan teks yang benar-benar cocok dengan pola hanya jika semua teks disimpan dalam satu bidang, sel, atau array. Persyaratan ini tidak berlaku untuk data terstruktur yang disimpan dalam file

yang tidak terstruktur, seperti tabel dalam file Adobe Portable Document Format (.pdf). Untuk data yang tidak terstruktur, seperti teks dalam file.pdf, Macie mengabaikan teks yang benar-benar cocok dengan pola, termasuk teks yang mencakup beberapa baris atau halaman.

## Contoh-contoh

Contoh berikut menunjukkan pola regex yang valid untuk beberapa skenario umum.

### Alamat email

Jika Anda menggunakan pengenalan data khusus untuk mendeteksi alamat email, Anda dapat mengabaikan alamat email yang dianggap tidak sensitif, seperti alamat email untuk organisasi Anda.

Untuk mengabaikan alamat email untuk domain tingkat kedua dan tingkat atas tertentu, Anda dapat menggunakan pola ini:

```
[a-zA-Z0-9_+\-\-]+@example\.com
```

Dimana *contoh* adalah nama domain tingkat kedua dan *com* adalah domain tingkat atas. Dalam hal ini, Macie mencocokkan dan mengabaikan alamat seperti johndoe@example.com dan john.doe@example.com.

Untuk mengabaikan alamat email untuk domain tertentu di domain tingkat atas generik (gTLD), seperti.com atau.gov, Anda dapat menggunakan pola ini:

```
[a-zA-Z0-9_+\-\-]+@example\.[a-zA-Z]{2,}
```

Di mana *contoh* adalah nama domain. Dalam hal ini, Macie mencocokkan dan mengabaikan alamat seperti johndoe@example.com, john.doe@example.gov, dan johndoe@example.edu.

Untuk mengabaikan alamat email untuk domain tertentu di salah satu domain tingkat atas kode negara (ccTLD), seperti.ca untuk Kanada atau .au untuk Australia, Anda dapat menggunakan pola ini:

```
[a-zA-Z0-9_+\-\-]+@example\.(ca | au)
```

Di mana *contoh* adalah nama domain dan *ca* dan *au* adalah ccTLD khusus untuk diabaikan. Dalam hal ini, Macie mencocokkan dan mengabaikan alamat seperti johndoe@example.ca dan john.doe@example.au.

Untuk mengabaikan alamat email untuk domain dan gTLD tertentu dan menyertakan domain tingkat ketiga dan keempat, Anda dapat menggunakan pola ini:

```
[a-zA-Z0-9_+\-\-]+@([a-zA-Z0-9-\-]+\.)?[a-zA-Z0-9-\-]+\.example\.com
```

Dimana *contoh* adalah nama domain dan *com* adalah gTLD. Dalam hal ini, Macie mencocokkan dan mengabaikan alamat seperti johndoe@www.example.com dan john.doe@www.team.example.com.

## Nomor telepon

Macie menyediakan pengidentifikasi data terkelola yang dapat mendeteksi nomor telepon untuk beberapa negara dan wilayah. Untuk mengabaikan nomor telepon tertentu, seperti nomor bebas pulsa atau nomor telepon publik untuk organisasi Anda, Anda dapat menggunakan pola seperti berikut ini.

Untuk mengabaikan nomor telepon AS bebas pulsa yang menggunakan kode area 800 dan diformat sebagai (800) ###-####:

```
^\(?800\)?[ -]?\d{3}[ -]?\d{4}$
```

Untuk mengabaikan bebas pulsa, nomor telepon AS yang menggunakan kode area 888 dan diformat sebagai (888) ###-####:

```
^\(?888\)?[ -]?\d{3}[ -]?\d{4}$
```

Untuk mengabaikan 10 digit, nomor telepon Prancis yang menyertakan kode 33 negara dan diformat sebagai +33 ## ## ## ##:

```
^\+33 \d( \d\d){4}$
```

Untuk mengabaikan nomor telepon AS dan Kanada yang menggunakan area tertentu dan kode pertukaran, jangan sertakan kode negara, dan diformat sebagai (###) ###-####:

```
^\(?123\)?[ -]?555[ -]?\d{4}$
```

Di mana *123* adalah kode area dan *555* adalah kode pertukaran.

Untuk mengabaikan nomor telepon AS dan Kanada yang menggunakan area tertentu dan kode pertukaran, sertakan kode negara, dan diformat sebagai +1 (###) ###-####:

```
^\+1\(?123\)?[ -]?555[ -]?\d{4}$
```

Di mana *123* adalah kode area dan *555* adalah kode pertukaran.

## Membuat dan mengelola daftar izinkan di Amazon Macie

Di Amazon Macie, daftar allow mendefinisikan teks tertentu atau pola teks yang ingin Macie abaikan saat memeriksa objek Amazon Simple Storage Service (Amazon S3) untuk data sensitif. Jika teks cocok dengan entri atau pola dalam daftar izinkan, Macie tidak melaporkan teks dalam temuan data sensitif, statistik, atau jenis hasil lainnya, meskipun teks tersebut cocok dengan kriteria [pengenal data terkelola atau pengenal data kustom](#).

Anda dapat membuat dan mengelola jenis daftar izinkan berikut di Macie.

### Teks yang telah ditetapkan

Gunakan jenis daftar ini untuk menentukan kata, frasa, dan jenis urutan karakter lainnya yang tidak sensitif, tidak mungkin berubah, dan tidak selalu mematuhi pola umum. Contohnya adalah nama perwakilan publik untuk organisasi Anda, nomor telepon tertentu, dan data sampel spesifik yang digunakan organisasi Anda untuk pengujian. Jika Anda menggunakan jenis daftar ini, Macie mengabaikan teks yang sama persis dengan entri dalam daftar.

Untuk jenis daftar ini, Anda membuat file teks biasa yang dibatasi baris yang mencantumkan teks tertentu untuk diabaikan. Anda kemudian menyimpan file dalam bucket S3 dan mengkonfigurasi pengaturan untuk Macie untuk mengakses daftar di bucket. Anda kemudian dapat membuat dan mengonfigurasi pekerjaan penemuan data sensitif untuk menggunakan daftar, atau menambahkan daftar ke setelan penemuan data sensitif otomatis untuk akun Anda. Ketika setiap pekerjaan mulai berjalan atau siklus analisis penemuan otomatis berikutnya dimulai, Macie mengambil versi terbaru daftar dari Amazon S3. Macie kemudian menggunakan versi daftar ketika memeriksa objek S3 untuk data sensitif. Jika Macie menemukan teks yang sama persis dengan entri dalam daftar, Macie tidak melaporkan kemunculan teks sebagai data sensitif.

### Ekspresi reguler

Gunakan jenis daftar ini untuk menentukan ekspresi reguler (regex) yang mendefinisikan pola teks untuk diabaikan. Contohnya adalah nomor telepon publik untuk organisasi Anda, alamat e-mail untuk domain organisasi Anda, dan data sampel berpola yang digunakan organisasi Anda untuk pengujian. Jika Anda menggunakan jenis daftar ini, Macie mengabaikan teks yang benar-benar cocok dengan pola regex yang ditentukan oleh daftar.

Untuk jenis daftar ini, Anda membuat regex yang mendefinisikan pola umum untuk teks yang tidak sensitif tetapi bervariasi atau kemungkinan akan berubah. Tidak seperti daftar teks yang telah ditentukan, Anda membuat dan menyimpan regex dan semua pengaturan daftar lainnya di Macie.

Anda kemudian dapat membuat dan mengonfigurasi pekerjaan penemuan data sensitif untuk menggunakan daftar, atau menambahkan daftar ke setelan penemuan data sensitif otomatis untuk akun Anda. Ketika pekerjaan tersebut berjalan atau Macie melakukan penemuan otomatis untuk akun Anda, Macie menggunakan versi terbaru regex daftar untuk menganalisis data. Jika Macie menemukan teks yang benar-benar cocok dengan pola yang ditentukan oleh daftar, Macie tidak melaporkan kemunculan teks sebagai data sensitif.

Untuk persyaratan rinci, rekomendasi, dan contoh dari setiap jenis daftar, lihat [Izinkan opsi dan persyaratan daftar](#). Anda dapat membuat sebanyak 10 daftar izinkan untuk akun Anda di setiap daftar yang didukung Wilayah AWS, hingga lima daftar allow yang menentukan teks yang telah ditentukan dan hingga lima daftar allow yang menentukan ekspresi reguler. Anda dapat membuat dan menggunakan daftar izinkan di semua Wilayah AWS tempat Macie tersedia kecuali Wilayah Asia Pacific (Osaka).

Untuk membuat dan mengelola daftar izinkan, Anda dapat menggunakan konsol Amazon Macie atau API Amazon Macie. Topik berikut menjelaskan caranya. Untuk API, topik mencakup contoh cara melakukan tugas-tugas ini dengan menggunakan [AWS Command Line Interface\(AWS CLI\)](#). Anda juga dapat melakukan tugas-tugas ini dengan menggunakan versi terkini dari alat baris AWS perintah atau AWS SDK, atau dengan mengirimkan permintaan HTTPS langsung ke Macie. Untuk informasi tentang alat AWS dan SDK, lihat [Alat untuk Membangun di AWS](#).

## Topik

- [Membuat daftar izinkan diizinkan](#)
- [Memeriksa status daftar izinkan diizinkan](#)
- [Mengubah daftar izinkan diizinkan](#)
- [Menghapus daftar izinkan diizinkan](#)

## Membuat daftar izinkan diizinkan

Cara Anda membuat daftar izinkan di Amazon Macie tergantung pada jenis daftar yang ingin Anda buat. Daftar allow dapat berupa file yang mencantumkan teks yang telah ditentukan untuk diabaikan, atau dapat berupa ekspresi reguler (regex) yang mendefinisikan pola teks untuk diabaikan. Pilih bagian untuk jenis daftar yang ingin Anda buat.

## Teks yang telah ditetapkan

Sebelum Anda membuat daftar izinkan jenis ini diizinkan, lakukan langkah-langkah berikut:

1. Dengan menggunakan editor teks, buat file teks biasa yang dibatasi baris yang mencantumkan teks tertentu untuk diabaikan—misalnya, file.txt, .text, atau .plain. Untuk informasi selengkapnya, lihat [Persyaratan sintaks untuk daftar teks yang telah ditentukan](#).
2. Unggah file ke bucket S3 dan catat nama bucket dan objeknya. Anda harus memasukkan nama-nama ini ketika mengonfigurasi pengaturan di Macie.
3. Pastikan bahwa pengaturan untuk bucket dan objek S3 memungkinkan Anda dan Macie untuk mengambil daftar dari bucket. Untuk informasi selengkapnya, lihat [Persyaratan penyimpanan untuk daftar teks yang telah ditentukan](#).
4. Jika Anda mengenkripsi objek S3, pastikan objek tersebut dienkripsi dengan kunci yang diizinkan untuk Anda dan Macie. Untuk informasi selengkapnya, lihat [Persyaratan enkripsi/Dekripsi untuk daftar teks yang telah ditentukan](#).

Setelah Anda mengambil langkah-langkah ini, Anda siap untuk mengkonfigurasi pengaturan daftar di Macie. Anda dapat mengonfigurasi pengaturan menggunakan konsol Amazon Macie atau API Amazon Macie.

## Console

Ikuti langkah-langkah ini untuk mengonfigurasi pengaturan pada daftar izinkan menggunakan konsol Amazon Macie.

Untuk mengonfigurasi pengaturan daftar izinkan diizinkan

1. Buka konsol Amazon Macie di <https://console.aws.amazon.com/macie/>.
2. Di panel navigasi, di bawah Pengaturan, pilih Izinkan daftar.
3. Pada halaman Izinkan daftar, pilih Buat.
4. Di bawah Pilih jenis daftar, pilih Teks yang telah ditentukan sebelumnya.
5. Di bawah Pengaturan daftar, gunakan opsi berikut untuk memasukkan pengaturan tambahan untuk daftar izinkan:
  - Untuk Nama, masukkan nama untuk daftar. Nama dapat berisi sebanyak 128 karakter.
  - Untuk Deskripsi, masukkan deskripsi singkat dari daftar. Deskripsi dapat berisi sebanyak 512 karakter.
  - Untuk nama bucket S3, masukkan nama lengkap bucket yang menyimpan daftar.

Di Amazon S3, Anda dapat menemukan nilai ini di bidang Name properti bucket. Nilai ini peka huruf besar kecil. Selain itu, jangan gunakan karakter wildcard atau nilai sebagian saat Anda memasukkan nama.

- Untuk nama objek S3, masukkan nama lengkap objek S3 yang menyimpan daftar.

Di Amazon S3, Anda dapat menemukan nilai ini di bidang Key properti objek. Jika nama menyertakan jalur, pastikan untuk menyertakan jalur lengkap saat Anda memasukkan nama, misalnya **allowlists/macie/mylist.txt**. Nilai ini peka huruf besar kecil. Selain itu, jangan gunakan karakter wildcard atau nilai sebagian saat Anda memasukkan nama.

6. (Opsional) Di bawah Tag, pilih Tambahkan tag, lalu masukkan sebanyak 50 tag untuk ditetapkan ke daftar allow.

Tag adalah label yang Anda tentukan dan tetapkan ke jenis AWS sumber daya tertentu. Setiap tanda terdiri dari kunci tanda yang diperlukan dan nilai tanda opsional. Tag dapat membantu Anda mengidentifikasi, mengategorikan, dan mengelola sumber daya dengan cara yang berbeda, seperti berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Untuk mempelajari selengkapnya, lihat [Menandai sumber daya Amazon Macie](#).

7. Setelah selesai, pilih Buat.

Macie menguji pengaturan daftar. Macie juga memverifikasi bahwa ia dapat mengambil daftar dari Amazon S3 dan mengurai konten daftar. Jika terjadi kesalahan, Macie menampilkan pesan yang menjelaskan kesalahan. Untuk informasi mendetail yang dapat membantu Anda memecahkan masalah, lihat [Pilihan dan persyaratan untuk daftar teks yang telah ditentukan](#). Setelah Anda mengatasi kesalahan apa pun, Anda dapat menyimpan pengaturan daftar.

## API

Untuk mengonfigurasi pengaturan daftar izinkan secara terprogram, gunakan [CreateAllowList](#) pengoperasian API Amazon Macie dan tentukan nilai yang sesuai untuk parameter yang diperlukan.

Untuk `criteria` parameter, gunakan `s3WordsList` objek untuk menentukan nama bucket S3 (`bucketName`) dan nama objek S3 (`objectKey`) yang menyimpan daftar. Untuk menentukan nama bucket, lihat Name bidang di Amazon S3. Untuk menentukan nama objek, lihat Key bidang di Amazon S3. Perhatikan bahwa nilai ini peka huruf besar dan kecil. Selain itu, jangan gunakan karakter wildcard atau nilai sebagian saat Anda menentukan nama-nama ini.





Di arn mana Amazon Resource Name (ARN) dari daftar izinkan yang dibuat, dan id merupakan pengidentifikasi unik untuk daftar.

Setelah menyimpan setelan daftar, Anda dapat [membuat dan mengonfigurasi pekerjaan penemuan data sensitif](#) untuk menggunakan daftar, atau [menambahkan daftar ke setelan penemuan data sensitif otomatis](#). Setiap kali pekerjaan tersebut mulai berjalan atau siklus analisis penemuan otomatis dimulai, Macie mengambil versi terbaru daftar dari Amazon S3. Macie kemudian menggunakan versi daftar ketika menganalisis data.

## Ekspresi reguler

Ketika Anda membuat daftar allow yang menentukan ekspresi reguler (regex), Anda menentukan regex dan semua pengaturan daftar lainnya langsung di Macie. Macie mendukung subset dari sintaks pola regex yang disediakan oleh [Pustaka Perl Compatible Regular Expressions \(PCRE\)](#). Untuk informasi selengkapnya, lihat [Dukungan dan rekomendasi sintaks](#).

Anda dapat membuat daftar Amazon Macie atau API Amazon Macie.


## Console

Ikuti langkah-langkah ini untuk membuat daftar izinkan menggunakan konsol Amazon Macie.

Untuk membuat daftar izinkan

1. Buka konsol Amazon Macie di <https://console.aws.amazon.com/macie/>.
2. Di panel navigasi, di bawah Pengaturan, pilih Izinkan daftar.
3. Pada halaman Izinkan daftar, pilih Buat.
4. Di bawah Pilih jenis daftar, pilih Ekspresi reguler.
5. Di bawah Pengaturan daftar, gunakan opsi berikut untuk memasukkan pengaturan tambahan untuk daftar izinkan:
  - Untuk Nama, masukkan nama untuk daftar. Nama dapat berisi sebanyak 128 karakter.
  - Untuk Deskripsi, masukkan deskripsi singkat dari daftar. Deskripsi dapat berisi sebanyak 512 karakter.
  - Untuk ekspresi reguler, masukkan regex yang mendefinisikan pola teks untuk diabaikan. Regex dapat berisi sebanyak 512 karakter.
6. (Opsional) Untuk Evaluasi, masukkan hingga 1.000 karakter di Data sampel kotak, lalu pilih Uji untuk menguji regex. Macie mengevaluasi data sampel dan melaporkan jumlah

kemunculan teks yang cocok dengan regex. Anda dapat mengulangi langkah ini sebanyak yang Anda inginkan untuk memperbaiki dan mengoptimalkan regex.

 Note

Kami menyarankan agar Anda menguji dan menyempurnakan regex menggunakan beberapa set data sampel. Jika Anda membuat regex yang terlalu umum, Macie mungkin mengabaikan kejadian teks yang Anda anggap sensitif. Jika regex terlalu spesifik, Macie mungkin tidak mengabaikan kejadian teks yang Anda anggap tidak sensitif.

7. (Opsional) Di bawah Tag, pilih Tambahkan tag, lalu masukkan sebanyak 50 tag untuk ditetapkan ke daftar allow.

Tag adalah label yang Anda tentukan dan tetapkan ke jenis AWS sumber daya tertentu. Setiap tanda terdiri dari kunci tanda yang diperlukan dan nilai tanda opsional. Tag dapat membantu Anda mengidentifikasi, mengategorikan, dan mengelola sumber daya dengan cara yang berbeda, seperti berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Untuk mempelajari selengkapnya, lihat [Menandai sumber daya Amazon Macie](#).

8. Setelah selesai, pilih Buat.

Macie menguji pengaturan daftar. Macie juga menguji regex untuk memverifikasi bahwa ia dapat mengkompilasi ekspresi. Jika terjadi kesalahan, Macie menampilkan pesan yang menjelaskan kesalahan. Untuk informasi mendetail yang dapat membantu Anda memecahkan masalah, lihat [Opsional dan persyaratan untuk ekspresi reguler dalam daftar izinkan](#). Setelah Anda mengatasi kesalahan apa pun, Anda dapat menyimpan daftar izinkan.

## API

Sebelum Anda membuat daftar allow jenis ini di Macie, sebaiknya Anda menguji dan menyempurnakan ekspresi reguler dengan beberapa set data sampel. Jika Anda membuat regex yang terlalu umum, Macie mungkin mengabaikan kejadian teks yang Anda anggap sensitif. Jika regex terlalu spesifik, Macie mungkin tidak mengabaikan kejadian teks yang Anda anggap tidak sensitif.

Untuk menguji ekspresi dengan Macie, Anda dapat menggunakan [TestCustomDataIdentifier](#) operasi Amazon Macie API atau, untuk AWS CLI, jalankan perintah [test-custom-data-identifier](#). Macie menggunakan kode dasar yang sama untuk mengkompilasi



```
{
  "arn": "arn:aws:macie2:us-west-2:123456789012:allow-list/
km2d4y22hp6rv05example",
  "id": "km2d4y22hp6rv05example"
}
```

Di `arn` mana Amazon Resource Name (ARN) dari daftar izinkan yang dibuat, dan `id` merupakan pengidentifikasi unik untuk daftar.

Setelah menyimpan daftar, Anda dapat [membuat dan mengonfigurasi pekerjaan penemuan data sensitif](#) untuk menggunakannya, atau [menambahkannya ke setelan penemuan data sensitif otomatis](#). Ketika pekerjaan tersebut berjalan atau Macie melakukan penemuan otomatis untuk akun Anda, Macie menggunakan versi terbaru regex daftar untuk menganalisis data.

## Memeriksa status daftar izinkan diizinkan

Penting untuk memeriksa status daftar izinkan Anda secara berkala. Jika tidak, kesalahan dapat menyebabkan Amazon Macie menghasilkan hasil analisis yang tidak terduga, seperti temuan data sensitif untuk teks yang Anda tentukan dalam daftar izinkan.

Jika Anda mengonfigurasi pekerjaan penemuan data sensitif untuk menggunakan daftar izinkan dan Macie tidak dapat mengakses atau menggunakan daftar saat tugas mulai berjalan, tugas akan terus berjalan. Namun, Macie tidak menggunakan daftar saat menganalisis objek S3. Demikian pula, jika siklus analisis dimulai untuk penemuan data sensitif otomatis dan Macie tidak dapat mengakses atau menggunakan daftar izinkan yang ditentukan, analisis berlanjut tetapi Macie tidak menggunakan daftar.

Kesalahan tidak mungkin terjadi untuk daftar allow yang menentukan ekspresi reguler (regex). Ini sebagian karena Macie secara otomatis menguji regex saat Anda membuat atau memperbarui pengaturan daftar. Selain itu, Anda menyimpan regex dan semua pengaturan daftar lainnya di Macie.

Namun, kesalahan dapat terjadi untuk daftar izinkan yang menentukan teks yang telah ditentukan, sebagian karena Anda menyimpan daftar di Amazon S3, bukan Macie. Penyebab umum kesalahan adalah:

- Bucket atau objek S3 dihapus.
- Bucket atau objek S3 diganti namanya dan pengaturan daftar di Macie tidak menentukan nama baru.

- Pengaturan izin bucket S3 diubah dan Macie kehilangan akses ke bucket dan objek.
- Pengaturan enkripsi untuk bucket S3 diubah dan Macie tidak dapat mendekripsi objek yang menyimpan daftar.
- Kebijakan untuk kunci enkripsi diubah dan Macie kehilangan akses ke kunci. Macie tidak dapat mendekripsi objek S3 yang menyimpan daftar.

#### Important

Karena kesalahan ini memengaruhi hasil analisis Anda, kami sarankan Anda memeriksa status daftar izinkan Anda secara berkala. Kami menyarankan Anda juga melakukan ini jika Anda mengubah pengaturan izin atau enkripsi untuk bucket S3 yang menyimpan daftar izinkan, atau Anda mengubah kebijakan untuk kunci AWS Key Management Service (AWS KMS) yang digunakan untuk mengenkripsi daftar.

Anda dapat memeriksa status daftar izin Anda menggunakan konsol Amazon Macie atau API Amazon Macie. Untuk informasi terperinci yang dapat membantu Anda memecahkan masalah kesalahan yang terjadi, lihat [Pilihan dan persyaratan untuk daftar teks yang telah ditentukan](#).

#### Console

Ikuti langkah-langkah ini untuk memeriksa status daftar izinkan Anda menggunakan konsol Amazon Macie.

Untuk memeriksa status daftar izinkan Anda diizinkan

1. Buka konsol Amazon Macie di <https://console.aws.amazon.com/macie/>.
2. Di panel navigasi, di bawah Pengaturan, pilih Izinkan daftar.
3. Pada halaman Izinkan daftar, pilih refresh



Macie menguji pengaturan untuk semua daftar izinkan Anda dan memperbarui bidang Status untuk menunjukkan status saat ini dari setiap daftar.

Jika daftar menentukan ekspresi reguler, statusnya biasanya OK. Ini berarti bahwa Macie dapat mengkompilasi ekspresi. Jika daftar menentukan teks yang telah ditetapkan, statusnya dapat berupa salah satu nilai berikut.

## OKE

Macie dapat mengambil dan mengurai isi daftar.

### Akses ditolak

Macie tidak diizinkan untuk mengakses objek S3 yang menyimpan daftar. Amazon S3 menolak permintaan untuk mengambil objek. Daftar juga dapat memiliki status ini jika objek dienkripsi dengan pelanggan yang dikelola AWS KMS key bahwa Macie tidak diizinkan untuk digunakan.

Untuk mengatasi kesalahan ini, tinjau kebijakan bucket dan pengaturan izin lainnya untuk bucket dan objek. Pastikan bahwa Macie diperbolehkan untuk mengakses dan mengambil objek. Jika objek dienkripsi dengan AWS KMS kunci yang dikelola pelanggan, tinjau juga kebijakan kunci dan pastikan bahwa Macie diizinkan untuk menggunakan kunci tersebut.

### Kesalahan

Sebuah kesalahan sementara atau internal terjadi ketika Macie mencoba untuk mengambil atau mengurai isi daftar. Daftar izinkan juga dapat memiliki status ini jika dienkripsi dengan kunci enkripsi yang tidak dapat diakses atau digunakan oleh Amazon S3 dan Macie.

Untuk mengatasi kesalahan ini, tunggu beberapa menit dan kemudian pilih refresh



lagi. Jika status terus menjadi Kesalahan, periksa pengaturan enkripsi untuk objek S3. Pastikan objek dienkripsi dengan kunci yang dapat diakses dan digunakan Amazon S3 dan Macie.

### Objek kosong

Macie dapat mengambil daftar dari Amazon S3 tetapi daftarnya tidak berisi konten apa pun.

Untuk mengatasi kesalahan ini, unduh objek dari Amazon S3 dan pastikan bahwa objek tersebut berisi entri yang benar. Jika entri benar, tinjau pengaturan daftar di Macie. Pastikan bahwa bucket dan objek nama yang ditentukan benar.

### Objek tidak ditemukan

Daftar ini tidak ada di Amazon S3.

Untuk mengatasi kesalahan ini, tinjau pengaturan daftar di Macie. Pastikan bahwa bucket dan objek nama yang ditentukan benar.

### Kuota terlampaui

Macie dapat mengakses daftar di Amazon S3. Namun, jumlah entri dalam daftar atau ukuran penyimpanan daftar melebihi kuota untuk daftar izinkan.

Untuk mengatasi kesalahan ini, hancurkan daftar menjadi beberapa file. Pastikan bahwa setiap file berisi kurang dari 100.000 entri. Juga pastikan bahwa ukuran setiap file kurang dari 35 MB. Kemudian, unggah setiap file ke Amazon S3. Setelah selesai, konfigurasi pengaturan daftar izinkan di Macie untuk setiap file. Anda dapat memiliki sebanyak lima daftar teks yang telah ditetapkan di masing-masing didukung Wilayah AWS.

### Tercekik

Amazon S3 mencekik permintaan untuk mengambil daftar.

Untuk mengatasi kesalahan ini, tunggu beberapa menit dan kemudian pilih refresh



lagi.

### Akses pengguna ditolak

Amazon S3 menolak permintaan untuk mengambil objek. Jika objek yang ditentukan ada, Anda tidak diizinkan untuk mengaksesnya atau dienkripsi dengan AWS KMS kunci yang tidak diizinkan untuk digunakan.

Untuk mengatasi kesalahan ini, bekerja dengan AWS administrator Anda untuk memastikan bahwa pengaturan daftar menentukan nama bucket dan objek yang benar, dan Anda telah membaca akses ke bucket dan objek. Jika objek dienkripsi, pastikan juga bahwa objek tersebut dienkripsi dengan kunci yang diizinkan untuk digunakan.

4. Untuk meninjau pengaturan dan status daftar tertentu, pilih nama daftar.

## API

Untuk memeriksa status daftar izinkan secara terprogram, gunakan [GetAllowList](#) pengoperasian API Amazon Macie atau, untuk AWS CLI, jalankan perintah. [get-allow-list](#)

Untuk id parameter, tentukan pengidentifikasi unik untuk daftar izinkan yang statusnya ingin Anda periksa. Untuk mendapatkan pengidentifikasi ini, Anda dapat menggunakan [ListAllowLists](#) operasi. `ListAllowLists` operasi mengambil informasi tentang semua daftar izinkan untuk akun Anda. Jika Anda menggunakan AWS CLI, Anda dapat menjalankan [list-allow-lists](#) perintah untuk mengambil informasi ini.

Saat Anda mengirimkan `GetAllowList` permintaan, Macie menguji semua pengaturan untuk daftar izinkan. Jika pengaturan menentukan ekspresi reguler (regex), Macie memverifikasi bahwa itu dapat mengkompilasi ekspresi. Jika pengaturan menentukan daftar teks yang telah ditetapkan, Macie memverifikasi bahwa itu dapat mengambil dan mengurai daftar.

Macie kemudian mengembalikan sebuah `GetAllowListResponse` objek yang menyediakan rincian daftar allow. Dalam `GetAllowListResponse` objek, status objek menunjukkan status daftar saat ini: kode status (`code`) dan, tergantung pada kode status, deskripsi singkat tentang status daftar (`description`).

Jika daftar allow menentukan regex, kode status biasanya OK dan tidak ada deskripsi terkait. Ini berarti bahwa Macie berhasil menyusun ekspresi.

Jika daftar allow menentukan teks yang telah ditentukan, kode status bervariasi tergantung pada hasil pengujian:

- Jika Macie berhasil mengambil dan mengurai daftar, kode statusnya adalah OK dan tidak ada deskripsi terkait.
- Jika kesalahan mencegah Macie mengambil atau mengurai daftar, kode status dan deskripsi menunjukkan sifat kesalahan yang terjadi.

Untuk daftar kemungkinan kode status dan deskripsi masing-masing kode, lihat [AllowListStatus](#) di Amazon Macie API Reference.

## Mengubah daftar izinkan diizinkan

Setelah membuat daftar izinkan, Anda dapat mengubah sebagian besar pengaturan daftar di Amazon Macie. Misalnya, Anda dapat mengubah nama dan deskripsi daftar, dan Anda dapat menambahkan dan mengedit tag daftar. Satu-satunya pengaturan yang tidak dapat Anda ubah adalah jenis daftar. Misalnya, jika daftar allow yang ada menetapkan ekspresi reguler, Anda tidak dapat mengubah jenisnya menjadi teks yang telah ditentukan sebelumnya.



Jika daftar allow menentukan teks yang telah ditentukan, Anda juga dapat mengubah entri dalam daftar. Untuk melakukan ini, perbarui file yang berisi entri, lalu unggah versi baru file ke Amazon S3. Lain kali Macie bersiap untuk menggunakan daftar, Macie mengambil versi terbaru dari file dari Amazon S3. Saat Anda mengunggah file baru, pastikan Anda menyimpannya di bucket dan objek S3 yang sama. Atau, jika Anda mengubah nama bucket atau objek, pastikan Anda memperbarui pengaturan daftar di Macie.

Anda dapat mengubah pengaturan izinkan menggunakan konsol Amazon Macie atau API Amazon Macie.

## Console

Ikuti langkah-langkah ini untuk mengubah pengaturan pada daftar izinkan menggunakan konsol Amazon Macie.

Untuk mengubah daftar izinkan diizinkan

1. Buka konsol Amazon Macie di <https://console.aws.amazon.com/macie/>.
2. Di panel navigasi, di bawah Pengaturan, pilih Izinkan daftar.
3. Pada halaman Izinkan daftar, pilih nama izinkan yang ingin Anda ubah. Halaman daftar izinkan membuka dan menampilkan pengaturan saat ini untuk daftar.
4. Untuk menetapkan atau mengedit tag untuk daftar izinkan, pilih Kelola tag di bagian Tag. Kemudian ubah tanda sesuai kebutuhan. Setelah selesai, pilih Simpan.
5. Untuk mengubah pengaturan lain untuk daftar izinkan, pilih Edit di bagian Pengaturan daftar. Kemudian ubah pengaturan yang Anda inginkan:
  - Nama - Masukkan nama baru untuk daftar. Nama dapat berisi sebanyak 128 karakter.
  - Deskripsi - Masukkan deskripsi baru dari daftar. Deskripsi dapat berisi sebanyak 512 karakter.
  - Jika daftar allow menentukan teks yang telah ditetapkan:
    - Nama bucket S3 - Masukkan nama lengkap bucket yang saat ini menyimpan daftar.

Di Amazon S3, Anda dapat menemukan nilai ini di bidang Name properti bucket. Nilai ini peka huruf besar kecil. Selain itu, jangan gunakan karakter wildcard atau nilai sebagian saat Anda memasukkan nama.

- Nama objek S3 - Masukkan nama lengkap objek S3 yang saat ini menyimpan daftar.

Di Amazon S3, Anda dapat menemukan nilai ini di bidang Key properti objek. Jika nama menyertakan jalur, pastikan untuk menyertakan jalur lengkap saat Anda memasukkan nama, misalnya `allowlists/macie/mylist.txt`. Nilai ini peka huruf besar kecil. Selain itu, jangan gunakan karakter wildcard atau nilai sebagian saat Anda memasukkan nama.

- Jika daftar allow menentukan ekspresi reguler (regex), masukkan regex baru di kotak Regular expression. Regex dapat berisi sebanyak 512 karakter.

Setelah Anda memasukkan regex baru, opsional mengujinya. Untuk melakukannya, masukkan hingga 1.000 karakter di kotak Data sampel, lalu pilih Uji. Macie mengevaluasi data sampel dan melaporkan jumlah kemunculan teks yang cocok dengan regex. Anda dapat mengulangi langkah ini sebanyak yang Anda inginkan untuk memperbaiki dan mengoptimalkan regex sebelum Anda menyimpan perubahan.

Setelah Anda selesai mengubah pengaturan, pilih Simpan.

Macie menguji pengaturan daftar. Untuk daftar teks yang telah ditentukan, Macie juga memverifikasi bahwa teks tersebut dapat mengambil daftar dari Amazon S3 dan mengurai konten daftar. Untuk regex, Macie juga memverifikasi bahwa ia dapat mengkompilasi ekspresi. Jika terjadi kesalahan, Macie menampilkan pesan yang menjelaskan kesalahan. Untuk informasi mendetail yang dapat membantu Anda memecahkan masalah, lihat [Izinkan opsi dan persyaratan daftar](#). Setelah Anda mengatasi kesalahan apa pun, Anda dapat menyimpan perubahan Anda.

## API

Untuk mengubah daftar izinkan secara terprogram, gunakan [UpdateAllowList](#) pengoperasian Amazon Macie API atau, untuk AWS CLI, jalankan perintah. [update-allow-list](#) Dalam permintaan, gunakan parameter yang didukung untuk menentukan nilai baru untuk setiap pengaturan yang ingin Anda ubah. Perhatikan bahwa `criteria`, `id`, dan `name` parameter yang diperlukan. Jika Anda tidak ingin mengubah nilai untuk parameter yang diperlukan, tentukan nilai saat ini untuk parameter.

Misalnya, perintah berikut mengubah nama dan deskripsi daftar izinkan yang sudah ada. Contoh ini diformat untuk Microsoft Windows dan menggunakan karakter kelanjutan baris caret (^) untuk meningkatkan keterbacaan.

```
C:\> aws macie2 update-allow-list ^
```



## Menghapus daftar izinkan diizinkan

Saat Anda menghapus daftar izinkan di Amazon Macie, Anda menghapus semua pengaturan daftar secara permanen. Pengaturan ini tidak dapat dipulihkan setelah dihapus. Jika pengaturan menentukan daftar teks yang telah ditentukan yang Anda simpan di Amazon S3, Macie tidak menghapus objek S3 yang menyimpan daftar. Hanya pengaturan di Macie yang dihapus.

Jika Anda mengonfigurasi pekerjaan penemuan data sensitif untuk menggunakan daftar izinkan dan Anda kemudian menghapus daftar, pekerjaan akan berjalan sesuai jadwal. Namun, hasil pekerjaan Anda, baik temuan data sensitif maupun hasil penemuan data sensitif, mungkin melaporkan teks yang sebelumnya Anda tentukan dalam daftar izinkan. Demikian pula, jika Anda mengkonfigurasi penemuan data sensitif otomatis untuk menggunakan daftar dan Anda kemudian menghapus daftar, siklus analisis harian akan dilanjutkan. Namun, temuan data sensitif, statistik, atau jenis hasil lainnya mungkin melaporkan teks yang sebelumnya Anda tentukan dalam daftar izinkan.

Sebelum Anda menghapus daftar izinkan, kami sarankan Anda [meninjau inventaris pekerjaan Anda](#) untuk mengidentifikasi pekerjaan yang menggunakan daftar dan dijadwalkan untuk dijalankan di future. Dalam inventaris, panel detail menunjukkan apakah pekerjaan dikonfigurasi untuk menggunakan daftar izinkan dan, jika demikian, yang mana. Selain itu, [periksa setelah penemuan data sensitif otomatis Anda](#). Anda mungkin menentukan bahwa yang terbaik adalah mengubah daftar daripada menghapusnya.

Sebagai perlindungan tambahan, Macie memeriksa pengaturan untuk semua pekerjaan Anda saat Anda mencoba menghapus daftar izinkan. Jika Anda mengonfigurasi pekerjaan untuk menggunakan daftar dan salah satu pekerjaan tersebut memiliki status selain Lengkap atau Dibatalkan, Macie tidak menghapus daftar tersebut kecuali Anda memberikan konfirmasi tambahan.

Anda dapat menghapus daftar izinkan menggunakan konsol Amazon Macie atau API Amazon Macie.

### Console

Ikuti langkah-langkah ini untuk menghapus daftar izinkan menggunakan konsol Amazon Macie.

Untuk menghapus daftar izinkan diizinkan

1. Buka konsol Amazon Macie di <https://console.aws.amazon.com/macie/>.
2. Di panel navigasi, di bawah Pengaturan, pilih Izinkan daftar.
3. Pada halaman Izinkan daftar, pilih kotak centang untuk daftar izinkan yang ingin Anda hapus.
4. Dari menu Tindakan, pilih Hapus.

5. Ketika diminta untuk mengonfirmasi, masukkan **delete**, lalu pilih Hapus.

## API

Untuk menghapus daftar izinkan secara terprogram, gunakan [DeleteAllowList](#) operasi API Amazon Macie. Untuk `id` parameter, tentukan pengidentifikasi unik untuk daftar izinkan untuk Anda hapus. Anda bisa mendapatkan pengidentifikasi ini dengan menggunakan [ListAllowLists](#) operasi. `ListAllowLists` Operasi mengambil informasi tentang semua daftar izinkan untuk akun Anda. Jika Anda menggunakan AWS CLI, Anda dapat menjalankan [list-allow-lists](#) perintah untuk mengambil informasi ini.

Untuk `ignoreJobChecks` parameter, tentukan apakah akan memaksa penghapusan daftar, bahkan jika pekerjaan penemuan data sensitif dikonfigurasi untuk menggunakan daftar:

- Jika Anda menentukan `false`, Macie memeriksa pengaturan untuk semua pekerjaan Anda yang memiliki status selain COMPLETE atau CANCELLED. Jika tidak ada pekerjaan yang dikonfigurasi untuk menggunakan daftar, Macie menghapus daftar secara permanen. Jika salah satu pekerjaan tersebut dikonfigurasi untuk menggunakan daftar, Macie menolak permintaan Anda dan mengembalikan kesalahan HTTP 400 (`ValidationException`). Pesan kesalahan menunjukkan jumlah pekerjaan yang berlaku hingga 200 pekerjaan.
- Jika Anda menentukan `true`, Macie menghapus daftar secara permanen tanpa memeriksa pengaturan untuk pekerjaan Anda.

Untuk menghapus daftar allow dengan menggunakan AWS CLI, jalankan [delete-allow-list](#) perintah. Misalnya:

```
C:\> aws macie2 delete-allow-list --id nkr81bmtu2542yyexample --ignore-job-checks false
```

Dimana *nkr81bmtu2542yyexample* adalah pengenal unik untuk daftar allow untuk dihapus.

Jika berhasil, Macie mengembalikan respons HTTP 200 kosong. Jika tidak, Macie mengembalikan HTTP 4 xx atau respon 500 yang menunjukkan mengapa operasi gagal.

Jika daftar allow ditentukan teks yang telah ditetapkan, Anda opsional dapat menghapus objek S3 yang menyimpan daftar. Namun, menjaga objek ini dapat membantu untuk memastikan bahwa Anda memiliki riwayat tetap temuan dan hasil penemuan data atau investigasi.

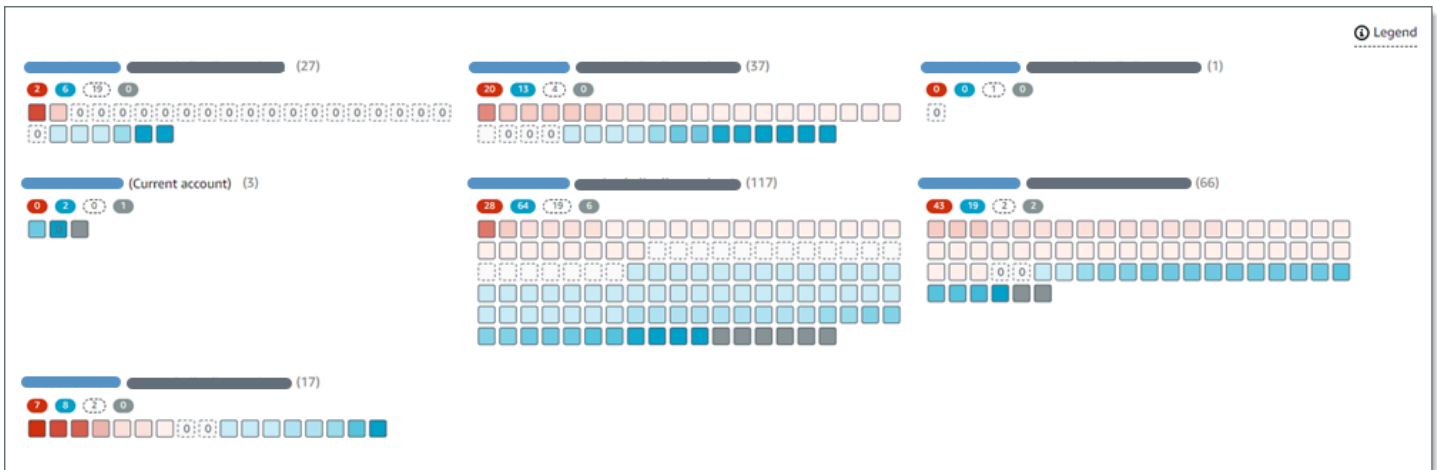
# Melakukan penemuan data sensitif otomatis dengan Amazon Macie

Untuk visibilitas luas ke tempat data sensitif berada di kawasan data Amazon Simple Storage Service (Amazon S3) Anda, konfigurasi Amazon Macie untuk melakukan penemuan data sensitif otomatis untuk akun atau organisasi Anda. Dengan penemuan data sensitif otomatis, Macie terus mengevaluasi inventaris bucket S3 Anda dan menggunakan teknik pengambilan sampel untuk mengidentifikasi dan memilih objek S3 representatif di bucket Anda. Macie kemudian mengambil dan menganalisis objek yang dipilih, memeriksa mereka untuk data sensitif.

Secara default, Macie menganalisis objek S3 dengan menggunakan kumpulan pengidentifikasi data terkelola yang kami rekomendasikan untuk penemuan data sensitif otomatis. Anda dapat menyesuaikan analisis dengan mengkonfigurasi Macie untuk menggunakan spesifik [pengidentifikasi data terkelola](#), [pengidentifikasi data kustom](#), dan [mengizinkan daftar](#) saat melakukan penemuan data sensitif otomatis untuk akun atau organisasi Anda. Selain itu, Macie secara otomatis memilih dan menganalisis objek dari semua bucket S3 Anda. Jika Anda adalah administrator Macie untuk suatu organisasi, ini mencakup objek dalam bucket S3 yang dimiliki akun anggota Anda. Anda dapat menyesuaikan cakupan analisis dengan mengecualikan bucket tertentu—misalnya, bucket S3 yang biasanya menyimpan AWS data logging.

Ketika analisis berlangsung setiap hari, Macie menghasilkan catatan data sensitif yang ditemukannya dan analisis yang dilakukannya: temuan data sensitif, yang melaporkan data sensitif yang ditemukan Macie di objek S3 individu, dan hasil penemuan data sensitif, yang mencatat detail tentang analisis objek S3 individu. Macie juga memperbarui statistik, data inventaris, dan informasi lain yang diberikannya tentang data Amazon S3 Anda.

Misalnya, peta panas interaktif di konsol menyediakan representasi visual sensitivitas data di seluruh data estate Anda:



Fitur-fitur ini dirancang untuk membantu Anda mengevaluasi sensitivitas data di seluruh data estate Amazon S3 Anda, dan menelusuri untuk menyelidiki dan menilai masing-masing akun, bucket, dan objek. Mereka juga dapat membantu Anda menentukan di mana harus melakukan analisis yang lebih dalam dan lebih cepat [menjalankan pekerjaan penemuan data sensitif](#). Dikombinasikan dengan informasi yang disediakan Macie tentang keamanan dan privasi data Amazon S3 Anda, Anda juga dapat menggunakan fitur-fitur ini untuk mengidentifikasi kasus di mana perbaikan segera mungkin diperlukan—misalnya, bucket yang dapat diakses publik tempat Macie menemukan data sensitif.

Untuk mengonfigurasi dan menggunakan penemuan data sensitif otomatis, akun Anda harus berupa akun Macie mandiri atau akun administrator Macie untuk suatu organisasi.

## Topik

- [Cara kerja penemuan data sensitif otomatis](#)
- [Mengonfigurasi penemuan data sensitif otomatis untuk akun Anda](#)
- [Mengelola penemuan data sensitif otomatis untuk bucket S3 individual](#)
- [Menilai cakupan penemuan data sensitif otomatis](#)
- [Meninjau statistik dan hasil penemuan data sensitif otomatis](#)
- [Penilaian sensitivitas untuk bucket S3](#)
- [Pengaturan default untuk penemuan data sensitif otomatis](#)

## Cara kerja penemuan data sensitif otomatis

Saat Anda mengaktifkan Amazon Macie untuk Akun AWS, Macie menciptakan AWS Identity and Access Management (IAM) [peran terkait layanan](#) untuk akun Anda saat ini Wilayah AWS. Kebijakan izin

untuk peran ini memungkinkan Macie memanggil yang lain Layanan AWS dan monitor AWS sumber daya atas nama Anda. Dengan menggunakan peran ini, Macie menghasilkan dan mengelola inventaris lengkap bucket Amazon Simple Storage Service (Amazon S3) Anda di Wilayah. Inventaris mencakup informasi tentang masing-masing bucket S3 Anda dan objek dalam bucket. Jika Anda adalah administrator Macie untuk suatu organisasi, inventaris berisi informasi tentang bucket S3 yang dimiliki akun anggota Anda. Untuk informasi selengkapnya, lihat [Mengelola beberapa akun](#).

Jika penemuan data sensitif otomatis diaktifkan untuk akun Macie Anda, Macie mengevaluasi data inventaris setiap hari untuk mengidentifikasi objek S3 yang memenuhi syarat untuk penemuan otomatis. Sebagai bagian dari evaluasi, Macie juga memilih sampling objek representatif untuk dianalisis. Macie kemudian mengambil dan menganalisis versi terbaru dari setiap objek yang dipilih dari Amazon S3, memeriksa setiap objek untuk data sensitif.

Seiring kemajuan analisis setiap hari, Macie memperbarui statistik, data inventaris, dan informasi lain yang diberikannya tentang data Amazon S3 Anda. Macie juga menghasilkan catatan data sensitif yang ditemukannya dan analisis yang dilakukannya. Data yang dihasilkan memberikan wawasan tentang tempat Macie menemukan data sensitif di data estate Amazon S3 Anda, yang mencakup semua bucket S3 yang dipantau dan dianalisis Macie untuk akun Anda. Data dapat membantu Anda menilai keamanan dan privasi data sensitif Anda, menentukan tempat untuk melakukan penyelidikan lebih dalam, dan mengidentifikasi kasus-kasus di mana perbaikan diperlukan.

Untuk demonstrasi singkat tentang cara kerja penemuan data sensitif otomatis, tonton video berikut: [Ringkasan penemuan data otomatis Amazon Macie](#).

Untuk mengonfigurasi dan menggunakan penemuan data sensitif otomatis, akun Anda harus berupa akun Macie mandiri atau akun administrator Macie untuk suatu organisasi.

## Topik

- [Komponen utama](#)
- [Pertimbangan-pertimbangan](#)

## Komponen utama

Amazon Macie menggunakan kombinasi fitur dan teknik untuk melakukan penemuan data sensitif otomatis untuk data Amazon S3 Anda. Ini bekerja sama dengan fitur dan teknik yang digunakan Macie untuk membantu Anda [memantau data Amazon S3 Anda untuk keamanan dan kontrol akses](#).



## Memilih objek S3 untuk dianalisis

Setiap hari, Macie mengevaluasi data inventaris Amazon S3 Anda untuk mengidentifikasi objek S3 yang memenuhi syarat untuk dianalisis dengan penemuan data sensitif otomatis. Jika Anda adalah administrator Macie untuk suatu organisasi, ini mencakup data inventaris untuk bucket S3 yang dimiliki akun anggota Anda.

Sebagai bagian dari evaluasi, Macie menggunakan teknik sampling untuk memilih objek representatif untuk dianalisis. Teknik mendefinisikan kelompok objek yang memiliki metadata serupa dan cenderung memiliki konten yang sama. Grup didasarkan pada dimensi seperti nama bucket, awalan, kelas penyimpanan, ekstensi nama file, dan tanggal modifikasi terakhir. Macie kemudian memilih kumpulan sampel representatif dari setiap grup, mengambil versi terbaru dari setiap objek yang dipilih dari Amazon S3, dan menganalisis setiap objek yang dipilih untuk menentukan apakah objek tersebut berisi data sensitif. Ketika analisis selesai, Macie membuang salinan objeknya.

Strategi sampling memprioritaskan analisis terdistribusi. Secara umum, ini menggunakan pendekatan pertama yang luas untuk data estate Amazon S3 Anda. Setiap hari, kumpulan representatif objek S3 dipilih dari sebanyak mungkin bucket Anda berdasarkan ukuran penyimpanan total semua objek yang dapat diklasifikasikan dalam data estate Amazon S3 Anda. Misalnya, jika Macie telah menganalisis dan menemukan data sensitif dalam objek dalam satu bucket S3 dan belum menganalisis objek di bucket lain, bucket yang terakhir adalah prioritas yang lebih tinggi untuk analisis. Dengan pendekatan ini, Anda mendapatkan wawasan luas tentang sensitivitas data Amazon S3 Anda dengan lebih cepat. Bergantung pada ukuran data estate Anda, hasil analisis dapat mulai muncul dalam waktu 48 jam setelah memungkinkan penemuan data sensitif otomatis untuk akun Anda.

Strategi sampling juga memprioritaskan analisis berbagai jenis objek dan objek S3 yang baru saja dibuat atau diubah. Setiap sampel objek tunggal tidak dijamin konklusif. Oleh karena itu, analisis serangkaian objek yang beragam dapat menghasilkan wawasan yang lebih baik tentang jenis dan jumlah data sensitif yang mungkin terkandung dalam bucket S3. Selain itu, memprioritaskan objek baru atau yang baru saja diubah membantu analisis beradaptasi dengan perubahan pada inventaris bucket Anda. Misalnya, jika objek dibuat atau diubah setelah analisis sebelumnya, objek tersebut adalah prioritas yang lebih tinggi untuk analisis selanjutnya. Sebaliknya, jika objek sebelumnya dianalisis dan tidak berubah sejak analisis itu, Macie tidak menganalisis objek lagi. Pendekatan ini membantu Anda menetapkan garis dasar sensitivitas untuk bucket S3 individual. Kemudian, seiring kemajuan analisis inkremental yang berkelanjutan untuk akun Anda, penilaian

sensitivitas Anda terhadap masing-masing bucket dapat menjadi semakin dalam dan terperinci pada tingkat yang dapat diprediksi.

## Mendefinisikan ruang lingkup analisis

Secara default, Macie menyertakan semua bucket S3 yang dipantau dan dianalisis untuk akun Anda saat mengevaluasi data inventaris Anda dan memilih objek S3 untuk dianalisis. Jika Anda adalah administrator Macie untuk suatu organisasi, ini termasuk bucket yang dimiliki akun anggota Anda.

Anda dapat mengecualikan bucket S3 tertentu dari analisis. Misalnya, Anda mungkin lebih suka mengecualikan bucket yang biasanya disimpan AWS data logging, seperti AWS CloudTrail log acara. Untuk mengecualikan bucket, Anda dapat mengubah setelan penemuan data sensitif otomatis untuk akun atau bucket. Jika Anda melakukan ini, Macie mulai mengecualikan bucket ketika siklus evaluasi dan analisis harian berikutnya dimulai. Anda dapat mengecualikan sebanyak 1.000 ember dari analisis.

Jika Anda mengecualikan ember, Anda kemudian dapat memasukkannya lagi. Untuk melakukannya, ubah pengaturan penemuan data sensitif otomatis untuk akun Anda atau bucket lagi. Macie kemudian mulai menyertakan bucket ketika siklus evaluasi dan analisis harian berikutnya dimulai.

## Menentukan jenis data sensitif yang akan dideteksi dan dilaporkan

Secara default, Macie memeriksa objek S3 dengan menggunakan kumpulan pengidentifikasi data terkelola yang kami rekomendasikan untuk penemuan data sensitif otomatis. Untuk daftar pengidentifikasi data terkelola ini, lihat [Pengaturan default untuk penemuan data sensitif otomatis](#).

Anda dapat menyesuaikan analisis untuk fokus pada jenis data sensitif tertentu. Untuk melakukannya, ubah setelan penemuan data sensitif otomatis untuk akun Anda dengan salah satu cara berikut:

- Menambahkan atau menghapus pengidentifikasi data terkelola tertentu — Apengenal data terkelola adalah seperangkat kriteria dan teknik bawaan yang dirancang untuk mendeteksi jenis data sensitif tertentu, seperti nomor kartu kredit, AWS kunci akses rahasia, atau nomor paspor untuk negara atau wilayah tertentu. Untuk informasi selengkapnya, lihat [Menggunakan pengidentifikasi data terkelola](#).
- Menambahkan atau kemudian menghapus pengidentifikasi data kustom - Apengenal data kustom adalah seperangkat kriteria yang Anda tentukan untuk mendeteksi data sensitif. Dengan pengidentifikasi data kustom, Anda dapat mendeteksi data sensitif yang mencerminkan skenario tertentu organisasi Anda, kekayaan intelektual, atau data kepemilikan, seperti ID

karyawan, nomor akun pelanggan, atau klasifikasi data internal. Untuk informasi selengkapnya, lihat [Membangun pengidentifikasi data kustom](#).

- Tambahkan atau hapus daftar izinkan selanjutnya — Di Macie, daftar izinkan menetapkan teks atau pola teks yang ingin Macie abaikan di objek S3, biasanya pengecualian data sensitif untuk skenario atau lingkungan tertentu, seperti nama publik atau nomor telepon untuk organisasi Anda, atau data sampel yang digunakan organisasi Anda untuk pengujian. Untuk informasi selengkapnya, lihat [Mendefinisikan pengecualian data sensitif dengan daftar izinkan](#).

Jika Anda mengubah pengaturan, Macie menerapkan perubahan Anda saat siklus analisis harian berikutnya dimulai.

Anda juga dapat menyesuaikan pengaturan level bucket yang menentukan apakah jenis data sensitif tertentu disertakan dalam penilaian sensitivitas bucket. Untuk mempelajari caranya, lihat [Mengelola penemuan data sensitif otomatis untuk bucket S3 individual](#).

## Menghitung skor sensitivitas

Secara default, Macie secara otomatis menghitung skor sensitivitas untuk setiap bucket S3 yang dipantau dan dianalisis untuk akun Anda. Jika Anda adalah administrator Macie untuk suatu organisasi, ini termasuk bucket yang dimiliki akun anggota Anda.

Di Macie, skor sensitivitas adalah ukuran kuantitatif dari persimpangan dua dimensi utama: jumlah data sensitif yang ditemukan Macie dalam ember, dan jumlah data yang telah dianalisis Macie dalam ember. Skor sensitivitas bucket menentukan label sensitivitas yang ditugaskan Macie ke bucket. SEBUAH label sensitivitas adalah representasi kualitatif dari skor sensitivitas bucket — misalnya, Sensitif, Tidak sensitif, dan Belum dianalisis. Untuk detail tentang rentang skor sensitivitas dan label yang ditentukan Macie, lihat [Penilaian sensitivitas untuk bucket S3](#).

### Important

Skor dan label sensitivitas bucket S3 tidak menyiratkan atau menunjukkan kekritisannya atau pentingnya bucket atau objek bucket untuk organisasi Anda. Sebaliknya, mereka dimaksudkan untuk memberikan titik referensi yang dapat membantu Anda mengidentifikasi dan memantau potensi risiko keamanan.

Saat awalnya Anda mengaktifkan penemuan data sensitif otomatis untuk akun Anda, Macie secara otomatis menetapkan skor sensitivitas 50 dan yang Belum dianalisis label untuk setiap ember S3. Pengecualiannya adalah ember kosong. Sebuah ember kosong adalah bucket yang

tidak berisi objek atau semua objek bucket mengandung nol (0) byte data. Jika ini adalah kasus untuk ember, Macie memberikan skor 1 ke ember dan memberikan Tidak sensitif label ke ember.

Seiring kemajuan penemuan otomatis untuk akun Anda, Macie memperbarui skor sensitivitas dan label untuk mencerminkan hasil analisis. Misalnya:

- Jika Macie tidak menemukan data sensitif dalam suatu objek, Macie mengurangi skor sensitivitas bucket dan memperbarui label sensitivitas bucket seperlunya.
- Jika Macie menemukan data sensitif dalam suatu objek, Macie meningkatkan skor sensitivitas bucket dan memperbarui label sensitivitas bucket seperlunya.
- Jika Macie menemukan data sensitif dalam objek yang kemudian berubah, Macie menghapus deteksi data sensitif untuk objek dari skor sensitivitas bucket dan memperbarui label sensitivitas bucket jika diperlukan.
- Jika Macie menemukan data sensitif dalam objek yang kemudian dihapus, Macie menghapus deteksi data sensitif untuk objek dari skor sensitivitas bucket dan memperbarui label sensitivitas bucket jika diperlukan.

Anda dapat menyesuaikan pengaturan penilaian sensitivitas untuk masing-masing bucket S3 dengan menyertakan atau mengecualikan jenis data sensitif tertentu dari skor bucket. Anda juga dapat mengganti skor terhitung bucket dengan menetapkan skor maksimum secara manual (100) ke ember. Jika Anda menetapkan skor maksimum, bucket diberi label Sensitif. Untuk informasi selengkapnya, lihat [Mengelola penemuan otomatis untuk bucket S3 individual](#).

## Menghasilkan metadata, statistik, dan hasil

Jika penemuan data sensitif otomatis diaktifkan untuk akun Anda, Macie secara otomatis membuat dan mengelola data inventaris tambahan, statistik, dan informasi lain tentang bucket S3 yang dipantau dan dianalisis untuk akun Anda. Jika Anda adalah administrator Macie untuk suatu organisasi, ini termasuk bucket yang dimiliki akun anggota Anda.

Informasi tambahan menangkap hasil aktivitas penemuan data sensitif otomatis yang telah dilakukan Macie sejauh ini untuk akun Anda. Ini juga melengkapi informasi lain yang disediakan Macie tentang data Amazon S3 Anda, seperti akses publik dan pengaturan akses bersama untuk masing-masing bucket. Informasi tambahan meliputi:

- Statistik sensitivitas data agregat, seperti jumlah total bucket yang ditemukan Macie data sensitif dan berapa banyak bucket tersebut dapat diakses publik.
- Representasi visual yang interaktif dari sensitivitas data di seluruh kawasan data Amazon S3 Anda.

- Detail tingkat ember yang menunjukkan status analisis saat ini, seperti daftar objek yang telah dianalisis Macie dalam bucket, jenis data sensitif yang ditemukan Macie dalam bucket, dan jumlah kejadian dari setiap jenis data sensitif yang ditemukan Macie.

Untuk informasi selengkapnya, lihat [Meninjau statistik dan hasil penemuan data sensitif otomatis](#).

Informasi tambahan juga mencakup statistik dan detail yang dapat membantu Anda menilai dan memantau cakupan data Amazon S3 Anda. Anda dapat memeriksa status analisis untuk data estat Anda secara keseluruhan dan untuk masing-masing bucket S3 dalam inventaris bucket Anda. Anda juga dapat mengidentifikasi masalah yang mencegah Macie menganalisis objek dalam bucket tertentu. Jika Anda memperbaiki masalah, Anda dapat meningkatkan cakupan data Amazon S3 Anda selama siklus analisis berikutnya. Untuk informasi selengkapnya, lihat [Menilai cakupan penemuan data sensitif otomatis](#).

Macie secara otomatis menghitung ulang dan memperbarui informasi ini sambil melakukan penemuan data sensitif otomatis untuk akun Anda. Misalnya, jika Macie menemukan data sensitif dalam objek yang kemudian diubah atau dihapus, Macie memperbarui metadata bucket yang berlaku: menghapus objek dari daftar objek yang dianalisis; menghapus kejadian data sensitif yang ditemukan Macie di objek; menghitung ulang skor sensitivitas, jika skor dihitung secara otomatis; dan, memperbarui label sensitivitas seperlunya untuk mencerminkan skor baru.

Selain metadata dan statistik, Macie menghasilkan catatan data sensitif yang ditemukannya dan analisis yang dilakukannya: temuan data sensitif, yang melaporkan data sensitif yang ditemukan Macie di objek S3 individu, dan hasil penemuan data sensitif, yang mencatat detail tentang analisis objek S3 individu.

## Pertimbangan-pertimbangan

Saat Anda menggunakan Amazon Macie untuk melakukan penemuan data sensitif otomatis untuk data Amazon S3 Anda, ingatlah hal berikut:

- Pengaturan penemuan otomatis Anda hanya berlaku untuk saat ini Wilayah AWS. Akibatnya, analisis dan data yang dihasilkan hanya berlaku untuk ember dan objek S3 di Wilayah saat ini. Untuk melakukan penemuan otomatis dan mengakses data yang dihasilkan di Wilayah tambahan, aktifkan dan konfigurasi penemuan otomatis di setiap Wilayah tambahan.
- Jika Anda adalah administrator Macie untuk organisasi:

- Anda dapat melakukan penemuan otomatis untuk akun anggota hanya jika Macie diaktifkan untuk akun di Wilayah saat ini. Akun anggota tidak dapat melakukan penemuan otomatis untuk akun mereka sendiri.
- Akun anggota tidak dapat mengakses pengaturan penemuan otomatis yang berlaku untuk bucket S3 mereka. Hanya administrator Macie yang dapat mengakses pengaturan ini.
- Akun anggota tidak dapat mengakses statistik penemuan data sensitif dan hasil lain yang disediakan Macie secara langsung untuk bucket S3 mereka. Misalnya, akun anggota tidak dapat menggunakan konsol Amazon Macie untuk meninjau skor sensitivitas untuk bucket S3 mereka. Hanya administrator Macie yang dapat mengakses data ini.
- Jika setelah izin bucket S3 mencegah Macie mengambil informasi tentang atau mengakses bucket atau objek bucket, Macie tidak dapat melakukan penemuan otomatis untuk bucket. Macie hanya dapat memberikan subset informasi tentang bucket, seperti ID akun untuk Akun AWS yang memiliki bucket, nama bucket, dan ketika Macie baru-baru ini mengambil bucket dan metadata objek untuk bucket sebagai bagian dari [siklus penyegaran harian](#). Dalam inventaris bucket Anda, skor sensitivitas untuk bucket ini adalah 50 dan label sensitivitasnya adalah Belum dianalisis.

Untuk mengidentifikasi bucket S3 dengan cepat, lihat data cakupan penemuan otomatis Anda. Untuk informasi selengkapnya, lihat [Menilai cakupan penemuan data sensitif otomatis](#). Untuk menyelidiki masalah bucket tertentu, tinjau pengaturan kebijakan dan izin bucket di Amazon S3. Misalnya, bucket mungkin memiliki kebijakan bucket yang membatasi. Untuk informasi selengkapnya, lihat [Mengizinkan Macie untuk mengakses bucket S3 dan objek](#).

- Agar memenuhi syarat untuk seleksi dan analisis, objek S3 harus dapat diklasifikasikan. SEBUAH objek diklasifikasikan menggunakan kelas penyimpanan Amazon S3 yang didukung dan memiliki ekstensi nama file untuk file atau format penyimpanan yang didukung. Untuk informasi selengkapnya, lihat [Kelas dan format penyimpanan yang didukung](#).
- Jika objek S3 dienkripsi, Macie dapat menganalisisnya hanya jika dienkripsi dengan kunci yang dapat diakses Macie dan diizinkan untuk digunakan. Untuk informasi selengkapnya, lihat [Menganalisis objek S3 terenkripsi](#). Untuk mengidentifikasi kasus di mana pengaturan enkripsi mencegah Macie menganalisis satu atau beberapa objek dalam bucket, lihat data cakupan penemuan otomatis Anda. Untuk informasi selengkapnya, lihat [Menilai cakupan penemuan data sensitif otomatis](#).

## Mengonfigurasi penemuan data sensitif otomatis untuk akun Anda

Dengan penemuan data sensitif otomatis, Amazon Macie terus memilih objek sampel dari bucket Amazon Simple Storage Service (Amazon S3) dan menganalisis objek untuk menentukan apakah objek tersebut berisi data sensitif. Jika Anda administrator Macie untuk organisasi, ini termasuk objek dalam bucket S3 yang dimiliki akun anggota Anda. Seiring kemajuan analisis, Macie memperbarui statistik, data inventaris, dan informasi lain yang diberikannya tentang data Amazon S3 Anda. Macie juga menghasilkan catatan data sensitif yang ditemukannya dan analisis yang dilakukannya.

Untuk mengonfigurasi dan menggunakan penemuan data sensitif otomatis, akun Anda harus berupa akun Macie mandiri atau akun administrator Macie untuk organisasi. Jika Anda memiliki akun anggota dan ingin melakukan penemuan otomatis untuk bucket S3 Anda, hubungi administrator Macie untuk organisasi Anda. Untuk informasi selengkapnya, lihat [Mengelola beberapa akun](#).

### Topik

- [Sebelum Anda memulai](#)
- [Mengaktifkan penemuan data sensitif otomatis untuk akun Anda](#)
- [Mengonfigurasi setelah penemuan data sensitif otomatis untuk akun Anda](#)
- [Menonaktifkan penemuan data sensitif otomatis untuk akun Anda](#)

Saat Anda mengaktifkan, mengonfigurasi, atau menonaktifkan penemuan data sensitif otomatis untuk akun Anda, perubahan Anda hanya berlaku untuk saat iniWilayah AWS. Untuk membuat perubahan yang sama di Wilayah tambahan, ulangi langkah-langkah yang berlaku di setiap Wilayah tambahan.

### Sebelum Anda memulai

Sebelum Anda mengonfigurasi penemuan data sensitif otomatis untuk akun Anda, verifikasi bahwa Anda memiliki izin yang Anda butuhkan. Juga verifikasi bahwa Anda telah mengonfigurasi repositori untuk hasil penemuan data sensitif Anda.

Untuk memverifikasi izin Anda, gunakan AWS Identity and Access Management (IAM) untuk meninjau kebijakan IAM yang dilampirkan pada identitas IAM Anda. Kemudian bandingkan informasi dalam kebijakan tersebut dengan daftar tindakan berikut yang harus Anda lakukan:

- `macie2:GetMacieSession`
- `macie2:UpdateAutomatedDiscoveryConfiguration`



Tindakan pertama memungkinkan Anda mengakses akun Amazon Macie Anda. Tindakan kedua memungkinkan Anda mengubah pengaturan konfigurasi penemuan data sensitif otomatis untuk akun Anda. Ini termasuk mengaktifkan dan menonaktifkan konfigurasi. Secara opsional, verifikasi bahwa Anda juga diizinkan untuk melakukan `macie2:GetAutomatedDiscoveryConfiguration` tindakan. Tindakan ini memungkinkan Anda untuk mengambil pengaturan konfigurasi saat ini dan status konfigurasi saat ini.

Selain memverifikasi izin Anda, verifikasi bahwa Anda telah mengonfigurasi repositori untuk menyimpan hasil penemuan data sensitif Anda. Hasil penemuan data sensitif adalah catatan yang mencatat detail tentang analisis yang dilakukan Macie pada objek S3. Macie menciptakan hasil penemuan data sensitif untuk setiap objek S3 yang dianalisis saat melakukan penemuan data sensitif otomatis. Ini termasuk objek yang Macie tidak menemukan data sensitif, dan karenanya tidak menghasilkan temuan data sensitif, dan objek yang tidak dapat dianalisis Macie karena kesalahan atau masalah seperti pengaturan izin. Jika Macie menemukan data sensitif dalam suatu objek, hasil penemuan data sensitif mencakup data dari temuan yang sesuai. Ini berisi informasi tambahan juga. Hasil ini memberi Anda catatan analisis yang dapat membantu audit atau investigasi privasi dan perlindungan data.

Macie menyimpan hasil penemuan data sensitif Anda hanya selama 90 hari. Untuk mengakses hasil dan mengaktifkan penyimpanan dan retensi jangka panjang mereka, konfigurasi Macie untuk menyimpan hasilnya dalam bucket S3. Bucket dapat berfungsi sebagai repositori jangka panjang definitif untuk semua hasil penemuan data sensitif Anda.

Untuk memverifikasi bahwa Anda telah mengonfigurasi repositori ini untuk akun Anda, pilih Hasil penemuan di panel navigasi di konsol Amazon Macie. Jika Anda lebih suka melakukan ini secara terprogram, gunakan [GetClassificationExportConfiguration](#) pengoperasian Amazon Macie API. Untuk mempelajari cara mengkonfigurasi repositori ini, lihat [Menyimpan dan mempertahankan hasil penemuan data sensitif](#)

Jika Anda telah mengonfigurasi repositori, Macie membuat folder bernama `automated-sensitive-data-discovery` di repositori saat penemuan data sensitif otomatis awalnya diaktifkan untuk akun Anda. Folder ini menyimpan hasil penemuan data sensitif yang dibuat Macie saat melakukan penemuan otomatis untuk akun Anda.

## Mengaktifkan penemuan data sensitif otomatis untuk akun Anda

Saat Anda mengaktifkan penemuan data sensitif otomatis untuk akun Anda, Amazon Macie mulai mengevaluasi data inventaris Amazon S3 Anda dan melakukan aktivitas penemuan otomatis lainnya untuk akun Anda saat ini. Wilayah AWS Bergantung pada ukuran estate data Amazon S3 Anda,



statistik penemuan data sensitif dan hasil lainnya dapat mulai muncul dalam waktu 48 jam setelah memungkinkan penemuan otomatis untuk akun Anda.

Ikuti langkah-langkah berikut untuk mengaktifkan penemuan data sensitif otomatis untuk akun Anda dengan menggunakan konsol Amazon Macie. Untuk mengaktifkan penemuan otomatis secara terprogram, gunakan [UpdateAutomatedDiscoveryConfiguration](#) pengoperasian Amazon Macie API.

Untuk mengaktifkan penemuan data sensitif otomatis untuk akun Anda

1. [Buka konsol Amazon Macie di https://console.aws.amazon.com/macie/](https://console.aws.amazon.com/macie/).
2. Dengan menggunakan Wilayah AWS pemilih di sudut kanan atas halaman, pilih Wilayah tempat Anda ingin mengaktifkan penemuan data sensitif otomatis.
3. Di panel navigasi, di bawah Pengaturan, pilih Penemuan otomatis.
4. Di bagian Status, pilih Aktifkan.
5. Ketika diminta konfirmasi, pilih Aktifkan .

Setelah Anda mengaktifkan penemuan data sensitif otomatis, tinjau dan konfigurasi pengaturan Anda untuk menyempurnakan analisis yang selanjutnya dilakukan Macie.

## Mengonfigurasi setelah penemuan data sensitif otomatis untuk akun Anda

Jika penemuan data sensitif otomatis diaktifkan untuk akun Anda, Anda dapat menyesuaikan pengaturan penemuan otomatis untuk akun Anda guna menyempurnakan analisis yang dilakukan Amazon Macie. Pengaturan ini menentukan bucket S3 mana yang ingin Anda sertakan dalam analisis. Mereka juga menentukan jenis dan kemunculan data sensitif yang Anda ingin Macie deteksi dan laporkan—pengidentifikasi data terkelola, pengidentifikasi data khusus, dan mengizinkan daftar untuk digunakan saat menganalisis objek S3.

Secara default, Macie melakukan penemuan data sensitif otomatis untuk semua bucket S3 yang dipantau dan dianalisis untuk akun Anda. Jika Anda administrator Macie untuk suatu organisasi, ini termasuk bucket S3 yang dimiliki akun anggota Anda. Anda dapat mengecualikan ember tertentu dari analisis. Misalnya, Anda mungkin mengecualikan bucket yang biasanya menyimpan data AWS logging, seperti log AWS CloudTrail peristiwa. Jika Anda mengecualikan ember, Anda selanjutnya dapat memasukkannya lagi.

Selain itu, Macie menganalisis objek S3 dengan hanya menggunakan kumpulan pengidentifikasi data terkelola yang kami rekomendasikan untuk penemuan data sensitif otomatis. Macie tidak

menggunakan pengidentifikasi data khusus atau mengizinkan daftar yang telah Anda tetapkan. Untuk menyesuaikan analisis, Anda dapat mengonfigurasi Macie untuk menggunakan daftar izin tertentu, pengidentifikasi data kustom, dan pengidentifikasi data terkelola.

Bagian berikut memberikan informasi tambahan tentang setiap jenis pengaturan dan mereka menjelaskan cara mengubah pengaturan dengan menggunakan konsol Amazon Macie. Pilih bagian untuk mempelajari lebih lanjut. Untuk meninjau atau mengubah setelan secara terprogram, Anda dapat menggunakan operasi Amazon Macie API berikut [UpdateClassificationScope](#);, untuk menentukan bucket S3 mana yang akan dikecualikan dari analisis, dan, untuk menentukan daftar yang mengizinkan, pengidentifikasi data kustom, [UpdateSensitivityInspectionTemplated](#) dan pengidentifikasi data terkelola yang akan digunakan.

Jika Anda mengubah setelan, Macie menerapkan perubahan Anda saat siklus evaluasi dan analisis berikutnya dimulai untuk penemuan data sensitif otomatis, biasanya dalam 24 jam.

### Kecualikan atau sertakan bucket S3 dalam analisis

Secara default, Macie melakukan penemuan data sensitif otomatis untuk semua bucket S3 yang dipantau dan dianalisis untuk akun Anda. Jika Anda administrator Macie untuk suatu organisasi, ini termasuk bucket S3 yang dimiliki akun anggota Anda. Untuk menyempurnakan cakupan, Anda dapat mengecualikan sebanyak 1.000 ember dari analisis.

Jika Anda mengecualikan bucket S3, Macie berhenti menganalisis objek di bucket saat melakukan penemuan data sensitif otomatis untuk akun Anda. Statistik penemuan data sensitif yang ada dan detail untuk bucket persisten—misalnya, skor sensitivitas bucket saat ini tetap tidak berubah. Setelah Anda mengecualikan ember, Anda selanjutnya dapat memasukkannya lagi.

### Untuk mengecualikan atau menyertakan ember S3 tertentu

1. [Buka konsol Amazon Macie di https://console.aws.amazon.com/macie/](https://console.aws.amazon.com/macie/).
2. Dengan menggunakan Wilayah AWS pemilih di sudut kanan atas halaman, pilih Wilayah yang ingin Anda kecualikan atau sertakan bucket S3 tertentu dalam analisis penemuan otomatis.
3. Di panel navigasi, di bawah Pengaturan, pilih Penemuan otomatis. Halaman penemuan data sensitif otomatis muncul dan menampilkan pengaturan Anda saat ini. Pada halaman itu, bagian bucket S3 mencantumkan bucket S3 yang saat ini dikecualikan, atau ini menunjukkan bahwa semua bucket saat ini disertakan.
4. Di bagian bucket S3, pilih Edit.
5. Lakukan salah satu dari berikut:

- Untuk mengecualikan satu atau beberapa bucket S3, pilih Tambahkan bucket ke daftar pengecualian. Kemudian, di tabel bucket S3, pilih kotak centang untuk setiap bucket yang ingin Anda kecualikan. Tabel mencantumkan semua bucket S3 untuk akun Anda di Wilayah saat ini.
- Untuk menyertakan satu atau beberapa bucket S3 yang sebelumnya Anda kecualikan, pilih Hapus bucket dari daftar pengecualian. Kemudian, di tabel bucket S3, pilih kotak centang untuk setiap bucket yang ingin Anda sertakan. Tabel ini mencantumkan semua bucket yang saat ini dikecualikan dari penemuan data sensitif otomatis.

Untuk menemukan bucket tertentu dengan lebih mudah, masukkan kriteria pencarian di kotak pencarian di atas tabel. Anda juga dapat mengurutkan tabel berdasarkan nama bucket.

6. Ketika Anda selesai memilih bucket, pilih Tambah atau Hapus, tergantung pada opsi yang Anda pilih pada langkah sebelumnya.

### Menambahkan atau menghapus pengidentifikasi data terkelola dari analisis

Pengidentifikasi data terkelola adalah seperangkat kriteria dan teknik bawaan yang dirancang untuk mendeteksi jenis data sensitif tertentu — misalnya, nomor kartu kredit, kunci akses AWS rahasia, atau nomor paspor untuk negara atau wilayah tertentu. Secara default, Macie menganalisis objek S3 dengan menggunakan kumpulan pengidentifikasi data terkelola yang kami rekomendasikan untuk penemuan data sensitif otomatis. Untuk meninjau daftar pengidentifikasi yang disertakan dalam set ini, lihat [Pengaturan default untuk penemuan data sensitif otomatis](#).

Anda dapat menyesuaikan analisis agar fokus pada jenis data sensitif tertentu: menambahkan pengidentifikasi data terkelola untuk jenis data sensitif yang ingin dideteksi dan dilaporkan oleh Macie, dan menghapus pengidentifikasi data terkelola untuk jenis data sensitif yang tidak ingin Macie deteksi dan laporkan. Jika Anda menghapus pengenalan data terkelola, perubahan Anda tidak memengaruhi statistik penemuan data sensitif yang ada dan detail untuk bucket S3 Anda. Misalnya, jika Anda menghapus pengenalan data terkelola yang mendeteksi kunci akses AWS rahasia dan Macie sebelumnya mendeteksi jenis data sensitif tersebut dalam bucket, Macie terus melaporkan deteksi tersebut untuk bucket.

#### Tip

Alih-alih menghapus pengenalan data terkelola dari analisis selanjutnya dari semua bucket S3, Anda dapat mengecualikan jenis deteksi tersebut dari skor sensitivitas untuk bucket tertentu.

Untuk informasi selengkapnya, lihat [Mengelola penemuan data sensitif otomatis untuk bucket S3 individual](#).

Untuk menambah atau menghapus pengenalan data terkelola

1. [Buka konsol Amazon Macie di https://console.aws.amazon.com/macie/](https://console.aws.amazon.com/macie/).
2. Dengan menggunakan Wilayah AWS pemilih di sudut kanan atas halaman, pilih Wilayah tempat Anda ingin menambahkan atau menghapus pengidentifikasi data terkelola dari analisis penemuan otomatis.
3. Di panel navigasi, di bawah Pengaturan, pilih Penemuan otomatis. Pada halaman Penemuan data sensitif otomatis, bagian Pengidentifikasi data terkelola menampilkan pengaturan Anda saat ini, yang disusun menjadi dua tab:
  - Ditambahkan ke default - Tab ini mencantumkan pengidentifikasi data terkelola yang Anda tambahkan secara eksplisit. Macie menggunakan pengidentifikasi data terkelola ini selain yang ada di set default dan Anda belum menghapusnya secara eksplisit.
  - Dihapus dari default - Tab ini mencantumkan pengidentifikasi data terkelola yang Anda hapus secara eksplisit. Macie tidak menggunakan pengidentifikasi data terkelola ini.
4. Di bagian Pengidentifikasi data terkelola, pilih Edit.
5. Lakukan langkah-langkah berikut:
  - Untuk menambahkan satu atau beberapa pengidentifikasi data terkelola, pilih tab Ditambahkan ke default. Kemudian, dalam tabel, pilih kotak centang untuk setiap pengidentifikasi data terkelola yang ingin Anda tambahkan. Jika kotak centang sudah dipilih, Anda telah menambahkan pengenalan itu.
  - Untuk menghapus satu atau beberapa pengidentifikasi data terkelola, pilih tab Dihapus dari default. Kemudian, dalam tabel, pilih kotak centang untuk setiap pengidentifikasi data terkelola yang ingin Anda hapus. Jika kotak centang sudah dipilih, Anda telah menghapus pengenalan tersebut.

Pada setiap tab, tabel menampilkan daftar semua pengidentifikasi data terkelola yang saat ini disediakan Macie. Dalam tabel, setiap ID pengidentifikasi data terkelola menjelaskan jenis data sensitif yang dirancang untuk dideteksi oleh pengenalan—misalnya, USA\_PASSPORT\_NUMBER untuk nomor paspor AS. Untuk menemukan pengidentifikasi data terkelola tertentu dengan lebih mudah, masukkan kriteria pencarian di kotak pencarian di atas tabel. Anda dapat mengurutkan

tabel dengan memilih judul kolom. Untuk detail tentang setiap pengenalan, lihat [Menggunakan pengidentifikasi data terkelola](#).

6. Setelah selesai, pilih Simpan.

Menambahkan atau menghapus pengidentifikasi data kustom dari analisis

Pengidentifikasi data kustom adalah set kriteria yang Anda tetapkan untuk mendeteksi data sensitif. Kriteria terdiri dari ekspresi reguler (regex) yang menentukan pola teks untuk dicocokkan dan, opsional, urutan karakter dan aturan jarak yang menyempurnakan hasil. Untuk mempelajari selengkapnya, lihat [Membangun pengidentifikasi data kustom](#).

Secara default, Amazon Macie tidak menggunakan pengidentifikasi data khusus saat melakukan penemuan data sensitif otomatis. Jika Anda ingin Macie menggunakan pengidentifikasi data khusus tertentu, Anda dapat menambahkannya ke analisis. Macie kemudian menggunakan pengidentifikasi data kustom selain pengidentifikasi data terkelola yang juga Anda konfigurasi Macie untuk digunakan.

Jika Anda menambahkan pengenalan data kustom ke analisis, Anda selanjutnya dapat menghapusnya. Perubahan Anda tidak akan memengaruhi statistik dan detail penemuan data sensitif yang ada untuk bucket S3 Anda. Misalnya, jika Anda menghapus pengenalan data kustom yang sebelumnya menghasilkan deteksi untuk bucket, Macie terus melaporkan deteksi tersebut untuk bucket. Namun, pertimbangkan untuk mengecualikan jenis deteksi itu dari skor sensitivitas untuk ember tertentu alih-alih menghapus pengenalan dari analisis selanjutnya dari semua ember. Untuk informasi selengkapnya, lihat [Mengelola penemuan data sensitif otomatis untuk bucket S3 individual](#).

Untuk menambah atau menghapus pengenalan data kustom

1. [Buka konsol Amazon Macie di https://console.aws.amazon.com/macie/](https://console.aws.amazon.com/macie/).
2. Dengan menggunakan Wilayah AWS pemilih di sudut kanan atas halaman, pilih Wilayah tempat Anda ingin menambahkan atau menghapus pengidentifikasi data kustom dari analisis penemuan otomatis.
3. Di panel navigasi, di bawah Pengaturan, pilih Penemuan otomatis. Halaman penemuan data sensitif otomatis muncul dan menampilkan pengaturan Anda saat ini. Pada halaman tersebut, bagian Pengidentifikasi data kustom mencantumkan pengidentifikasi data kustom yang telah ditambahkan, atau menunjukkan bahwa Anda belum memilih pengidentifikasi data kustom apa pun untuk penemuan otomatis.
4. Di bagian Pengidentifikasi data kustom, pilih Edit.
5. Lakukan langkah-langkah berikut:

- Untuk menambahkan satu atau beberapa pengidentifikasi data kustom, pilih kotak centang untuk setiap pengidentifikasi data kustom yang ingin Anda tambahkan. Jika kotak centang sudah dipilih, Anda telah menambahkan pengenalan itu.
- Untuk menghapus satu atau beberapa pengidentifikasi data kustom, kosongkan kotak centang untuk setiap pengidentifikasi data kustom yang ingin Anda hapus. Jika kotak centang sudah dihapus, Macie saat ini tidak menggunakan pengenalan tersebut saat melakukan penemuan otomatis.

#### Tip

Untuk meninjau atau menguji pengaturan pengenalan data kustom sebelum menambahkan atau menghapusnya, pilih ikon tautan



di sebelah nama pengenalan. Macie membuka halaman yang menampilkan pengaturan pengidentifikasi.

Anda juga dapat menggunakan halaman ini untuk menguji pengidentifikasi dengan data sampel. Untuk melakukan ini, masukkan hingga 1.000 karakter teks di kotak Data sampel, lalu pilih Uji. Macie mengevaluasi data sampel dengan menggunakan pengenalan, dan kemudian melaporkan jumlah kecocokan.

6. Setelah selesai, pilih Simpan.

## Menambahkan atau menghapus daftar izinkan dari analisis

Di Amazon Macie, daftar izinkan mendefinisikan teks tertentu atau pola teks yang Anda ingin Macie abaikan saat memeriksa objek S3 untuk data sensitif. Jika teks cocok dengan entri atau pola dalam daftar izin, Macie tidak melaporkan teks, meskipun teks tersebut cocok dengan kriteria pengenalan data terkelola atau pengenalan data kustom. Untuk mempelajari selengkapnya, lihat [Mendefinisikan pengecualian data sensitif dengan daftar izinkan](#).

Secara default, Macie tidak menggunakan daftar izinkan saat melakukan penemuan data sensitif otomatis. Jika Anda ingin Macie menggunakan daftar izin tertentu, Anda dapat menambahkannya ke analisis. Jika Anda menambahkan daftar izinkan ke analisis, Anda selanjutnya dapat menghapusnya.

Untuk menambah atau menghapus daftar izinkan

1. [Buka konsol Amazon Macie di https://console.aws.amazon.com/macie/](https://console.aws.amazon.com/macie/).

2. Dengan menggunakan Wilayah AWS pemilih di sudut kanan atas halaman, pilih Wilayah tempat Anda ingin menambahkan atau menghapus daftar izinkan dari analisis penemuan otomatis.
3. Di panel navigasi, di bawah Pengaturan, pilih Penemuan otomatis. Halaman penemuan data sensitif otomatis muncul dan menampilkan pengaturan Anda saat ini. Pada halaman tersebut, bagian Izinkan daftar menunjukkan daftar yang mengizinkan yang telah Anda tambahkan, atau menunjukkan bahwa Anda belum memilih daftar izin apa pun untuk penemuan otomatis.
4. Di bagian Izinkan daftar, pilih Edit.
5. Lakukan langkah-langkah berikut:
  - Untuk menambahkan satu atau beberapa daftar izinkan, pilih kotak centang untuk setiap daftar izinkan yang ingin Anda tambahkan. Jika kotak centang sudah dipilih, Anda telah menambahkan daftar itu.
  - Untuk menghapus satu atau beberapa daftar izinkan, kosongkan kotak centang untuk setiap daftar izinkan yang ingin Anda hapus. Jika kotak centang sudah dihapus, Macie saat ini tidak menggunakan daftar itu saat melakukan penemuan otomatis.

 Tip

Untuk meninjau pengaturan daftar izinkan sebelum menambahkan atau menghapusnya, pilih ikon tautan



di sebelah nama daftar. Macie membuka halaman yang menampilkan pengaturan daftar.

6. Setelah selesai, pilih Simpan.

## Menonaktifkan penemuan data sensitif otomatis untuk akun Anda

Anda dapat menonaktifkan penemuan data sensitif otomatis untuk akun Anda kapan saja. Jika Anda menonaktifkan penemuan data sensitif otomatis, Macie berhenti melakukan semua aktivitas penemuan otomatis untuk akun Anda sebelum siklus evaluasi dan analisis berikutnya dimulai, biasanya dalam 24 jam. Selain itu, Anda kehilangan akses ke semua data statistik, data inventaris, dan informasi lain yang diproduksi dan diberikan secara langsung oleh Macie saat melakukan aktivitas tersebut. Misalnya, inventaris bucket S3 Anda tidak lagi menyertakan skor sensitivitas dan visualisasi, atau menganalisis statistik dan detail untuk masing-masing bucket S3.

Anda dapat terus mengakses temuan data sensitif yang dihasilkan Macie saat melakukan penemuan otomatis untuk akun Anda. Macie menyimpan temuan Anda selama 90 hari. Selain itu, data yang Anda simpan atau publikasikan ke orang lain Layanan AWS tetap utuh dan tidak terpengaruh, seperti hasil penemuan data sensitif di Amazon S3 dan menemukan peristiwa di Amazon EventBridge.

Jika Anda menonaktifkan penemuan data sensitif otomatis untuk akun Anda, Anda dapat mengaktifkannya lagi. Macie kemudian melanjutkan semua aktivitas penemuan otomatis untuk akun Anda. Jika Anda mengaktifkannya kembali dalam waktu 30 hari, Anda mendapatkan kembali akses ke semua data statistik, data inventaris, dan informasi lain yang sebelumnya diproduksi dan diberikan secara langsung oleh Macie saat melakukan aktivitas tersebut. Jika Anda tidak mengaktifkannya kembali dalam waktu 30 hari, Macie secara permanen menghapus data statistik dan informasi lain yang sebelumnya diproduksi dan diberikan secara langsung.

Ikuti langkah-langkah berikut untuk menonaktifkan penemuan data sensitif otomatis untuk akun Anda dengan menggunakan konsol Amazon Macie. Untuk menonaktifkan penemuan otomatis secara terprogram, gunakan [UpdateAutomatedDiscoveryConfiguration](#) pengoperasian Amazon Macie API.

Untuk menonaktifkan penemuan data sensitif otomatis untuk akun Anda

1. [Buka konsol Amazon Macie di https://console.aws.amazon.com/macie/](https://console.aws.amazon.com/macie/).
2. Dengan menggunakan Wilayah AWS pemilih di sudut kanan atas halaman, pilih Wilayah tempat Anda ingin menonaktifkan penemuan data sensitif otomatis.
3. Di panel navigasi, di bawah Pengaturan, pilih Penemuan otomatis.
4. Di bagian Status, pilih Nonaktifkan.
5. Ketika dimintai konfirmasi, pilih Nonaktifkan.

## Mengelola penemuan data sensitif otomatis untuk bucket S3 individual

Saat Anda meninjau dan mengevaluasi statistik dan hasil penemuan data sensitif otomatis, Anda dapat menyesuaikan penilaian sensitivitas dan pengaturan lain untuk bucket Amazon Simple Storage Service (Amazon S3) individual. Dengan menyesuaikan pengaturan ini, Anda dapat menyempurnakan penilaian sensitivitas data Amazon S3 Anda secara keseluruhan dan bucket tertentu di dalamnya. Anda juga dapat menangkap hasil investigasi yang Anda lakukan untuk bucket tertentu.

Anda dapat menyesuaikan setelan penemuan data sensitif otomatis untuk bucket S3 dengan cara berikut.



## Tetapkan skor sensitivitas

Secara default, Amazon Macie secara otomatis menghitung skor sensitivitas bucket. Skor didasarkan terutama pada jumlah data sensitif yang ditemukan Macie dalam bucket, dan jumlah data yang telah dianalisis Macie dalam bucket. Untuk informasi selengkapnya, lihat [Penilaian sensitivitas untuk bucket S3](#).

Anda dapat mengganti skor terhitung bucket dan menetapkan skor maksimum secara manual (100), yang juga berlaku untuk label ke ember. Jika Anda melakukan ini, Macie terus melakukan penemuan otomatis untuk ember. Namun, analisis selanjutnya tidak memengaruhi skor bucket. Untuk menghitung skor secara otomatis lagi, ubah pengaturan lagi.

### Kecualikan atau sertakan tipe data sensitif tertentu dalam skor sensitivitas

Jika dihitung secara otomatis, skor sensitivitas bucket sebagian didasarkan pada jumlah data sensitif yang ditemukan Macie di bucket. Ini terutama berasal dari sifat dan jumlah tipe data sensitif yang Macie telah ditemukan di bucket dan jumlah kejadian dari setiap jenis. Secara default, Macie menyertakan kejadian dari semua jenis data sensitif saat menghitung skor sensitivitas bucket.

Anda dapat menyesuaikan perhitungan dengan mengecualikan atau menyertakan jenis data sensitif tertentu dalam skor bucket. Misalnya, jika Macie mendeteksi alamat surat dalam bucket dan Anda menentukan bahwa ini dapat diterima, Anda dapat mengecualikan semua kejadian alamat surat dari skor bucket. Jika Anda mengecualikan tipe data sensitif, Macie terus memeriksa bucket untuk jenis data tersebut, dan melaporkan kejadian yang ditemukan. Namun, kejadian tersebut tidak memengaruhi skor yang dihitung bucket. Untuk menyertakan tipe data sensitif di toko yang dihitung lagi, ubah pengaturan lagi.

### Kecualikan atau sertakan bucket dalam analisis selanjutnya

Secara default, Macie melakukan penemuan otomatis untuk semua bucket S3 yang dipantau dan dianalisis untuk akun Anda. Jika Anda adalah administrator Macie untuk suatu organisasi, ini termasuk bucket S3 yang dimiliki akun anggota Anda. Anda dapat mengecualikan ember tertentu dari analisis. Misalnya, Anda mungkin mengecualikan bucket yang biasanya menyimpan data logging, seperti AWS CloudTrail log acara.

Jika Anda mengecualikan bucket, statistik penemuan data sensitif yang ada, dan detail untuk bucket terus berlanjut — misalnya, skor sensitivitas bucket saat ini tetap tidak berubah. Namun, Macie berhenti menganalisis objek di bucket saat melakukan penemuan otomatis untuk akun Anda. Setelah Anda mengecualikan ember, Anda kemudian dapat memasukkannya lagi.

Jika Anda mengubah setelan yang memengaruhi skor sensitivitas bucket S3, Macie segera mulai menghitung ulang dan memperbarui statistik penemuan data sensitif yang relevan dan informasi lain yang diberikannya tentang data Amazon S3 Anda. Misalnya, jika Anda menetapkan skor maksimum ke bucket, Macie menambah hitungan `Sensitifbucket` dalam statistik agregat untuk akun Anda.

Ikuti langkah-langkah ini untuk mengubah pengaturan dengan menggunakan konsol Amazon Macie. Untuk mengubah setelan secara terprogram, Anda dapat menggunakan operasi Amazon Macie API berikut ini: [UpdateResourceProfile](#), untuk menetapkan skor sensitivitas ke ember; [UpdateResourceProfileDetections](#), untuk mengecualikan atau selanjutnya menyertakan tipe data sensitif dalam skor bucket; dan, [UpdateClassificationScope](#) untuk mengecualikan atau memasukkan ember dalam analisis selanjutnya.

Untuk mengubah setelan penemuan data sensitif otomatis untuk bucket S3

1. Buka konsol Amazon Macie di <https://console.aws.amazon.com/macie/>.
2. Di panel navigasi, pilih Bucket S3.
3. Pada Ember S3 halaman, pilih ember S3 yang pengaturannya ingin Anda ubah. Anda dapat memilih ember dengan menggunakan salah satu tampilan tabel



atau peta interaktif



4. Di panel detail, lakukan salah satu hal berikut:

- Untuk mengganti skor yang dihitung dan menetapkan skor sensitivitas secara manual ke bucket, nyalakan **Tetapkan skor maksimum**

Ini mengubah skor bucket menjadi 100 dan menerapkan **Sensitif** label ke ember.

Untuk menetapkan skor yang dihitung Macie secara otomatis, matikan **Tetapkan skor maksimum**

- Untuk mengecualikan ember dari analisis selanjutnya, nyalakan **Kecualikan dari penemuan otomatis**

Jika sebelumnya Anda mengecualikan ember dari analisis, matikan **Kecualikan dari penemuan otomatis**  untuk memasukkannya lagi.

- Untuk mengecualikan atau menyertakan kejadian jenis data sensitif tertentu dalam skor sensitivitas bucket, pilih `Sensitivitas` tab. Dalam `Deteksi` tabel, pilih kotak centang untuk tipe data sensitif untuk mengecualikan atau menyertakan. Kemudian, pada `Tindakan` menu, pilih `Kecualikan` dari skor untuk mengecualikan jenis atau memilih `Sertakan` dalam skor untuk memasukkan jenisnya.

Di meja, Tipe data sensitif bidang menentukan pengenal unik (ID) untuk pengenal data terkelola yang mendeteksi data, atau nama pengenal data kustom yang mendeteksi data. ID pengenal data terkelola menjelaskan jenis data sensitif yang dirancang untuk dideteksi oleh pengenal—misalnya, `PASSPORT_NUMBER` untuk nomor paspor AS. Untuk detail tentang setiap pengenal data terkelola, lihat [Menggunakan pengidentifikasi data terkelola](#).

Jika Anda mengubah setelan yang memengaruhi skor sensitivitas bucket S3, Macie segera mulai menghitung ulang dan memperbarui statistik penemuan data sensitif yang relevan dan informasi lain tentang bucket S3.

## Menilai cakupan penemuan data sensitif otomatis

Saat penemuan data sensitif otomatis berlangsung untuk akun Anda, Amazon Macie menyediakan statistik dan detail untuk membantu Anda menilai dan memantau cakupannya atas data estate Amazon Simple Storage Service (Amazon S3) Anda. Dengan data ini, Anda dapat memeriksa status penemuan data sensitif otomatis untuk data estat Anda secara keseluruhan dan untuk masing-masing bucket S3 dalam inventaris bucket Anda. Anda juga dapat mengidentifikasi masalah yang mencegah Macie menganalisis objek dalam bucket tertentu. Jika Anda memperbaiki masalah, Anda dapat meningkatkan cakupan data Amazon S3 Anda selama siklus analisis berikutnya.

Data cakupan menyediakan snapshot status saat ini dari penemuan data sensitif otomatis untuk bucket S3 Anda di saat ini. Wilayah AWS Jika Anda adalah administrator Macie untuk suatu organisasi, ini termasuk bucket S3 yang dimiliki akun anggota Anda. Untuk setiap bucket, data menunjukkan apakah masalah terjadi ketika Macie mencoba menganalisis objek dalam bucket. Jika terjadi masalah, data menunjukkan sifat setiap masalah dan, dalam kasus tertentu, jumlah kejadian. Data diperbarui saat penemuan data sensitif otomatis berlangsung untuk akun Anda setiap hari. Jika Macie menganalisis atau mencoba menganalisis satu atau lebih objek dalam bucket selama siklus analisis harian, Macie memperbarui cakupan dan data lainnya untuk mencerminkan hasilnya.

Untuk jenis masalah tertentu, Anda dapat meninjau data secara agregat untuk semua bucket S3 Anda dan secara opsional menelusuri detail tambahan tentang setiap bucket. Misalnya, data cakupan

dapat membantu Anda dengan cepat mengidentifikasi semua bucket yang tidak diizinkan diakses Macie untuk akun Anda. Data cakupan juga melaporkan masalah tingkat objek yang terjadi. Masalah-masalah ini, disebut sebagai kesalahan klasifikasi, mencegah Macie menganalisis objek tertentu dalam bucket. Misalnya, Anda dapat menentukan berapa banyak objek yang tidak dapat dianalisis Macie dalam bucket karena objek dienkripsi dengan kunci AWS Key Management Service (AWS KMS) yang tidak lagi tersedia.

Jika Anda menggunakan konsol Amazon Macie untuk meninjau data cakupan, tampilan data Anda mencakup panduan untuk memperbaiki setiap jenis masalah. Topik selanjutnya di bagian ini juga memberikan panduan remediasi untuk setiap jenis.

## Topik

- [Meninjau data cakupan penemuan data sensitif otomatis](#)
- [Memperbaiki masalah cakupan untuk penemuan data sensitif otomatis](#)
  - [Akses ditolak](#)
  - [Kesalahan klasifikasi: Konten tidak valid](#)
  - [Kesalahan klasifikasi: Enkripsi tidak valid](#)
  - [Kesalahan klasifikasi: Kunci KMS tidak valid](#)
  - [Kesalahan klasifikasi: Izin ditolak](#)
  - [Tak terklasifikasi](#)

## Meninjau data cakupan penemuan data sensitif otomatis

Untuk meninjau dan menilai cakupan penemuan data sensitif otomatis untuk akun Anda, Anda dapat menggunakan konsol Amazon Macie atau Amazon Macie API. Konsol dan API menyediakan data yang menunjukkan status analisis saat ini untuk bucket Amazon Simple Storage Service (Amazon S3) di saat ini. Wilayah AWS Data tersebut mencakup informasi tentang masalah yang membuat celah dalam analisis:

- Bucket S3 yang tidak diizinkan diakses Macie. Macie tidak dapat menganalisis objek apa pun dalam ember ini karena pengaturan izin ember mencegah Macie mengakses ember dan objek ember.
- Bucket S3 yang tidak menyimpan objek yang dapat diklasifikasikan. Macie tidak dapat menganalisis objek apa pun dalam bucket ini karena semua objek menggunakan kelas penyimpanan Amazon S3 yang tidak didukung Macie, atau mereka memiliki ekstensi nama file untuk format file atau penyimpanan yang tidak didukung Macie.

- Bucket S3 yang belum dapat dianalisis oleh Macie karena kesalahan klasifikasi tingkat objek. Macie berusaha menganalisis satu atau lebih objek dalam ember ini. Namun, Macie tidak dapat menganalisis objek karena masalah dengan pengaturan izin tingkat objek, konten objek, atau kuota.

Data cakupan diperbarui saat penemuan data sensitif otomatis berlangsung untuk akun Anda setiap hari. Jika Anda adalah administrator Macie untuk suatu organisasi, data tersebut menyertakan informasi untuk bucket S3 yang dimiliki akun anggota Anda.

#### Note

Data cakupan tidak secara eksplisit menyertakan hasil untuk pekerjaan penemuan data sensitif yang telah Anda buat dan jalankan. Namun, memperbaiki masalah cakupan yang memengaruhi hasil penemuan data sensitif otomatis Anda kemungkinan juga akan meningkatkan cakupan oleh pekerjaan penemuan data sensitif yang kemudian Anda jalankan. Untuk menilai cakupan pekerjaan, [tinjau statistik dan hasil pekerjaan](#). Jika peristiwa log pekerjaan atau hasil lain menunjukkan masalah cakupan, panduan perbaikan nanti di bagian ini dapat membantu Anda mengatasi beberapa masalah.

Untuk meninjau data cakupan penemuan data sensitif otomatis

Anda dapat menggunakan konsol Amazon Macie atau Amazon Macie API untuk meninjau data cakupan akun atau organisasi Anda. Di konsol, satu halaman menyediakan tampilan data cakupan terpadu untuk semua bucket S3 Anda, termasuk pembatalan masalah yang baru-baru ini terjadi untuk setiap bucket. Halaman ini juga menyediakan opsi untuk meninjau kelompok data berdasarkan jenis masalah. Untuk melacak penyelidikan Anda tentang masalah pada bucket tertentu, Anda dapat mengeksport data dari halaman ke file nilai dipisahkan koma (CSV).

#### Console

Ikuti langkah-langkah berikut untuk meninjau data cakupan penemuan data sensitif otomatis dengan menggunakan konsol Amazon Macie.

Untuk meninjau data cakupan

1. Buka konsol Amazon Macie di <https://console.aws.amazon.com/macie/>.
2. Di panel navigasi, pilih Cakupan sumber daya.

3. Pada halaman Cakupan sumber daya, pilih tab untuk jenis data cakupan yang ingin Anda tinjau:

- Semua - Mencantumkan semua bucket S3 yang dipantau dan dianalisis Macie untuk akun Anda.

Untuk setiap bucket, bidang Issues menunjukkan apakah masalah mencegah Macie menganalisis objek di bucket. Jika nilai untuk bidang ini adalah None, Macie telah menganalisis setidaknya satu objek bucket atau Macie belum mencoba menganalisis objek bucket apa pun. Jika ada masalah, bidang ini menunjukkan sifat masalah dan cara memperbaiki masalah. Untuk kesalahan klasifikasi tingkat objek, mungkin juga menunjukkan (dalam tanda kurung) jumlah kejadian kesalahan.

- Akses ditolak - Mencantumkan bucket S3 yang tidak diizinkan diakses Macie. Pengaturan izin untuk bucket ini mencegah Macie mengakses bucket dan objek bucket. Akibatnya, Macie tidak dapat menganalisis objek apa pun dalam ember ini.
- Kesalahan klasifikasi - Mencantumkan bucket S3 yang belum dianalisis Macie karena kesalahan klasifikasi tingkat objek—masalah dengan pengaturan izin tingkat objek, konten objek, atau kuota.

Untuk setiap bucket, bidang Issues menunjukkan sifat dari setiap jenis kesalahan yang terjadi dan mencegah Macie menganalisis objek di bucket. Hal ini juga menunjukkan bagaimana untuk memperbaiki setiap jenis kesalahan. Tergantung pada kesalahan, mungkin juga menunjukkan (dalam tanda kurung) jumlah kejadian kesalahan.

- Unclassifiable - Daftar ember S3 yang Macie tidak dapat menganalisis karena mereka tidak menyimpan objek diklasifikasikan. Semua objek dalam bucket ini menggunakan kelas penyimpanan Amazon S3 yang tidak didukung atau memiliki ekstensi nama file untuk format file atau penyimpanan yang tidak didukung. Akibatnya, Macie tidak dapat menganalisis objek apa pun dalam ember ini.

4. Untuk menelusuri dan meninjau data pendukung untuk bucket S3, pilih nama bucket. Kemudian lihat panel detail bucket untuk statistik dan informasi lainnya tentang bucket.

5. Untuk mengekspor tabel ke file CSV, pilih Ekspor ke CSV di bagian atas halaman. File CSV yang dihasilkan berisi subset metadata untuk setiap bucket S3 dalam tabel, hingga 50.000 bucket. File ini mencakup bidang masalah Cakupan. Nilai untuk bidang ini menunjukkan apakah masalah mencegah Macie menganalisis objek dalam bucket dan, jika demikian, sifat masalah.

## API

Untuk meninjau data cakupan secara terprogram, tentukan kriteria filter dalam kueri yang Anda kirimkan menggunakan [DescribeBuckets](#) pengoperasian Amazon Macie API. Operasi ini mengembalikan susunan objek. Setiap objek berisi data statistik dan informasi lain tentang bucket S3 yang cocok dengan kriteria filter.

Dalam kriteria filter, sertakan kondisi untuk jenis data cakupan yang ingin Anda tinjau:

- Untuk mengidentifikasi bucket yang tidak diizinkan diakses Macie karena pengaturan izin bucket, sertakan kondisi di mana nilai untuk bidang sama. `errorCode ACCESS_DENIED`
- Untuk mengidentifikasi bucket yang diizinkan diakses Macie dan belum dianalisis, sertakan kondisi di mana nilai untuk `sensitivityScore` bidang sama 50 dan nilai untuk `errorCode` bidang tidak sama. `ACCESS_DENIED`
- Untuk mengidentifikasi bucket yang tidak dapat dianalisis Macie karena semua objek bucket menggunakan kelas atau format penyimpanan yang tidak didukung, sertakan kondisi di mana nilai untuk `classifiableSizeInBytes` bidang sama 0 dan nilai untuk bidang lebih besar dari. `sizeInBytes 0`
- Untuk mengidentifikasi bucket yang Macie telah menganalisis setidaknya satu objek, sertakan kondisi di mana nilai untuk `sensitivityScore` bidang berada dalam kisaran 1-99 tetapi tidak sama dengan. 50 Untuk juga menyertakan bucket tempat Anda menetapkan skor maksimum secara manual, kisarannya harus 1—100.
- Untuk mengidentifikasi bucket yang belum dianalisis Macie karena kesalahan klasifikasi tingkat objek, sertakan kondisi di mana nilai untuk bidang sama. `sensitivityScore -1` Untuk kemudian meninjau rincian jenis dan jumlah kesalahan yang terjadi untuk bucket tertentu, gunakan [GetResourceProfile](#) operasi.

Jika Anda menggunakan [AWS Command Line Interface\(AWS CLI\)](#), tentukan kriteria filter dalam kueri yang Anda kirimkan dengan menjalankan perintah [describe-bucket](#). Untuk meninjau rincian jenis dan jumlah kesalahan yang terjadi untuk bucket S3 tertentu, jika ada, jalankan [get-resource-profile](#) perintah.

Misalnya, AWS CLI perintah berikut menggunakan kriteria filter untuk mengambil detail semua bucket S3 yang tidak diizinkan diakses Macie karena pengaturan izin bucket.

Contoh ini diformat untuk Linux, macOS, atau Unix:

```
$ aws macie2 describe-buckets --criteria '{"errorCode":{"eq":["ACCESS_DENIED"]}}'
```

Contoh ini diformat untuk Microsoft Windows:

```
C:\> aws macie2 describe-buckets --criteria={"errorCode":{"eq":["ACCESS_DENIED\n"]}}
```

Jika permintaan Anda berhasil, Macie mengembalikan array. `buckets` Array berisi objek untuk setiap bucket S3 yang ada di saat ini Wilayah AWS dan cocok dengan kriteria filter.

Jika tidak ada ember S3 cocok dengan kriteria filter, Macie mengembalikan array kosong. `buckets`

```
{
  "buckets": []
}
```

Untuk informasi selengkapnya tentang menentukan kriteria filter dalam kueri, termasuk contoh kriteria umum, lihat. [Memfilter inventaris bucket S3 Anda](#)

## Memperbaiki masalah cakupan untuk penemuan data sensitif otomatis

Amazon Macie melaporkan beberapa jenis masalah yang mengurangi cakupan penemuan data sensitif otomatis dari data Amazon Simple Storage Service (Amazon S3) Anda. Informasi berikut dapat membantu Anda menyelidiki dan memperbaiki masalah ini.

Jenis dan detail masalah

- [Akses ditolak](#)
- [Kesalahan klasifikasi: Konten tidak valid](#)
- [Kesalahan klasifikasi: Enkripsi tidak valid](#)
- [Kesalahan klasifikasi: Kunci KMS tidak valid](#)
- [Kesalahan klasifikasi: Izin ditolak](#)
- [Tak terklasifikasi](#)



**Tip**

Untuk menyelidiki kesalahan klasifikasi tingkat objek untuk bucket S3, mulailah dengan meninjau daftar sampel objek untuk bucket. Daftar ini menunjukkan objek mana yang dianalisis atau dianalisis Macie dalam bucket, hingga 100 objek.

Untuk meninjau daftar di konsol Amazon Macie, pilih bucket di halaman bucket S3, lalu pilih tab Object samples di panel detail bucket. Untuk meninjau daftar secara terprogram, gunakan [ListResourceProfileArtifacts](#) pengoperasian Amazon Macie API. Jika status analisis untuk objek dilewati (SKIPPED), objek mungkin telah menyebabkan kesalahan.

**Akses ditolak**

Masalah ini menunjukkan bahwa setelah izin bucket S3 mencegah Macie mengakses bucket dan objek bucket. Macie tidak dapat mengambil dan menganalisis objek apa pun di ember.

**Detail**

Penyebab paling umum untuk jenis masalah ini adalah kebijakan bucket yang membatasi. Kebijakan bucket adalah kebijakan berbasis sumber daya AWS Identity and Access Management (IAM) yang menentukan tindakan mana yang dapat dilakukan oleh prinsipal (pengguna, akun, layanan, atau entitas lain) pada bucket S3, dan kondisi di mana prinsipal dapat melakukan tindakan tersebut. Kebijakan bucket yang membatasi menggunakan Deny pernyataan eksplisit Allow atau yang memberikan atau membatasi akses ke data bucket berdasarkan kondisi tertentu. Misalnya, kebijakan bucket mungkin berisi Deny pernyataan Allow atau yang menolak akses ke bucket kecuali alamat IP sumber tertentu digunakan untuk mengakses bucket.

Jika kebijakan bucket untuk bucket S3 berisi Deny pernyataan eksplisit dengan satu atau beberapa kondisi, Macie mungkin tidak diizinkan untuk mengambil dan menganalisis objek bucket untuk mendeteksi data sensitif. Macie hanya dapat memberikan sebagian informasi tentang bucket, seperti nama bucket dan tanggal pembuatan.

**Panduan remediasi**

Untuk mengatasi masalah ini, perbarui kebijakan bucket untuk bucket S3. Pastikan bahwa kebijakan memungkinkan Macie untuk mengakses bucket dan objek bucket. Untuk mengizinkan akses ini, tambahkan kondisi untuk peran (`AWSServiceRoleForAmazonMacie`) terkait layanan Macie ke kebijakan. Kondisi ini harus mengecualikan peran terkait layanan Macie agar tidak cocok dengan Deny pembatasan dalam kebijakan. Hal ini dapat dilakukan dengan menggunakan kunci

konteks kondisi `aws:PrincipalArn` global dan Amazon Resource Name (ARN) peran terkait layanan Macie untuk akun Anda.

Jika Anda memperbarui kebijakan bucket dan Macie mendapatkan akses ke bucket S3, Macie akan mendeteksi perubahan tersebut. Ketika ini terjadi, Macie akan memperbarui statistik, data inventaris, dan informasi lain yang diberikannya tentang data Amazon S3 Anda. Selain itu, objek bucket akan menjadi prioritas yang lebih tinggi untuk analisis selama siklus analisis berikutnya.

## Referensi tambahan

Untuk informasi selengkapnya tentang memperbarui kebijakan bucket S3 agar Macie dapat mengakses bucket, lihat [Mengizinkan Amazon Macie untuk mengakses bucket S3 dan objek](#). Untuk informasi tentang penggunaan kebijakan bucket untuk mengontrol akses ke bucket, lihat kebijakan [Bucket dan kebijakan pengguna serta Cara Amazon S3 mengotorisasi permintaan](#) di Panduan Pengguna Amazon Simple Storage Service.

## Kesalahan klasifikasi: Konten tidak valid

Jenis kesalahan klasifikasi terjadi jika Macie mencoba untuk menganalisis objek dalam ember S3 dan objek cacat atau objek berisi konten yang melebihi kuota penemuan data sensitif. Macie tidak bisa menganalisis objeknya.

## Detail

Kesalahan ini biasanya terjadi karena objek S3 adalah file cacat atau rusak. Akibatnya, Macie tidak dapat mengurai dan menganalisis semua data dalam file.

Kesalahan ini juga dapat terjadi jika analisis objek S3 akan melebihi kuota penemuan data sensitif untuk file individual. Misalnya, ukuran penyimpanan objek melebihi kuota ukuran untuk jenis file tersebut.

Untuk kedua kasus tersebut, Macie tidak dapat menyelesaikan analisisnya terhadap objek S3 dan status analisis untuk objek dilewati (). SKIPPED

## Panduan remediasi

Untuk menyelidiki kesalahan ini, unduh objek S3 dan periksa pemformatan dan isi file. Juga menilai isi file terhadap kuota Macie untuk penemuan data sensitif.

Jika Anda tidak memperbaiki kesalahan ini, Macie akan mencoba menganalisis objek lain di bucket S3. Jika Macie menganalisis objek lain berhasil, Macie akan memperbarui data cakupan dan informasi lain yang diberikannya tentang bucket.

## Referensi tambahan

Untuk daftar kuota penemuan data sensitif, termasuk kuota untuk jenis file tertentu, lihat. [Kuota Amazon Macie](#) Untuk informasi tentang cara Macie memperbarui skor sensitivitas dan informasi lain yang diberikannya tentang bucket S3, lihat. [Cara kerja penemuan data sensitif otomatis](#)

## Kesalahan klasifikasi: Enkripsi tidak valid

Jenis kesalahan klasifikasi ini terjadi jika Macie mencoba menganalisis objek dalam bucket S3 dan objek dienkripsi dengan kunci yang disediakan pelanggan. Objek menggunakan enkripsi SSE-C, yang berarti bahwa Macie tidak dapat mengambil dan menganalisis objek.

## Detail

Amazon S3 mendukung beberapa opsi enkripsi untuk objek S3. Untuk sebagian besar opsi ini, Macie dapat mendekripsi objek dengan menggunakan peran terkait layanan Macie untuk akun Anda. Namun, ini tergantung pada jenis enkripsi yang digunakan.

Agar Macie mendekripsi objek S3, objek harus dienkripsi dengan kunci yang dapat diakses Macie dan diizinkan untuk digunakan. Jika objek dienkripsi dengan kunci yang disediakan pelanggan, Macie tidak dapat menyediakan materi kunci yang diperlukan untuk mengambil objek dari Amazon S3. Akibatnya, Macie tidak dapat menganalisis objek dan status analisis untuk objek dilewati (). SKIPPED

## Panduan remediasi

Untuk mengatasi kesalahan ini, enkripsi objek S3 dengan kunci terkelola Amazon S3 atau AWS Key Management Service kunci (). AWS KMS Jika Anda lebih suka menggunakan AWS KMS kunci, kunci dapat AWS dikelola kunci KMS, atau kunci KMS yang dikelola pelanggan yang diizinkan untuk digunakan Macie.

Untuk mengenkripsi objek S3 yang ada dengan kunci yang dapat diakses dan digunakan Macie, Anda dapat mengubah pengaturan enkripsi untuk objek. Untuk mengenkripsi objek baru dengan kunci yang dapat diakses dan digunakan Macie, ubah pengaturan enkripsi default untuk bucket S3. Juga pastikan bahwa kebijakan bucket tidak memerlukan objek baru untuk dienkripsi dengan kunci yang disediakan pelanggan.

Jika Anda tidak memperbaiki kesalahan ini, Macie akan mencoba menganalisis objek lain di bucket S3. Jika Macie menganalisis objek lain berhasil, Macie akan memperbarui data cakupan dan informasi lain yang diberikannya tentang bucket.

## Referensi tambahan

Untuk informasi tentang persyaratan dan opsi untuk menggunakan Macie untuk menganalisis objek S3 terenkripsi, lihat [Menganalisis objek Amazon S3 terenkripsi dengan Amazon Macie](#). Untuk informasi tentang opsi enkripsi dan pengaturan untuk bucket S3, lihat [Melindungi data dengan enkripsi dan Mengatur perilaku enkripsi sisi server default untuk bucket S3 di Panduan Pengguna Amazon Simple Storage Service](#).

## Kesalahan klasifikasi: Kunci KMS tidak valid

Jenis kesalahan klasifikasi ini terjadi jika Macie mencoba menganalisis objek dalam bucket S3 dan objek dienkripsi dengan kunci AWS Key Management Service (AWS KMS) yang tidak lagi tersedia. Macie tidak dapat mengambil dan menganalisis objek.

## Detail

AWS KMS menyediakan opsi untuk menonaktifkan dan menghapus pelanggan yang dikelola. AWS KMS keys Jika objek S3 dienkripsi dengan kunci KMS yang dinonaktifkan, dijadwalkan untuk dihapus, atau dihapus, Macie tidak dapat mengambil dan mendekripsi objek. Akibatnya, Macie tidak dapat menganalisis objek dan status analisis untuk objek dilewati (). SKIPPED Agar Macie menganalisis objek terenkripsi, objek harus dienkripsi dengan kunci yang dapat diakses Macie dan diizinkan untuk digunakan.

## Panduan remediasi

Untuk memperbaiki kesalahan ini, aktifkan kembali atau batalkan penghapusan terjadwal yang berlaku AWS KMS key, tergantung pada status kunci saat ini. Jika kunci yang berlaku sudah dihapus, kesalahan ini tidak dapat diperbaiki.

Untuk menentukan yang AWS KMS key digunakan untuk mengenkripsi objek S3, Anda dapat mulai dengan menggunakan Macie untuk meninjau pengaturan enkripsi sisi server untuk bucket S3. Jika pengaturan enkripsi default untuk bucket dikonfigurasi untuk menggunakan kunci KMS, detail bucket menunjukkan kunci mana yang digunakan. Anda kemudian dapat memeriksa status kunci itu. Atau, Anda dapat menggunakan Amazon S3 untuk meninjau pengaturan enkripsi untuk bucket dan objek individual dalam bucket.

Jika Anda tidak memperbaiki kesalahan ini, Macie akan mencoba menganalisis objek lain di bucket S3. Jika Macie menganalisis objek lain berhasil, Macie akan memperbarui data cakupan dan informasi lain yang diberikannya tentang bucket.

## Referensi tambahan

Untuk informasi tentang menggunakan Macie untuk meninjau pengaturan enkripsi sisi server untuk bucket S3, lihat. [Meninjau detail ember S3 Untuk informasi tentang mengaktifkan kembali atau membatalkan penghapusan terjadwal AWS KMS key, lihat Mengaktifkan dan menonaktifkan kunci dan Menjadwalkan dan membatalkan penghapusan kunci di Panduan Pengembang. AWS Key Management Service](#)

## Kesalahan klasifikasi: Izin ditolak

Jenis kesalahan klasifikasi ini terjadi jika Macie mencoba menganalisis objek dalam bucket S3 dan Macie tidak dapat mengambil atau mendekripsi objek karena pengaturan izin untuk objek atau pengaturan izin untuk kunci yang digunakan untuk mengenkripsi objek. Macie tidak dapat mengambil dan menganalisis objek.

## Detail

Kesalahan ini biasanya terjadi karena objek S3 dienkripsi dengan kunci pengelolaan pelanggan AWS Key Management Service (AWS KMS) yang Macie tidak diizinkan untuk digunakan. Jika objek dienkripsi dengan pelanggan yang dikelola AWS KMS key, kebijakan kunci harus mengizinkan Macie mendekripsi data dengan menggunakan kunci.

Kesalahan ini juga dapat terjadi jika pengaturan izin Amazon S3 mencegah Macie mengambil objek S3. Kebijakan bucket untuk bucket S3 mungkin membatasi akses ke objek bucket tertentu atau hanya mengizinkan prinsipal tertentu (pengguna, akun, layanan, atau entitas lain) untuk mengakses objek. Atau daftar kontrol akses (ACL) untuk objek mungkin membatasi akses ke objek. Akibatnya, Macie mungkin tidak diizinkan untuk mengakses objek.

Untuk salah satu kasus sebelumnya, Macie tidak dapat mengambil dan menganalisis objek, dan status analisis untuk objek dilewati (). SKIPPED

## Panduan remediasi

Untuk memperbaiki kesalahan ini, tentukan apakah objek S3 dienkripsi dengan pelanggan yang dikelola. AWS KMS key Jika ya, pastikan kebijakan kunci memungkinkan peran (AWSServiceRoleForAmazonMacie) terkait layanan Macie untuk mendekripsi data dengan kunci. Bagaimana Anda mengizinkan akses ini tergantung pada apakah akun yang memiliki AWS KMS key juga memiliki bucket S3 yang menyimpan objek. Jika akun yang sama memiliki kunci KMS dan bucket, pengguna akun harus memperbarui kebijakan kunci. Jika satu akun memiliki

kunci KMS dan akun yang berbeda memiliki bucket, pengguna akun yang memiliki kunci harus mengizinkan akses lintas akun ke kunci tersebut.

**i** Tip

Anda dapat secara otomatis membuat daftar semua pelanggan yang dikelola AWS KMS keys yang perlu diakses Macie untuk menganalisis objek dalam bucket S3 untuk akun Anda. Untuk melakukan ini, jalankan skrip AWS KMS Permission Analyzer, yang tersedia dari repositori [Amazon Macie Scripts aktif](#). GitHub Script juga dapat menghasilkan script tambahan dari AWS Command Line Interface (AWS CLI) perintah. Anda opsional dapat menjalankan perintah tersebut untuk memperbarui pengaturan konfigurasi yang diperlukan dan kebijakan untuk kunci KMS yang Anda tentukan.

Jika Macie sudah diizinkan untuk menggunakan yang berlaku AWS KMS key atau objek S3 tidak dienkripsi dengan kunci KMS yang dikelola pelanggan, pastikan bahwa kebijakan bucket memungkinkan Macie mengakses objek. Juga verifikasi bahwa ACL objek memungkinkan Macie untuk membaca data objek dan metadata.

Untuk kebijakan bucket, Anda dapat mengizinkan akses ini dengan menambahkan ketentuan untuk peran terkait layanan Macie ke kebijakan. Kondisi ini harus mengecualikan peran terkait layanan Macie agar tidak cocok dengan Deny pembatasan dalam kebijakan. Hal ini dapat dilakukan dengan menggunakan kunci konteks kondisi `aws:PrincipalArn` global dan Amazon Resource Name (ARN) peran terkait layanan Macie untuk akun Anda.

Untuk objek ACL, Anda dapat mengizinkan akses ini dengan bekerja dengan pemilik objek untuk menambahkan Anda Akun AWS sebagai penerima dengan READ izin untuk objek. Macie kemudian dapat menggunakan peran terkait layanan untuk akun Anda untuk mengambil dan menganalisis objek. Juga pertimbangkan untuk mengubah pengaturan Kepemilikan Objek untuk bucket. Anda dapat menggunakan pengaturan ini untuk menonaktifkan ACL untuk semua objek di bucket dan memberikan izin kepemilikan ke akun yang memiliki bucket.

Jika Anda tidak memperbaiki kesalahan ini, Macie akan mencoba menganalisis objek lain di bucket S3. Jika Macie menganalisis objek lain berhasil, Macie akan memperbarui data cakupan dan informasi lain yang diberikannya tentang bucket.

## Referensi tambahan

Untuk informasi selengkapnya tentang mengizinkan Macie mendekripsi data dengan pelanggan yang dikelola AWS KMS key, lihat. [Mengizinkan Amazon Macie menggunakan pelanggan yang](#)

[dikelola AWS KMS key](#) Untuk informasi tentang memperbarui kebijakan bucket S3 agar Macie dapat mengakses bucket, lihat. [Mengizinkan Amazon Macie untuk mengakses bucket S3 dan objek](#)

Untuk informasi tentang memperbarui kebijakan kunci, lihat [Mengubah kebijakan kunci](#) di Panduan AWS Key Management Service Developer. Untuk informasi tentang penggunaan pelanggan yang dikelola AWS KMS keys untuk mengenkripsi objek S3, lihat [Menggunakan enkripsi sisi server dengan AWS KMS kunci](#) di Panduan Pengguna Amazon Simple Storage Service.

Untuk informasi tentang penggunaan kebijakan bucket untuk mengontrol akses ke bucket S3, lihat kebijakan [Bucket dan kebijakan pengguna serta Cara Amazon S3 mengotorisasi permintaan](#) di Panduan Pengguna Amazon Simple Storage Service. Untuk informasi tentang penggunaan pengaturan ACL atau Kepemilikan Objek untuk mengontrol akses ke objek S3, lihat [Mengelola akses dengan ACL](#) dan [Mengontrol kepemilikan objek dan menonaktifkan ACL untuk bucket Anda](#) di Panduan Pengguna Amazon Simple Storage Service.

Tak terklasifikasi

Masalah ini menunjukkan bahwa semua objek dalam bucket S3 disimpan menggunakan kelas penyimpanan Amazon S3 yang tidak didukung atau format file atau penyimpanan yang tidak didukung. Macie tidak dapat menganalisis benda apa pun di ember.

Detail

Agar memenuhi syarat untuk pemilihan dan analisis, objek S3 harus menggunakan kelas penyimpanan Amazon S3 yang didukung Macie. Objek juga harus memiliki ekstensi nama file untuk file atau format penyimpanan yang didukung Macie. Jika objek tidak memenuhi kriteria ini, objek diperlakukan sebagai objek unclassifiable. Macie tidak mencoba untuk mengambil atau menganalisis data dalam objek unclassifiable.

Jika semua objek dalam bucket S3 adalah objek yang tidak dapat diklasifikasikan, bucket keseluruhan adalah bucket yang tidak dapat diklasifikasikan. Macie tidak dapat melakukan penemuan data sensitif otomatis untuk bucket.

Panduan remediasi

Untuk mengatasi masalah ini, tinjau aturan konfigurasi siklus hidup dan pengaturan lain yang menentukan kelas penyimpanan mana yang digunakan untuk menyimpan objek di bucket

S3. Pertimbangkan untuk menyesuaikan pengaturan tersebut untuk menggunakan kelas penyimpanan yang didukung Macie. Anda juga dapat mengubah kelas penyimpanan objek yang ada di bucket.

Juga menilai format file dan penyimpanan objek yang ada di bucket S3. Untuk menganalisis objek, pertimbangkan untuk memindahkan data, baik sementara atau permanen, ke objek baru yang menggunakan format yang didukung.

Jika objek ditambahkan ke bucket S3 dan mereka menggunakan kelas penyimpanan dan format yang didukung, Macie akan mendeteksi objek saat berikutnya mengevaluasi inventaris bucket Anda. Ketika ini terjadi, Macie akan berhenti melaporkan bahwa bucket tidak dapat diklasifikasikan dalam statistik, data cakupan, dan informasi lain yang disediakan tentang data Amazon S3 Anda. Selain itu, objek baru akan menjadi prioritas yang lebih tinggi untuk analisis selama siklus analisis berikutnya.

#### Referensi tambahan

Untuk informasi tentang kelas penyimpanan Amazon S3 serta format file dan penyimpanan yang didukung Macie, lihat [Kelas dan format penyimpanan yang didukung oleh Amazon Macie](#). Untuk informasi tentang aturan konfigurasi siklus hidup dan opsi kelas penyimpanan yang disediakan Amazon S3, lihat [Mengelola siklus hidup penyimpanan Anda dan Menggunakan kelas penyimpanan Amazon S3 di Panduan Pengguna Amazon Simple Storage Service](#).

## Meninjau statistik dan hasil penemuan data sensitif otomatis

Saat penemuan data sensitif otomatis diaktifkan untuk akun Anda, Amazon Macie secara otomatis menghasilkan dan memelihara data inventaris tambahan, statistik, dan informasi lainnya tentang bucket Amazon Simple Storage Service (Amazon S3) yang dipantau dan dianalisis untuk akun Anda. Jika Anda administrator Macie untuk suatu organisasi, ini termasuk bucket S3 yang dimiliki akun anggota Anda.

Informasi tambahan menangkap hasil aktivitas penemuan data sensitif otomatis yang telah dilakukan Macie sejauh ini untuk akun Anda. Ini juga melengkapi informasi lain yang disediakan Macie tentang data Amazon S3 Anda, seperti akses publik dan pengaturan enkripsi untuk masing-masing bucket S3. Selain metadata dan statistik, Macie menghasilkan catatan data sensitif yang ditemukannya dan analisis yang dilakukannya — temuan data sensitif dan hasil penemuan data sensitif.

Seiring kemajuan analisis penemuan data sensitif otomatis untuk akun Anda, fitur dan data berikut dapat membantu Anda meninjau dan mengevaluasi hasilnya:



- **Dasbor ringkasan** - Menyediakan statistik agregat untuk estat data Amazon S3 Anda. Statistik tersebut mencakup data untuk metrik utama seperti jumlah total bucket tempat Macie menemukan data sensitif, dan berapa banyak bucket tersebut yang dapat diakses publik. Mereka juga menyertakan data tentang masalah yang memengaruhi cakupan data estate Anda.
- **Peta panas bucket S3** - Menyediakan representasi visual interaktif dari sensitivitas data di seluruh kawasan data Anda, dikelompokkan berdasarkan Akun AWS. Untuk setiap akun, peta menyertakan statistik sensitivitas agregat dan menggunakan warna untuk menunjukkan skor sensitivitas saat ini untuk setiap bucket yang dimiliki akun. Peta juga menggunakan simbol untuk membantu Anda mengidentifikasi bucket yang dapat diakses publik, tidak dapat dianalisis oleh Macie, dan banyak lagi.
- **Tabel bucket S3** - Memberikan informasi ringkasan untuk setiap bucket S3 di inventaris Anda. Untuk setiap bucket, tabel menyertakan data seperti nama bucket dan skor sensitivitas saat ini, jumlah objek yang dapat dianalisis Macie di bucket, dan apakah Anda telah mengonfigurasi pekerjaan penemuan data sensitif apa pun untuk menganalisis objek di bucket secara berkala. Anda dapat secara opsional mengeksport data dari tabel ke file nilai yang dipisahkan koma (CSV).
- **Panel detail** — Memberikan detail dan statistik untuk bucket S3 yang Anda pilih di peta panas atau tabel. Rinciannya mencakup daftar objek yang telah dianalisis Macie dalam ember, dan rincian jenis dan jumlah kemunculan data sensitif yang ditemukan Macie di ember. Anda juga dapat menggunakan panel untuk mengelola pengaturan penemuan otomatis untuk masing-masing bucket.
- **Temuan data sensitif** — Berikan laporan terperinci tentang data sensitif yang ditemukan Macie di objek S3 individu. Rinciannya termasuk ketika Macie menemukan data sensitif, dan jenis dan jumlah kejadian data sensitif yang ditemukan Macie. Detailnya juga mencakup informasi tentang bucket dan objek S3 yang terpengaruh, termasuk pengaturan akses publik bucket dan kapan objek tersebut baru-baru ini diubah.
- **Hasil penemuan data sensitif** — Memberikan catatan analisis yang dilakukan Macie untuk objek S3 individu. Ini termasuk objek yang Macie tidak menemukan data sensitif, dan karena itu tidak menghasilkan temuan data sensitif, dan objek yang tidak dapat dianalisis Macie karena masalah atau kesalahan.

Dengan data ini, Anda dapat mengevaluasi sensitivitas data di seluruh kawasan data Amazon S3 dan menelusuri untuk mengevaluasi dan menyelidiki masing-masing bucket dan objek S3. Dikombinasikan dengan informasi yang disediakan Macie tentang keamanan dan privasi data Amazon S3 Anda, Anda juga dapat mengidentifikasi kasus di mana perbaikan segera mungkin diperlukan—misalnya, bucket yang dapat diakses publik tempat Macie menemukan data sensitif.

Data tambahan dapat membantu Anda menilai dan memantau cakupan data estate Amazon S3 Anda. Dengan data cakupan, Anda dapat memeriksa status analisis untuk data estate Anda secara keseluruhan dan untuk bucket S3 individual dalam inventaris bucket Anda. Anda juga dapat mengidentifikasi masalah yang mencegah Macie menganalisis objek dalam ember tertentu. Jika Anda memperbaiki masalah, Anda dapat meningkatkan cakupan data Amazon S3 Anda selama siklus analisis berikutnya. Untuk informasi selengkapnya, lihat [Menilai cakupan penemuan data sensitif otomatis](#).

## Topik

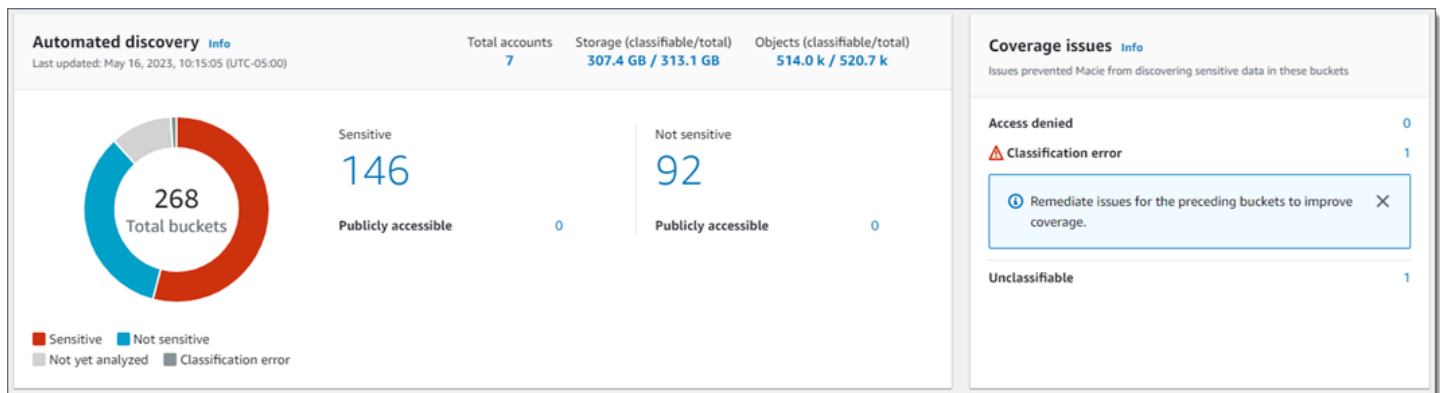
- [Meninjau statistik sensitivitas data agregat di dasbor Ringkasan](#)
- [Memvisualisasikan sensitivitas data dengan peta bucket S3](#)
- [Menilai sensitivitas data dengan tabel bucket S3](#)
- [Meninjau detail sensitivitas data untuk masing-masing bucket S3](#)
- [Menganalisis temuan data sensitif yang dihasilkan oleh penemuan otomatis](#)
- [Mengakses hasil penemuan data sensitif yang dihasilkan oleh penemuan otomatis](#)

## Meninjau statistik sensitivitas data agregat di dasbor Ringkasan

Di konsol Amazon Macie, dasbor Ringkasan menyediakan snapshot statistik agregat dan data temuan untuk data Amazon Simple Storage Service (Amazon S3) saat ini. Wilayah AWS Ini dirancang untuk membantu Anda menilai postur keamanan keseluruhan data Amazon S3 Anda.

Statistik dasbor mencakup data untuk metrik keamanan utama seperti jumlah bucket S3 yang dapat diakses publik atau dibagikan dengan yang lain. Akun AWS Dasbor juga menampilkan grup data temuan agregat untuk akun Anda—misalnya, bucket S3 yang menghasilkan temuan terbanyak selama tujuh hari sebelumnya. Jika Anda administrator Macie untuk suatu organisasi, dasbor menyediakan statistik dan data gabungan untuk semua akun di organisasi Anda. Anda dapat secara opsional memfilter data berdasarkan akun.

Jika penemuan data sensitif otomatis diaktifkan untuk akun Anda, dasbor Ringkasan menyertakan statistik penemuan data sensitif otomatis. Statistik menangkap status dan hasil aktivitas penemuan data sensitif otomatis yang telah dilakukan Macie sejauh ini untuk data Amazon S3 Anda. Sebagai contoh:



Statistik di bagian Penemuan otomatis memberikan gambaran tentang status saat ini dan hasil aktivitas penemuan data sensitif otomatis. Data tidak menyertakan hasil pekerjaan penemuan data sensitif yang telah Anda buat dan jalankan.

Statistik di bagian Masalah cakupan menunjukkan apakah masalah mencegah Macie menganalisis objek dalam bucket S3 individu. Statistik ini tidak secara eksplisit menyertakan data untuk pekerjaan penemuan data sensitif yang telah Anda buat dan jalankan. Namun, memulihkan masalah cakupan yang memengaruhi hasil penemuan data sensitif otomatis Anda kemungkinan juga akan meningkatkan cakupan oleh pekerjaan yang kemudian Anda jalankan.

## Topik

- [Menampilkan dasbor Ringkasan](#)
- [Memahami statistik penemuan data sensitif otomatis di dasbor Ringkasan](#)

## Menampilkan dasbor Ringkasan

Ikuti langkah-langkah ini untuk menampilkan dasbor Ringkasan di konsol Amazon Macie. Jika Anda lebih suka menanyakan statistik secara terprogram, Anda dapat menggunakan [GetBucketStatistics](#) pengoperasian Amazon Macie API.

## Untuk menampilkan dasbor Ringkasan

1. [Buka konsol Amazon Macie di https://console.aws.amazon.com/macie/](https://console.aws.amazon.com/macie/).
2. Di panel navigasi, pilih Ringkasan. Macie menampilkan dasbor Ringkasan.
3. Untuk menelusuri dan meninjau data pendukung untuk item di dasbor, pilih item tersebut.

Jika Anda administrator Macie untuk organisasi, dasbor menampilkan statistik dan data gabungan untuk akun dan akun anggota di organisasi Anda. Untuk mem-filter dasbor dan menampilkan data hanya untuk akun tertentu, masukkan ID akun di kotak Akun di atas dasbor.

## Memahami statistik penemuan data sensitif otomatis di dasbor Ringkasan

Dasbor Ringkasan di konsol Amazon Macie menyertakan statistik agregat yang dapat membantu Anda memantau penemuan data sensitif otomatis untuk data Amazon S3 Anda. Misalnya, Anda dapat menggunakan statistik dasbor untuk menentukan dengan cepat berapa banyak bucket S3 Amazon Macie telah menemukan data sensitif, dan berapa banyak bucket tersebut yang dapat diakses publik. Dasbor menyediakan snapshot status saat ini dan hasil analisis untuk data Amazon S3 Anda saat ini. Wilayah AWS

Anda juga dapat menggunakan statistik dasbor untuk menilai cakupan data Amazon S3 Anda, dan mengidentifikasi masalah yang mencegah Macie menganalisis objek dalam bucket S3 individual. Misalnya, Anda dapat menentukan berapa banyak bucket yang tidak diizinkan untuk diakses Macie untuk akun Anda.

Di dasbor, statistik penemuan data sensitif otomatis diatur terutama ke dalam bagian berikut:

- [Penyimpanan dan penemuan data sensitif](#)
- [Penemuan otomatis](#)
- [Masalah cakupan](#)

Statistik individu di setiap bagian adalah sebagai berikut. Untuk informasi tentang statistik di bagian lain dari dasbor Ringkasan, lihat [Memahami komponen dasbor Ringkasan](#).

### Penyimpanan dan penemuan data sensitif

Di bagian atas bagian Penemuan otomatis, Anda akan menemukan statistik yang menunjukkan berapa banyak data yang Anda simpan di Amazon S3, dan berapa banyak data yang dapat dianalisis Macie untuk mendeteksi data sensitif. Sebagai contoh:

Total accounts	Storage (classifiable/total)	Objects (classifiable/total)
7	307.4 GB / 313.1 GB	514.0 k / 520.7 k

Di bagian ini:

- **Total akun** — Jumlah total bucket Akun AWS yang ada di inventaris bucket S3 Anda. Jika Anda administrator Macie untuk suatu organisasi, ini adalah jumlah total akun Macie yang Anda kelola untuk organisasi Anda. Jika Anda memiliki akun Macie mandiri, nilai ini adalah 1.
- **Penyimpanan**
  - **Dapat Diklasifikasikan** — Ukuran total penyimpanan dari semua objek yang dapat dianalisis oleh Macie di dalam bucket.
  - **Total** — Ukuran total penyimpanan semua objek dalam bucket, termasuk objek yang tidak dapat dianalisis oleh Macie.

Jika salah satu objek adalah file kompresi, nilai-nilai ini tidak mencerminkan ukuran asli dari file-file tersebut setelah mereka diekstrak. Jika versioning diaktifkan untuk salah satu bucket, nilai-nilai ini didasarkan pada ukuran penyimpanan versi terbaru dari setiap objek dalam bucket tersebut.

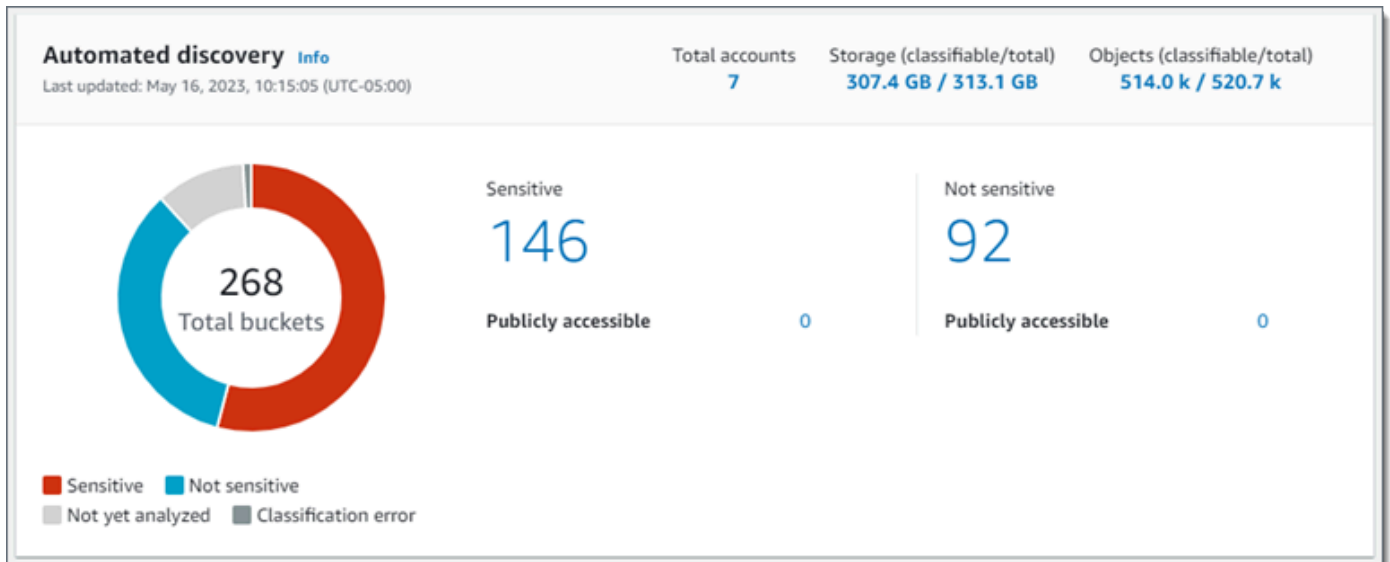
- **Objek**
  - **Dapat Diklasifikasikan** — Jumlah total dari objek yang dapat dianalisis oleh Macie di dalam bucket.
  - **Total** — Jumlah total dari objek di dalam bucket, termasuk objek yang tidak dapat dianalisis oleh Macie.

Dalam statistik sebelumnya, data dan objek dapat diklasifikasikan jika mereka menggunakan kelas penyimpanan Amazon S3 yang didukung dan mereka memiliki ekstensi nama file untuk file atau format penyimpanan yang didukung. Untuk informasi selengkapnya, lihat [Kelas dan format penyimpanan yang didukung](#).

Perhatikan bahwa statistik Penyimpanan dan Objek tidak menyertakan data tentang objek dalam bucket yang tidak diizinkan diakses oleh Macie. Untuk mengidentifikasi bucket di mana hal ini terjadi, pilih Statistik akses ditolak di bagian Masalah cakupan di dasbor.

## Penemuan otomatis

Statistik ini terutama menangkap status dan hasil aktivitas penemuan data sensitif otomatis yang telah dilakukan Macie sejauh ini untuk data Amazon S3 Anda. Sebagai contoh:



Statistik individu di bagian ini adalah sebagai berikut.

Jumlah ember

Bagan donat menunjukkan jumlah total bucket dalam inventaris bucket S3 Anda. Bagan mengelompokkan bucket ke dalam kategori berdasarkan skor sensitivitas masing-masing bucket saat ini:

- Sensitif (merah) — Jumlah total ember yang skor sensitivitasnya berkisar antara 51 hingga 100.
- Tidak sensitif (biru) — Jumlah total ember yang skor sensitivitasnya berkisar antara 1 hingga 49.
- Belum dianalisis (abu-abu muda) — Jumlah total ember yang skor sensitivitasnya 50.
- Kesalahan klasifikasi (abu-abu gelap) — Jumlah total ember yang skor sensitivitasnya -1.

Untuk detail tentang rentang skor sensitivitas dan label yang didefinisikan Macie, lihat.

[Penilaian sensitivitas untuk bucket S3](#)

Untuk meninjau statistik tambahan untuk grup, arahkan kursor ke grup:

- Bucket — Jumlah total ember.
- Dapat diakses publik — Jumlah total ember yang memungkinkan masyarakat umum memiliki akses membaca atau menulis ke ember.
- Byte yang dapat diklasifikasikan — Ukuran penyimpanan total semua objek yang dapat dianalisis Macie dalam ember. Objek ini menggunakan kelas penyimpanan Amazon S3 yang didukung dan mereka memiliki ekstensi nama file untuk format file atau penyimpanan

yang didukung. Untuk informasi selengkapnya, lihat [Kelas dan format penyimpanan yang didukung](#).

- Total byte — Ukuran penyimpanan total semua ember.

Dalam statistik sebelumnya, nilai ukuran penyimpanan didasarkan pada ukuran penyimpanan versi terbaru dari setiap objek dalam ember. Jika salah satu objek adalah file kompresi, nilai-nilai ini tidak mencerminkan ukuran asli dari file-file tersebut setelah mereka diekstrak.

### Sensitif

Area ini menunjukkan jumlah total bucket S3 yang saat ini memiliki skor sensitivitas mulai dari 51 hingga 100. Dalam grup ini, Publicly accessible menunjukkan jumlah total bucket yang juga memungkinkan masyarakat umum untuk memiliki akses membaca atau menulis ke bucket.

### Tidak sensitif

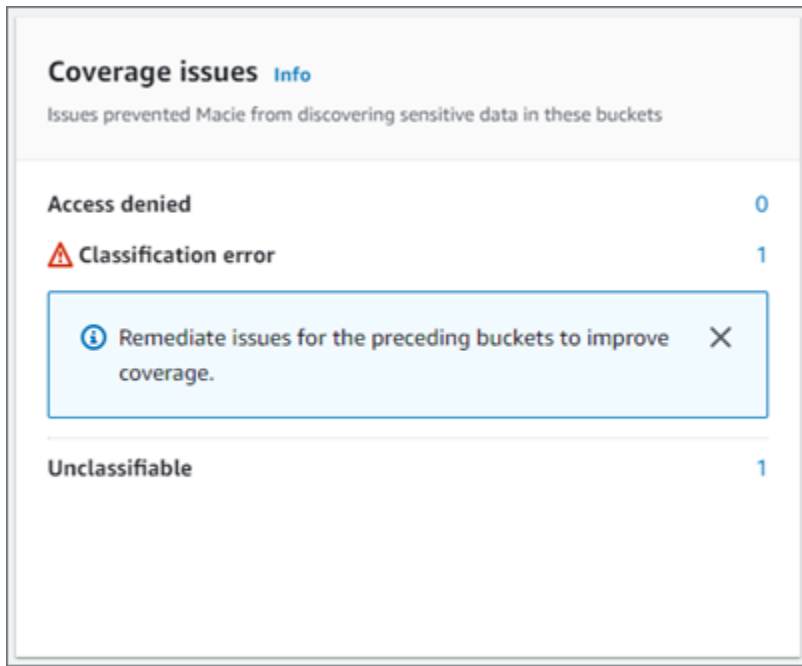
Area ini menunjukkan jumlah total bucket S3 yang saat ini memiliki skor sensitivitas mulai dari 1 hingga 49. Dalam grup ini, Publicly accessible menunjukkan jumlah total bucket yang juga memungkinkan masyarakat umum untuk memiliki akses membaca atau menulis ke bucket.

Untuk menentukan dan menghitung nilai statistik yang dapat diakses publik, Macie menganalisis kombinasi pengaturan tingkat akun dan ember untuk setiap bucket, seperti pengaturan blokir akses publik untuk akun dan bucket, serta kebijakan bucket untuk bucket. Untuk informasi selengkapnya, lihat [Cara Macie memantau keamanan data Amazon S3](#).

Perhatikan bahwa statistik di bagian Penemuan otomatis tidak menyertakan hasil pekerjaan penemuan data sensitif yang telah Anda buat dan jalankan.

### Masalah cakupan

Statistik ini menunjukkan apakah jenis masalah tertentu mencegah Macie menganalisis objek dalam ember S3 individu. Sebagai contoh:



Di bagian ini:

- Akses ditolak — Jumlah total bucket yang tidak diizinkan untuk diakses oleh Macie. Macie tidak bisa menganalisis benda apa pun di ember ini. Pengaturan izin ember mencegah Macie mengakses ember dan objek ember.
- Kesalahan klasifikasi — Jumlah total bucket yang belum dianalisis Macie karena kesalahan klasifikasi tingkat objek. Macie berusaha menganalisis satu atau lebih objek dalam ember ini. Namun, Macie tidak dapat menganalisis objek karena masalah dengan pengaturan izin tingkat objek, konten objek, atau kuota.
- Tidak dapat diklasifikasikan — Jumlah total ember yang tidak menyimpan objek yang dapat diklasifikasikan. Macie tidak bisa menganalisis benda apa pun di ember ini. Semua objek menggunakan kelas penyimpanan Amazon S3 yang tidak didukung Macie, atau mereka memiliki ekstensi nama file untuk format file atau penyimpanan yang tidak didukung Macie.

Pilih nilai statistik untuk menampilkan detail tambahan dan, jika berlaku, panduan remediasi. Jika Anda memperbaiki masalah akses dan kesalahan klasifikasi, Anda dapat meningkatkan cakupan data Amazon S3 Anda selama siklus analisis berikutnya. Untuk informasi selengkapnya, lihat [Menilai cakupan penemuan data sensitif otomatis](#).

Perhatikan bahwa statistik di bagian Masalah cakupan tidak secara eksplisit menyertakan data untuk pekerjaan penemuan data sensitif yang telah Anda buat dan jalankan. Namun, memulihkan masalah cakupan yang memengaruhi hasil penemuan data sensitif otomatis Anda kemungkinan juga akan meningkatkan cakupan oleh pekerjaan yang kemudian Anda jalankan.

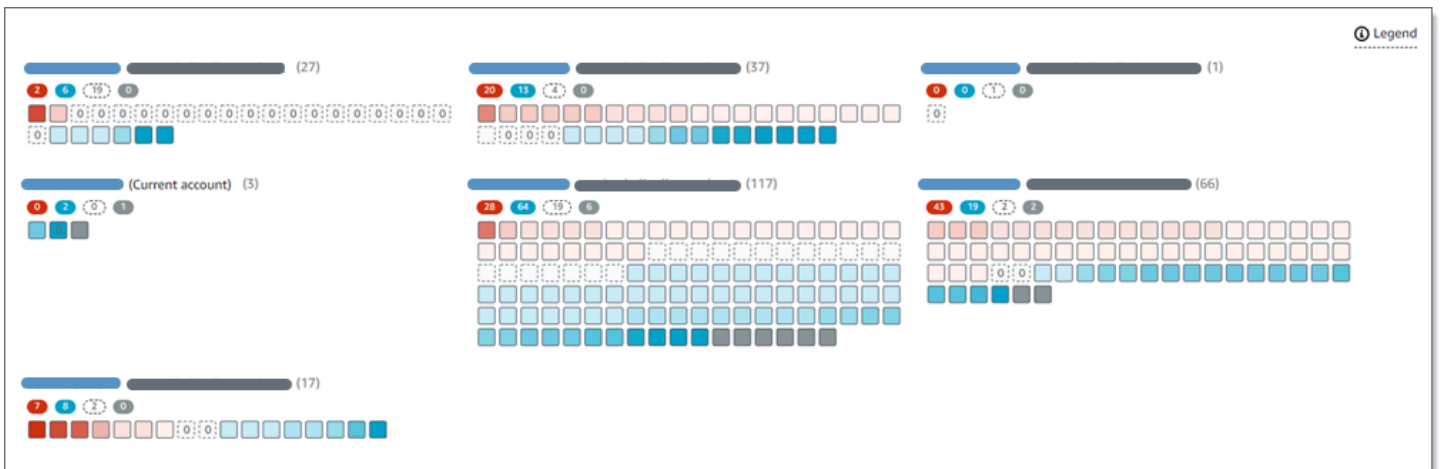


Untuk informasi tentang bagian lain dari dasbor Ringkasan, lihat [Memahami komponen dasbor Ringkasan](#).

## Memvisualisasikan sensitivitas data dengan peta bucket S3

Di konsol Amazon Macie, peta panas bucket S3 menyediakan representasi visual interaktif dari sensitivitas data di seluruh kawasan data Amazon Simple Storage Service (Amazon S3) saat ini. Wilayah AWS Ini menangkap hasil aktivitas penemuan data sensitif otomatis yang telah dilakukan Macie sejauh ini untuk akun Anda.

Jika Anda administrator Macie untuk organisasi, peta akan menyertakan hasil untuk bucket S3 yang dimiliki akun anggota Anda, dikelompokkan berdasarkan Akun AWS dan diurutkan berdasarkan ID akun. Sebagai contoh:



Setiap halaman peta menampilkan data hingga 99 akun atau 1.000 bucket, tergantung pada ukuran organisasi Anda atau data estate Amazon S3.

Untuk menampilkan peta, pilih bucket S3 di panel navigasi di konsol. Kemudian pilih map



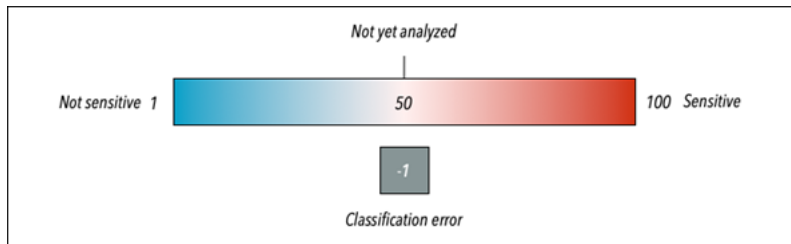
di bagian atas halaman. Peta hanya tersedia jika penemuan data sensitif otomatis saat ini diaktifkan untuk akun Anda. Ini tidak termasuk hasil dari pekerjaan penemuan data sensitif yang telah Anda buat dan jalankan.

### Topik

- [Menafsirkan data di peta bucket S3](#)
- [Berinteraksi dengan peta bucket S3](#)

## Menafsirkan data di peta bucket S3

Di peta bucket S3, setiap kotak mewakili bucket S3 di inventaris bucket Anda. Warna kotak mewakili skor sensitivitas ember saat ini, yang mengukur persimpangan dua dimensi utama: jumlah data sensitif yang ditemukan Macie di ember, dan jumlah data yang telah dianalisis Macie dalam ember. Intensitas rona warna menunjukkan di mana skor bucket berada dalam rentang nilai sensitivitas data, seperti yang ditunjukkan pada gambar berikut.







Secara umum, Anda dapat menafsirkan intensitas warna dan rona sebagai berikut:

- **Biru** — Jika skor sensitivitas bucket saat ini berkisar dari 1 hingga 49, kotak bucket berwarna biru dan label sensitivitas bucket tidak sensitif. Intensitas rona biru mencerminkan jumlah objek unik yang telah dianalisis Macie dalam ember relatif terhadap jumlah total objek unik dalam ember. Rona yang lebih gelap menunjukkan skor sensitivitas yang lebih rendah.
- **Tidak ada warna** — Jika skor sensitivitas bucket saat ini adalah 50, kotak bucket tidak berwarna dan label sensitivitas bucket belum dianalisis. Selain itu, alun-alun memiliki batas putus-putus.
- **Merah** — Jika skor sensitivitas bucket saat ini berkisar antara 51 hingga 100, kotak bucket berwarna merah dan label sensitivitas bucket Sensitif. Intensitas rona merah mencerminkan jumlah data sensitif yang ditemukan Macie di ember. Rona yang lebih gelap menunjukkan skor sensitivitas yang lebih tinggi.
- **Abu-abu** — Jika skor sensitivitas bucket saat ini adalah -1, kotak bucket berwarna abu-abu gelap dan label sensitivitas bucket adalah kesalahan Klasifikasi. Intensitas rona tidak bervariasi.

Untuk detail tentang rentang skor sensitivitas dan label yang didefinisikan Macie, lihat [Penilaian sensitivitas untuk bucket S3](#)

Di peta, kotak untuk ember S3 mungkin juga berisi simbol. Simbol menunjukkan kesalahan, masalah, atau jenis pertimbangan lain yang dapat memengaruhi evaluasi sensitivitas bucket Anda. Simbol juga dapat menunjukkan potensi masalah dengan keamanan ember — misalnya, ember dapat diakses publik. Tabel berikut mencantumkan simbol yang digunakan Macie untuk memberi tahu Anda tentang kasus-kasus ini.

Simbol	Definisi	Deskripsi
	Akses ditolak	<p>Macie tidak diizinkan mengakses bucket atau objek bucket. Akibatnya, Macie tidak dapat menganalisis objek apa pun di ember.</p> <p>Masalah ini biasanya terjadi karena bucket memiliki kebijakan bucket yang membatasi. Untuk informasi tentang cara mengatasi masalah ini, lihat <a href="#">Mengizinkan Macie untuk mengakses bucket S3 dan objek</a>.</p>
	Dapat diakses publik	<p>Masyarakat umum telah membaca atau menulis akses ke ember.</p> <p>Untuk membuat penentuan ini, Macie menganalisis kombinasi pengaturan tingkat akun dan ember untuk setiap bucket, seperti pengaturan blokir akses publik untuk akun dan bucket, dan kebijakan bucket untuk bucket. Untuk informasi selengkapnya, lihat <a href="#">Cara Macie memantau keamanan data Amazon S3</a>.</p>
	Tidak dapat diklasifikasikan	Macie tidak dapat menganalisis objek apa pun di ember. Semua objek bucket menggunakan kelas

Simbol	Definisi	Deskripsi
		<p>penyimpanan Amazon S3 yang tidak didukung Macie, atau mereka memiliki ekstensi nama file untuk format file atau penyimpanan yang tidak didukung Macie.</p> <p>Agar Macie menganalisis objek, objek harus menggunakan kelas penyimpanan yang didukung dan memiliki ekstensi nama file untuk file atau format penyimpanan yang didukung. Untuk informasi selengkapnya, lihat <a href="#">Kelas dan format penyimpanan yang didukung</a>.</p>
	Nol byte	Bucket tidak berisi objek apapun untuk dianalisis Macie. Bucket kosong atau semua objek dalam bucket berisi nol (0) byte data.

## Berinteraksi dengan peta bucket S3

Saat Anda meninjau peta bucket S3, Anda dapat berinteraksi dengannya dengan berbagai cara untuk mengungkapkan dan mengevaluasi data dan detail tambahan untuk masing-masing akun dan bucket. Ikuti langkah-langkah ini untuk menampilkan peta di konsol Amazon Macie dan berinteraksi dengan berbagai fitur yang disediakan peta.

Untuk berinteraksi dengan peta bucket S3

1. [Buka konsol Amazon Macie di https://console.aws.amazon.com/macie/](https://console.aws.amazon.com/macie/).
2. Di panel navigasi, pilih Bucket S3. Halaman bucket S3 menampilkan peta inventaris bucket Anda. Jika halaman menampilkan inventaris Anda dalam format tabel, pilih map



di bagian atas halaman.

3. Di bagian atas halaman, pilih segarkan



secara opsional untuk mengambil metadata bucket terbaru dari Amazon S3.

4. Di peta bucket S3, lakukan salah satu hal berikut:

- Untuk menentukan berapa banyak bucket yang memiliki label sensitivitas tertentu, lihat lencana berwarna tepat di bawah ID Akun AWS . Lencana menampilkan jumlah bucket agregat, dipecah berdasarkan label sensitivitas.

Misalnya, lencana merah melaporkan jumlah total ember yang dimiliki oleh akun dan memiliki label Sensitif. Skor sensitivitas untuk ember ini berkisar antara 51 hingga 100. Lencana biru melaporkan jumlah total ember yang dimiliki oleh akun dan memiliki label Tidak sensitif. Skor sensitivitas untuk ember ini berkisar dari 1 hingga 49.

- Untuk meninjau subset informasi tentang ember, arahkan kursor ke kotak ember. Popover menampilkan nama bucket dan skor sensitivitas saat ini.

Popover juga menampilkan jumlah total objek yang dapat dianalisis Macie dalam ember dan ukuran penyimpanan total dari versi terbaru dari objek tersebut. Objek-objek ini dapat diklasifikasikan. Mereka menggunakan kelas penyimpanan Amazon S3 yang didukung dan mereka memiliki ekstensi nama file untuk format file atau penyimpanan yang didukung. Untuk informasi selengkapnya, lihat [Kelas dan format penyimpanan yang didukung](#).

- Untuk memfilter peta dan hanya menampilkan bucket yang memiliki nilai spesifik untuk bidang, letakkan kursor Anda di kotak filter, lalu tambahkan kondisi filter untuk bidang tersebut. Macie menerapkan kriteria kondisi dan menampilkan kondisi di bawah kotak filter. Untuk lebih menyempurnakan hasilnya, tambahkan syarat filter untuk bidang tambahan. Untuk informasi selengkapnya, lihat [Memfilter inventaris bucket S3 Anda](#).
  - Untuk menelusuri dan menampilkan hanya bucket yang dimiliki oleh akun tertentu, pilih ID akun untuk akun tersebut. Macie membuka tab baru yang memfilter dan menampilkan data hanya untuk akun itu.
5. Untuk meninjau semua statistik penemuan data sensitif dan informasi lain yang disediakan Macie tentang bucket tertentu, pilih kotak bucket, lalu lihat panel detail. Untuk informasi selengkapnya, lihat [Meninjau detail sensitivitas data untuk masing-masing bucket S3](#).

 Tip

Pada tab Bucket details pada panel, Anda dapat memutar dan menelusuri banyak bidang. Untuk menampilkan bucket yang memiliki nilai yang sama untuk bidang, pilih



di bidang tersebut. Untuk menampilkan bucket yang memiliki nilai lain untuk bidang, pilih



di bidang tersebut.

## Menilai sensitivitas data dengan tabel bucket S3

Di konsol Amazon Macie, tabel bucket S3 menampilkan informasi ringkasan tentang masing-masing bucket Amazon Simple Storage Service (Amazon S3) Anda saat ini. Wilayah AWS Jika Anda administrator Macie untuk suatu organisasi, ini mencakup informasi tentang bucket S3 yang dimiliki akun anggota Anda. Jika Anda lebih suka mengakses data secara terprogram, Anda dapat menggunakan [DescribeBuckets](#) pengoperasian Amazon Macie API.

Di konsol, Anda dapat mengurutkan dan memfilter tabel untuk menyesuaikan tampilan Anda. Anda juga dapat mengeksport data dari tabel ke file nilai yang dipisahkan koma (CSV). Jika Anda memilih bucket S3 di tabel, panel detail menampilkan informasi tambahan tentang bucket. Ini termasuk detail dan statistik yang menangkap hasil aktivitas penemuan data sensitif otomatis yang telah dilakukan Macie untuk bucket sejauh ini. Ini juga mencakup data untuk pengaturan dan metrik yang memberikan wawasan tentang keamanan dan privasi data bucket. Selain meninjau detail bucket, Anda dapat menggunakan panel detail untuk menyesuaikan pengaturan penemuan data sensitif otomatis untuk bucket. Untuk mempelajari caranya, lihat [Mengelola penemuan data sensitif otomatis untuk bucket S3 individual](#).

Untuk menilai sensitivitas data dengan menggunakan tabel bucket S3

1. [Buka konsol Amazon Macie di https://console.aws.amazon.com/macie/](https://console.aws.amazon.com/macie/).
2. Di panel navigasi, pilih Bucket S3.
3. Pada halaman bucket S3, pilih table



di bagian atas halaman. Macie menampilkan jumlah ember dalam inventaris Anda dan tabel ember.

4. Di bagian atas halaman, pilih segarkan



secara opsional untuk mengambil metadata bucket terbaru dari Amazon S3.

Jika ikon informasi



muncul di samping nama bucket, kami merekomendasikan Anda untuk melakukan hal ini. Ikon informasi menunjukkan bahwa bucket dibuat selama 24 jam terakhir, mungkin setelah Macie terakhir mengambil bucket dan metadata objek dari Amazon S3 sebagai bagian dari [siklus penyegaran harian](#).

5. Di tabel bucket S3, tinjau informasi ringkasan tentang setiap bucket di inventaris Anda:

- Sensitivitas — Skor sensitivitas bucket saat ini. Untuk informasi tentang kisaran skor sensitivitas yang didefinisikan Macie, lihat. [Penilaian sensitivitas untuk bucket S3](#)
- Bucket – Nama bucket.
- Akun — ID akun untuk pemilik bucket. Akun AWS
- Objek yang dapat diklasifikasikan – Jumlah total objek yang dapat dianalisis Macie untuk mendeteksi data sensitif dalam bucket.
- Ukuran yang dapat diklasifikasikan – Ukuran penyimpanan total semua objek yang dapat dianalisis Macie untuk mendeteksi data sensitif dalam bucket.

Nilai ini tidak mencerminkan ukuran sebenarnya dari objek terkompresi setelah didekompresi. Selain itu, jika versioning diaktifkan untuk bucket, nilai ini didasarkan pada ukuran penyimpanan versi terbaru dari setiap objek dalam bucket.

- Dipantau berdasarkan pekerjaan - Menentukan apakah ada pekerjaan penemuan data sensitif yang dikonfigurasi untuk menganalisis objek secara berkala dalam ember setiap hari, mingguan, atau bulanan.

Jika nilai untuk bidang ini Ya, bucket secara eksplisit disertakan dalam tugas berkala atau bucket yang sesuai dengan kriteria untuk tugas berkala dalam 24 jam terakhir. Selain itu, status dari setidaknya salah satu tugas tersebut tidak Dibatalkan. Macie memperbarui data ini setiap hari.

- Pekerjaan terbaru — Jika ada pekerjaan penemuan data sensitif satu kali atau berkala yang dikonfigurasi untuk menganalisis objek dalam bucket, nilai untuk bidang ini menunjukkan tanggal dan waktu terbaru ketika salah satu pekerjaan tersebut mulai berjalan. Jika tidak, bidang ini akan kosong.

Dalam data sebelumnya, objek dapat diklasifikasikan jika mereka menggunakan kelas penyimpanan Amazon S3 yang didukung dan mereka memiliki ekstensi nama file untuk file atau format penyimpanan yang didukung. Anda dapat mendeteksi data sensitif dalam objek dengan menggunakan Macie. Untuk informasi selengkapnya, lihat [Kelas dan format penyimpanan yang didukung](#).

6. Untuk menganalisis inventaris Anda dengan menggunakan tabel, lakukan salah satu hal berikut ini:
  - Untuk mengurutkan tabel dengan bidang tertentu, klik judul kolom untuk bidang. Untuk mengubah urutan pengurutan, klik judul kolom lagi.
  - Untuk memfilter tabel dan hanya menampilkan bucket yang memiliki nilai spesifik untuk bidang, letakkan kursor Anda di kotak filter, lalu tambahkan kondisi filter untuk bidang tersebut. Macie menerapkan kriteria kondisi dan menampilkan kondisi di bawah kotak filter. Untuk lebih menyempurnakan hasilnya, tambahkan syarat filter untuk bidang tambahan. Untuk informasi selengkapnya, lihat [Memfilter inventaris bucket S3 Anda](#).
  - Untuk meninjau detail dan statistik untuk bucket tertentu, pilih nama bucket dalam tabel, lalu merujuk ke panel detail. Untuk informasi selengkapnya, lihat [Meninjau detail bucket S3](#).

 Tip

Pada tab Bucket details pada panel, Anda dapat memutar dan menelusuri banyak bidang. Untuk menampilkan bucket yang memiliki nilai yang sama untuk bidang, pilih



di bidang tersebut. Untuk menampilkan bucket yang memiliki nilai lain untuk bidang, pilih



di bidang tersebut.

7. Untuk mengekspor data dari tabel ke file CSV, pilih kotak centang untuk setiap baris yang ingin Anda ekspor, atau pilih kotak centang di judul kolom pilihan untuk memilih semua baris. Kemudian pilih Ekspor ke CSV di bagian atas halaman. Anda dapat mengekspor hingga 50.000 baris dari tabel.
8. Untuk melakukan analisis objek yang lebih dalam dan lebih cepat dalam satu ember atau beberapa, pilih kotak centang untuk setiap bucket, lalu pilih Buat pekerjaan. Untuk informasi selengkapnya, lihat [Membuat tugas penemuan data sensitif](#).



## Meninjau detail sensitivitas data untuk masing-masing bucket S3

Di konsol Amazon Macie, Anda dapat menggunakan panel detail di halaman bucket S3 untuk meninjau statistik dan informasi lainnya tentang bucket Amazon Simple Storage Service (Amazon S3) individual yang dipantau dan dianalisis Macie untuk akun Anda. Jika Anda administrator Macie untuk suatu organisasi, ini termasuk bucket S3 yang dimiliki akun anggota Anda.

Statistik dan informasi mencakup detail yang memberikan wawasan tentang keamanan dan privasi data bucket S3. Jika penemuan data sensitif otomatis diaktifkan untuk akun Anda, mereka juga menangkap hasil aktivitas penemuan data sensitif otomatis yang telah dilakukan Macie sejauh ini untuk sebuah bucket. Misalnya, Anda dapat menemukan daftar objek yang telah dianalisis Macie dalam ember, dan rincian jenis dan jumlah kemunculan data sensitif yang ditemukan Macie dalam ember. Perhatikan bahwa data tidak menyertakan hasil pekerjaan penemuan data sensitif yang telah Anda buat dan jalankan.


Macie secara otomatis menghitung ulang dan memperbarui statistik dan detail ini saat melakukan penemuan data sensitif otomatis untuk akun Anda. Sebagai contoh:

- Jika Macie tidak menemukan data sensitif dalam objek S3, Macie mengurangi skor sensitivitas bucket dan memperbarui label sensitivitas bucket seperlunya. Macie juga menambahkan objek ke daftar objek yang dianalisis dalam ember.
- Jika Macie menemukan data sensitif dalam objek S3, Macie menambahkan kejadian tersebut ke rincian tipe data sensitif yang ditemukan Macie di bucket. Macie juga meningkatkan skor sensitivitas bucket dan memperbarui label sensitivitas bucket seperlunya. Selain itu, Macie menambahkan objek ke daftar objek yang dianalisis dalam ember. Tugas-tugas ini selain membuat temuan data sensitif untuk objek.
- Jika Macie menemukan data sensitif dalam objek S3 yang kemudian diubah atau dihapus, Macie menghapus kejadian data sensitif untuk objek tersebut dari rincian bucket tipe data sensitif. Macie juga mengurangi skor sensitivitas bucket dan memperbarui label sensitivitas bucket seperlunya. Selain itu, Macie menghapus objek dari daftar objek yang dianalisis dalam ember.
- Jika Macie mencoba menganalisis objek S3 tetapi masalah atau kesalahan mencegah Macie melakukannya, Macie menambahkan objek ke daftar objek yang dianalisis dalam ember, dan menunjukkan bahwa ia tidak dapat menganalisis objek tersebut.

Selain meninjau statistik dan detail, Anda dapat menggunakan panel untuk menyesuaikan pengaturan penemuan data sensitif otomatis untuk bucket S3. Misalnya, Anda dapat menyertakan

atau mengecualikan jenis data sensitif tertentu dari skor bucket. Untuk informasi selengkapnya, lihat [Mengelola penemuan otomatis untuk bucket S3 individual](#).

Untuk meninjau detail sensitivitas data untuk bucket S3

1. [Buka konsol Amazon Macie di https://console.aws.amazon.com/macie/](https://console.aws.amazon.com/macie/).
2. Di panel navigasi, pilih Bucket S3. Halaman bucket S3 menampilkan peta interaktif inventaris bucket Anda. Secara opsional pilih table  di bagian atas halaman untuk menampilkan inventaris Anda dalam format tabel sebagai gantinya.
3. Di peta atau tabel bucket S3, pilih nama bucket S3 yang detailnya ingin Anda tinjau. Panel detail menampilkan statistik dan informasi lainnya tentang bucket.

Bagian atas panel menunjukkan informasi umum tentang bucket: nama bucket, dan ID akun untuk Akun AWS yang memiliki bucket. Ini juga menyediakan opsi untuk [mengubah pengaturan penemuan data sensitif otomatis tertentu](#) untuk bucket. Pengaturan dan informasi tambahan tentang bucket diatur ke dalam tab berikut:

- [Sensitivitas](#)
- [Detail ember](#)
- [Sampel objek](#)
- [Penemuan data sensitif](#)

Pengaturan dan informasi individual pada setiap tab adalah sebagai berikut.

### Sensitivitas

Tab ini menunjukkan skor sensitivitas bucket saat ini, mulai dari -1 hingga 100. Untuk informasi tentang kisaran skor sensitivitas yang didefinisikan Macie, lihat [Penilaian sensitivitas untuk bucket S3](#)

Tab ini juga menyediakan rincian jenis data sensitif yang ditemukan Macie di objek bucket, dan jumlah kemunculan setiap jenis:

- Tipe data sensitif — Pengenal unik (ID) untuk pengenal data terkelola yang mendeteksi data, atau nama pengidentifikasi data kustom yang mendeteksi data.

ID pengidentifikasi data terkelola menjelaskan jenis data sensitif yang dirancang untuk dideteksi oleh pengenalan—misalnya, USA\_PASSPORT\_NUMBER untuk nomor paspor AS. Untuk detail tentang setiap pengenalan data terkelola, lihat [Menggunakan pengidentifikasi data terkelola](#).

- Hitungan — Jumlah total kemunculan data yang terdeteksi oleh pengidentifikasi data terkelola atau kustom.
- Status penilaian — Menentukan apakah kemunculan data disertakan atau dikecualikan dari skor sensitivitas bucket.

Jika Anda mengonfigurasi Macie untuk menghitung skor bucket secara otomatis, Anda dapat menyesuaikan perhitungan dengan menyertakan atau mengecualikan jenis data sensitif tertentu dari skor bucket: pilih kotak centang untuk pengenalan data yang ingin Anda sertakan atau keculikan, lalu pilih opsi yang Anda inginkan di menu Tindakan. Untuk informasi selengkapnya, lihat [Mengelola penemuan otomatis untuk bucket S3 individual](#).

Jika Macie belum menemukan data sensitif dalam objek yang saat ini disimpan bucket, bagian ini menampilkan pesan Tidak ditemukan deteksi.

Perhatikan bahwa tab Sensitivitas tidak menyertakan data untuk objek yang dianalisis Macie dan kemudian diubah atau dihapus. Jika objek diubah atau dihapus dari ember setelah Macie menganalisisnya, Macie secara otomatis menghitung ulang dan memperbarui statistik dan data yang sesuai untuk mengecualikan objek.

## Detail ember

Tab ini memberikan detail tentang pengaturan bucket, termasuk pengaturan keamanan data dan privasi. Misalnya, Anda dapat meninjau rincian setelah akses publik bucket, dan menentukan apakah bucket mereplikasi objek atau dibagikan dengan yang lain. Akun AWS

Sebagai catatan khusus, bidang Terakhir diperbarui menunjukkan kapan Macie baru-baru ini mengambil metadata dari Amazon S3 untuk bucket atau objek bucket. Bidang run penemuan otomatis terbaru menunjukkan kapan Macie baru-baru ini menganalisis objek dalam ember saat melakukan penemuan otomatis.

Tab ini juga menyediakan statistik tingkat objek yang dapat membantu Anda menilai berapa banyak data yang dapat dianalisis Macie dalam bucket. Ini juga menunjukkan apakah ada pekerjaan penemuan data sensitif yang dikonfigurasi untuk menganalisis objek dalam ember. Jika ada, Anda dapat mengakses detail tentang pekerjaan yang berjalan paling baru dan kemudian secara opsional menampilkan temuan apa pun yang dihasilkan oleh pekerjaan tersebut.

Untuk detail tambahan tentang informasi di tab ini, lihat [Meninjau detail ember S3](#).

## Sampel objek

Tab ini mencantumkan objek yang telah dianalisis Macie di bucket saat melakukan penemuan data sensitif otomatis. Secara opsional pilih nama objek untuk membuka konsol Amazon S3 dan menampilkan properti objek.

Daftar ini mencakup data hingga 100 objek. Daftar diisi berdasarkan nilai untuk bidang sensitivitas Objek: Sensitif, diikuti oleh Tidak Sensitif, diikuti oleh objek yang tidak dapat dianalisis Macie.

Dalam daftar, bidang Sensitivitas objek menunjukkan apakah Macie menemukan data sensitif dalam suatu objek:

- Sensitif — Macie menemukan setidaknya satu kejadian data sensitif dalam objek.
- Tidak sensitif - Macie tidak menemukan data sensitif di objek.
- — (dash) — Macie tidak dapat menyelesaikan analisisnya terhadap objek karena masalah atau kesalahan.

Bidang hasil Klasifikasi menunjukkan apakah Macie mampu menganalisis suatu objek:

- Lengkap — Macie menyelesaikan analisisnya terhadap objek.
- Partial — Macie menganalisis hanya sebagian data dalam objek karena masalah atau kesalahan. Misalnya, objek adalah file arsip yang berisi file dalam format yang tidak didukung.
- Dilewati — Macie tidak dapat menganalisis data apa pun di objek karena masalah atau kesalahan. Misalnya, objek dienkripsi dengan kunci yang Macie tidak diizinkan untuk digunakan.

Perhatikan bahwa daftar tidak menyertakan objek yang diubah atau dihapus setelah Macie menganalisis atau mencoba menganalisisnya. Macie secara otomatis menghapus objek dari daftar jika objek tersebut kemudian diubah atau dihapus.

## Penemuan data sensitif

Tab ini menyediakan statistik penemuan data sensitif teragregat otomatis untuk bucket:

- Byte yang dianalisis — Jumlah total data, dalam byte, yang telah dianalisis Macie dalam ember.
- Byte yang dapat diklasifikasikan — Ukuran penyimpanan total, dalam byte, dari semua objek yang dapat dianalisis Macie dalam ember. Objek ini menggunakan kelas penyimpanan Amazon S3 yang didukung dan mereka memiliki ekstensi nama file untuk format file atau penyimpanan

yang didukung. Untuk informasi selengkapnya, lihat [Kelas dan format penyimpanan yang didukung](#).

- Deteksi total — Jumlah total kejadian data sensitif yang ditemukan Macie di ember. Ini termasuk kejadian yang saat ini ditekan oleh pengaturan penilaian sensitivitas untuk bucket.

Bagan yang dianalisis Objek menunjukkan jumlah total objek yang telah dianalisis Macie dalam ember. Ini juga memberikan representasi visual dari jumlah objek yang Macie lakukan atau tidak menemukan data sensitif. Legenda di bawah grafik menunjukkan rincian hasil ini:

- Objek sensitif (merah) — Jumlah total objek yang ditemukan Macie setidaknya satu kejadian data sensitif.
- Bukan objek sensitif (biru) — Jumlah total objek yang tidak ditemukan Macie data sensitif.
- Objek dilewati (abu-abu gelap) — Jumlah total objek yang tidak dapat dianalisis Macie karena masalah atau kesalahan.

Area di bawah legenda bagan memberikan rincian kasus di mana Macie tidak dapat menganalisis objek karena jenis masalah izin tertentu atau kesalahan kriptografi terjadi:

- Dilewati: Enkripsi tidak valid — Jumlah total objek yang dienkripsi dengan kunci yang disediakan pelanggan. Macie tidak dapat mengakses kunci ini.
- Lewati: KMS tidak valid — Jumlah total objek yang dienkripsi dengan AWS Key Management Service (AWS KMS) kunci yang tidak lagi tersedia. Objek ini dienkripsi dengan AWS KMS keys yang dinonaktifkan, dijadwalkan untuk dihapus, atau dihapus. Macie tidak bisa menggunakan kunci ini.
- Dilewati: Izin ditolak — Jumlah total objek yang Macie tidak diizinkan untuk mengakses karena pengaturan izin untuk objek, atau pengaturan izin untuk kunci yang digunakan untuk mengenkripsi objek.

Untuk detail tentang ini dan jenis masalah dan kesalahan lainnya yang dapat terjadi, lihat [Memperbaiki masalah cakupan untuk penemuan data sensitif otomatis](#). Jika Anda memperbaiki masalah dan kesalahan, Anda dapat meningkatkan cakupan data bucket selama siklus analisis berikutnya.

Statistik pada tab Penemuan Data Sensitif tidak menyertakan data untuk objek yang diubah atau dihapus setelah Macie menganalisis atau mencoba menganalisisnya. Jika objek diubah atau dihapus dari ember setelah Macie menganalisis atau mencoba menganalisisnya, Macie secara otomatis menghitung ulang statistik ini untuk mengecualikan objek.

## Menganalisis temuan data sensitif yang dihasilkan oleh penemuan otomatis

Saat melakukan penemuan data sensitif otomatis, Amazon Macie membuat temuan data sensitif untuk setiap objek Amazon Simple Storage Service (Amazon S3) Simple Storage Service (Amazon S3) tempat ia menemukan data sensitif. Temuan data sensitif adalah laporan rinci dari data sensitif yang ditemukan Macie di objek S3. Setiap temuan data sensitif memberikan peringkat keparahan dan detail seperti:

- Tanggal dan waktu ketika Macie menemukan data sensitif.
- Kategori dan tipe data sensitif yang ditemukan Macie.
- Jumlah kejadian dari setiap tipe data sensitif yang Macie temukan.
- Bagaimana Macie menemukan data sensitif, penemuan data sensitif otomatis, atau pekerjaan penemuan data sensitif.
- Nama, pengaturan akses publik, tipe enkripsi, dan informasi lainnya tentang bucket S3 yang terpengaruh dan objek.

Bergantung pada jenis file atau format penyimpanan objek S3 yang terpengaruh, detailnya juga dapat mencakup lokasi sebanyak 15 kemunculan data sensitif yang ditemukan Macie. Temuan data sensitif tidak termasuk data sensitif yang ditemukan Macie. Sebaliknya, temuan ini menyediakan informasi yang dapat Anda gunakan untuk penyelidikan lebih lanjut dan remediasi sebagaimana diperlukan.

Macie menyimpan temuan data sensitif Anda selama 90 hari. Anda dapat mengaksesnya dengan menggunakan konsol Amazon Macie atau Amazon Macie API. Anda juga dapat memantau dan memproses temuan dengan menggunakan aplikasi, layanan, dan sistem lain. Untuk informasi selengkapnya, lihat [Menganalisis temuan](#).

Untuk menganalisis temuan yang dihasilkan oleh penemuan data sensitif otomatis

Untuk mengidentifikasi dan menganalisis temuan data sensitif yang dibuat Macie saat melakukan penemuan data sensitif otomatis untuk akun Anda, Anda dapat memfilter temuan Anda. Dengan filter, Anda menggunakan atribut temuan tertentu untuk membangun tampilan dan kueri khusus untuk temuan. Anda dapat menggunakan konsol Amazon Macie untuk memfilter temuan, atau mengirimkan kueri secara terprogram menggunakan Amazon Macie API.

### Console

Ikuti langkah-langkah ini untuk mengidentifikasi dan menganalisis temuan dengan menggunakan konsol Amazon Macie.

Untuk menganalisis temuan yang dihasilkan oleh penemuan otomatis

1. [Buka konsol Amazon Macie di https://console.aws.amazon.com/macie/](https://console.aws.amazon.com/macie/).
2. Di panel navigasi, pilih Temuan.
3. (Opsional) Untuk menampilkan temuan yang ditekan oleh [aturan penekanan](#), ubah pengaturan Status Finding. Pilih Semua untuk menampilkan temuan yang ditekan dan tidak ditekan, atau pilih Diarsipkan untuk menampilkan hanya temuan yang ditekan. Untuk kemudian menyembunyikan temuan yang ditekan lagi, pilih Current.
4. Tempatkan kursor Anda di kotak kriteria Filter. Dalam daftar bidang yang muncul, pilih Jenis asal.

Bidang ini menentukan bagaimana Macie menemukan data sensitif yang menghasilkan temuan, penemuan data sensitif otomatis, atau pekerjaan penemuan data sensitif. Untuk menemukan bidang ini dalam daftar bidang filter, Anda dapat menelusuri daftar lengkap, atau memasukkan bagian dari nama bidang untuk mempersempit daftar bidang.

5. Pilih AUTOMATED\_SENSITIVE\_DATA\_DISCOVERY sebagai nilai untuk bidang, lalu pilih Terapkan. Macie menerapkan kriteria filter dan menambahkan kondisi ke token filter di kotak kriteria Filter.
6. (Opsional) Untuk menyempurnakan hasil, tambahkan kondisi filter untuk bidang tambahan —misalnya, Dibuat pada rentang waktu saat temuan dibuat, nama bucket S3 untuk nama bucket yang terpengaruh, atau Jenis deteksi data sensitif untuk tipe sensitif yang terdeteksi dan menghasilkan temuan. Untuk informasi selengkapnya, lihat [Memfilter temuan](#).

Jika Anda ingin menggunakan rangkaian kondisi ini lagi, Anda dapat menyimpannya sebagai aturan filter. Untuk melakukan ini, pilih Simpan aturan di kotak Kriteria filter. Masukkan nama, dan deskripsi secara opsional untuk aturan. Setelah selesai, pilih Simpan.

## API

Untuk mengidentifikasi dan menganalisis temuan secara terprogram, tentukan kriteria filter dalam kueri yang Anda kirimkan menggunakan [ListFindings](#) atau [GetFindingStatistics](#) pengoperasian Amazon Macie API. ListFindingsOperasi mengembalikan array ID pencarian, satu ID untuk setiap temuan yang cocok dengan kriteria filter. Anda kemudian dapat menggunakan ID tersebut untuk mengambil detail dari setiap temuan. GetFindingStatisticsOperasi mengembalikan data statistik agregat tentang semua temuan yang cocok dengan kriteria filter, dikelompokkan berdasarkan bidang yang Anda tentukan dalam permintaan Anda. Untuk informasi lebih lanjut tentang memfilter temuan secara terprogram, lihat [Memfilter temuan](#)

Dalam kriteria filter, sertakan kondisi untuk `originType` bidang tersebut. Bidang ini menentukan bagaimana Macie menemukan data sensitif yang menghasilkan temuan, penemuan data sensitif otomatis, atau pekerjaan penemuan data sensitif. Nilai untuk bidang ini adalah `AUTOMATED_SENSITIVE_DATA_DISCOVERY` jika temuan dihasilkan saat melakukan penemuan otomatis.

Untuk mengidentifikasi dan menganalisis temuan dengan menggunakan [AWS Command Line Interface \(AWS CLI\)](#), jalankan [daftar-temuan atau get-finding-statistics](#) perintah. Contoh berikut menggunakan `list-findings` perintah untuk mengambil ID temuan untuk semua temuan tingkat keparahan tinggi yang dihasilkan oleh penemuan data sensitif otomatis saat ini. Wilayah AWS

Untuk Linux, macOS, atau Unix, menggunakan karakter garis miring terbalik (`\`) untuk meningkatkan keterbacaan:

```
$ aws macie2 list-findings \
--finding-criteria '{"criterion":{"classificationDetails.originType":{"eq":
["AUTOMATED_SENSITIVE_DATA_DISCOVERY"]},"severity.description":{"eq":["High"]}}}'
```

Untuk Microsoft Windows, menggunakan karakter kelanjutan baris tanda sisipan (`^`) untuk meningkatkan keterbacaan:

```
C:\> aws macie2 list-findings ^
--finding-criteria={"criterion\":{"classificationDetails.originType\":{"eq
\":["AUTOMATED_SENSITIVE_DATA_DISCOVERY\"]},"severity.description\":{"eq\":
["High\"]}}}
```

Di mana:

- `classificationDetails.originType` menentukan nama JSON dari bidang tipe Origin, dan:
  - `eq` menentukan operator yang sama.
  - `AUTOMATED_SENSITIVE_DATA_DISCOVERY` adalah nilai yang disebutkan untuk bidang tersebut.
- `severity.description` menentukan nama JSON dari bidang Keparahan, dan:
  - `eq` menentukan operator yang sama.
  - `High` adalah nilai yang disebutkan untuk bidang tersebut.



Jika perintah berhasil berjalan, Macie mengembalikan array `findingIds`. Array mencantumkan pengenal unik untuk setiap temuan yang cocok dengan kriteria filter, seperti yang ditunjukkan pada contoh berikut.

```
{
  "findingIds": [
    "1f1c2d74db5d8caa76859ec52example",
    "6cfa9ac820dd6d55cad30d851example",
    "702a6fd8750e567d1a3a63138example",
    "826e94e2a820312f9f964cf60example",
    "274511c3fdcd87010a19a3a42example"
  ]
}
```

Jika tidak ada temuan yang cocok dengan kriteria filter, Macie mengembalikan `findingIds` array kosong.

```
{
  "findingIds": []
}
```

## Mengakses hasil penemuan data sensitif yang dihasilkan oleh penemuan otomatis

Amazon Macie membuat catatan analisis untuk setiap objek Amazon Simple Storage Service (Amazon S3) yang dipilihnya untuk dianalisis saat melakukan penemuan data sensitif otomatis untuk akun atau organisasi Anda. Catatan ini, disebut sebagai hasil penemuan data sensitif, mencatat detail tentang analisis yang dilakukan Macie pada objek S3 individu. Ini termasuk objek yang Macie tidak mendeteksi data sensitif, dan karenanya tidak menghasilkan temuan, dan objek yang tidak dapat dianalisis Macie karena kesalahan atau masalah seperti pengaturan izin atau penggunaan file atau format penyimpanan yang tidak didukung.

Jika Macie mendeteksi data sensitif dalam objek S3, hasil penemuan data sensitif mencakup data dari temuan yang sesuai. Ini memberikan informasi tambahan juga, seperti lokasi tempat terjadinya 1.000 kejadian dari setiap tipe data sensitif yang Macie temukan dalam objek. Sebagai contoh:

- Nomor kolom dan baris untuk sel atau bidang di buku kerja Microsoft Excel, file CSV, atau file TSV
- Jalur ke bidang atau array dalam file JSON atau JSON Lines
- Nomor baris untuk baris dalam file teks non-biner selain file CSV, JSON, JSON Lines, atau TSV, misalnya, file HTML, TXT, atau XML

- Nomor halaman untuk halaman dalam file Format Dokumen Portabel Adobe (PDF)
- Indeks catatan dan jalur ke bidang dalam catatan di kontainer objek Apache Avro atau file Apache Parquet

Jika objek S3 yang terpengaruh adalah file arsip, seperti file.tar atau .zip, hasil penemuan data sensitif juga menyediakan data lokasi terperinci untuk kemunculan data sensitif dalam file individual yang diekstrak Macie dari arsip. Macie tidak menyertakan informasi ini dalam temuan data sensitif untuk file arsip. Untuk melaporkan data lokasi, hasil penemuan data sensitif menggunakan skema [JSON standar](#).

Hasil penemuan data sensitif tidak termasuk data sensitif yang ditemukan Macie. Sebagai gantinya, dokumen ini memberi Anda catatan analisis yang dapat membantu untuk audit privasi dan perlindungan data atau investigasi.

Macie menyimpan hasil penemuan data sensitif Anda selama 90 hari. Anda tidak dapat mengaksesnya langsung di konsol Amazon Macie atau dengan Amazon Macie API. Sebagai gantinya, Anda mengonfigurasi Macie untuk mengenkripsi dan menyimpannya dalam ember S3. Bucket dapat berfungsi sebagai repositori jangka panjang definitif untuk semua hasil penemuan data sensitif Anda. Anda kemudian dapat secara opsional mengakses dan menanyakan hasil di repositori itu.

Untuk menentukan lokasi repositori ini untuk akun Anda, pilih Hasil Discovery di panel navigasi di konsol Amazon Macie. Untuk melakukan ini secara terprogram, gunakan [GetClassificationExportConfiguration](#) pengoperasian Amazon Macie API. Jika Anda belum mengonfigurasi repositori ini untuk akun Anda, lihat [Menyimpan dan mempertahankan hasil penemuan data sensitif](#) untuk mempelajari caranya.

Setelah Anda mengonfigurasi Macie untuk menyimpan hasil penemuan data sensitif Anda dalam bucket S3, Macie menulis hasilnya ke file JSON Lines (.jsonl), dan mengenkripsi dan menambahkan file tersebut ke bucket sebagai file GNU Zip (.gz). Untuk penemuan data sensitif otomatis, Macie menambahkan file ke folder bernama automated-sensitive-data-discovery dalam bucket.

Seperti halnya temuan data sensitif, hasil penemuan data sensitif mematuhi skema standar. Anda juga dapat secara opsional melakukan kueri, memantau dan memprosesnya menggunakan aplikasi, layanan, dan sistem lainnya.

**i** Tip

Untuk contoh terperinci dan instruksional tentang bagaimana Anda dapat menanyakan dan menggunakan hasil penemuan data sensitif untuk menganalisis dan melaporkan potensi risiko keamanan data, lihat [Cara menanyakan dan memvisualisasikan hasil penemuan data sensitif Macie dengan posting QuickSight blog Amazon Athena dan Amazon](#) di Blog Keamanan.AWS

Untuk contoh kueri Athena yang dapat Anda gunakan untuk menganalisis hasil penemuan data sensitif, kunjungi repositori [Amazon Macie Results Analytics](#). GitHub Repositori ini juga menyediakan instruksi untuk mengkonfigurasi Athena untuk mengambil dan mendekripsi hasil Anda, dan skrip untuk membuat tabel untuk hasil.

## Penilaian sensitivitas untuk bucket S3

Jika penemuan data sensitif otomatis diaktifkan untuk akun Anda, Amazon Macie secara otomatis menghitung dan menetapkan skor sensitivitas ke setiap bucket Amazon Simple Storage Service (Amazon S3) yang dipantau dan dianalisis untuk akun Anda. Skor sensitivitas adalah representasi kuantitatif dari jumlah data sensitif yang mungkin berisi bucket S3. Berdasarkan skor itu, Macie juga memberikan label sensitivitas untuk setiap bucket. Label sensitivitas adalah representasi kualitatif dari skor sensitivitas bucket. Nilai-nilai ini dapat berfungsi sebagai titik referensi untuk menentukan di mana data sensitif mungkin berada di kawasan data Amazon S3 Anda, serta mengidentifikasi serta memantau potensi risiko keamanan untuk data tersebut.

Secara default, skor dan label sensitivitas bucket S3 mencerminkan hasil aktivitas penemuan data sensitif otomatis yang telah dilakukan Macie sejauh ini untuk bucket. Mereka tidak mencerminkan hasil pekerjaan penemuan data sensitif yang telah Anda buat dan jalankan. Selain itu, baik skor maupun label tidak menyiratkan atau menunjukkan kekritisian atau pentingnya objek bucket atau bucket untuk organisasi Anda. Namun, Anda dapat mengganti skor terhitung bucket dengan menetapkan skor maksimum (100) secara manual ke bucket, yang juga menetapkan label Sensitif ke bucket.

### Topik

- [Sensitivitas mencetak dimensi dan rentang](#)
- [Memantau skor sensitivitas](#)

## Sensitivitas mencetak dimensi dan rentang

Jika dihitung oleh Amazon Macie, skor sensitivitas bucket S3 adalah ukuran kuantitatif dari persimpangan dua dimensi utama:

- Jumlah data sensitif yang ditemukan Macie di bucket. Ini terutama berasal dari sifat dan jumlah tipe data sensitif yang Macie telah ditemukan di bucket dan jumlah kejadian dari setiap jenis.
- Jumlah data yang Macie telah dianalisis dalam ember. Ini terutama berasal dari jumlah objek unik yang Macie telah dianalisis dalam bucket relatif terhadap jumlah total objek unik dalam bucket.

Skor sensitivitas bucket S3 juga menentukan label sensitivitas yang ditugaskan Macie ke bucket. Label sensitivitas adalah representasi kualitatif dari skor — misalnya, Sensitif atau Tidak sensitif. Pada konsol Amazon Macie, skor sensitivitas bucket juga menentukan warna yang digunakan Macie untuk merepresentasikan bucket dalam visualisasi data, seperti yang ditunjukkan pada gambar berikut.



Skor sensitivitas berkisar dari -1 sampai 100, seperti yang dijelaskan dalam tabel berikut. Untuk menilai input ke skor bucket S3, Anda dapat merujuk ke statistik penemuan data sensitif dan detail lain yang disediakan Macie tentang bucket.

Skor sensitivitas	Label sensitivitas	Informasi tambahan
-1	Kesalahan klasifikasi	<p>Macie belum menganalisis objek bucket apa pun karena kesalahan klasifikasi tingkat objek—masalah dengan pengaturan izin tingkat objek, konten objek, atau kuota.</p> <p>Ketika Macie mencoba menganalisis satu atau lebih objek dalam ember,</p>

Skor sensitivitas	Label sensitivitas	Informasi tambahan
		<p>kesalahan terjadi. Misalnya, objek adalah file cacat, atau objek dienkripsi dengan kunci yang Macie tidak dapat mengakses atau tidak diizinkan untuk digunakan. Data cakupan untuk bucket dapat membantu Anda menyelidiki dan memulihkan kesalahan. Untuk informasi selengkapnya, lihat <a href="#">Menilai cakupan penemuan data sensitif otomatis</a>.</p> <p>Macie akan terus mencoba menganalisis objek dalam ember. Jika Macie menganalisis objek berhasil, Macie akan memperbarui skor sensitivitas bucket dan label untuk mencerminkan hasil analisis.</p>

Skor sensitivitas	Label sensitivitas	Informasi tambahan
1-49	Tidak sensitif	<p>Dalam kisaran ini, skor yang lebih tinggi, seperti 49, menunjukkan bahwa Macie telah menganalisis relatif sedikit objek dalam ember. Skor yang lebih rendah, seperti 1, menunjukkan bahwa Macie telah menganalisis banyak objek dalam bucket (relatif terhadap jumlah total objek dalam bucket) dan mendeteksi relatif sedikit jenis dan kemunculan data sensitif pada objek tersebut.</p> <p>Skor 1 juga dapat menunjukkan bahwa bucket tidak berisi objek apa pun atau semua objek dalam bucket mengandung nol (0) byte data. Statistik objek dalam detail bucket dapat membantu Anda menentukan apakah ini masalahnya. Untuk informasi selengkapnya, lihat <a href="#">Meninjau detail bucket S3</a>.</p>

Skor sensitivitas	Label sensitivitas	Informasi tambahan
50	Belum dianalisis	<p>Macie belum mencoba menganalisis atau menganalisis objek bucket apa pun. Macie secara otomatis menetapkan skor ini ke bucket ketika Anda awalnya mengaktifkan penemuan otomatis untuk akun Anda atau bucket ditambahkan ke inventaris bucket Anda.</p> <p>Skor 50 juga dapat menunjukkan bahwa pengaturan izin bucket mencegah Macie mengakses bucket atau objek bucket. Hal ini biasanya disebabkan oleh kebijakan bucket yang ketat. Rincian bucket dapat membantu Anda menentukan apakah ini masalahnya karena Macie hanya dapat memberikan sebagian informasi tentang bucket. Untuk informasi tentang cara mengatasi masalah ini, lihat <a href="#">Mengizinkan Macie untuk mengakses bucket S3 dan objek</a>.</p>

Skor sensitivitas	Label sensitivitas	Informasi tambahan
51-99	Sensitif	Dalam kisaran ini, skor yang lebih tinggi, seperti 99, menunjukkan bahwa Macie telah menganalisis banyak objek dalam bucket (relatif terhadap jumlah total objek dalam bucket) dan mendeteksi banyak jenis dan kejadian data sensitif pada objek tersebut. Skor yang lebih rendah, seperti 51, menunjukkan bahwa Macie telah menganalisis sejumlah objek dalam bucket (relatif terhadap jumlah total objek dalam bucket) dan mendeteksi setidaknya beberapa jenis dan kejadian data sensitif pada objek tersebut.
100	Sensitif	Skor secara manual ditugaskan ke ember, mengesampingkan skor yang dihitung. Macie tidak menetapkan skor ini untuk ember.

## Memantau skor sensitivitas

Saat awalnya Anda mengaktifkan penemuan data sensitif otomatis untuk akun Anda, Amazon Macie secara otomatis menetapkan skor sensitivitas 50 untuk setiap bucket S3. Macie juga memberikan skor ini ke bucket saat bucket ditambahkan ke inventaris bucket Anda. Berdasarkan skor itu, label sensitivitas setiap bucket Belum dianalisis. Pengecualian adalah bucket kosong, yang merupakan bucket yang tidak berisi objek atau semua objek dalam bucket mengandung nol (0) byte data. Jika ini



adalah kasus untuk bucket, Macie memberikan skor 1 ke bucket dan label sensitivitas bucket Tidak sensitif.

Saat penemuan data sensitif otomatis berlangsung untuk akun Anda setiap hari, Macie memperbarui skor sensitivitas dan label untuk bucket S3 Anda untuk mencerminkan hasil analisis. Misalnya:

- Jika Macie tidak menemukan data sensitif dalam suatu objek, Macie mengurangi skor sensitivitas bucket dan memperbarui label sensitivitas bucket seperlunya.
- Jika Macie menemukan data sensitif dalam suatu objek, Macie meningkatkan skor sensitivitas bucket dan memperbarui label sensitivitas bucket seperlunya.
- Jika Macie menemukan data sensitif dalam objek yang kemudian berubah, Macie menghapus deteksi data sensitif untuk objek dari skor sensitivitas bucket dan memperbarui label sensitivitas bucket jika diperlukan.
- Jika Macie menemukan data sensitif dalam objek yang kemudian dihapus, Macie menghapus deteksi data sensitif untuk objek dari skor sensitivitas bucket dan memperbarui label sensitivitas bucket jika diperlukan.
- Jika objek ditambahkan ke bucket yang sebelumnya kosong dan Macie menemukan data sensitif dalam objek, Macie meningkatkan skor sensitivitas bucket dan memperbarui label sensitivitas bucket seperlunya.
- Jika pengaturan izin bucket mencegah Macie mengambil informasi tentang atau mengakses bucket atau objek bucket, Macie mengubah skor sensitivitas bucket menjadi 50 dan mengubah label sensitivitas bucket menjadi Belum dianalisis.

Bergantung pada jumlah data yang Anda simpan di Amazon S3, hasil analisis dapat mulai muncul dalam waktu 48 jam setelah memungkinkan penemuan data sensitif otomatis untuk akun Anda.

Anda dapat menyesuaikan pengaturan penilaian sensitivitas untuk akun Anda, yang mengubah pengaturan untuk analisis selanjutnya dari semua bucket S3 Anda. Anda juga dapat menyesuaikan pengaturan untuk masing-masing bucket S3. Untuk pengaturan tingkat akun, Anda dapat mulai menyertakan atau mengecualikan daftar izin tertentu, pengidentifikasi data kustom, atau pengidentifikasi data terkelola dari analisis. Anda juga dapat mengecualikan ember tertentu dari analisis. Untuk informasi selengkapnya, lihat [Mengonfigurasi setelan penemuan otomatis untuk akun Anda](#).

Untuk menyesuaikan pengaturan penilaian untuk bucket tertentu, Anda dapat menyertakan atau mengecualikan jenis data sensitif tertentu dari skor bucket. Anda juga dapat menentukan apakah

akan menetapkan skor yang dihitung secara otomatis ke bucket. Untuk informasi selengkapnya, lihat [Mengelola penemuan otomatis untuk bucket S3 individual](#).

## Pengaturan default untuk penemuan data sensitif otomatis

Jika penemuan data sensitif otomatis diaktifkan untuk akun Anda, Amazon Macie secara otomatis memilih dan menganalisis objek sampel dari semua bucket Amazon Simple Storage Service (Amazon S3) yang dipantau dan dianalisis untuk akun Anda. Jika Anda adalah administrator Macie untuk suatu organisasi, ini termasuk bucket S3 yang dimiliki akun anggota Anda. Untuk menyempurnakan cakupan analisis, Anda dapat mengecualikan bucket tertentu dari penemuan data sensitif otomatis. Anda dapat melakukan ini dengan dua cara: oleh [mengubah setelan penemuan data sensitif otomatis untuk akun Anda](#), dan oleh [mengubah setelan penemuan data sensitif otomatis untuk masing-masing bucket](#).

Secara default, Macie menganalisis objek S3 dengan hanya menggunakan kumpulan pengidentifikasi data terkelola yang kami rekomendasikan untuk penemuan data sensitif otomatis. Macie tidak menggunakan pengidentifikasi data kustom atau mengizinkan daftar yang telah Anda tetapkan. Untuk menyesuaikan analisis, Anda dapat mengonfigurasi Macie untuk menggunakan pengidentifikasi data terkelola tertentu, pengidentifikasi data kustom, dan daftar izinkan. Anda dapat melakukan ini dengan [mengubah setelan penemuan data sensitif otomatis untuk akun Anda](#).

### Topik

- [Pengidentifikasi data terkelola default untuk penemuan data sensitif otomatis](#)
- [Pembaruan ke setelan default untuk penemuan data sensitif otomatis](#)

## Pengidentifikasi data terkelola default untuk penemuan data sensitif otomatis

Secara default, Amazon Macie menganalisis objek S3 dengan hanya menggunakan kumpulan pengenalan data terkelola yang kami rekomendasikan untuk penemuan data sensitif otomatis. Kumpulan pengidentifikasi data terkelola default ini dirancang untuk mendeteksi kategori umum dan jenis data sensitif. Berdasarkan penelitian kami, ini dapat mendeteksi kategori umum dan jenis data sensitif sekaligus mengoptimalkan hasil penemuan otomatis Anda dengan mengurangi kebisingan.

Set defaultnya dinamis. Saat merilis pengidentifikasi data terkelola baru, kami menambahkannya ke set default jika kemungkinan besar akan mengoptimalkan hasil penemuan data sensitif otomatis Anda lebih lanjut. Seiring waktu, kami mungkin juga menambahkan atau menghapus pengidentifikasi data terkelola yang ada dari set. Penghapusan pengenalan data terkelola tidak memengaruhi statistik

dan detail penemuan data sensitif yang ada untuk bucket S3 Anda. Misalnya, jika kita menghapus pengenal data terkelola untuk jenis data sensitif yang sebelumnya terdeteksi Macie di bucket, Macie terus melaporkan deteksi tersebut untuk bucket. Jika kami menambahkan atau menghapus pengenal data terkelola dari set default, kami memperbarui halaman ini untuk menunjukkan sifat dan waktu perubahan. Untuk peringatan otomatis tentang perubahan ini, Anda dapat berlangganan RSS feed di [Riwayat dokumen Macie](#) halaman.

Topik berikut mencantumkan pengidentifikasi data terkelola yang saat ini berada dalam kumpulan default, yang diatur berdasarkan kategori dan jenis data sensitif. Mereka menentukan pengenal unik (ID) untuk setiap pengidentifikasi data terkelola di set. ID ini menjelaskan jenis data sensitif yang dirancang untuk dideteksi oleh pengenal data terkelola, misalnya: PGP\_PRIVATE\_KEY untuk kunci pribadi PGP dan USA\_PASSPORT\_NUMBER untuk nomor paspor AS. Jika Anda mengubah setelan penemuan data sensitif otomatis untuk akun, Anda dapat menggunakan ID ini untuk mengecualikan pengenal data terkelola secara eksplisit dari analisis berikutnya.

Topik

- [Kredensial](#)
- [Informasi keuangan](#)
- [Informasi yang dapat diidentifikasi secara pribadi \(PII\)](#)

Untuk detail tentang pengidentifikasi data terkelola tertentu atau daftar lengkap semua pengidentifikasi data terkelola yang saat ini disediakan Macie, lihat [Menggunakan pengidentifikasi data terkelola](#).

Kredensial

Untuk mendeteksi kemunculan data kredensial di objek S3, Macie menggunakan pengenal data terkelola berikut secara default.

Tipe data sensitif	ID pengenal data terkelola
AWS secret access key	AWS_CREDENTIALS
Header Otorisasi Dasar HTTP	HTTP_BASIC_AUTH_HEADER
Kunci pribadi OpenSSH	OPENSSSH_PRIVATE_KEY
Kunci pribadi PGP	PGP_PRIVATE_KEY

Tipe data sensitif	ID pengenalan data terkelola
Kunci pribadi Standar Kriptografi Kunci Publik (PKCS)	PKCS
kunci pribadi PuTTY	PUTTY_PRIVATE_KEY

### Informasi keuangan

Untuk mendeteksi kejadian informasi keuangan di objek S3, Macie menggunakan pengenalan data terkelola berikut secara default.

Tipe data sensitif	ID pengenalan data terkelola
Data strip magnetik kartu kredit	CREDIT_CARD_MAGNETIC_STRIPE
Nomor kartu kredit	CREDIT_CARD_NUMBER (untuk nomor kartu kredit di dekat kata kunci)

### Informasi yang dapat diidentifikasi secara pribadi (PII)

Untuk mendeteksi kejadian informasi identitas pribadi (PII) di objek S3, Macie menggunakan pengenalan data terkelola berikut secara default.

Tipe data sensitif	ID pengenalan data terkelola
Nomor identifikasi lisensi	CANADA_DRIVERS_LICENSE, DRIVERS_LICENSE (untuk AS), UK_DRIVERS_LICENSE
Nomor Roll Pemilu	UK_ELECTORAL_ROLL_NUMBER
Nomor identifikasi nasional	FRANCE_NATIONAL_IDENTIFICATION_NUMBER, GERMANY_NATIONAL_IDENTIFICATION_NUMBER, ITALY_NATIONAL_IDENTIFICATION_NUMBER, SPAIN_DNI_NUMBER

Tipe data sensitif	ID pengenal data terkelola
Nomor Asuransi Nasional (NINO)	UK_NATIONAL_INSURANCE_NUMBER
Nomor paspor	CANADA_PASSPORT_NUMBER, FRANCE_PASSPORT_NUMBER, GERMANY_PASSPORT_NUMBER, ITALY_PASSPORT_NUMBER, SPAIN_PASSPORT_NUMBER, UK_PASSPORT_NUMBER, USA_PASSPORT_NUMBER
Nomor Pokok Wajib Pajak (SIN)	CANADA_SOCIAL_INSURANCE_NUMBER
Nomor Jaminan Sosial (SSN)	SPAIN_SOCIAL_SECURITY_NUMBER, USA_SOCIAL_SECURITY_NUMBER
Nomor identifikasi wajib pajak atau referensi	AUSTRALIA_TAX_FILE_NUMBER, BRAZIL_CPF_NUMBER, FRANCE_TAX_IDENTIFICATION_NUMBER, GERMANY_TAX_IDENTIFICATION_NUMBER, SPAIN_NIE_NUMBER, SPAIN_NIF_NUMBER, SPAIN_TAX_IDENTIFICATION_NUMBER, USA_INDIVIDUAL_TAX_IDENTIFICATION_NUMBER

## Pembaruan ke setelan default untuk penemuan data sensitif otomatis

Tabel berikut menjelaskan perubahan pada pengaturan yang digunakan Amazon Macie secara default untuk penemuan data sensitif otomatis. Untuk peringatan otomatis tentang perubahan ini, berlangganan RSS feed pada [Riwayat dokumen Macie](#) halaman.

Perubahan	Deskripsi	Tanggal
Mengimplementasikan sekumpulan pengenal data	Konfigurasi penemuan data sensitif otomatis baru sekarang didasarkan pada	Agustus 2, 2023

Perubahan	Deskripsi	Tanggal
terkelola default yang baru dan dinamis	<p>dinamika <a href="#">kumpulan default pengenalan data terkelola</a>. Jika Anda mengaktifkan penemuan data sensitif otomatis untuk pertama kalinya pada atau setelah tanggal ini, konfigurasi Anda didasarkan pada kumpulan dinamis.</p> <p>Jika Anda mengaktifkan penemuan data sensitif otomatis untuk pertama kalinya sebelum tanggal ini, konfigurasi Anda didasarkan pada kumpulan pengidentifikasi data terkelola yang berbeda. Untuk informasi lebih lanjut, lihat catatan setelah tabel ini.</p>	
Ketersediaan umum	Rilis awal penemuan data sensitif otomatis.	November 28, 2022

Jika awalnya Anda mengaktifkan penemuan data sensitif otomatis untuk akun Anda sebelum 2 Agustus 2023, konfigurasi Anda tidak didasarkan pada kumpulan dinamis pengenalan data terkelola default. Konfigurasi Anda didasarkan pada kumpulan pengenalan data terkelola statis yang kami tetapkan untuk rilis awal penemuan data sensitif otomatis, seperti yang tercantum dalam tabel di bawah ini.

Untuk menentukan kapan awalnya Anda mengaktifkan penemuan data sensitif otomatis untuk akun, pilih Penemuan otomatis di panel navigasi di konsol Amazon Macie, dan kemudian lihat tanggal yang diaktifkan di Status bagian. Untuk melakukan ini secara terprogram, gunakan [GetAutomatedDiscoveryConfiguration](#) pengoperasian Amazon Macie API dan mengacu pada nilai untuk `firstEnabledAt` bidang. Jika tanggal sebelum 2 Agustus 2023, dan Anda ingin mulai

menggunakan kumpulan dinamis pengidentifikasi data terkelola default, hubungi AWS Support untuk bantuan.

Tabel berikut mencantumkan semua pengenalan data yang dikelola yang ada di set statis. Tabel ini diurutkan pertama berdasarkan kategori data sensitif dan kemudian dengan tipe data sensitif. Untuk detail tentang pengidentifikasi data terkelola tertentu, lihat [Menggunakan pengidentifikasi data terkelola](#).

Kategori data sensitif	Tipe data sensitif	ID pengenalan data terkelola
Kredensial	AWS secret access key	AWS_CREDENTIALS
Kredensial	Header Otorisasi Dasar HTTP	HTTP_BASIC_AUTH_HEADER
Kredensial	Kunci pribadi OpenSSH	OPENSSSH_PRIVATE_KEY
Kredensial	Kunci pribadi PGP	PGP_PRIVATE_KEY
Kredensial	Kunci pribadi Standar Kriptografi Kunci Publik (PKCS)	PKCS
Kredensial	kunci pribadi PuTTY	PUTTY_PRIVATE_KEY
Informasi keuangan	Nomor rekening bank	BANK_ACCOUNT_NUMBER (untuk nomor rekening bank Kanada dan AS), FRANCE_BANK_ACCOUNT_NUMBER, GERMANY_BANK_ACCOUNT_NUMBER, ITALY_BANK_ACCOUNT_NUMBER, SPAIN_BANK_ACCOUNT_NUMBER, UK_BANK_ACCOUNT_NUMBER
Informasi keuangan	Tanggal kedaluwarsa kartu kredit	CREDIT_CARD_EXPIRATION

Kategori data sensitif	Tipe data sensitif	ID pengenalan data terkelola
Informasi keuangan	Data strip magnetik kartu kredit	CREDIT_CARD_MAGNET_IC_STRIPE
Informasi keuangan	Nomor kartu kredit	CREDIT_CARD_NUMBER (untuk nomor kartu kredit di dekat kata kunci)
Informasi keuangan	Kode verifikasi kartu kredit	CREDIT_CARD_SECURITY_CODE
Informasi pribadi: Informasi kesehatan pribadi (PHI)	Nomor Penegak Hukum Narkoba Pemerintah (DEA)	US_DRUG_ENFORCEMENT_AGENCY_NUMBER
Informasi pribadi: PHI	Nomor Klaim Asuransi Kesehatan (HICN)	USA_HEALTH_INSURANCE_CLAIM_NUMBER
Informasi pribadi: PHI	Nomor asuransi atau identifikasi medis	CANADA_HEALTH_NUMBER, EUROPEAN_HEALTH_INSURANCE_CARD_NUMBER, FINLAND_EUROPEAN_HEALTH_INSURANCE_NUMBER, FRANCE_HEALTH_INSURANCE_NUMBER, UK_NHS_NUMBER, USA_MEDICARE_BENEFICIARY_IDENTIFIER
Informasi pribadi: PHI	Kode Sistem Pengkodean Prosedur Umum Pemeliharaan Kesehatan (HCPCS)	USA_HEALTHCARE_PROCEDURE_CODE
Informasi pribadi: PHI	Kode Obat Nasional (NDC)	USA_NATIONAL_DRUG_CODE



Kategori data sensitif	Tipe data sensitif	ID pengenalan data terkelola
Informasi pribadi: PHI	Pengidentifikasi Penyedia Nasional (NPI)	USA_NATIONAL_PROVIDER_IDENTIFIER
Informasi pribadi: PHI	Pengidentifikasi perangkat unik (UDI)	MEDICAL_DEVICE_UDI
Informasi pribadi: Informasi yang dapat diidentifikasi secara pribadi (PII)	Tanggal lahir	DATE_OF_BIRTH

Kategori data sensitif	Tipe data sensitif	ID pengenal data terkelola
Informasi pribadi: PII	Nomor identifikasi lisensi	AUSTRALIA_DRIVERS_LICENSE, AUSTRIA_DRIVERS_LICENSE, BELGIUM_DRIVERS_LICENSE, BULGARIA_DRIVERS_LICENSE, CANADA_DRIVERS_LICENSE, CROATIA_DRIVERS_LICENSE, CYPRUS_DRIVERS_LICENSE, CZECHIA_DRIVERS_LICENSE, DENMARK_DRIVERS_LICENSE, DRIVERS_LICENSE (untuk AS), ESTONIA_DRIVERS_LICENSE, FINLAND_DRIVERS_LICENSE, FRANCE_DRIVERS_LICENSE, GERMANY_DRIVERS_LICENSE, GREECE_DRIVERS_LICENSE, HUNGARY_DRIVERS_LICENSE, IRELAND_DRIVERS_LICENSE, ITALY_DRIVERS_LICENSE, LATVIA_DRIVERS_LICENSE, LITHUANIA_DRIVERS_LICENSE, LUXEMBOURG_DRIVERS_LICENSE, MALTA_DRIVERS_LICENSE, NETHERLANDS_DRIVER

Kategori data sensitif	Tipe data sensitif	ID pengenal data terkelola
		S_LICENSE, POLAND_DRIVERS_LICENSE, PORTUGAL_DRIVERS_LICENSE, ROMANIA_DRIVERS_LICENSE, SLOVAKIA_DRIVERS_LICENSE, SLOVENIA_DRIVERS_LICENSE, SPAIN_DRIVERS_LICENSE, SWEDEN_DRIVERS_LICENSE, UK_DRIVERS_LICENSE
Informasi pribadi: PII	Nomor Roll Pemilu	UK_ELECTORAL_ROLL_NUMBER
Informasi pribadi: PII	Nama lengkap	NAME
Informasi pribadi: PII	Koordinat Global Positioning System (GPS)	LATITUDE_LONGITUDE
Informasi pribadi: PII	Alamat surat-menyurat	ADDRESS, BRAZIL_CEP_CODE
Informasi pribadi: PII	Nomor identifikasi nasional	BRAZIL_RG_NUMBER, FRANCE_NATIONAL_IDENTIFICATION_NUMBER, GERMANY_NATIONAL_IDENTIFICATION_NUMBER, ITALY_NATIONAL_IDENTIFICATION_NUMBER, SPAIN_DNI_NUMBER
Informasi pribadi: PII	Nomor Asuransi Nasional (NINO)	UK_NATIONAL_INSURANCE_NUMBER

Kategori data sensitif	Tipe data sensitif	ID pengenal data terkelola
Informasi pribadi: PII	Nomor paspor	CANADA_PASSPORT_NUMBER, FRANCE_PASSPORT_NUMBER, GERMANY_PASSPORT_NUMBER, ITALY_PASSPORT_NUMBER, SPAIN_PASSPORT_NUMBER, UK_PASSPORT_NUMBER, USA_PASSPORT_NUMBER
Informasi pribadi: PII	Nomor tempat tinggal permanen	CANADA_NATIONAL_IDENTIFICATION_NUMBER
Informasi pribadi: PII	Nomor telepon	BRAZIL_PHONE_NUMBER, FRANCE_PHONE_NUMBER, GERMANY_PHONE_NUMBER, ITALY_PHONE_NUMBER, PHONE_NUMBER (untuk Canada dan US), SPAIN_PHONE_NUMBER, UK_PHONE_NUMBER
Informasi pribadi: PII	Nomor Pokok Wajib Pajak (SIN)	CANADA_SOCIAL_INSURANCE_NUMBER
Informasi pribadi: PII	Nomor Jaminan Sosial (SSN)	SPAIN_SOCIAL_SECURITY_NUMBER, USA_SOCIAL_SECURITY_NUMBER

Kategori data sensitif	Tipe data sensitif	ID pengenal data terkelola
Informasi pribadi: PII	Nomor identifikasi wajib pajak atau referensi	AUSTRALIA_TAX_FILE_NUMBER, BRAZIL_CN_PJ_NUMBER, BRAZIL_CPF_NUMBER, FRANCE_TAX_IDENTIFICATION_NUMBER, GERMANY_TAX_IDENTIFICATION_NUMBER, SPAIN_NIE_NUMBER, SPAIN_NIF_NUMBER, SPAIN_TAX_IDENTIFICATION_NUMBER, UK_TAX_IDENTIFICATION_NUMBER, USA_INDIVIDUAL_TAX_IDENTIFICATION_NUMBER
Informasi pribadi: PII	Nomor identifikasi Mesin (VIN)	VEHICLE_IDENTIFICATION_NUMBER

## Menjalankan tugas penemuan data sensitif di Amazon Macie

Dengan Amazon Macie, Anda dapat membuat dan menjalankan pekerjaan penemuan data sensitif untuk mengotomatiskan penemuan, pencatatan, dan pelaporan data sensitif di bucket Amazon Simple Storage Service (Amazon S3). Pekerjaan penemuan data sensitif adalah serangkaian tugas pemrosesan dan analisis otomatis yang dilakukan Macie untuk mendeteksi dan melaporkan data sensitif di objek Amazon S3. Setiap pekerjaan memberikan laporan terperinci tentang data sensitif yang ditemukan Macie dan analisis yang dilakukan Macie. Dengan membuat dan menjalankan pekerjaan, Anda dapat membangun dan mempertahankan tampilan komprehensif data yang disimpan organisasi Anda di Amazon S3 dan risiko keamanan atau kepatuhan apa pun untuk data tersebut.

Untuk membantu Anda memenuhi dan mempertahankan kepatuhan terhadap persyaratan keamanan dan privasi data Anda, Macie menyediakan beberapa opsi untuk menjadwalkan dan menentukan

ruang lingkup pekerjaan. Anda dapat mengonfigurasi tugas agar hanya sekali menjalankan analisis dan penilaian sesuai permintaan, atau secara berulang untuk analisis, penilaian, dan pemantauan berkala. Anda juga menentukan luas dan kedalaman analisis pekerjaan — bucket S3 spesifik yang Anda pilih atau bucket yang sesuai dengan kriteria tertentu. Anda dapat secara opsional memperbaiki ruang lingkup analisis itu dengan memilih opsi tambahan. Pilihan termasuk kustom termasuk dan mengecualikan kriteria yang berasal dari properti objek S3, seperti tag, awalan, dan ketika objek terakhir diubah.

Untuk setiap pekerjaan, Anda juga menentukan jenis data sensitif yang ingin dideteksi dan dilaporkan oleh Macie. Anda dapat mengonfigurasi pekerjaan untuk menggunakan [pengidentifikasi data terkelola](#) yang disediakan Macie, [pengidentifikasi data khusus](#) yang Anda tentukan, atau kombinasi keduanya. Dengan memilih pengidentifikasi data terkelola dan kustom tertentu untuk suatu pekerjaan, Anda dapat menyesuaikan analisis agar fokus pada jenis data sensitif tertentu. Untuk menyempurnakan analisis, Anda juga dapat mengkonfigurasi pekerjaan untuk menggunakan [daftar izinkan](#) yang Anda tentukan. Izinkan daftar menentukan pola teks dan teks yang ingin diabaikan Macie, biasanya pengecualian data sensitif untuk skenario atau lingkungan tertentu organisasi Anda.

Setiap pekerjaan menghasilkan catatan data sensitif yang ditemukan Macie dan analisis yang dilakukan Macie - temuan data sensitif dan hasil penemuan data sensitif. Sebuah temuan data sensitif adalah laporan rinci data sensitif yang Macie ditemukan dalam objek S3. Hasil penemuan data sensitif adalah catatan yang mencatat detail tentang analisis objek S3. Macie membuat hasil penemuan data sensitif untuk setiap objek yang dianalisis oleh tugas yang dikonfigurasi oleh Anda. Ini termasuk objek yang Macie tidak menemukan data sensitif, dan oleh karena itu tidak menghasilkan temuan data sensitif, dan objek yang Macie tidak dapat menganalisis karena kesalahan atau masalah. Setiap tipe catatan mematuhi skema standar, yang dapat membantu Anda melakukan kueri, memantau, dan memproses catatan agar memenuhi persyaratan keamanan dan kepatuhan Anda.

## Topik

- [Opsi ruang lingkup untuk tugas penemuan data sensitif](#)
- [Membuat tugas penemuan data sensitif](#)
- [Meninjau statistik dan hasil untuk pekerjaan penemuan data sensitif](#)
- [Memantau pekerjaan penemuan data sensitif dengan Amazon CloudWatch Logs](#)
- [Mengelola tugas penemuan data sensitif](#)
- [Biaya prakiraan dan pemantauan biaya untuk tugas penemuan data sensitif](#)
- [Pengidentifikasi data terkelola direkomendasikan untuk pekerjaan penemuan data sensitif](#)

## Opsi ruang lingkup untuk tugas penemuan data sensitif

Dengan lowongan penemuan data sensitif, Anda menentukan cakupan data Amazon Simple Storage Service (Amazon S3) yang dianalisis Amazon Macie untuk mendeteksi dan melaporkan data sensitif. Untuk membantu Anda melakukan hal ini, Macie menyediakan beberapa opsi tugas khusus yang dapat Anda pilih saat Anda membuat dan mengonfigurasi suatu tugas.

Opsi ruang lingkup

- [Bucket S3](#)
- [Sertakan objek S3 yang ada](#)
- [Kedalaman pengambilan sampel](#)
- [Kriteria objek S3](#)

### Bucket S3

Saat membuat pekerjaan penemuan data sensitif, Anda menentukan bucket S3 mana yang berisi objek yang ingin dianalisis Macie saat pekerjaan berjalan. Anda dapat melakukannya dengan salah satu dari dua cara, dengan memilih bucket S3 tertentu dari inventaris bucket Anda atau dengan menentukan kriteria kustom yang berasal dari properti bucket S3.

Pilih ember tertentu

Dengan opsi ini, Anda secara eksplisit memilih setiap bucket S3 yang Anda ingin untuk dianalisis tugas. Kemudian, ketika tugas berjalan, tugas tersebut hanya menganalisis objek di bucket yang dipilih. Jika Anda mengonfigurasi pekerjaan untuk dijalankan secara berkala setiap hari, mingguan, atau bulanan, pekerjaan menganalisis objek dalam ember yang sama setiap kali dijalankan.

Konfigurasi ini sangat membantu untuk kasus-kasus saat Anda lebih memilih untuk melakukan analisis yang ditargetkan dari set data tertentu. Hal ini memberi Anda kontrol yang tepat dan dapat diprediksi atas bucket yang akan dianalisis tugas.

Tentukan kriteria bucket

Dengan opsi ini, Anda menentukan kriteria runtime yang menentukan bucket S3 mana yang menganalisis pekerjaan. Kriteria tersebut terdiri dari satu syarat atau lebih yang berasal dari properti bucket, seperti pengaturan dan tanda akses publik. Ketika pekerjaan berjalan, ia mengidentifikasi bucket yang sesuai dengan kriteria Anda, dan kemudian menganalisis objek

dalam bucket tersebut. Jika Anda mengonfigurasi pekerjaan untuk dijalankan secara berkala, pekerjaan melakukan ini setiap kali dijalankan. Akibatnya, tugas dapat menganalisis objek dalam bucket yang berbeda setiap kali berjalan, tergantung pada perubahan inventaris bucket dan kriteria yang Anda tetapkan.

Konfigurasi ini sangat membantu untuk kasus saat Anda ingin ruang lingkup analisis tugas secara dinamis beradaptasi dengan perubahan pada inventaris bucket Anda. Jika Anda mengonfigurasi pekerjaan untuk menggunakan kriteria bucket dan dijalankan secara berkala, pekerjaan akan secara otomatis mengidentifikasi bucket baru yang cocok dengan kriteria dan memeriksa bucket tersebut untuk data sensitif.

Topik di bagian ini memberikan detail tambahan tentang setiap opsi.

## Topik

- [Memilih ember S3 tertentu](#)
- [Menentukan kriteria bucket S3](#)

## Memilih ember S3 tertentu

Jika Anda memilih untuk secara eksplisit memilih setiap bucket S3 yang ingin Anda analisis, Macie memberi Anda inventaris lengkap bucket Anda saat ini. Wilayah AWS Anda kemudian dapat meninjau inventaris dan memilih bucket yang Anda inginkan. Untuk mempelajari cara Macie menghasilkan dan memelihara inventaris ini untuk Anda, lihat [Cara Macie memantau keamanan data Amazon S3](#).

Jika Anda administrator Macie untuk suatu organisasi, inventaris mencakup bucket yang dimiliki oleh akun anggota di organisasi Anda. Anda dapat memilih sebanyak 1.000 dari bucket ini, yang mencakup 1.000 akun.

Untuk membantu Anda membuat pilihan bucket, inventaris menyediakan detail dan statistik untuk setiap bucket. Ini termasuk jumlah data yang dapat dianalisis pekerjaan di setiap bucket— objek yang dapat diklasifikasikan adalah objek yang menggunakan kelas [penyimpanan Amazon S3 yang didukung](#) dan memiliki ekstensi nama file untuk file atau format penyimpanan [yang didukung](#). Inventaris juga menunjukkan apakah tugas yang ada dikonfigurasi untuk menganalisis objek dalam suatu bucket. Detail ini dapat membantu Anda memperkirakan luas tugas dan meningkatkan pilihan bucket Anda.

Dalam tabel inventaris:



- Sensitivitas — Menunjukkan skor sensitivitas bucket saat ini, jika [penemuan data sensitif otomatis](#) diaktifkan untuk akun Anda.
- Objek yang dapat diklasifikasikan - Menunjukkan jumlah total objek yang dapat dianalisis pekerjaan dalam ember.
- Ukuran yang dapat diklasifikasikan - Menunjukkan ukuran penyimpanan total semua objek yang dapat dianalisis pekerjaan dalam ember.


Jika bucket berisi objek terkompresi, nilai ini tidak mencerminkan ukuran sebenarnya dari objek tersebut setelah didekompresi. Jika versioning diaktifkan untuk suatu bucket, nilai-nilai ini didasarkan pada ukuran penyimpanan versi terbaru dari setiap objek di bucket tersebut.


- Dipantau oleh pekerjaan - Menunjukkan apakah ada pekerjaan yang ada dikonfigurasi untuk menganalisis objek secara berkala dalam ember setiap hari, mingguan, atau bulanan.

Jika nilai untuk bidang ini Ya, bucket secara eksplisit disertakan dalam tugas berkala atau bucket yang sesuai dengan kriteria untuk tugas berkala dalam 24 jam terakhir. Selain itu, status dari setidaknya salah satu tugas tersebut tidak Dibatalkan. Macie memperbarui data ini setiap hari.


- Lari pekerjaan terbaru — Jika pekerjaan periodik atau satu kali yang ada dikonfigurasi untuk menganalisis objek dalam ember, bidang ini menunjukkan tanggal dan waktu terbaru ketika salah satu pekerjaan tersebut mulai berjalan. Jika tidak, bidang ini akan kosong.

Jika ikon informasi

 muncul di samping setiap nama bucket dalam tabel, kami rekomendasikan Anda mengambil metadata bucket terbaru dari Amazon S3. Untuk melakukannya, pilih segarkan

 di atas tabel. Ikon informasi menunjukkan bahwa bucket dibuat pada 24 jam terakhir, mungkin setelah Macie terakhir mengambil bucket dan metadata objek dari Amazon S3 sebagai bagian dari siklus penyegaran harian. Untuk informasi selengkapnya, lihat [Penyegaran data](#).

Jika ikon peringatan

 muncul di samping nama bucket di tabel, Macie tidak diizinkan mengakses bucket atau objek bucket. Macie hanya dapat memberikan sebagian informasi tentang bucket, seperti nama bucket. Ini berarti bahwa pekerjaan tidak akan dapat menganalisis objek dalam ember. Untuk menyelidiki masalah ini, tinjau pengaturan kebijakan dan izin bucket di Amazon S3. Misalnya, bucket mungkin memiliki

kebijakan bucket yang membatasi. Untuk informasi selengkapnya, lihat [Mengizinkan Macie untuk mengakses bucket S3 dan objek](#).

Untuk menyesuaikan tampilan inventaris Anda dan menemukan bucket tertentu dengan lebih mudah, Anda dapat memfilter tabel dengan memasukkan kriteria filter di kotak filter. Tabel berikut menunjukkan beberapa contoh.

Untuk menunjukkan bucket yang...	Terapkan filter ini...
Dimiliki oleh akun tertentu	ID Akun = <i>ID 12 digit untuk akun</i>
Dapat diakses secara publik	Izin efektif = Publik
Tidak termasuk dalam tugas berkala	Dipantau secara aktif oleh pekerjaan = Salah
Tidak termasuk dalam tugas berkala atau satu kali	Didefinisikan dalam pekerjaan = Salah
Memiliki kunci tanda khusus	Kunci tanda = <i>kunci tanda tersebut</i>
Mempunyai nilai tanda khusus	Nilai tanda = <i>Nilai tanda tersebut</i>
Berisi objek yang tidak terenkripsi (atau gunakan enkripsi di sisi klien)	Jumlah objek berdasarkan enkripsi adalah Tidak ada enkripsi dan Dari = 1

\* Kunci dan nilai tanda sensitif huruf besar dan kecil. Anda juga harus menentukan nilai yang lengkap dan valid untuk bidang ini dalam filter. Anda tidak dapat menentukan nilai parsial atau menggunakan karakter wildcard.

Untuk menampilkan detail bucket, pilih nama bucket dan lihat panel detail. Dari sana, Anda juga bisa:

- Putar dan telusuri bidang tertentu dengan memilih kaca pembesar untuk bidang tersebut. Pilih



untuk menampilkan bucket dengan nilai yang sama, atau pilih



untuk menampilkan bucket dengan nilai lain.

- Ambil metadata terbaru untuk objek di bucket. Hal ini dapat membantu jika Anda baru saja membuat bucket atau membuat perubahan signifikan pada objek bucket selama 24 jam terakhir. Untuk mengambil data, pilih segarkan



di bagian panel Statistik objek. Opsi ini tersedia untuk bucket yang berisi 30.000 objek atau kurang.

### Menentukan kriteria bucket S3

Jika Anda memilih untuk menentukan kriteria bucket untuk suatu tugas, Macie menyediakan opsi untuk menentukan dan menguji kriteria tersebut. Ini adalah kriteria runtime yang menentukan bucket S3 mana yang berisi objek untuk pekerjaan yang akan dianalisis. Setiap kali pekerjaan berjalan, itu mengidentifikasi bucket yang sesuai dengan kriteria Anda, dan kemudian menganalisis objek dalam ember yang sesuai. Jika Anda administrator Macie untuk suatu organisasi, ini termasuk bucket yang dimiliki oleh akun anggota di organisasi Anda.

### Menentukan kriteria bucket

Kriteria bucket terdiri dari satu syarat atau lebih yang berasal dari properti bucket S3. Setiap syarat, yang juga disebut sebagai kriteria, terdiri dari bagian berikut:

- Bidang berbasis properti, seperti ID Akun atau Izin efektif.
- Operator, baik sama (eq) atau tidak sama (neq).
- Satu nilai atau lebih.
- Pernyataan penyertaan dan pengecualian yang menunjukkan apakah Anda ingin tugas menganalisis (disertakan) atau melewati (dikecualikan) bucket yang sesuai dengan syarat.

Jika Anda menentukan lebih dari satu nilai untuk suatu bidang, Macie menggunakan logika OR untuk menggabungkan nilai-nilai tersebut. Jika Anda menentukan lebih dari satu syarat untuk kriteria tersebut, Macie menggunakan logika AND untuk menggabungkan syarat-syarat tersebut. Selain itu, syarat pengecualian lebih diutamakan daripada syarat penyertaan. Misalnya, jika Anda menyertakan bucket yang dapat diakses publik dan mengecualikan bucket yang memiliki tanda tertentu, tugas akan menganalisis objek dalam setiap bucket yang dapat diakses publik kecuali bucket memiliki satu tanda yang ditentukan.

Anda dapat menentukan syarat yang berasal dari salah satu bidang berbasis properti berikut untuk bucket S3.

#### ID Akun

Pengenal unik (ID) untuk pemilik bucket. Akun AWS Untuk menentukan beberapa nilai untuk bidang ini, masukkan ID untuk setiap akun dan pisahkan setiap entri dengan koma.

Perhatikan bahwa Macie tidak mendukung penggunaan karakter wildcard atau nilai sebagian untuk bidang ini.

### Nama ember

Nama dari suatu bucket. Bidang ini berkorelasi dengan bidang Nama, bukan bidang Amazon Resource Name (ARN), di Amazon S3. Untuk menentukan beberapa nilai untuk bidang ini, masukkan nama setiap bucket dan pisahkan setiap entri dengan koma.

Perhatikan bahwa nilai peka huruf besar dan kecil. Selain itu, Macie tidak mendukung penggunaan karakter wildcard atau nilai parsial untuk bidang ini.

### Izin yang efektif

Menentukan apakah bucket dapat diakses oleh publik. Anda dapat memilih satu atau beberapa nilai berikut untuk bidang ini:

- Bukan publik - Masyarakat umum tidak memiliki akses baca atau tulis ke ember.
- Publik — Masyarakat umum telah membaca atau menulis akses ke ember.
- Tidak diketahui - Macie tidak dapat mengevaluasi pengaturan akses publik untuk ember.

Untuk menentukan nilai bucket ini, Macie menganalisis kombinasi pengaturan tingkat akun dan ember untuk bucket: pengaturan blokir akses publik untuk akun; pengaturan blokir akses publik untuk bucket; kebijakan bucket untuk bucket; dan, daftar kontrol akses (ACL) untuk bucket.

### Akses bersama

Menentukan apakah bucket dibagikan dengan yang lainAkun AWS, identitas akses CloudFront asal Amazon (OAI), atau kontrol akses CloudFront asal (OAC). Anda dapat memilih satu atau beberapa nilai berikut untuk bidang ini:

- Eksternal — Bucket dibagikan dengan satu atau beberapa hal berikut atau kombinasi berikut ini: CloudFront OAI, CloudFront OAC, atau akun yang berada di luar (bukan bagian dari) organisasi Anda.
- Internal — Bucket dibagikan dengan satu atau beberapa akun yang bersifat internal (bagian dari) organisasi Anda. Itu tidak dibagikan dengan CloudFront OAI atau OAC.
- Tidak dibagikan - Bucket tidak dibagikan dengan akun lain, CloudFront OAI, atau CloudFront OAC.
- Tidak diketahui - Macie tidak dapat mengevaluasi pengaturan akses bersama untuk bucket.

Untuk menentukan apakah bucket dibagikan dengan yang lainAkun AWS, Macie menganalisis kebijakan bucket dan ACL untuk bucket tersebut. Selain itu, suatu Organisasi merupakan set

akun Macie yang dikelola secara terpusat sebagai grup dari akun-akun terkait melalui AWS Organizations atau dengan undangan Macie. Untuk informasi tentang opsi Amazon S3 untuk berbagi bucket, lihat [Manajemen identitas dan akses di Amazon S3](#) di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

Untuk menentukan apakah bucket dibagikan dengan CloudFront OAI atau OAC, Macie menganalisis kebijakan bucket untuk bucket tersebut. CloudFront OAI atau OAC memungkinkan pengguna untuk mengakses objek bucket melalui satu atau beberapa distribusi tertentu CloudFront. Untuk informasi tentang CloudFront OAI dan OAC, lihat [Membatasi akses ke asal Amazon S3](#) di Panduan Pengembang Amazon. CloudFront

## Tag

Tanda yang terkait dengan bucket. Tag adalah label yang dapat Anda tentukan dan tetapkan ke jenis AWS sumber daya tertentu, termasuk bucket S3. Setiap tanda terdiri dari kunci tanda yang diperlukan dan nilai tanda opsional. Untuk informasi tentang menandai bucket S3, lihat [Menggunakan tag bucket S3 alokasi biaya di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon](#).

Untuk tugas penemuan data sensitif, Anda dapat menggunakan tipe syarat ini untuk menyertakan atau mengecualikan bucket yang memiliki kunci tag tertentu, nilai tanda tertentu, atau kunci tanda dan nilai tanda tertentu (sebagai pasangan). Misalnya:

- Jika Anda menentukan **Project** sebagai kunci tag dan tidak menentukan nilai tag apa pun untuk suatu kondisi, bucket apa pun yang memiliki kunci tag Project cocok dengan kriteria kondisi, terlepas dari nilai tag yang terkait dengan kunci tag tersebut.
- Jika Anda menentukan **Development** dan **Test** sebagai nilai tag dan tidak menentukan kunci tag apa pun untuk suatu kondisi, bucket apa pun yang memiliki nilai **Test** tag **Development** atau cocok dengan kriteria kondisi, terlepas dari kunci tag yang terkait dengan nilai tag tersebut.

Untuk menentukan beberapa kunci tanda dalam suatu syarat, masukkan setiap kunci tanda di bidang Kunci dan pisahkan setiap entri dengan koma. Untuk menentukan beberapa nilai tanda dalam suatu syarat, masukkan setiap kunci tanda di bidang Nilai dan pisahkan setiap entri dengan koma.

Perhatikan bahwa kunci dan nilai tanda sensitif huruf besar dan kecil. Selain itu, Macie tidak mendukung penggunaan karakter wildcard atau nilai parsial di syarat tanda.

## Menguji kriteria bucket

Saat Anda menentukan kriteria bucket, Anda dapat menguji dan meningkatkan kriteria dengan melihat pratinjau hasilnya. Untuk melakukannya, perluas bagian Pratinjau hasil kriteria yang muncul di bawah kriteria pada konsol tersebut. Bagian ini menampilkan tabel semua bucket yang saat ini cocok dengan kriteria.

Tabel ini juga memberikan wawasan tentang jumlah data yang dapat dianalisis pekerjaan di setiap bucket— objek yang dapat diklasifikasikan adalah objek yang menggunakan kelas [penyimpanan Amazon S3 yang didukung](#) dan memiliki ekstensi nama file untuk file atau format penyimpanan [yang didukung](#). Tabel juga menunjukkan apakah tugas yang ada dikonfigurasi untuk secara berkala menganalisis objek dalam suatu bucket.

Di tabel:

- Sensitivitas — Menunjukkan skor sensitivitas bucket saat ini, jika [penemuan data sensitif otomatis](#) diaktifkan untuk akun Anda.
- Objek yang dapat diklasifikasikan - Menunjukkan jumlah total objek yang dapat dianalisis pekerjaan dalam ember.
- Ukuran yang dapat diklasifikasikan - Menunjukkan ukuran penyimpanan total semua objek yang dapat dianalisis pekerjaan dalam ember.

Jika bucket berisi objek terkompresi, nilai ini tidak mencerminkan ukuran sebenarnya dari objek tersebut setelah didekompresi. Jika versioning diaktifkan untuk suatu bucket, nilai-nilai ini didasarkan pada ukuran penyimpanan versi terbaru dari setiap objek di bucket tersebut.

- Dipantau oleh pekerjaan - Menunjukkan apakah ada pekerjaan yang ada dikonfigurasi untuk menganalisis objek secara berkala dalam ember setiap hari, mingguan, atau bulanan.

Jika nilai untuk bidang ini Ya, bucket secara eksplisit disertakan dalam tugas berkala atau bucket yang sesuai dengan kriteria untuk tugas berkala dalam 24 jam terakhir. Selain itu, status dari setidaknya salah satu tugas tersebut tidak Dibatalkan. Macie memperbarui data ini setiap hari.

Jika icon peringatan



muncul di samping nama bucket, Macie tidak diizinkan mengakses bucket atau objek bucket. Macie hanya dapat memberikan sebagian informasi tentang bucket, seperti nama bucket. Ini berarti bahwa pekerjaan tidak akan dapat menganalisis objek dalam ember. Untuk menyelidiki masalah ini, tinjau pengaturan kebijakan dan izin bucket di Amazon S3. Misalnya, bucket mungkin memiliki kebijakan

bucket yang membatasi. Untuk informasi selengkapnya, lihat [Mengizinkan Macie untuk mengakses bucket S3 dan objek](#).

Untuk menyempurnakan kriteria bucket untuk pekerjaan, gunakan opsi filter untuk menambah, mengubah, atau menghapus kondisi dari kriteria. Macie kemudian memperbarui tabel untuk menunjukkan perubahan Anda.

## Sertakan objek S3 yang ada

Anda dapat menggunakan tugas penemuan data sensitif untuk melakukan analisis berkelanjutan tambahan terhadap objek di bucket S3. Jika Anda mengonfigurasi suatu tugas untuk berjalan secara berkala, Macie melakukannya untuk Anda secara otomatis—setiap pelaksanaan hanya menganalisis objek-objek yang dibuat atau diubah setelah pelaksanaan sebelumnya. Dengan opsi Sertakan objek yang ada, Anda memilih titik awal untuk tambahan pertama:

- Untuk menganalisis semua objek yang ada segera setelah Anda selesai membuat tugas, berikan tanda centang pada kotak centang untuk opsi ini.
- Untuk menunggu dan menganalisis hanya pada objek yang dibuat atau diubah setelah Anda membuat tugas dan sebelum pelaksanaan tugas pertama, Hapus tanda centang pada kotak centang untuk opsi ini.

Menghapus centang pada kotak centang ini sangat membantu untuk kasus saat Anda telah menganalisis data dan ingin terus menganalisisnya secara berkala. Misalnya, jika sebelumnya Anda menggunakan layanan atau aplikasi lain untuk mengklasifikasikan data dan Anda baru saja mulai menggunakan Macie, Anda dapat menggunakan opsi ini untuk memastikan penemuan dan klasifikasi data Anda yang berkelanjutan tanpa menimbulkan biaya yang tidak perlu atau menduplikasi data klasifikasi.

Setiap pelaksanaan tugas berkala selanjutnya secara otomatis hanya menganalisis objek yang dibuat atau diubah setelah pelaksanaan sebelumnya.

Untuk kedua tugas berkala dan satu kali, Anda juga dapat mengonfigurasi tugas untuk menganalisis hanya objek yang dibuat atau diubah sebelum atau setelah waktu tertentu atau selama rentang waktu tertentu. Untuk melakukannya, tambahkan [kriteria objek](#) yang menggunakan tanggal modifikasi terakhir untuk objek.

## Kedalaman pengambilan sampel

Dengan opsi ini, Anda menentukan persentase objek S3 yang memenuhi syarat yang ingin dianalisis Macie saat pekerjaan penemuan data sensitif berjalan. Objek yang memenuhi syarat adalah objek yang: menggunakan [kelas penyimpanan Amazon S3 yang didukung](#), memiliki ekstensi nama file untuk [file atau format penyimpanan yang didukung](#), dan cocok dengan kriteria lain yang Anda tentukan untuk pekerjaan tersebut.

Jika nilai ini kurang dari 100%, Macie memilih objek yang memenuhi syarat untuk dianalisis secara acak, hingga persentase yang ditentukan, dan menganalisis semua data dalam objek tersebut. Misalnya, jika Anda mengonfigurasi suatu tugas untuk menganalisis 10.000 objek dan Anda menentukan kedalaman pengambilan sampel sebesar 20%, tugas akan menganalisis sekitar 2.000 objek yang memenuhi syarat yang dipilih secara acak.

Mengurangi kedalaman pengambilan sampel dari suatu tugas dapat menurunkan biaya dan mengurangi durasi tugas. Ini membantu untuk kasus saat data dalam objek sangat konsisten dan Anda ingin menentukan mana yang berisi data sensitif, apakah bucket S3 atau objek.

Perhatikan bahwa opsi ini mengendalikan persentase objek yang dianalisis, bukan persentase byte yang dianalisis. Jika Anda memasukkan kedalaman pengambilan sampel yang kurang dari 100%, Macie menganalisis semua data di setiap objek yang dipilih, bukan persentase data di setiap objek yang dipilih.

## Kriteria objek S3

Untuk menyempurnakan cakupan pekerjaan penemuan data sensitif, Anda juga dapat menentukan kriteria khusus yang menentukan objek S3 mana yang disertakan atau dikecualikan Macie dari analisis pekerjaan. Kriteria bucket terdiri dari satu syarat atau lebih yang berasal dari properti objek S3. Syarat ini berlaku untuk objek di semua bucket S3 tempat tugas dikonfigurasi untuk melakukan analisis. Jika bucket berisi beberapa versi objek, syarat tersebut berlaku untuk versi terbaru dari objek.

Jika Anda menentukan beberapa syarat sebagai kriteria objek, Macie menggunakan logika AND untuk menggabungkan syarat tersebut. Selain itu, syarat pengecualian lebih diutamakan daripada syarat penyertaan. Misalnya, jika Anda menyertakan objek yang memiliki ekstensi nama file .pdf dan mengecualikan objek yang lebih besar dari 5 MB, tugas menganalisis setiap objek yang memiliki ekstensi nama file .pdf, kecuali objek lebih besar dari 5 MB.

Anda dapat menentukan syarat yang berasal dari salah satu properti objek S3 berikut.



## Ekstensi nama file

Ini berkorelasi dengan ekstensi nama file dari objek S3. Anda dapat menggunakan tipe syarat ini untuk menyertakan atau mengecualikan objek berdasarkan tipe file. Untuk melakukannya pada beberapa tipe file, masukkan ekstensi nama file untuk setiap tipe dan pisahkan setiap entri dengan koma—misalnya: **docx, pdf, xlsx**. Jika Anda memasukkan beberapa ekstensi nama file sebagai nilai untuk suatu syarat, Macie menggunakan logika OR untuk menggabungkan nilai tersebut.

Perhatikan bahwa nilai peka huruf besar dan kecil. Selain itu, Macie tidak mendukung penggunaan nilai parsial atau karakter wildcard di tipe syarat ini.

Untuk informasi tentang tipe file yang dapat dianalisis oleh Macie, lihat [Format file dan penyimpanan yang didukung](#).

## Terakhir dimodifikasi

Hal ini berkorelasi dengan bidang Terakhir dimodifikasi di Amazon S3. Di Amazon S3, bidang ini menyimpan tanggal dan waktu ketika sebuah objek S3 dibuat atau terakhir diubah, mana yang terbaru.

Untuk tugas penemuan data sensitif, syarat ini dapat berupa tanggal tertentu, tanggal dan waktu tertentu, atau rentang waktu eksklusif:

- Untuk menganalisis objek yang terakhir diubah setelah tanggal atau tanggal dan waktu tertentu, masukkan nilai-nilai di bidang Dari.
- Untuk menganalisis objek yang terakhir diubah sebelum tanggal atau tanggal dan waktu tertentu, masukkan nilai-nilai di bidang Hingga.
- Untuk menganalisis objek yang terakhir diubah selama rentang waktu tertentu, gunakan bidang Dari untuk memasukkan nilai-nilai untuk tanggal atau tanggal dan waktu pertama dalam rentang waktu. Gunakan bidang Hingga untuk memasukkan nilai untuk tanggal atau tanggal dan waktu terakhir dalam rentang waktu.
- Untuk menganalisis objek yang terakhir diubah kapan saja selma satu waktu tertentu, masukkan tanggal di bidang tanggal Dari. Masukkan tanggal untuk hari berikutnya di bidang tanggal Hingga. Kemudian verifikasi bahwa kedua bidang waktu tersebut kosong. (Macie memperlakukan bidang waktu kosong sebagai `00:00:00`.) Misalnya, untuk menganalisis objek yang berubah pada 9 Agustus 2022, masukkan **2022/08/09** di bidang Dari tanggal, masukkan **2022/08/10** di bidang Tanggal, dan jangan masukkan nilai di bidang waktu mana pun.

Masukkan nilai waktu apa pun di Coordinated Universal Time (UTC) dan gunakan notasi 24 jam.

## Awalan

Hal ini berkorelasi dengan bidang Kunci di Amazon S3. Di Amazon S3, bidang ini menyimpan nama objek S3, termasuk prefiks objek. Suatu prefiks mirip dengan jalur direktori di bucket. Ini memungkinkan Anda untuk mengelompokkan objek yang sama dalam suatu bucket, seperti Anda menyimpan file yang sama bersama dalam folder pada sistem file. Untuk informasi tentang prefiks dan folder objek di Amazon S3, lihat [Mengatur objek di konsol Amazon S3 menggunakan folder](#) di Panduan Pengguna Amazon Simple Storage Service.

Anda dapat menggunakan tipe syarat ini untuk menyertakan atau mengecualikan objek yang kuncinya (nama) dimulai dengan nilai tertentu. Misalnya, untuk mengecualikan semua objek yang kuncinya dimulai AWSLogs, masukkan **AWSLogs** sebagai nilai untuk kondisi Awalan, lalu pilih Kecualikan.

Jika Anda memasukkan beberapa prefiks sebagai nilai untuk suatu syarat, Macie menggunakan logika OR untuk menggabungkan nilai tersebut. Misalnya, jika Anda memasukkan **AWSLogs1** dan **AWSLogs2** sebagai nilai untuk suatu kondisi, objek apa pun yang kuncinya dimulai dengan AWSLogs1 atau AWSLogs2 cocok dengan kriteria kondisi.

Ketika Anda memasukkan nilai untuk syarat Prefiks, ingatlah berikut ini:

- Kunci peka huruf besar dan kecil.
- Macie tidak mendukung penggunaan karakter wildcard dalam nilai-nilai ini.
- Di Amazon S3, kunci objek tidak termasuk nama bucket yang berisi objek. Untuk alasan ini, jangan tentukan nama bucket dalam nilai ini.
- Jika prefiks menyertakan pembatas, sertakan pembatas dalam nilai. Misalnya, enter **AWSLogs/eventlogs** untuk menentukan kondisi untuk semua objek yang kuncinya dimulai dengan AWSLogs/eventlogs. Macie mendukung pembatas Amazon S3 default, yang merupakan garis miring (/), dan pembatas kustom.

Perhatikan juga bahwa objek cocok dengan kriteria kondisi hanya jika kunci objek sama persis dengan nilai yang Anda masukkan, dimulai dengan karakter pertama dalam kunci objek. Selain itu, Macie menerapkan suatu syarat untuk menyelesaikan nilai Kunci untuk sebuah objek, termasuk nama file objek.

Misalnya, jika kunci objek adalah AWSLogs/eventlogs/testlog.csv dan Anda memasukkan salah satu nilai berikut untuk suatu kondisi, objek tersebut cocok dengan kriteria kondisi:

- **AWSLogs**

- **AWSLogs/event**
- **AWSLogs/eventlogs/**
- **AWSLogs/eventlogs/testlog**
- **AWSLogs/eventlogs/testlog.csv**

Namun, jika Anda masuk **eventlogs**, objek tidak cocok dengan kriteria—nilai kondisi tidak termasuk bagian pertama dari kunci,/. AWSLogs Demikian pula, jika Anda masuk **awslogs**, objek tidak cocok dengan kriteria karena perbedaan kapitalisasi.

## Ukuran penyimpanan

Hal ini berkorelasi dengan bidang Ukuran di Amazon S3. Di Amazon S3, bidang ini menunjukkan ukuran penyimpanan total objek S3. Jika objek adalah file terkompresi, nilai ini tidak mencerminkan ukuran sebenarnya dari file setelah didekompresi.

Anda dapat menggunakan tipe syarat ini menyertakan atau mengecualikan objek yang lebih kecil dari ukuran tertentu, lebih besar dari ukuran tertentu, atau jatuh dalam kisaran ukuran tertentu. Macie menerapkan tipe syarat ini untuk semua tipe objek, termasuk file terkompresi atau arsip dan file yang dikandungnya. Untuk informasi tentang pembatasan berbasis ukuran untuk setiap format yang didukung, lihat [Kuota Amazon Macie](#).

## Tag

Tag yang terkait dengan objek S3. Tag adalah label yang dapat Anda tentukan dan tetapkan ke jenis AWS sumber daya tertentu, termasuk objek S3. Setiap tanda terdiri dari kunci tanda yang diperlukan dan nilai tanda opsional. Untuk informasi tentang penandaan objek S3, lihat [Mengategorikan penyimpanan Anda menggunakan tanda](#) di Panduan Pengguna Amazon Simple Storage Service.

Untuk tugas penemuan data sensitif, Anda dapat menggunakan tipe syarat ini untuk menyertakan atau mengecualikan objek yang memiliki tanda tertentu. Ini bisa menjadi kunci tanda tertentu atau kunci tanda dan nilai tanda tertentu (sebagai pasangan). Jika Anda memasukkan beberapa tanda sebagai nilai untuk suatu syarat, Macie menggunakan logika OR untuk menggabungkan nilai tersebut. Misalnya, jika Anda menentukan **Project1** dan **Project2** sebagai kunci tag untuk suatu kondisi, objek apa pun yang memiliki kunci tag Project1 atau Project2 cocok dengan kriteria kondisi.

Perhatikan bahwa kunci dan nilai tanda sensitif huruf besar dan kecil. Selain itu, Macie tidak mendukung penggunaan nilai parsial atau karakter wildcard di tipe syarat ini.

## Membuat tugas penemuan data sensitif

Dengan Amazon Macie, Anda dapat membuat dan menjalankan pekerjaan penemuan data sensitif untuk mengotomatiskan penemuan, pencatatan, dan pelaporan data sensitif di bucket Amazon Simple Storage Service (Amazon S3). Pekerjaan penemuan data sensitif adalah serangkaian tugas pemrosesan dan analisis otomatis yang dilakukan Macie untuk mendeteksi dan melaporkan data sensitif di objek Amazon S3. Saat analisis berlangsung, Macie memberikan laporan terperinci tentang data sensitif yang ditemukannya dan analisis yang dilakukannya: temuan data sensitif, yang melaporkan data sensitif yang ditemukan Macie di objek S3 individu, dan hasil penemuan data sensitif, yang mencatat detail tentang analisis objek S3 individu. Untuk informasi selengkapnya, lihat [Meninjau statistik dan hasil tugas](#).

Saat membuat pekerjaan, Anda mulai dengan menentukan bucket S3 mana yang berisi objek yang ingin dianalisis Macie saat pekerjaan berjalan — bucket khusus yang Anda pilih atau bucket yang cocok dengan kriteria tertentu. Kemudian Anda menentukan seberapa sering untuk menjalankan tugas—sekali, atau secara berkala setiap hari, mingguan, atau bulanan. Anda juga dapat memilih opsi untuk menyempurnakan ruang lingkup analisis pekerjaan. Opsi termasuk kriteria kustom yang berasal dari properti objek S3, seperti tag, awalan, dan ketika objek terakhir dimodifikasi.

Setelah menentukan jadwal dan cakupan pekerjaan, Anda menentukan pengidentifikasi data terkelola dan pengidentifikasi data kustom yang ingin digunakan oleh pekerjaan tersebut:

- Pengidentifikasi data terkelola adalah seperangkat kriteria dan teknik bawaan yang dirancang untuk mendeteksi jenis data sensitif tertentu — misalnya, nomor kartu kredit, kunci akses AWS rahasia, atau nomor paspor untuk negara atau wilayah tertentu. Pengidentifikasi ini dapat mendeteksi daftar tipe data sensitif yang besar dan terus bertambah untuk banyak negara dan wilayah, termasuk beberapa jenis data kredensial, informasi keuangan, dan informasi identitas pribadi (PII). Untuk informasi selengkapnya, lihat [Menggunakan pengidentifikasi data terkelola](#).
- Pengidentifikasi data kustom adalah set kriteria yang Anda tetapkan untuk mendeteksi data sensitif. Dengan pengenalan data khusus, Anda dapat mendeteksi data sensitif yang mencerminkan skenario, kekayaan intelektual, atau data hak milik organisasi Anda—misalnya, ID karyawan, nomor akun pelanggan, atau klasifikasi data internal. Anda dapat melengkapi pengidentifikasi data terkelola yang disediakan Macie. Untuk informasi selengkapnya, lihat [Membangun pengidentifikasi data kustom](#).

Anda kemudian secara opsional memilih daftar izinkan yang Anda inginkan untuk digunakan oleh pekerjaan itu. Daftar izin menentukan teks atau pola teks yang ingin diabaikan oleh Macie, biasanya

pengecualian data sensitif untuk skenario atau lingkungan tertentu Anda—misalnya, nama publik atau nomor telepon untuk organisasi Anda, atau data sampel yang digunakan organisasi Anda untuk pengujian. Untuk informasi selengkapnya, lihat [Mendefinisikan pengecualian data sensitif dengan daftar izinkan](#).

Ketika Anda selesai memilih opsi ini, Anda siap untuk memasukkan pengaturan umum untuk pekerjaan, seperti nama dan deskripsi pekerjaan. Anda kemudian dapat meninjau dan menyimpan pekerjaan.

## Tugas

- [Sebelum Anda memulai](#)
- [Langkah 1: Pilih bucket S3](#)
- [Langkah 2: Tinjau pilihan atau kriteria bucket S3 Anda](#)
- [Langkah 3: Tentukan jadwal dan perbaiki ruang lingkup](#)
- [Langkah 4: Pilih pengidentifikasi data terkelola](#)
- [Langkah 5: Pilih pengidentifikasi data khusus](#)
- [Langkah 6: Pilih daftar izinkan](#)
- [Langkah 7: Masukkan pengaturan umum](#)
- [Langkah 8: Tinjau dan buat](#)

## Sebelum Anda memulai

Sebelum membuat tugas, sebaiknya lakukan langkah-langkah berikut:

- Verifikasi bahwa Anda mengonfigurasi Macie untuk menyimpan hasil penemuan data sensitif Anda di bucket S3. Untuk melakukannya, pilih Hasil penemuan di panel navigasi di konsol Amazon Macie. Kemudian verifikasi bahwa Anda memasuki pengaturan. Untuk mempelajari tentang pengaturan ini, lihat [Menyimpan dan mempertahankan hasil penemuan data sensitif](#).
- Buat pengidentifikasi data kustom apa pun yang Anda ingin untuk digunakan tugas. Untuk mempelajari caranya, lihat [Membangun pengidentifikasi data kustom](#).
- Buat daftar izinkan apa pun yang Anda inginkan untuk digunakan oleh pekerjaan itu. Untuk mempelajari caranya, lihat [Membuat dan mengelola daftar izinkan](#).
- Jika Anda ingin menganalisis objek S3 yang dienkripsi, pastikan Macie dapat mengakses dan menggunakan kunci enkripsi yang sesuai. Untuk informasi selengkapnya, lihat [Menganalisis objek S3 terenkripsi](#).

- Jika Anda ingin menganalisis objek dalam bucket S3 yang memiliki kebijakan bucket restriktif, pastikan Macie diizinkan mengakses objek. Untuk informasi selengkapnya, lihat [Mengizinkan Macie untuk mengakses bucket S3 dan objek](#).

Jika Anda melakukan hal-hal ini sebelum Anda membuat pekerjaan, Anda merampingkan penciptaan pekerjaan dan membantu memastikan bahwa pekerjaan dapat menganalisis data yang Anda inginkan.

## Langkah 1: Pilih bucket S3

Langkah pertama dalam membuat pekerjaan adalah menentukan bucket S3 mana yang berisi objek yang ingin Anda analisis Macie saat pekerjaan berjalan. Anda memiliki dua pilihan untuk melakukan hal ini:

- Pilih bucket tertentu — Dengan opsi ini, Anda secara eksplisit memilih setiap bucket S3 yang ingin dianalisis oleh pekerjaan. Kemudian, ketika tugas berjalan, tugas tersebut hanya menganalisis objek di bucket yang dipilih.
- Tentukan kriteria bucket — Dengan opsi ini, Anda menentukan kriteria runtime yang menentukan bucket S3 mana yang dianalisis pekerjaan. Kriteria tersebut terdiri dari satu syarat atau lebih yang berasal dari properti bucket. Lalu, ketika tugas berjalan, tugas mengidentifikasi bucket yang sesuai dengan kriteria Anda dan menganalisis objek di bucket tersebut.

Untuk informasi detail tentang opsi ini, lihat [Opsi ruang lingkup untuk tugas](#).

Bagian berikut memberikan instruksi untuk memilih dan mengkonfigurasi setiap opsi. Pilih bagian untuk opsi yang Anda inginkan.

### Pilih bucket tertentu

Jika Anda memilih untuk secara eksplisit memilih setiap bucket S3 yang ingin dianalisis oleh pekerjaan, Macie memberi Anda inventaris lengkap bucket Anda saat ini. Wilayah AWS Anda kemudian dapat menggunakan inventaris ini untuk memilih satu bucket atau lebih untuk dianalisis tugas. Untuk mempelajari tentang inventaris ini, lihat [Memilih ember S3 tertentu](#).

Jika Anda administrator Macie untuk suatu organisasi, inventaris mencakup bucket yang dimiliki oleh akun anggota di organisasi Anda. Anda dapat mengonfigurasi tugas untuk menganalisis objek dalam sebanyak 1.000 bucket ini, mencakup sebanyak 1.000 akun.

## Memilih bucket tertentu untuk tugas

1. [Buka konsol Amazon Macie di https://console.aws.amazon.com/macie/](https://console.aws.amazon.com/macie/).
2. Di panel navigasi, pilih Tugas.
3. Pilih Buat tugas.
4. Pada halaman Pilih bucket S3, pilih Pilih bucket tertentu. Macie menampilkan tabel semua bucket untuk akun Anda di Wilayah saat ini.
5. Di bagian Select S3 bucket, pilih refresh



secara opsional untuk mengambil metadata bucket terbaru dari Amazon S3.

Jika ikon informasi



muncul di samping nama bucket, kami rekomendasikan Anda untuk melakukan hal ini. Ikon informasi menunjukkan bahwa bucket dibuat selama 24 jam terakhir, mungkin setelah Macie terakhir mengambil bucket dan metadata objek dari Amazon S3 sebagai bagian dari [siklus penyegaran harian](#).

6. Pada tabel, beri tanda centang pada kotak centang untuk setiap bucket yang Anda ingin untuk dianalisis tugas.

### Tip

- Untuk menemukan bucket tertentu dengan lebih mudah, masukkan kriteria filter di kotak filter di atas tabel. Anda dapat mengurutkan tabel dengan memilih judul kolom.
- Untuk menentukan apakah Anda sudah mengonfigurasi pekerjaan untuk menganalisis objek secara berkala dalam ember, lihat bidang Dipantau berdasarkan pekerjaan. Jika Ya muncul di bidang, bucket secara eksplisit disertakan dalam pekerjaan periodik atau bucket cocok dengan kriteria untuk pekerjaan periodik dalam 24 jam terakhir. Selain itu, status dari setidaknya salah satu tugas tersebut tidak Dibatalkan. Macie memperbarui data ini setiap hari.
- Untuk menentukan kapan pekerjaan periodik atau satu kali yang ada baru-baru ini menganalisis objek dalam ember, lihat bidang pekerjaan terbaru. Untuk informasi tambahan tentang tugas tersebut, lihat detail bucket.
- Untuk menampilkan detail bucket, pilih nama bucket. Selain informasi terkait tugas, panel detail menyediakan statistik dan informasi lain tentang bucket, seperti

pengaturan akses publik bucket. Untuk mempelajari selengkapnya tentang Data ini, lihat [Meninjau inventaris bucket S3 Anda](#).

7. Setelah selesai memilih bucket, pilih Selanjutnya.

Pada langkah berikutnya, Anda akan meninjau dan memverifikasi pilihan Anda.

menentukan kriteria bucket

Jika Anda memilih untuk menentukan kriteria runtime yang menentukan bucket S3 mana yang dianalisis pekerjaan, Macie menyediakan opsi untuk membantu Anda memilih bidang, operator, dan nilai untuk kondisi individual dalam kriteria. Untuk mempelajari selengkapnya tentang opsi ini, lihat [Menentukan kriteria bucket S3](#).

Untuk menentukan kriteria bucket untuk tugas

1. [Buka konsol Amazon Macie di https://console.aws.amazon.com/macie/](https://console.aws.amazon.com/macie/).
2. Di panel navigasi, pilih Tugas.
3. Pilih Buat tugas.
4. Pada halaman Pilih bucket S3, pilih Tentukan kriteria bucket.
5. Di bawah Tentukan kriteria bucket, lakukan hal berikut untuk menambahkan syarat pada kriteria:
  - a. Tempatkan kursor Anda di kotak filter, lalu pilih properti bucket yang akan digunakan untuk kondisi tersebut.
  - b. Di kotak pertama, pilih operator untuk kondisi, Sama atau Tidak sama.
  - c. Di kotak berikutnya, masukkan satu atau lebih nilai untuk properti.

Tergantung pada tipe dan sifat dari properti bucket, Macie menampilkan opsi yang berbeda untuk memasukkan nilai. Misalnya, jika Anda memilih properti Izin efektif, Macie menampilkan daftar nilai yang akan dipilih. Jika Anda memilih properti Account ID, Macie menampilkan kotak teks di mana Anda dapat memasukkan satu atau beberapa Akun AWS ID. Untuk memasukkan beberapa nilai dalam kotak teks, masukkan setiap nilai dan pisahkan setiap entri dengan koma.

- d. Pilih Apply (Terapkan). Macie menambahkan kondisi dan menampilkannya di bawah kotak filter.



Secara default, Macie menambahkan syarat dengan menyertakan pernyataan. Ini berarti bahwa tugas dikonfigurasi untuk menganalisis (termasuk) objek di bucket yang cocok dengan syarat tersebut. Untuk melewati (mengecualikan) bucket yang cocok dengan kondisi, pilih Sertakan untuk kondisi, lalu pilih Kecualikan.

- e. Ulangi langkah sebelumnya untuk setiap syarat tambahan yang ingin Anda tambahkan.
6. Untuk menguji kriteria Anda, perluas bagian Pratinjau hasil kriteria. Bagian ini menampilkan tabel semua bucket yang saat ini cocok dengan kriteria.
7. Untuk memperbaiki kriteria Anda, lakukan salah satu hal berikut:
  - Untuk menghapus suatu kondisi, pilih X untuk kondisi tersebut.
  - Untuk mengubah suatu kondisi, hapus kondisi dengan memilih X untuk kondisi tersebut. Kemudian tambahkan syarat yang memiliki pengaturan yang benar.
  - Untuk menghapus semua syarat, pilih Hapus filter.

Macie memperbarui tabel hasil kriteria untuk menunjukkan perubahan Anda.

8. Setelah selesai menentukan kriteria bucket, pilih Selanjutnya.

Pada langkah berikutnya, Anda akan meninjau dan memverifikasi kriteria Anda.

## Langkah 2: Tinjau pilihan atau kriteria bucket S3 Anda

Untuk langkah ini, verifikasi bahwa Anda memilih pengaturan yang benar pada langkah sebelumnya:

- Tinjau pilihan bucket Anda - Jika Anda memilih bucket S3 tertentu untuk pekerjaan itu, tinjau tabel bucket dan ubah pilihan bucket Anda seperlunya. Tabel ini memberikan wawasan ke dalam ruang lingkup dan biaya analisis tugas yang diproyeksikan. Data didasarkan pada ukuran dan tipe objek yang saat ini disimpan di bucket.

Dalam tabel, bidang Estimasi biaya menunjukkan total perkiraan biaya (dalam Dolar AS) untuk menganalisis objek dalam ember S3. Setiap perkiraan menunjukkan jumlah data terkompresi yang diproyeksikan yang akan dianalisis tugas di bucket. Jika setiap objek adalah file terkompresi atau arsip, perkiraan mengasumsikan bahwa file menggunakan rasio kompresi 3:1 dan tugas dapat menganalisis semua file yang diekstraksi. Untuk informasi selengkapnya, lihat [Biaya tugas prakiraan dan pemantauan](#).

- Tinjau kriteria bucket Anda - Jika Anda menentukan kriteria bucket untuk pekerjaan tersebut, tinjau setiap kondisi dalam kriteria. Untuk mengubah kriteria, pilih Sebelumnya, lalu gunakan opsi

filter pada langkah sebelumnya untuk memasukkan kriteria yang benar. Setelah selesai, pilih **Selanjutnya**.

Setelah selesai meninjau dan memverifikasi pengaturan, pilih **Selanjutnya**.

### Langkah 3: Tentukan jadwal dan perbaiki ruang lingkup

Untuk langkah ini, tentukan seberapa sering Anda ingin tugas berjalan—sekali, atau secara berkala setiap hari, mingguan, atau bulanan. Anda juga dapat memilih berbagai opsi untuk menyempurnakan ruang lingkup analisis tugas. Untuk mempelajari tentang opsi ini, lihat [Opsi ruang lingkup untuk tugas](#).

Untuk menentukan jadwal dan menyempurnakan ruang lingkup tugas

1. Pada halaman **Perbaiki cakupan**, tentukan seberapa sering Anda ingin pekerjaan dijalankan:
  - Untuk menjalankan tugas hanya sekali, segera setelah Anda selesai membuatnya, pilih **Tugas satu kali**.
  - Untuk menjalankan tugas secara berkala dan secara berulang, pilih **Tugas terjadwal**. Untuk **Frekuensi pembaruan**, pilih apakah akan menjalankan tugas setiap hari, mingguan, atau bulanan. Kemudian gunakan opsi **Sertakan objek yang ada** untuk menentukan ruang lingkup tugas pertama yang dijalankan:
    - Berikan tanda centang pada kotak centang untuk menganalisis semua objek yang ada segera setelah Anda selesai membuat tugas. Setiap pelaksanaan selanjutnya secara otomatis hanya menganalisis objek yang dibuat atau diubah setelah pelaksanaan sebelumnya.
    - Hapus tanda centang pada kotak centang ini untuk melewati analisis semua objek yang ada. Tugas pertama yang dijalankan hanya menganalisis objek yang dibuat atau diubah setelah Anda selesai membuat tugas dan sebelum tugas pertama dijalankan. Setiap pelaksanaan selanjutnya hanya menganalisis objek yang dibuat atau diubah setelah pelaksanaan sebelumnya.

Menghapus centang pada kotak centang ini sangat membantu untuk kasus saat Anda telah menganalisis data dan ingin terus menganalisisnya secara berkala. Misalnya, jika sebelumnya Anda menggunakan layanan atau aplikasi lain untuk mengklasifikasikan data dan Anda baru saja mulai menggunakan Macie, Anda dapat menggunakan opsi ini untuk memastikan penemuan dan klasifikasi data Anda yang berkelanjutan tanpa menimbulkan biaya yang tidak perlu atau menduplikasi data klasifikasi.

2. (Opsional) Untuk menentukan persentase objek yang Anda ingin untuk dianalisis tugas, masukkan persentase di kotak Kedalaman pengambilan sampel.

Jika nilai ini kurang dari 100%, Macie memilih objek untuk dianalisis secara acak, hingga persentase yang ditentukan, dan menganalisis semua data dalam objek tersebut. Nilai defaultnya adalah 100%.

3. (Opsional) Untuk menambahkan kriteria tertentu yang menentukan objek S3 yang disertakan atau dikecualikan dari analisis tugas, perluas bagian Pengaturan tambahan, lalu masukkan kriteria. Kriteria ini terdiri dari kondisi individu yang berasal dari properti objek:
  - Untuk menganalisis (sertakan) objek yang memenuhi syarat tertentu, masukkan tipe dan nilai syarat, lalu pilih sertakan.
  - Untuk melewati (kecualikan) objek yang memenuhi syarat tertentu, masukkan tipe dan nilai syarat, lalu pilih kecualikan.

Ulangi langkah ini untuk setiap syarat penyertaan dan pengecualian yang Anda inginkan.

Jika Anda memasukkan beberapa kondisi, kondisi pengecualian apa pun lebih diutamakan daripada kondisi termasuk. Misalnya, jika Anda menyertakan objek yang memiliki ekstensi nama file .pdf dan mengecualikan objek yang lebih besar dari 5 MB, tugas menganalisis setiap objek yang memiliki ekstensi nama file .pdf, kecuali objek lebih besar dari 5 MB.

4. Setelah selesai, pilih Selanjutnya.

## Langkah 4: Pilih pengidentifikasi data terkelola

Untuk langkah ini, tentukan pengidentifikasi data terkelola mana yang ingin digunakan pekerjaan saat menganalisis objek S3. Anda memiliki dua opsi:

- Gunakan pengaturan yang disarankan - Dengan opsi ini, pekerjaan menganalisis objek S3 dengan menggunakan kumpulan pengidentifikasi data terkelola yang kami rekomendasikan untuk pekerjaan. Set ini dirancang untuk mendeteksi kategori umum dan jenis data sensitif. Untuk meninjau daftar pengidentifikasi data terkelola yang saat ini ada di set, lihat [Pengidentifikasi data terkelola direkomendasikan untuk pekerjaan](#). Kami memperbarui daftar itu setiap kali kami menambahkan atau menghapus pengenalan data terkelola dari set.
- Gunakan pengaturan khusus - Dengan opsi ini, pekerjaan menganalisis objek S3 dengan menggunakan pengidentifikasi data terkelola yang Anda pilih. Ini bisa menjadi semua atau hanya beberapa pengidentifikasi data terkelola yang saat ini tersedia. Anda juga dapat mengonfigurasi

pekerjaan untuk tidak menggunakan pengidentifikasi data terkelola apa pun. Pekerjaan hanya dapat menggunakan pengidentifikasi data khusus yang Anda pilih di langkah berikutnya. Untuk meninjau daftar pengidentifikasi data terkelola yang saat ini tersedia, lihat [Referensi cepat: Pengidentifikasi data terkelola Amazon Macie](#). Kami memperbarui daftar itu setiap kali kami merilis pengenalan data terkelola baru.

Saat Anda memilih salah satu opsi, Macie menampilkan tabel pengidentifikasi data terkelola. Dalam tabel, bidang Tipe data sensitif menentukan pengenalan unik (ID) untuk pengenalan data terkelola. ID ini menjelaskan jenis data sensitif yang dirancang untuk dideteksi oleh pengenalan data terkelola, misalnya: USA\_PASSPORT\_NUMBER untuk nomor paspor AS, CREDIT\_CARD\_NUMBER untuk nomor kartu kredit, dan PGP\_PRIVATE\_KEY untuk kunci pribadi PGP. Untuk menemukan pengidentifikasi tertentu dengan lebih cepat, Anda dapat mengurutkan dan memfilter tabel berdasarkan kategori atau jenis data sensitif.

Untuk memilih pengidentifikasi data terkelola untuk pekerjaan

1. Pada halaman Pilih pengidentifikasi data terkelola, di bawah opsi pengenalan data terkelola, lakukan salah satu hal berikut:
  - Untuk menggunakan kumpulan pengidentifikasi data terkelola yang kami rekomendasikan untuk pekerjaan, pilih Direkomendasikan.

Jika Anda memilih opsi ini dan Anda mengonfigurasi pekerjaan untuk dijalankan lebih dari sekali, setiap proses secara otomatis menggunakan semua pengidentifikasi data terkelola yang ada di set yang disarankan saat proses dimulai. Ini termasuk pengidentifikasi data terkelola baru yang kami rilis dan tambahkan ke set. Ini tidak termasuk pengidentifikasi data terkelola yang kami hapus dari set dan tidak lagi merekomendasikan untuk pekerjaan.

- Untuk hanya menggunakan pengidentifikasi data terkelola tertentu yang Anda pilih, pilih Kustom, lalu pilih Gunakan pengidentifikasi data terkelola tertentu. Kemudian, dalam tabel, pilih kotak centang untuk setiap pengidentifikasi data terkelola yang Anda inginkan untuk digunakan oleh pekerjaan tersebut.

Jika Anda memilih opsi ini dan Anda mengonfigurasi pekerjaan untuk dijalankan lebih dari sekali, setiap proses hanya menggunakan pengidentifikasi data terkelola yang Anda pilih. Dengan kata lain, pekerjaan menggunakan pengidentifikasi data terkelola yang sama ini setiap kali dijalankan.

- Untuk menggunakan semua pengidentifikasi data terkelola yang disediakan Macie saat ini, pilih Kustom, lalu pilih Gunakan pengidentifikasi data terkelola tertentu. Kemudian, di tabel, pilih kotak centang di judul kolom pilihan untuk memilih semua baris.

Jika Anda memilih opsi ini dan Anda mengonfigurasi pekerjaan untuk dijalankan lebih dari sekali, setiap proses hanya menggunakan pengidentifikasi data terkelola yang Anda pilih. Dengan kata lain, pekerjaan menggunakan pengidentifikasi data terkelola yang sama ini setiap kali dijalankan.

- Untuk tidak menggunakan pengidentifikasi data terkelola dan hanya menggunakan pengidentifikasi data kustom, pilih Kustom, lalu pilih Jangan gunakan pengidentifikasi data terkelola apa pun. Kemudian, pada langkah berikutnya, pilih pengidentifikasi data khusus yang akan digunakan.

2. Setelah selesai, pilih Selanjutnya.

## Langkah 5: Pilih pengidentifikasi data khusus

Untuk langkah ini, pilih pengidentifikasi data kustom apa pun yang ingin digunakan pekerjaan saat menganalisis objek S3. Pekerjaan akan menggunakan pengidentifikasi yang dipilih selain pengidentifikasi data terkelola yang Anda konfigurasi pekerjaan yang akan digunakan. Untuk mempelajari lebih lanjut tentang pengenalan data kustom, lihat [Membangun pengidentifikasi data kustom](#).

Cara memilih pengidentifikasi data kustom untuk tugas

1. Pada halaman Pilih pengidentifikasi data kustom, beri tanda centang pada kotak centang untuk setiap pengenalan data kustom yang Anda ingin untuk digunakan tugas. Anda dapat memilih sebanyak 30 pengidentifikasi data kustom.

### Tip

Untuk meninjau atau menguji pengaturan untuk pengenalan data kustom sebelum Anda memilihnya, pilih ikon tautan



di sebelah nama pengenalan. Macie membuka halaman yang menampilkan pengaturan pengidentifikasi.

Anda juga dapat menggunakan halaman ini untuk menguji pengidentifikasi dengan data sampel. Untuk melakukan ini, masukkan hingga 1.000 karakter teks di kotak Data

sampel, lalu pilih Uji. Macie mengevaluasi data sampel dengan menggunakan pengenalan, dan kemudian melaporkan jumlah kecocokan.

2. Setelah selesai memilih pengidentifikasi data kustom, pilih Selanjutnya.


## Langkah 6: Pilih daftar izinkan

Untuk langkah ini, pilih daftar izinkan yang Anda inginkan untuk digunakan saat menganalisis objek S3. Untuk mempelajari lebih lanjut tentang daftar izinkan, lihat [Mendefinisikan pengecualian data sensitif dengan daftar izinkan](#).

Untuk memilih daftar izinkan untuk pekerjaan

1. Pada halaman Pilih izinkan daftar, pilih kotak centang untuk setiap daftar izinkan yang Anda inginkan untuk digunakan oleh pekerjaan tersebut. Anda dapat memilih sebanyak 10 daftar.

### Tip

Untuk meninjau pengaturan daftar izinkan sebelum Anda memilihnya, pilih ikon tautan () di sebelah nama daftar. Macie membuka halaman yang menampilkan pengaturan daftar. Jika daftar menentukan ekspresi reguler (regex), Anda juga dapat menggunakan halaman ini untuk menguji regex dengan data sampel. Untuk melakukan ini, masukkan hingga 1.000 karakter teks di kotak Data sampel, lalu pilih Uji. Macie mengevaluasi data sampel dengan menggunakan regex, dan kemudian melaporkan jumlah kecocokan.

2. Setelah selesai memilih daftar izinkan, pilih Berikutnya.

## Langkah 7: Masukkan pengaturan umum

Untuk langkah ini, tentukan nama dan, secara opsional, deskripsi pekerjaan.

Anda juga dapat menetapkan tag untuk pekerjaan. Tag adalah label yang Anda tentukan dan tetapkan ke jenis AWS sumber daya tertentu. Setiap tanda terdiri dari kunci tanda yang diperlukan dan nilai tanda opsional. Tag dapat membantu Anda mengidentifikasi, mengkategorikan, dan mengelola sumber daya dengan cara yang berbeda, seperti berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Untuk mempelajari selengkapnya, lihat [Menandai sumber daya Amazon Macie](#).

Untuk memasukkan pengaturan umum untuk pekerjaan

1. Pada halaman Masukkan pengaturan umum, masukkan nama untuk pekerjaan di kotak Nama Job. Nama dapat berisi sebanyak 500 karakter.
2. (Opsional) Untuk Deskripsi tugas, masukkan deskripsi singkat tentang grup keamanan. Deskripsi dapat berisi sebanyak 200 karakter.
3. (Opsional) Untuk Tag, pilih Tambahkan tag, lalu masukkan sebanyak 50 tag untuk ditetapkan ke pekerjaan.
4. Setelah selesai, pilih Selanjutnya.

## Langkah 8: Tinjau dan buat

Untuk langkah terakhir ini, tinjau pengaturan konfigurasi pekerjaan dan verifikasi bahwa pengaturannya benar. Ini adalah langkah yang penting. Setelah Anda membuat pekerjaan, Anda tidak dapat mengubah pengaturan ini. Hal ini membantu memastikan bahwa Anda memiliki riwayat tetap akan temuan dan hasil penemuan data sensitif untuk audit atau investigasi privasi dan perlindungan data yang Anda lakukan.

Tergantung pada pengaturan tugas, Anda juga dapat meninjau total estimasi biaya (dalam Dolar AS) dari menjalankan tugas satu kali. Jika Anda memilih bucket S3 tertentu untuk tugas tersebut, perkiraannya didasarkan pada ukuran dan tipe objek di bucket yang Anda pilih, dan berapa banyak data yang dapat dianalisis tugas. Jika Anda menentukan kriteria bucket untuk tugas tersebut, perkiraannya didasarkan pada ukuran dan tipe objek di sebanyak 500 bucket yang saat ini sesuai dengan kriteria, dan berapa banyak data yang dapat dianalisis tugas. Untuk mempelajari tentang perkiraan ini, lihat [Biaya tugas prakiraan dan pemantauan](#).

Untuk meninjau dan membuat tugas

1. Pada halaman Tinjau dan buat, tinjau setiap pengaturan dan verifikasi bahwa pengaturan sudah benar. Untuk mengubah pengaturan, pilih Edit di bagian yang berisi pengaturan, lalu masukkan pengaturan yang benar. Anda juga dapat menggunakan tab navigasi untuk membuka halaman yang berisi pengaturan.
2. Setelah selesai memverifikasi pengaturan, pilih Kirim untuk membuat dan menyimpan tugas. Macie memeriksa pengaturan dan memberi tahu Anda tentang masalah apa pun yang harus diatasi.

**Note**

Jika Anda belum mengonfigurasi repositori untuk hasil penemuan data sensitif, Macie menampilkan peringatan dan tidak menyimpan tugas tersebut. Untuk mengatasi masalah ini, pilih Konfigurasi di bagian Repositori untuk hasil penemuan data sensitif. Kemudian masukkan pengaturan konfigurasi untuk repositori. Untuk mempelajari caranya, lihat [Menyimpan dan mempertahankan hasil penemuan data sensitif](#). Setelah Anda memasukkan pengaturan, kembali ke halaman Tinjau dan buat lalu pilih refresh



di bagian Repositori untuk hasil penemuan data sensitif pada halaman.

Meskipun kami tidak merekomendasikan hal ini, Anda sementara dapat membatalkan persyaratan repositori dan menyimpan tugas. Jika Anda melakukan ini, Anda berisiko kehilangan hasil penemuan tugas—Macie akan mempertahankan hasilnya hanya selama 90 hari. Untuk sementara membatalkan persyaratan, beri tanda centang pada kotak centang untuk opsi batalkan.

3. Jika Macie memberi tahu Anda tentang masalah yang harus diatasi, atasi masalah, lalu pilih Kirim lagi untuk membuat dan menyimpan pekerjaan.

Jika Anda mengonfigurasi tugas untuk berjalan sekali, setiap hari, atau pada hari tertentu dalam seminggu atau sebulan, Macie mulai menjalankan tugas segera setelah Anda menyimpannya. Jika tidak, Macie mempersiapkan untuk menjalankan tugas pada hari tertentu dalam seminggu atau sebulan. Untuk memantau tugas, Anda dapat [Periksa status tugas](#).

## Meninjau statistik dan hasil untuk pekerjaan penemuan data sensitif

Ketika Anda menjalankan tugas penemuan data sensitif, Amazon Macie secara otomatis menghitung dan melaporkan data statistik tertentu untuk tugas tersebut. Misalnya, Macie melaporkan berapa kali pekerjaan telah berjalan dan perkiraan jumlah objek Amazon Simple Storage Service (Amazon S3) Simple Storage Service (Amazon S3) yang belum diproses oleh pekerjaan selama proses saat ini. Macie juga menghasilkan beberapa jenis hasil untuk pekerjaan: peristiwa log, temuan data sensitif, dan hasil penemuan data sensitif.

### Topik

- [Jenis hasil untuk pekerjaan penemuan data sensitif](#)
- [Meninjau statistik dan hasil untuk tugas penemuan data sensitif](#)



## Jenis hasil untuk pekerjaan penemuan data sensitif

Saat pekerjaan penemuan data sensitif berlangsung, Amazon Macie menghasilkan jenis hasil berikut untuk pekerjaan itu.

### Log peristiwa

Ini adalah catatan peristiwa yang terjadi saat tugas sedang berjalan. Macie secara otomatis mencatat dan menerbitkan data untuk peristiwa tertentu ke Amazon CloudWatch Logs. Data dalam log ini menyediakan catatan perubahan pada kemajuan atau status tugas, seperti tanggal dan waktu yang tepat ketika tugas mulai atau selesai berjalan. Data log juga menyediakan detail tentang kesalahan tingkat akun atau bucket yang terjadi saat tugas berjalan.

Log acara dapat membantu Anda memantau tugas dan mengatasi masalah apa pun yang mencegah tugas menganalisis data yang Anda inginkan. Jika pekerjaan menggunakan kriteria runtime untuk menentukan bucket S3 mana yang akan dianalisis, peristiwa log juga dapat membantu Anda menentukan apakah dan bucket S3 mana yang cocok dengan kriteria saat pekerjaan dijalankan.

Anda dapat mengakses peristiwa log menggunakan CloudWatch konsol Amazon atau Amazon CloudWatch Logs API. Untuk membantu Anda menavigasi ke log acara untuk tugas, konsol Amazon Macie menyediakan tautan ke log acara tersebut. Untuk informasi selengkapnya, lihat [Tugas pemantauan](#).

### Penemuan data sensitif

Ini adalah laporan data sensitif yang ditemukan Macie di objek S3. Setiap temuan memberikan peringkat kepelikan dan detail seperti:

- Tanggal dan waktu ketika Macie menemukan data sensitif.
- Kategori dan tipe data sensitif yang ditemukan Macie.
- Jumlah kejadian dari setiap tipe data sensitif yang Macie temukan.
- Pengidentifikasi unik untuk tugas yang menghasilkan temuan.
- Nama, pengaturan akses publik, tipe enkripsi, dan informasi lainnya tentang bucket S3 yang terpengaruh dan objek.

Bergantung pada jenis file atau format penyimpanan objek S3 yang terpengaruh, detailnya juga dapat mencakup lokasi sebanyak 15 kemunculan data sensitif yang ditemukan Macie. Untuk melaporkan data lokasi, temuan data sensitif menggunakan skema [JSON standar](#).

Temuan data sensitif tidak termasuk data sensitif yang ditemukan Macie. Sebaliknya, temuan ini menyediakan informasi yang dapat Anda gunakan untuk penyelidikan lebih lanjut dan remediasi sebagaimana diperlukan.

Macie menyimpan temuan data sensitif selama 90 hari. Anda dapat mengaksesnya dengan menggunakan konsol Amazon Macie atau Amazon Macie API. Anda juga dapat memantau dan memprosesnya menggunakan aplikasi, layanan, dan sistem lainnya. Untuk informasi selengkapnya, lihat [Menganalisis temuan](#).

## Hasil penemuan data sensitif

Ini adalah catatan yang mencatat detail tentang analisis objek S3. Macie secara otomatis membuat hasil penemuan data sensitif untuk setiap objek yang Anda konfigurasi pekerjaan untuk dianalisis. Ini termasuk objek yang Macie tidak menemukan data sensitif, dan karena itu tidak menghasilkan temuan data sensitif, dan objek yang tidak dapat dianalisis Macie karena kesalahan atau masalah seperti pengaturan izin atau penggunaan file atau format penyimpanan yang tidak didukung.

Jika Macie menemukan data sensitif dalam objek S3, hasil penemuan data sensitif mencakup data dari temuan data sensitif yang sesuai. Ini memberikan informasi tambahan juga, seperti lokasi tempat terjadinya 1.000 kejadian dari setiap tipe data sensitif yang Macie temukan dalam objek. Sebagai contoh:

- Nomor kolom dan baris untuk sel atau bidang di buku kerja Microsoft Excel, file CSV, atau file TSV
- Jalur ke bidang atau array dalam file JSON atau JSON Lines
- Nomor baris untuk baris dalam file teks non-biner selain file CSV, JSON, JSON Lines, atau TSV, misalnya, file HTML, TXT, atau XML
- Nomor halaman untuk halaman dalam file Format Dokumen Portabel Adobe (PDF)
- Indeks catatan dan jalur ke bidang dalam catatan di kontainer objek Apache Avro atau file Apache Parquet

Jika objek S3 yang terpengaruh adalah file arsip, seperti file.tar atau .zip, hasil penemuan data sensitif juga menyediakan data lokasi terperinci untuk kemunculan data sensitif dalam file individual yang diekstrak Macie dari arsip. Macie tidak menyertakan informasi ini dalam temuan data sensitif untuk file arsip. Untuk melaporkan data lokasi, hasil penemuan data sensitif menggunakan skema [JSON standar](#).

Hasil penemuan data sensitif tidak termasuk data sensitif yang ditemukan Macie. Sebagai gantinya, dokumen ini memberi Anda catatan analisis yang dapat membantu untuk audit privasi dan perlindungan data atau investigasi.

Macie menyimpan hasil penemuan data sensitif Anda selama 90 hari. Anda tidak dapat mengaksesnya langsung di konsol Amazon Macie atau dengan Amazon Macie API. Sebagai gantinya, Anda mengonfigurasi Macie untuk mengenkripsi dan menyimpannya dalam ember S3. Bucket dapat berfungsi sebagai repositori jangka panjang definitif untuk semua hasil penemuan data sensitif Anda. Anda kemudian dapat secara opsional mengakses dan menanyakan hasil di repositori itu. Untuk mempelajari cara mengonfigurasi pengaturan ini, lihat [Menyimpan dan mempertahankan hasil penemuan data sensitif](#).

Setelah Anda mengonfigurasi pengaturan, Macie menulis hasil penemuan data sensitif Anda ke file JSON Lines (.jsonl), dan mengenkripsi dan menambahkan file tersebut ke bucket S3 sebagai file GNU Zip (.gz). Untuk membantu Anda menavigasi ke hasil tersebut, konsol Amazon Macie menyediakan tautan ke hasil tersebut.

Temuan data sensitif dan hasil penemuan data sensitif keduanya mematuhi skema standar. Anda juga dapat secara opsional melakukan kueri, memantau dan memprosesnya menggunakan aplikasi, layanan, dan sistem lainnya.

#### Tip

Untuk contoh terperinci dan instruksional tentang bagaimana Anda dapat menanyakan dan menggunakan hasil penemuan data sensitif untuk menganalisis dan melaporkan potensi risiko keamanan data, lihat [Cara menanyakan dan memvisualisasikan hasil penemuan data sensitif Macie dengan posting QuickSight blog Amazon Athena dan Amazon](#) di Blog Keamanan. AWS

Untuk contoh kueri Amazon Athena yang dapat Anda gunakan untuk menganalisis hasil penemuan data sensitif, kunjungi repositori [Amazon Macie Results Analytics](#). GitHub Repositori ini juga menyediakan instruksi untuk mengkonfigurasi Athena untuk mengambil dan mendekripsi hasil Anda, dan skrip untuk membuat tabel untuk hasil.

## Meninjau statistik dan hasil untuk tugas penemuan data sensitif

Untuk meninjau statistik pemrosesan dan hasil untuk setiap pekerjaan penemuan data sensitif, Anda dapat menggunakan konsol Amazon Macie atau Amazon Macie API. Ikuti langkah-langkah ini untuk meninjau statistik dan hasil pekerjaan dengan menggunakan konsol.

Untuk mengakses statistik pemrosesan pekerjaan secara terprogram, gunakan [DescribeClassificationJob](#) pengoperasian Amazon Macie API. Untuk akses terprogram ke temuan yang dihasilkan oleh suatu pekerjaan, gunakan [ListFindings](#) pengoperasian Amazon Macie API dan tentukan pengenal unik pekerjaan dalam kondisi filter untuk bidang tersebut. `classificationDetails.jobId` Untuk mempelajari caranya, lihat [Membuat dan menerapkan filter untuk temuan](#). Anda kemudian dapat menggunakan [GetFindings](#) operasi untuk mengambil rincian temuan.

Untuk meninjau statistik dan hasil tugas

1. [Buka konsol Amazon Macie di https://console.aws.amazon.com/macie/](https://console.aws.amazon.com/macie/).
2. Di panel navigasi, pilih Tugas.
3. Pada halaman Tugas, pilih nama tugas yang statistik dan hasilnya ingin Anda tinjau. Panel detail menampilkan statistik, pengaturan, dan informasi lainnya tentang tugas.
4. Di panel detail, lakukan salah satu hal berikut:
  - Untuk meninjau statistik pemrosesan untuk tugas, lihat bagian panel Statistik. Bagian ini menampilkan statistik seperti berapa kali tugas telah berjalan dan perkiraan jumlah objek yang belum diproses oleh tugas selama menjalankannya.
  - Untuk meninjau peristiwa log untuk pekerjaan, pilih Tampilkan hasil di bagian atas panel, lalu pilih Tampilkan CloudWatch log. Macie membuka CloudWatch konsol Amazon dan menampilkan tabel peristiwa log yang diterbitkan Macie untuk pekerjaan itu.
  - Untuk meninjau semua temuan data sensitif yang dihasilkan tugas, pilih Tampilkan hasil di bagian atas panel, lalu pilih Tampilkan temuan. Macie membuka halaman Temuan dan menampilkan semua temuan dari tugas. Untuk meninjau detail temuan tertentu, pilih temuannya, lalu lihat panel detail.

### Tip

Di panel detail pencarian, Anda dapat menggunakan tautan di bidang Lokasi hasil terperinci untuk menavigasi ke hasil penemuan data sensitif terkait di Amazon S3:

- Jika temuan berlaku untuk arsip besar atau file terkompresi, tautan menampilkan folder yang berisi hasil penemuan untuk file. Arsip atau file terkompresi besar jika menghasilkan lebih dari 100 hasil penemuan.
  - Jika temuan berlaku untuk arsip atau file terkompresi kecil, tautan menampilkan file yang berisi hasil penemuan untuk file. Arsip atau file terkompresi kecil jika menghasilkan lebih dari 100 hasil penemuan.
  - Jika temuan berlaku untuk tipe file lain, tautan menampilkan file yang berisi hasil penemuan untuk file.
- Untuk meninjau semua hasil penemuan data sensitif yang dihasilkan tugas, pilih Tampilkan hasil di bagian atas panel, lalu pilih Tampilkan klasifikasi. Macie membuka konsol Amazon S3 dan menampilkan folder yang berisi semua hasil penemuan untuk tugas tersebut. Opsi ini hanya tersedia setelah Anda mengonfigurasi Macie ke [simpan hasil penemuan data sensitif](#) di bucket S3.

## Memantau pekerjaan penemuan data sensitif dengan Amazon CloudWatch Logs

Selain [memantau status keseluruhan](#) dari tugas penemuan data sensitif, Anda dapat memantau dan menganalisis peristiwa tertentu yang terjadi saat tugas berlangsung. Anda dapat melakukan ini dengan menggunakan data logging mendekati waktu nyata yang Amazon Macie terbitkan secara otomatis ke Amazon Logs. CloudWatch Data dalam log ini menyediakan catatan perubahan kemajuan atau status tugas, seperti tanggal dan waktu yang tepat ketika tugas mulai berjalan, dijeda, atau selesai berjalan.

Data log juga menyediakan detail tentang kesalahan tingkat akun atau bucket yang terjadi saat tugas berjalan. Sebagai contoh, jika pengaturan izin untuk bucket S3 mencegah tugas untuk menganalisis objek di bucket ember, maka Macie akan mencatat suatu peristiwa. Peristiwa tersebut menunjukkan ketika terjadi kesalahan, dan mengidentifikasi semua bucket yang terpengaruh dan akun yang memiliki bucket. Data untuk tipe peristiwa ini dapat membantu Anda mengidentifikasi, menyelidiki, dan mengatasi kesalahan yang mencegah Macie dari menganalisis data yang Anda inginkan.

Dengan Amazon CloudWatch Logs, Anda dapat memantau, menyimpan, dan mengakses file log dari beberapa sistem, aplikasi, dan Layanan AWS, termasuk Macie. Anda juga dapat menanyakan dan menganalisis data log, dan mengonfigurasi CloudWatch Log untuk memberi tahu Anda saat peristiwa tertentu terjadi atau ambang batas terpenuhi. CloudWatch Log juga menyediakan fitur untuk

pengarsipan data log dan mengekspor data ke Amazon S3. Untuk mempelajari lebih lanjut tentang CloudWatch Log, lihat [Panduan Pengguna Amazon CloudWatch Logs](#).

## Topik

- [Cara pencatatan bekerja untuk tugas penemuan data sensitif](#)
- [Meninjau log untuk tugas penemuan data sensitif](#)
- [Skema log acara untuk tugas penemuan data sensitif](#)
- [Tipe log acara untuk tugas penemuan data sensitif](#)

## Cara pencatatan bekerja untuk tugas penemuan data sensitif

Saat Anda mulai menjalankan pekerjaan penemuan data sensitif, Macie secara otomatis membuat dan mengonfigurasi sumber daya yang sesuai di Amazon CloudWatch Logs untuk mencatat peristiwa untuk semua pekerjaan Anda saat ini. Wilayah AWS Macie kemudian mempublikasikan data peristiwa ke sumber daya tersebut secara otomatis ketika tugas Anda berjalan. Kebijakan izin untuk [Peran yang terhubung dengan layanan](#) Macie untuk akun Anda memungkinkan Macie untuk melakukan tugas-tugas ini atas nama Anda. Anda tidak perlu mengambil langkah apa pun untuk membuat atau mengonfigurasi sumber daya di CloudWatch Log, atau mencatat data peristiwa untuk pekerjaan Anda.

Di CloudWatch Log, log diatur ke dalam grup log. Setiap grup log berisi pengaliran log. Setiap pengaliran log berisi log acara. Tujuan umum dari masing-masing sumber daya ini adalah sebagai berikut:

- Grup log adalah kumpulan pengaliran log yang berbagi pengaturan penyimpanan, pemantauan, dan kontrol akses yang sama—misalnya, pengumpulan log untuk semua tugas penemuan data sensitif Anda.
- Pengaliran log adalah urutan log acara yang berbagi sumber yang sama—misalnya, tugas penemuan data sensitif individu.
- Peristiwa log adalah catatan aktivitas yang dicatat oleh aplikasi atau sumber daya—misalnya, peristiwa individual yang dicatat dan dipublikasikan Macie untuk tugas penemuan data sensitif tertentu.

Macie mempublikasikan peristiwa untuk semua tugas penemuan data sensitif Anda ke satu grup log, dan setiap tugas memiliki pengaliran log unik di grup log tersebut. Grup log memiliki prefiks dan nama berikut:

```
/aws/macie/classificationjobs
```

Jika grup log ini sudah ada, Macie menggunakannya untuk menyimpan log acara untuk tugas Anda. Hal ini dapat membantu jika organisasi Anda menggunakan konfigurasi otomatis, seperti [AWS CloudFormation](#), untuk membuat grup log dengan periode retensi log yang telah ditentukan sebelumnya, pengaturan enkripsi, tanda, filter metrik, dan sebagainya untuk peristiwa tugas.

Jika grup log ini tidak ada, Macie membuatnya dengan pengaturan default yang digunakan CloudWatch Log untuk grup log baru. Pengaturan mencakup periode penyimpanan log Never Exire, yang berarti bahwa CloudWatch Log menyimpan log tanpa batas waktu. Untuk mengubah periode penyimpanan grup log, Anda dapat menggunakan CloudWatch konsol Amazon atau Amazon CloudWatch Logs API. Untuk mempelajari caranya, lihat [Bekerja dengan grup log dan aliran log](#) di Panduan Pengguna Amazon CloudWatch Logs.

Dalam grup log ini, Macie menciptakan pengaliran log unik untuk setiap tugas yang Anda jalankan, saat tugas berjalan untuk pertama kalinya. Nama pengaliran log merupakan pengidentifikasi unik untuk tugas, seperti `85a55dc0fa6ed0be5939d0408example`, dalam format berikut.

```
/aws/macie/classificationjobs/85a55dc0fa6ed0be5939d0408example
```

Setiap pengaliran log berisi semua log acara yang Macie catat dan publikasikan untuk tugas yang sesuai. Untuk tugas berkala, ini termasuk peristiwa untuk semua pelaksanaan tugas. Jika Anda menghapus pengaliran log untuk tugas berkala, Macie akan membuat pengaliran lagi pada waktu berikutnya saat tugas berjalan. Jika Anda menghapus pengaliran log untuk tugas satu kali, Anda tidak dapat memulihkannya.

Perhatikan bahwa pencatatan diaktifkan secara default untuk semua tugas Anda. Anda tidak dapat menonaktifkannya atau mencegah Macie memublikasikan peristiwa pekerjaan ke CloudWatch Log. Jika Anda tidak ingin menyimpan log, Anda dapat mengurangi retensi penyimpanan grup log menjadi paling sedikit satu hari. Pada akhir periode penyimpanan, CloudWatch Log secara otomatis menghapus data peristiwa kedaluwarsa dari grup log.

## Meninjau log untuk tugas penemuan data sensitif

Anda dapat meninjau log untuk pekerjaan penemuan data sensitif Anda dengan menggunakan CloudWatch konsol Amazon atau Amazon CloudWatch Logs API. Konsol tersebut dan API menyediakan fitur yang dirancang untuk membantu Anda meninjau dan menganalisis data log. Anda

dapat menggunakan fitur ini untuk bekerja dengan aliran log dan peristiwa untuk pekerjaan Anda karena Anda akan bekerja dengan jenis data log lainnya di CloudWatch Log.

Misalnya, Anda dapat mencari dan memfilter data kumpulan untuk mengidentifikasi tipe peristiwa tertentu yang terjadi untuk semua tugas Anda selama rentang waktu tertentu. Atau Anda dapat melakukan tinjauan yang ditargetkan dari semua peristiwa yang terjadi untuk pekerjaan tertentu. CloudWatch Log juga menyediakan opsi untuk memantau data log, menentukan filter metrik, dan membuat alarm khusus.


### Tip

Untuk menavigasi ke log acara untuk tugas tertentu dengan menggunakan konsol Amazon Macie, lakukan hal berikut: pada Tugas, pilih nama tugas. Di bagian atas panel detail, pilih Tampilkan hasil, lalu pilih Tampilkan CloudWatch log. Macie membuka CloudWatch konsol Amazon dan menampilkan tabel peristiwa log untuk pekerjaan itu.

Untuk meninjau log untuk pekerjaan Anda ( CloudWatch konsol Amazon)

1. Buka CloudWatch konsol di <https://console.aws.amazon.com/cloudwatch/>.
2. Dengan menggunakan pemilih Wilayah AWS di bagian atas kanan pada halaman, pilih Wilayah tempat Anda menjalankan tugas yang lognya ingin Anda tinjau.
3. Pada panel navigasi, pilih Log, lalu pilih Grup log.
4. Pada halaman Grup log, pilih grup log /aws/macie/classificationjobs. CloudWatch Log menampilkan tabel aliran log untuk pekerjaan yang telah Anda jalankan. Ada satu pengaliran unik untuk setiap tugas. Nama setiap pengaliran berkorelasi dengan pengidentifikasi unik untuk suatu tugas.
5. Di bawah Pengaliran log, lakukan salah satu langkah berikut:
  - Untuk meninjau log acara untuk tugas tertentu, pilih pengaliran log untuk tugas tersebut. Untuk menemukan aliran lebih mudah, masukkan pengenal unik pekerjaan di kotak filter di atas tabel. Setelah Anda memilih aliran CloudWatch log, Log menampilkan tabel peristiwa log untuk pekerjaan itu.
  - Untuk meninjau peristiwa log untuk semua pekerjaan Anda, pilih Cari semua aliran log. CloudWatch Log menampilkan tabel peristiwa log untuk semua pekerjaan Anda.



6. (Opsional) Pada kotak filter di atas tabel, masukkan istilah, frasa, atau nilai yang menentukan karakteristik peristiwa tertentu untuk ditinjau. Untuk informasi selengkapnya, lihat [Cari data log menggunakan pola filter](#) di Panduan Pengguna Amazon CloudWatch Logs.
7. Untuk meninjau detail peristiwa log tertentu, pilih panah kanan  di baris untuk acara tersebut. CloudWatch Log menampilkan rincian acara dalam format JSON.

Saat Anda membiasakan diri dengan data dalam peristiwa log, Anda juga dapat melakukan tugas seperti [membuat filter metrik](#) yang mengubah data log menjadi CloudWatch metrik numerik, dan [membuat alarm khusus](#) yang memudahkan Anda mengidentifikasi dan merespons peristiwa log tertentu. Untuk informasi selengkapnya, lihat [Panduan Pengguna Amazon CloudWatch Logs](#).

### Skema log acara untuk tugas penemuan data sensitif

Setiap peristiwa log untuk pekerjaan penemuan data sensitif adalah objek JSON yang sesuai dengan skema peristiwa Amazon CloudWatch Logs dan berisi kumpulan bidang standar. Beberapa tipe peristiwa memiliki bidang tambahan yang menyediakan informasi yang sangat berguna untuk tipe peristiwa tersebut. Misalnya, peristiwa untuk kesalahan tingkat akun menyertakan ID akun untuk yang terpengaruh. Akun AWS Peristiwa untuk kesalahan tingkat bucket termasuk nama bucket S3 yang terpengaruh. Untuk daftar detail acara pekerjaan yang dipublikasikan Macie ke CloudWatch Log, lihat [Tipe log acara untuk tugas](#)

Contoh berikut menunjukkan skema log acara untuk tugas penemuan data sensitif. Dalam contoh ini, peristiwa tersebut melaporkan bahwa Macie tidak mampu menganalisis objek apa pun di bucket S3 karena Amazon S3 menolak akses ke bucket.

```
{
  "adminAccountId": "123456789012",
  "jobId": "85a55dc0fa6ed0be5939d0408example",
  "eventType": "BUCKET_ACCESS_DENIED",
  "occurredAt": "2021-04-14T17:11:30.574809Z",
  "description": "Macie doesn't have permission to access the affected S3 bucket.",
  "jobName": "My_Macie_Job",
  "operation": "ListObjectsV2",
  "runDate": "2021-04-14T17:08:30.345809Z",
  "affectedAccount": "111122223333",
  "affectedResource": {
    "type": "S3_BUCKET_NAME",
    "value": "DOC-EXAMPLE-BUCKET"
  }
}
```

```
}
```

Pada contoh sebelumnya, Macie mencoba mencantumkan objek di bucket dengan menggunakan operasi [ListObjectsV2](#) dari Amazon S3 API. Ketika Macie mengirim permintaan ke Amazon S3, Amazon S3 menolak akses ke bucket.

Bidang berikut ini umum untuk semua log acara untuk tugas penemuan data sensitif:

- `adminAccountId`— Pengenal unik untuk Akun AWS yang menciptakan pekerjaan.
- `jobId`— Pengenal unik untuk pekerjaan itu.
- `eventTypeJenis` peristiwa yang terjadi. Untuk daftar lengkap dari nilai yang memungkinkan dan deskripsi masing-masing, lihat [Tipe log acara untuk tugas](#).
- `occurredAtTanggal` dan waktu, dalam Coordinated Universal Time (UTC) dan format ISO 8601 yang diperpanjang, ketika peristiwa terjadi.
- `description`— Penjelasan singkat tentang acara tersebut.
- `jobName`— Nama khusus pekerjaan.

Tergantung pada tipe dan sifat peristiwa, log acara juga dapat berisi bidang-bidang berikut:

- `affectedAccount`— Pengidentifikasi unik untuk Akun AWS yang memiliki sumber daya yang terpengaruh.
- `affectedResource`— Objek yang memberikan rincian tentang sumber daya yang terpengaruh. Dalam objek, `type` bidang menentukan bidang yang menyimpan metadata tentang sumber daya. Bidang `value` menentukan nilai untuk bidang (`type`).
- `operation`— Operasi yang Macie coba lakukan dan menyebabkan kesalahan.
- `runDateTanggal` dan waktu, dalam Coordinated Universal Time (UTC) dan format ISO 8601 yang diperpanjang, saat pekerjaan atau pekerjaan yang berlaku dimulai.

## Tipe log acara untuk tugas penemuan data sensitif

Macie mempublikasikan log acara untuk tiga kategori peristiwa:

- Peristiwa status tugas, yang mencatat perubahan status atau kemajuan tugas atau tugas yang dijalankan.
- Peristiwa kesalahan tingkat akun, yang mencatat kesalahan yang mencegah Macie menganalisis data Amazon S3 untuk Akun AWS tertentu.

- Peristiwa kesalahan tingkat bucket, yang mencatat kesalahan yang mencegah Macie menganalisis data di bucket S3 tertentu.

Topik dalam bagian ini mencantumkan dan menjelaskan tipe peristiwa yang diterbitkan Macie untuk setiap kategori.

## Topik

- [Peristiwa status tugas](#)
- [Peristiwa kesalahan tingkat akun](#)
- [Peristiwa kesalahan tingkat bucket](#)

## Peristiwa status tugas

Peristiwa status tugas mencatat perubahan status atau kemajuan tugas atau tugas yang dijalankan. Untuk tugas berkala, Macie mencatat dan mempublikasikan peristiwa ini untuk kedua tugas secara keseluruhan dan tugas individu yang dijalankan. Untuk informasi tentang penentuan status tugas secara keseluruhan, lihat [Memeriksa status tugas penemuan data sensitif](#).

Contoh berikut menggunakan data sampel untuk menunjukkan struktur dan sifat bidang dalam peristiwa status tugas. Dalam contoh ini, peristiwa SCHEDULED\_RUN\_COMPLETED menunjukkan bahwa pelaksanaan terjadwal tugas berkala selesai dijalankan. Pelaksanaan tersebut dimulai pada 14 April 2021, pukul 17:09:30 UTC, seperti yang ditunjukkan oleh bidang `runDate`. Pelaksanaan tersebut selesai pada 14 April 2021, pukul 17:16:30 UTC, seperti yang ditunjukkan oleh bidang `occurredAt`.

```
{
  "adminAccountId": "123456789012",
  "jobId": "ffad0e71455f38a4c7c220f3cexample",
  "eventType": "SCHEDULED_RUN_COMPLETED",
  "occurredAt": "2021-04-14T17:16:30.574809Z",
  "description": "The scheduled job run finished running.",
  "jobName": "My_Daily_Macie_Job",
  "runDate": "2021-04-14T17:09:30.574809Z"
}
```

Tabel berikut mencantumkan dan menjelaskan jenis peristiwa status pekerjaan yang dicatat dan diterbitkan oleh Macie ke CloudWatch Log. Kolom Tipe peristiwa menunjukkan nama dari setiap peristiwa seperti yang muncul di bidang `eventType` suatu acara. Kolom Deskripsi menyediakan

penjelasan singkat dari peristiwa seperti yang muncul di bidang `description` suatu acara. Informasi tambahan memberikan informasi tentang tipe tugas yang berlaku untuk peristiwa tersebut. Tabel diurutkan pertama berdasarkan urutan kronologis umum saat peristiwa mungkin terjadi, lalu dalam urutan abjad naik berdasarkan tipe peristiwa.

Tipe peristiwa	Deskripsi	Informasi tambahan
TUGAS_DIBUAT	Tugas tersebut dibuat.	Berlaku untuk tugas satu kali dan berkala.
TUGAS_SATU_KALI_DI_MULAI	Tugas mulai berjalan.	Hanya berlaku untuk tugas satu kali.
PELAKSANAAN_TERJADWAL_DIMULAI	Pelaksanaan tugas terjadwal mulai berjalan.	Hanya berlaku tugas berkala. Untuk mencatat awal tugas satu kali, Macie mempublikasikan peristiwa TUGAS_SATU_KALI_DIMULAI, bukan tipe peristiwa.
BUCKET_COCOK_DENGAN_KRITERIA	Bucket yang terpengaruh cocok dengan kriteria bucket yang ditentukan untuk tugas tersebut.	Berlaku untuk pekerjaan satu kali dan berkala yang menggunakan kriteria bucket runtime untuk menentukan bucket S3 mana yang akan dianalisis.  <code>affectedResource</code> Objek menentukan nama bucket yang cocok dengan kriteria dan dimasukkan dalam analisis pekerjaan.
	Tugas mulai berjalan tetapi saat ini tidak ada bucket yang	Berlaku untuk pekerjaan satu kali dan berkala yang

Tipe peristiwa	Deskripsi	Informasi tambahan
TIDAK_ADA_BUCKET_YANG_COCCOK_DENGAN_KRITERIA	cocok dengan kriteria bucket yang ditentukan untuk tugas tersebut. Tugas tersebut tidak menganalisis data apa pun.	menggunakan kriteria bucket runtime untuk menentukan bucket S3 mana yang akan dianalisis.
PELAKSANAAN_TERJADWAL_SELESAI	Pelaksanaan tugas terjadwal selesai berjalan.	Hanya berlaku tugas berkala. Untuk mencatat penyelesaian tugas satu kali, Macie mempublikasikan peristiwa TUGAS_SELESAI bukan tipe peristiwa ini.
TUGAS_DIJEDA_PENGGUNA	Tugas dijeda oleh pengguna.	Berlaku untuk tugas satu kali dan berkala yang Anda hentikan sementara (dijeda).
TUGAS_DILANJUTKAN_OLEH_PENGGUNA	Tugas dilanjutkan oleh pengguna.	Berlaku untuk tugas satu kali dan berkala yang Anda hentikan sementara (dijeda) lalu dilanjutkan kembali.

Tipe peristiwa	Deskripsi	Informasi tambahan
TUGAS_YANG_DIJEDA_OLEH_KUOTA_LAYANAN_MACIE_TERPENUHI	Tugas dijeda oleh Macie. Penyelesaian tugas akan melebihi kuota bulanan untuk akun terdampak.	<p>Berlaku untuk tugas satu kali dan berkala yang Macie hentikan sementara (dijeda).</p> <p>Macie secara otomatis menghentikan sementara pekerjaan ketika pemrosesan tambahan oleh pekerjaan atau pekerjaan akan melebihi <a href="#">kuota penemuan data sensitif</a> bulanan untuk satu atau lebih akun yang dianalisis data pekerjaan tersebut. Untuk menghindari masalah ini, pertimbangkan untuk meningkatkan kuota untuk akun yang terkena dampak.</p>

Tipe peristiwa	Deskripsi	Informasi tambahan
TUGAS_YANG_DILANJUTKAN_KUOTA_LAYANAN_MACIE_DIANGKAT	Tugas dilanjutkan oleh Macie. Service Quotas bulanan diangkat untuk akun yang terkena dampak.	<p>Berlaku untuk tugas satu kali dan berkala yang Macie hentikan sementara (dijeda) lalu dilanjutkan kembali.</p> <p>Jika Macie secara otomatis menghentikan sementara pekerjaan satu kali, Macie secara otomatis melanjutkan pekerjaan ketika bulan berikutnya dimulai atau kuota penemuan data sensitif bulanan ditingkatkan untuk semua akun yang terpengaruh, mana yang terjadi lebih dulu. Jika Macie secara otomatis menghentikan sementara pekerjaan berkala, Macie secara otomatis melanjutkan pekerjaan ketika putaran berikutnya dijadwalkan untuk dimulai atau bulan berikutnya dimulai, mana yang terjadi lebih dulu.</p>

Tipe peristiwa	Deskripsi	Informasi tambahan
TUGAS_DIBATALKAN	Tugas dibatalkan.	<p>Berlaku untuk tugas satu kali dan berkala yang Anda hentikan secara permanen (dibatalkan) atau, untuk tugas satu kali, yang dijeda dan tidak dilanjutkan dalam waktu 30 hari.</p> <p>Jika Anda menangguk atau menonaktifkan Macie, tipe peristiwa ini juga berlaku untuk tugas yang aktif atau dijeda saat Anda menangguk atau menonaktifkan Macie. Macie secara otomatis membatalkan tugas Anda di Wilayah AWS jika Anda menangguk atau menonaktifkan Macie di Wilayah.</p>
TUGAS_SELESAI	Tugas selesai berjalan.	<p>Hanya berlaku untuk tugas satu kali. Untuk mencatat penyelesaian pelaksanaan tugas satu kali, Macie mempublikasikan peristiwa PELAKSANAAN_TERJAD_WAL_SELESAI bukan tipe peristiwa ini.</p>



## Peristiwa kesalahan tingkat akun

Peristiwa kesalahan tingkat akun mencatat kesalahan yang mencegah Macie menganalisis objek di bucket S3 yang dimiliki oleh Akun AWS tertentu. Bidang `affectedAccount` di setiap peristiwa menentukan ID akun untuk akun tersebut.

Contoh berikut menggunakan data sampel untuk menunjukkan struktur dan sifat bidang di peristiwa kesalahan tingkat akun. Dalam contoh ini, peristiwa `ACCOUNT_ACCESS_DENIED` menunjukkan bahwa Macie tidak mampu menganalisis objek di setiap bucket S3 yang dimiliki oleh akun `444455556666`.

```
{
  "adminAccountId": "123456789012",
  "jobId": "85a55dc0fa6ed0be5939d0408example",
  "eventType": "ACCOUNT_ACCESS_DENIED",
  "occurredAt": "2021-04-14T17:08:30.585709Z",
  "description": "Macie doesn't have permission to access S3 bucket data for the
affected account.",
  "jobName": "My_Macie_Job",
  "operation": "ListBuckets",
  "runDate": "2021-04-14T17:05:27.574809Z",
  "affectedAccount": "444455556666"
}
```

Tabel berikut mencantumkan dan menjelaskan jenis peristiwa kesalahan tingkat akun yang dicatat dan diterbitkan oleh Macie ke Log. CloudWatch Kolom Tipe peristiwa menunjukkan nama dari setiap peristiwa seperti yang muncul di bidang `eventType` suatu acara. Kolom Deskripsi menyediakan penjelasan singkat dari peristiwa seperti yang muncul di bidang `description` suatu acara. Kolom Informasi tambahan menyediakan tips yang berlaku untuk menyelidiki atau mengatasi kesalahan yang terjadi. Tabel diurutkan berdasarkan urutan abjad naik menurut tipe peristiwa.

Tipe peristiwa	Deskripsi	Informasi tambahan
AKSES_AKUN_DITOLAK	Macie tidak memiliki izin untuk mengakses data bucket S3 untuk akun yang terkena dampak.	Hal ini biasanya terjadi karena bucket yang dimiliki oleh akun memiliki kebijakan bucket ketat. Untuk informasi tentang cara mengatasi masalah ini, lihat <a href="#">Mengizinkan Macie untuk</a>

Tipe peristiwa	Deskripsi	Informasi tambahan
		<p><a href="#">mengakses bucket S3 dan objek.</a></p> <p>Nilai untuk bidang operation dalam peristiwa tersebut dapat membantu Anda menentukan pengaturan izin yang mencegah Macie mengakses data S3 untuk akun tersebut. Bidang ini menunjukkan operasi Amazon S3 yang coba dilakukan Macie ketika kesalahan terjadi.</p>
AKUN_DINONAKTIFKAN	Tugas melewatkan sumber daya yang dimiliki oleh akun yang terkena dampak. Macie dinonaktifkan untuk akun.	Untuk mengatasi masalah ini, aktifkan kembali Macie untuk akun di Wilayah AWS yang sama.

Tipe peristiwa	Deskripsi	Informasi tambahan
AKUN_DIPISAHKAN	Tugas melewatkan sumber daya yang dimiliki oleh akun yang terkena dampak. Akun tersebut tidak lagi dikaitkan dengan akun administrator Macie sebagai akun anggota.	<p>Hal ini terjadi jika Anda, sebagai administrator Macie untuk organisasi, mengonfigurasi tugas untuk menganalisis data untuk akun anggota terkait dan akun anggota kemudian dihapus dari organisasi Anda.</p> <p>Untuk mengatasi masalah ini, kaitkan kembali akun yang terpengaruh dengan akun administrator Macie sebagai akun anggota. Untuk informasi selengkapnya, lihat <a href="#">Mengelola beberapa akun</a>.</p>
AKUN_TERISOLASI	Tugas melewatkan sumber daya yang dimiliki oleh akun yang terkena dampak. Akun AWS terisolasi.	–
WILAYAH_AKUN_DINONAKTIFKAN	Tugas melewatkan sumber daya yang dimiliki oleh akun yang terkena dampak. Akun AWS tidak aktif di Wilayah AWS ini.	–

Tipe peristiwa	Deskripsi	Informasi tambahan
AKUN_DITANGGUHKAN	Tugas dibatalkan atau melewati sumber daya yang dimiliki oleh akun yang terkena dampak. Macie ditangguhkan untuk akun.	<p>Jika akun yang ditentukan adalah akun Anda sendiri, Macie secara otomatis membatalkan pekerjaan ketika Anda menangguhkan Macie di Wilayah yang sama. Untuk mengatasi masalah ini, aktifkan kembali Macie di Wilayah tersebut.</p> <p>Jika akun yang ditentukan adalah akun anggota, aktifkan kembali Macie untuk akun tersebut di Wilayah yang sama.</p>
AKUN_DIAKHIRI	Tugas melewati sumber daya yang dimiliki oleh akun yang terkena dampak. Akun AWS diakhiri.	–

### Peristiwa kesalahan tingkat bucket

Peristiwa kesalahan tingkat bucket mencatat kesalahan yang mencegah Macie menganalisis objek di bucket S3 tertentu. Bidang `affectedAccount` di setiap peristiwa menentukan ID akun untuk Akun AWS yang memiliki bucket tersebut. `affectedResourceObjek` dalam setiap acara menentukan nama bucket.

Contoh berikut menggunakan data sampel untuk menunjukkan struktur dan sifat bidang di peristiwa kesalahan tingkat bucket. Dalam contoh ini, peristiwa `BUCKET_ACCESS_DENIED` menunjukkan bahwa Macie tidak mampu menganalisis objek di bucket S3 yang bernama `DOC-EXAMPLE-BUCKET`. Saat Macie mencoba membuat daftar objek di bucket dengan menggunakan operasi [ListObjectsV2](#) dari Amazon S3 API, Amazon S3 menolak akses ke bucket.

```
{
  "adminAccountId": "123456789012",
  "jobId": "85a55dc0fa6ed0be5939d0408example",
  "eventType": "BUCKET_ACCESS_DENIED",
  "occurredAt": "2021-04-14T17:11:30.574809Z",
  "description": "Macie doesn't have permission to access the affected S3 bucket.",
  "jobName": "My_Macie_Job",
  "operation": "ListObjectsV2",
  "runDate": "2021-04-14T17:09:30.685209Z",
  "affectedAccount": "111122223333",
  "affectedResource": {
    "type": "S3_BUCKET_NAME",
    "value": "DOC-EXAMPLE-BUCKET"
  }
}
```

Tabel berikut mencantumkan dan menjelaskan jenis peristiwa kesalahan tingkat ember yang dicatat dan diterbitkan oleh Macie ke Log. CloudWatch Kolom Tipe peristiwa menunjukkan nama dari setiap peristiwa seperti yang muncul di bidang eventType suatu acara. Kolom Deskripsi menyediakan penjelasan singkat dari peristiwa seperti yang muncul di bidang description suatu acara. Kolom Informasi tambahan menyediakan tips yang berlaku untuk menyelidiki atau mengatasi kesalahan yang terjadi. Tabel diurutkan berdasarkan urutan abjad naik menurut tipe peristiwa.

Tipe peristiwa	Deskripsi	Informasi tambahan
AKSES_BUCKET_DITOLAK	Macie tidak memiliki izin untuk mengakses bucket S3 yang terkena dampak.	Ini biasanya terjadi karena bucket memiliki kebijakan bucket yang membatasi. Untuk informasi tentang cara mengatasi masalah ini, lihat <a href="#">Mengizinkan Macie untuk mengakses bucket S3 dan objek</a> .  Nilai untuk bidang operation dalam peristiwa tersebut dapat membantu Anda menentukan pengaturan

Tipe peristiwa	Deskripsi	Informasi tambahan
		<p>izin yang mencegah Macie mengakses bucket. Bidang ini menunjukkan operasi Amazon S3 yang coba dilakukan Macie ketika kesalahan terjadi.</p>
<p>BUCKET_DETAILS_UNAVAILABLE</p>	<p>Masalah sementara mencegah Macie mengambil detail tentang ember dan objek ember.</p>	<p>Ini terjadi jika masalah sementara mencegah Macie mengambil bucket dan metadata objek yang diperlukan untuk menganalisis objek bucket. Misalnya, pengecualian Amazon S3 terjadi ketika Macie mencoba memverifikasi bahwa itu diizinkan untuk mengakses bucket.</p> <p>Untuk mengatasi masalah untuk pekerjaan satu kali, pertimbangkan untuk membuat dan menjalankan pekerjaan baru satu kali untuk menganalisis objek dalam ember. Untuk pekerjaan terjadwal, Macie akan mencoba untuk mengambil metadata lagi selama menjalankan pekerjaan berikutnya.</p>
<p>BUCKET_TIDAK_ADA</p>	<p>Bucket S3 yang terkena tidak ada lagi.</p>	<p>Hal ini biasanya terjadi karena bucket telah dihapus.</p>

Tipe peristiwa	Deskripsi	Informasi tambahan
BUCKET_DI_WILAYAH_BERBEDA	Bucket S3 yang terkena dampak dipindahkan ke Wilayah AWS berbeda.	–
PEMILIK_BUCKET_DIUBAH	Pemilik bucket S3 yang terkena dampak berubah. Macie tidak memiliki izin untuk mengakses bucket lagi.	Hal ini biasanya terjadi jika kepemilikan bucket dipindahkan ke Akun AWS yang bukan bagian organisasi Anda. Kolom <code>affectedAccount</code> dalam peristiwa menunjukkan ID akun untuk akun yang sebelumnya dimiliki bucket.

## Mengelola tugas penemuan data sensitif

Untuk membantu Anda mengelola pekerjaan penemuan data sensitif Anda, Amazon Macie menyediakan inventaris lengkap pekerjaan Anda di masing-masing pekerjaan. Wilayah AWS Dengan inventaris ini, Anda dapat mengelola tugas Anda sebagai koleksi tunggal, dan mengakses pengaturan konfigurasi, status, dan statistik pemrosesan untuk tugas individu. Anda juga dapat mengakses [temuan data sensitif dan hasil lainnya](#) yang dihasilkan setiap tugas.

Selain tugas ini, Anda dapat membuat variasi khusus dari tugas individu—salin tugas yang ada, sesuaikan pengaturan untuk salinan, lalu simpan salinan sebagai tugas baru. Hal ini dapat membantu untuk kasus-kasus saat Anda ingin menganalisis set data yang berbeda dengan cara yang sama, atau set data yang sama dengan cara yang berbeda. Atau Anda ingin menyesuaikan pengaturan konfigurasi untuk tugas yang ada—batalkan tugas yang ada, salin, lalu sesuaikan dan simpan salinan sebagai tugas baru.

### Topik




- [Meninjau inventaris pekerjaan penemuan data sensitif Anda](#)
- [Meninjau pengaturan konfigurasi untuk pekerjaan penemuan data sensitif](#)
- [Memeriksa status tugas penemuan data sensitif](#)
- [Menjeda, melanjutkan, atau membatalkan tugas penemuan data sensitif](#)

- [Menyalin tugas penemuan data sensitif](#)

## Meninjau inventaris pekerjaan penemuan data sensitif Anda

Halaman Pekerjaan di konsol Amazon Macie menyediakan informasi tentang semua pekerjaan penemuan data sensitif untuk akun Anda saat ini. Wilayah AWS Untuk setiap pekerjaan, tabel menampilkan informasi ringkasan yang mencakup: status pekerjaan saat ini; apakah pekerjaan berjalan secara terjadwal dan berkala; dan, apakah pekerjaan menganalisis sejumlah bucket S3 tertentu atau menganalisis bucket S3 yang sesuai dengan kriteria runtime. Jika Anda memilih tugas dalam tabel, panel detail menampilkan pengaturan konfigurasi dan informasi lainnya tentang tugas.

Untuk meninjau inventaris pekerjaan Anda

1. [Buka konsol Amazon Macie di https://console.aws.amazon.com/macie/](https://console.aws.amazon.com/macie/).
2. Di panel navigasi, pilih Tugas. Halaman Tugas membuka dan menampilkan jumlah tugas dalam inventaris Anda dan tabel tugas tersebut.
3. Untuk menemukan tugas tertentu dengan lebih cepat, lakukan hal-hal berikut:
  - Untuk mengurutkan tabel berdasarkan bidang tertentu, klik judul kolom untuk bidang. Untuk mengubah urutan pengurutan, klik judul kolom lagi.
  - Untuk hanya menampilkan pekerjaan yang memiliki nilai spesifik untuk bidang, letakkan cursor Anda di kotak filter. Pada menu yang muncul, pilih bidang yang akan digunakan untuk filter, dan masukkan nilai untuk filter. Lalu, pilih Terapkan.
  - Untuk menyembunyikan pekerjaan yang memiliki nilai spesifik untuk bidang, letakkan cursor Anda di kotak filter. Pada menu yang muncul, pilih bidang yang akan digunakan untuk filter, dan masukkan nilai untuk filter. Lalu, pilih Terapkan. Di kotak filter, pilih ikon sama dengan  untuk filter. Hal ini mengubah operator filter dari Sama menjadi Tidak Sama .
  - Untuk menghapus filter, pilih ikon hapus filter  agar filter akan dihapus.
4. Untuk meninjau pengaturan konfigurasi dan detail lainnya untuk tugas tertentu, pilih nama tugas dalam tabel, lalu lihat panel detail.



## Meninjau pengaturan konfigurasi untuk pekerjaan penemuan data sensitif

Di konsol Amazon Macie, Anda dapat menggunakan panel detail di halaman Pekerjaan untuk meninjau pengaturan konfigurasi dan informasi lainnya tentang pekerjaan penemuan data sensitif individual. Misalnya, Anda dapat meninjau daftar bucket S3 yang dikonfigurasi pekerjaan untuk dianalisis dan pengidentifikasi data terkelola yang digunakan pekerjaan untuk menganalisis objek di bucket tersebut.

### Note

Anda tidak dapat mengubah pengaturan konfigurasi apa pun untuk pekerjaan yang ada. Hal ini membantu memastikan bahwa Anda memiliki riwayat tetap akan temuan dan hasil penemuan data sensitif untuk audit atau investigasi privasi dan perlindungan data yang Anda lakukan. Jika Anda ingin mengubah pekerjaan yang ada, [batalkan pekerjaan](#). Kemudian [salin tugas tersebut](#), konfigurasi salinan untuk menggunakan pengaturan yang Anda inginkan, dan simpan salinan sebagai tugas baru.

Jika Anda melakukan ini, Anda juga harus mengambil langkah-langkah untuk memastikan bahwa pekerjaan baru tidak menganalisis data yang ada dengan cara yang sama lagi. Untuk melakukan ini, perhatikan tanggal dan waktu saat Anda membatalkan tugas yang ada. Kemudian konfigurasi ruang lingkup tugas baru untuk hanya menyertakan objek yang dibuat atau diubah setelah Anda membatalkan tugas asli. Misalnya, gunakan [kriteria objek](#) untuk menambahkan kondisi pengecualian terakhir yang dimodifikasi yang menentukan tanggal dan waktu saat Anda membatalkan pekerjaan asli.

Untuk meninjau pengaturan konfigurasi pekerjaan

1. [Buka konsol Amazon Macie di https://console.aws.amazon.com/macie/](https://console.aws.amazon.com/macie/).
2. Di panel navigasi, pilih Tugas.
3. Pada halaman Jobs, pilih nama pekerjaan yang pengaturannya ingin Anda tinjau. Panel detail menampilkan pengaturan konfigurasi dan informasi lainnya tentang tugas. Tergantung pada pengaturan pekerjaan, panel berisi bagian berikut.

### Informasi umum

Bagian ini memberikan informasi umum tentang pekerjaan—misalnya, Amazon Resource Name (ARN) pekerjaan, kapan pekerjaan terbaru mulai dijalankan, dan status pekerjaan saat

ini. Jika Anda menghentikan sementara pekerjaan, bagian ini juga menunjukkan kapan Anda menjeda pekerjaan, dan kapan pekerjaan atau pekerjaan terbaru berjalan berakhir atau akan kedaluwarsa jika Anda tidak melanjutkannya.

## Statistik

Bagian ini menunjukkan statistik pemrosesan untuk pekerjaan tersebut—misalnya, berapa kali pekerjaan telah berjalan dan perkiraan jumlah objek yang belum diproses pekerjaan selama proses saat ini.

## Lingkup

Bagian ini menunjukkan seberapa sering pekerjaan berjalan. Ini juga menunjukkan pengaturan yang menyempurnakan cakupan pekerjaan—misalnya, kedalaman pengambilan sampel dan [kriteria objek apa pun yang menyertakan atau mengecualikan objek S3](#) dari analisis pekerjaan.

## Ember S3

Bagian ini muncul di panel jika pekerjaan dikonfigurasi untuk menganalisis bucket yang Anda pilih secara eksplisit saat membuat pekerjaan. Ini menunjukkan jumlah pekerjaan Akun AWS yang dikonfigurasi untuk menganalisis data. Ini juga menunjukkan jumlah ember yang dikonfigurasi pekerjaan untuk dianalisis dan nama-nama ember tersebut (dikelompokkan berdasarkan akun).

Untuk menampilkan daftar lengkap akun dan bucket dalam format JSON, pilih nomor di bidang Total Bucket.

## Kriteria bucket S3

Bagian ini muncul di panel jika pekerjaan menggunakan kriteria runtime untuk menentukan bucket mana yang akan dianalisis. Ini mencantumkan kriteria bahwa pekerjaan dikonfigurasi untuk digunakan.

Untuk menampilkan kriteria dalam format JSON, pilih Detail, lalu pilih tab Kriteria di jendela yang muncul.

Untuk meninjau tabel bucket yang saat ini cocok dengan kriteria, pilih Detail, lalu pilih tab Bucket yang cocok di jendela yang muncul. Secara opsional pilih segarkan



untuk mengambil data terbaru.

**i** Tip

Jika tugas telah berjalan, Anda juga dapat menentukan apakah setiap bucket cocok dengan kriteria ketika tugas berjalan dan, jika demikian, nama bucket tersebut. Untuk melakukannya, tinjau peristiwa log untuk pekerjaan: pilih Tampilkan hasil di bagian atas panel, lalu pilih Tampilkan CloudWatch log. Macie membuka CloudWatch konsol Amazon dan menampilkan tabel peristiwa log untuk pekerjaan itu. Peristiwa tersebut mencakup BUCKET\_MATCHED\_THE\_CRITERIA acara untuk setiap ember yang sesuai dengan kriteria dan dimasukkan dalam analisis pekerjaan. Untuk informasi selengkapnya, lihat [Tugas pemantauan](#).

### Pengidentifikasi data khusus

Bagian ini muncul di panel jika pekerjaan dikonfigurasi untuk menggunakan satu atau beberapa [pengidentifikasi data kustom](#). Ini menentukan nama-nama pengidentifikasi data kustom tersebut.

### Izinkan daftar

Bagian ini muncul di panel jika pekerjaan dikonfigurasi untuk menggunakan satu atau beberapa [daftar izinkan](#). Ini menentukan nama-nama daftar tersebut. Untuk meninjau pengaturan dan status daftar, pilih ikon tautan



di sebelah nama daftar.

### Pengidentifikasi data terkelola

Bagian ini menunjukkan [pengidentifikasi data terkelola](#) mana yang dikonfigurasi untuk digunakan oleh pekerjaan. Ini ditentukan oleh jenis pemilihan pengenalan data terkelola untuk pekerjaan:

- Direkomendasikan — Gunakan pengidentifikasi data terkelola yang ada di [set yang direkomendasikan](#) saat pekerjaan berjalan.
- Sertakan yang dipilih — Gunakan hanya pengidentifikasi data terkelola yang tercantum di bagian Pilihan.
- Sertakan semua — Gunakan semua pengidentifikasi data terkelola yang tersedia saat pekerjaan berjalan.

- Kecualikan yang dipilih — Gunakan semua pengidentifikasi data terkelola yang tersedia saat pekerjaan berjalan, kecuali yang tercantum di bagian Pilihan.
- Kecualikan semua — Jangan gunakan pengidentifikasi data terkelola apa pun. Gunakan hanya pengidentifikasi data kustom yang ditentukan.

Untuk meninjau pengaturan ini dalam format JSON, pilih Detail.

## Tag

Bagian ini muncul di panel jika tag dikaitkan dengan pekerjaan. Ini mencantumkan tag tersebut.

Tag adalah label yang Anda tentukan dan tetapkan ke jenis AWS sumber daya tertentu. Setiap tanda terdiri dari kunci tanda yang diperlukan dan nilai tanda opsional. Tag dapat membantu Anda mengidentifikasi, mengkategorikan, dan mengelola sumber daya dengan cara yang berbeda, seperti berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya.

Untuk mempelajari selengkapnya, lihat [Menandai sumber daya Amazon Macie](#).

4. Untuk meninjau dan menyimpan pengaturan pekerjaan dalam format JSON, pilih pengenal unik untuk pekerjaan (ID Pekerjaan) di bagian atas panel, lalu pilih Unduh.

## Memeriksa status tugas penemuan data sensitif

Bila Anda membuat tugas penemuan data sensitif, status awalnya adalah Aktif (Menjalankan) atau Aktif (Idle), tergantung pada tipe dan jadwal tugas. Tugas kemudian melewati status tambahan, yang dapat Anda pantau saat tugas berlangsung.

### Tip

Selain memantau status keseluruhan dari tugas, Anda dapat memantau dan menganalisis peristiwa tertentu yang terjadi saat tugas berlangsung. Anda dapat melakukan ini dengan menggunakan data logging yang secara otomatis diterbitkan Macie ke Amazon CloudWatch Logs. Data log ini juga menyediakan catatan perubahan pada status tugas dan detail tentang kesalahan tingkat akun atau bucket yang terjadi saat tugas berjalan. Untuk informasi selengkapnya, lihat [Tugas pemantauan](#).

Untuk memeriksa status tugas

1. [Buka konsol Amazon Macie di https://console.aws.amazon.com/macie/](https://console.aws.amazon.com/macie/).

2. Di panel navigasi, pilih Tugas.
3. Pada halaman Tugas, cari tugas yang statusnya ingin Anda periksa. Bidang Status menunjukkan status pekerjaan saat ini.

#### Aktif (Menganggur)

Untuk pekerjaan berkala, proses sebelumnya selesai dan proses terjadwal berikutnya tertunda. Nilai ini tidak berlaku untuk tugas satu kali.

#### Aktif (Berlari)

Untuk pekerjaan satu kali, pekerjaan saat ini sedang berlangsung. Untuk tugas berkala, pelaksanaan terjadwal sedang berlangsung.

#### Dibatalkan

Untuk semua jenis pekerjaan, pekerjaan dihentikan secara permanen (dibatalkan).

Tugas memiliki status ini jika Anda secara eksplisit membatalkannya atau, jika itu adalah tugas satu kali, Anda menjeda tugas dan tidak melanjutkannya dalam waktu 30 hari.

Pekerjaan juga dapat memiliki status ini jika Anda sebelumnya [menangguhkan Macie](#) saat iniWilayah AWS.

#### Lengkap

Untuk pekerjaan satu kali, pekerjaan berjalan dengan sukses dan sekarang selesai. Nilai ini tidak berlaku untuk tugas berkala. Sebaliknya, status tugas berkala berubah menjadi Aktif (Idle) ketika setiap pelaksanaannya selesai dengan berhasil.

#### Dijeda (Oleh Macie)

Untuk semua jenis pekerjaan, pekerjaan dihentikan sementara (dijeda) oleh Macie.

Pekerjaan memiliki status ini jika penyelesaian pekerjaan atau pekerjaan akan melebihi [kuota penemuan data sensitif](#) bulanan untuk akun Anda. Ketika ini terjadi, Macie secara otomatis menjeda tugas tersebut. Macie secara otomatis melanjutkan pekerjaan ketika bulan kalender berikutnya dimulai (dan kuota bulanan diatur ulang untuk akun Anda) atau Anda menambah kuota untuk akun Anda.

Jika Anda administrator Macie untuk organisasi dan Anda mengonfigurasi pekerjaan untuk menganalisis data akun anggota, pekerjaan juga dapat memiliki status ini jika penyelesaian

pekerjaan atau pekerjaan akan melebihi kuota penemuan data sensitif bulanan untuk akun anggota.

Jika pekerjaan sedang berjalan dan analisis objek yang memenuhi syarat mencapai kuota ini untuk akun anggota, pekerjaan berhenti menganalisis objek yang dimiliki oleh akun tersebut. Ketika pekerjaan selesai menganalisis objek untuk semua akun lain yang belum memenuhi kuota, Macie secara otomatis menghentikan sementara pekerjaan. Jika ini adalah pekerjaan satu kali, Macie secara otomatis melanjutkan pekerjaan ketika bulan kalender berikutnya dimulai atau kuota ditingkatkan untuk semua akun yang terpengaruh, mana yang terjadi lebih dulu. Jika ini adalah pekerjaan berkala, Macie secara otomatis melanjutkan pekerjaan ketika proses berikutnya dijadwalkan untuk dimulai atau bulan kalender berikutnya dimulai, mana yang terjadi lebih dulu. Jika jadwal berjalan dimulai sebelum bulan kalender berikutnya dimulai atau kuota ditingkatkan untuk akun yang terpengaruh, pekerjaan tidak menganalisis objek yang dimiliki oleh akun.

### Dijeda (Oleh pengguna)

Untuk semua jenis pekerjaan, pekerjaan dihentikan sementara (dijeda) oleh Anda.

Jika Anda menjeda tugas satu kali dan Anda tidak melanjutkan dalam waktu 30 hari, tugas akan kedaluwarsa dan Macie membatalkannya. Jika Anda menjeda tugas berkala saat tugas sedang aktif berjalan dan Anda tidak melanjutkannya dalam waktu 30 hari, tugas akan kedaluwarsa dan Macie membatalkan pelaksanaan tersebut. Untuk memeriksa tanggal kedaluwarsa untuk tugas yang dijeda atau pelaksanaan tugas, pilih nama tugas dalam tabel, lalu lihat bidang Kedaluwarsa di bagian Detail status dari panel detail.

Jika tugas dibatalkan atau dijeda, Anda dapat melihat detail tugas untuk menentukan apakah tugas mulai berjalan atau, untuk tugas berkala, dijalankan setidaknya sekali sebelum dibatalkan atau dijeda. Untuk melakukan ini, pilih nama tugas dalam tabel, lalu lihat panel detail. Pada panel tersebut, bidang Jumlah pelaksanaan menunjukkan jumlah tugas yang telah dijalankan. Bidang Waktu akhir terakhir menunjukkan tanggal dan waktu terbaru ketika tugas mulai berjalan.

Tergantung pada status tugas saat ini, Anda dapat menjeda, melanjutkan, atau membatalkan tugas secara opsional.

### Menjeda, melanjutkan, atau membatalkan tugas penemuan data sensitif

Setelah membuat tugas penemuan data sensitif, Anda dapat menjeda sementara atau membatalkannya secara permanen. Ketika Anda menjeda tugas yang aktif berjalan, Macie segera

mulai menjeda semua tugas pemrosesan untuk tugas tersebut. Ketika Anda menjeda tugas yang aktif berjalan, Macie segera mulai menghentikan semua tugas pemrosesan untuk tugas tersebut. Anda tidak dapat melanjutkan atau memulai ulang tugas setelah dibatalkan.

Jika Anda menghentikan tugas satu kali, Anda dapat melanjutkannya dalam 30 hari. Ketika Anda melanjutkan tugas, Macie segera melanjutkan pemrosesan dari titik tempat Anda menjeda tugas—Macie tidak memulai ulang tugas dari awal. Jika Anda tidak melanjutkan tugas satu dalam waktu 30 hari jeda, tugas akan kedaluwarsa dan Macie membatalkannya.

Jika Anda menjeda tugas berkala, Anda dapat melanjutkannya kapan saja. Jika Anda melanjutkan tugas berkala dan tugas idle saat Anda menjedanya, Macie melanjutkan tugas sesuai jadwal dan pengaturan konfigurasi lain yang Anda pilih saat Anda membuat tugas. Jika Anda melanjutkan tugas berkala dan tugas berjalan secara aktif saat Anda menjedanya, cara Macie melanjutkan tugas tergantung pada saat Anda melanjutkan tugas:

- Ketika Anda melanjutkan tugas dalam waktu 30 hari jeda, Macie segera melanjutkan pelaksanaan terjadwal terbaru dari titik tempat Anda menjeda tugas—Macie tidak memulai ulang tugas dari awal.
- Jika Anda tidak melanjutkan tugas dalam waktu 30 hari jeda, pelaksanaan terjadwal terbaru akan kedaluwarsa dan Macie membatalkan semua tugas pemrosesan yang tersisa untuk pelaksanaan tersebut. Ketika Anda kemudian melanjutkan tugas, Macie melanjutkan tugas sesuai jadwal dan pengaturan konfigurasi lain yang Anda pilih saat Anda membuat tugas.

Untuk membantu Anda menentukan kapan tugas yang dijeda atau pelaksanaan tugas akan kedaluwarsa, Macie menambahkan tanggal kedaluwarsa ke detail tugas saat tugas dijeda. Untuk memeriksa tanggal ini, pilih nama tugas dalam tabel pada halaman Tugas, lalu lihat bidang Kedaluwarsa di bagian Detail status dari panel detail. Selain itu, kami akan memberi tahu Anda sekitar tujuh hari sebelum tugas atau pelaksanaan tugas akan kedaluwarsa. Kami akan memberi tahu Anda lagi saat tugas atau pelaksanaan tugas kedaluwarsa dan dibatalkan. Untuk memberi tahu Anda, kami mengirim email ke alamat yang terkait dengan AndaAkun AWS. Kami juga membuat AWS Health acara dan CloudWatch Acara Amazon untuk akun Anda.

Untuk menjeda, melanjutkan, atau membatalkan tugas

1. [Buka konsol Amazon Macie di https://console.aws.amazon.com/macie/](https://console.aws.amazon.com/macie/).
2. Di panel navigasi, pilih Tugas.

3. Pada halaman Tugas, berikan tanda centang pada kotak centang untuk tugas yang ingin Anda jeda, lanjutkan, atau batalkan, lalu lakukan salah satu hal berikut pada menu Tindakan:
  - Untuk menjeda tugas sementara, pilih Jeda. Opsi ini hanya tersedia jika status tugas saat ini adalah Aktif (Idle), Aktif (Berjalan), atau Dijeda (Oleh Macie).
  - Untuk melanjutkan tugas, pilih Lanjutkan. Opsi ini hanya tersedia jika status tugas saat ini adalah Dijeda (Oleh pengguna).
  - Untuk membatalkan tugas ini secara permanen, pilih Batal. Jika Anda memilih opsi ini, Anda tidak dapat melanjutkan atau memulai ulang tugas tersebut.

## Menyalin tugas penemuan data sensitif

Untuk segera membuat tugas penemuan data sensitif baru yang mirip dengan tugas yang ada, Anda dapat membuat salinan tugas tersebut, mengedit pengaturan salinan, lalu menyimpan salinan sebagai tugas baru. Hal ini dapat membantu untuk kasus saat Anda ingin membuat variasi kustom dari tugas yang ada. Atau Anda ingin menyesuaikan pengaturan konfigurasi untuk tugas yang ada dengan membatalkan tugas, lalu menyalin, mengubah, dan menyimpan pengaturan sebagai tugas baru.

### Untuk menyalin tugas

1. [Buka konsol Amazon Macie di https://console.aws.amazon.com/macie/](https://console.aws.amazon.com/macie/).
2. Di panel navigasi, pilih Tugas.
3. Beri tanda centang pada kotak centang untuk tugas yang ingin Anda salin.
4. Dari menu Tindakan, pilih Salin ke baru.
5. Selesaikan langkah-langkah di konsol tersebut untuk meninjau dan menyesuaikan pengaturan untuk salinan tugas. Untuk langkah Perbaiki cakupan, pertimbangkan untuk memilih opsi yang mencegah pekerjaan menganalisis data yang ada dengan cara yang sama lagi:
  - Untuk tugas satu kali, gunakan [kriteria objek](#) untuk hanya menyertakan objek yang dibuat atau diubah setelah waktu tertentu. Misalnya, jika Anda membuat salinan tugas yang dibatalkan, tambahkan syarat Terakhir Dimodifikasi yang menentukan tanggal dan waktu ketika Anda membatalkan tugas yang ada.
  - Untuk tugas berkala, hapus tanda centang pada kotak centang Masukkan objek yang ada. Jika Anda melakukan ini, tugas yang dijalankan pertama kali akan hanya menganalisis objek yang dibuat atau diubah setelah Anda membuat tugas dan sebelum tugas pertama dijalankan.



Anda juga dapat menggunakan [kriteria objek](#) untuk mengecualikan objek yang terakhir diubah sebelum tanggal dan waktu tertentu.

Untuk detail tambahan tentang ini dan langkah-langkah lainnya, lihat [Membuat tugas penemuan data sensitif](#).

6. Setelah selesai, pilih Kirim untuk menyimpan salinan sebagai tugas baru.

## Biaya prakiraan dan pemantauan biaya untuk tugas penemuan data sensitif

Harga Amazon Macie sebagian didasarkan pada jumlah data yang Anda analisis dengan menjalankan tugas penemuan data sensitif. Untuk memprakirakan dan memantau perkiraan biaya untuk menjalankan tugas penemuan data sensitif, Anda dapat meninjau perkiraan biaya yang disediakan Macie saat Anda membuat tugas dan setelah Anda mulai menjalankan tugas.

Untuk meninjau dan memantau biaya aktual Anda, Anda dapat menggunakan AWS Billing and Cost Management. AWS Billing and Cost Management menyediakan fitur yang dirancang untuk membantu Anda melacak dan menganalisis biaya untuk Layanan AWS akun atau organisasi Anda. Ini juga menyediakan fitur yang dapat membantu Anda memprakirakan biaya penggunaan berdasarkan data historis. Untuk mempelajari selengkapnya, lihat [Panduan Pengguna AWS Billing](#).

Untuk informasi tentang harga Macie, lihat [Harga Amazon Macie](#).

Topik

- [Memprakirakan biaya tugas penemuan data sensitif](#)
- [Memantau perkiraan biaya untuk tugas penemuan data sensitif](#)

## Memprakirakan biaya tugas penemuan data sensitif

Ketika Anda membuat tugas penemuan data sensitif, Amazon Macie dapat menghitung dan menampilkan tugas biaya selama dua langkah kunci dalam proses pembuatan tugas: ketika Anda meninjau tabel bucket S3 yang Anda pilih untuk tugas (langkah 2) dan ketika Anda meninjau semua pengaturan untuk tugas (langkah 8). Perkiraan ini dapat membantu Anda menentukan apakah akan menyesuaikan pengaturan tugas sebelum menyimpan tugas. Ketersediaan dan sifat perkiraan tergantung pada pengaturan yang Anda pilih untuk tugas tersebut.

## Meninjau perkiraan biaya untuk bucket individu (langkah 2)

Jika Anda secara eksplisit memilih bucket individu untuk dianalisis tugas, Anda dapat meninjau perkiraan biaya analisis objek di masing-masing bucket tersebut. Macie menampilkan perkiraan ini selama langkah 2 dari proses pembuatan tugas, saat Anda meninjau pilihan bucket Anda. Pada tabel untuk langkah ini, bidang Estimasi biaya menunjukkan total perkiraan biaya (dalam dolar AS) menjalankan tugas sekali untuk menganalisis objek dalam bucket.

Setiap perkiraan mencerminkan jumlah data terkompresi yang diproyeksikan yang akan dianalisis tugas di bucket, berdasarkan ukuran dan tipe objek yang saat ini disimpan dalam bucket.

Perkiraan ini juga mencerminkan harga Macie untuk saat ini. Wilayah AWS

Hanya objek yang dapat diklasifikasikan yang disertakan dalam perkiraan biaya untuk bucket. Objek yang dapat diklasifikasikan adalah objek S3 yang menggunakan [kelas penyimpanan Amazon S3 didukung](#) dan memiliki ekstensi nama file untuk file atau format penyimpanan yang [didukung](#). Jika setiap objek adalah file terkompresi atau arsip, perkiraan mengasumsikan bahwa file menggunakan rasio kompresi 3:1 dan tugas dapat menganalisis semua file yang diekstraksi.

## Meninjau perkiraan total biaya tugas (langkah 8)

Jika Anda membuat tugas satu kali atau Anda membuat dan mengonfigurasi tugas berkala untuk menyertakan objek S3 yang ada, Macie menghitung dan menampilkan total biaya perkiraan tugas selama langkah terakhir dari proses penciptaan tugas. Anda dapat meninjau perkiraan ini saat Anda meninjau dan memverifikasi semua pengaturan yang dipilih untuk tugas tersebut.

Perkiraan ini menunjukkan total biaya yang diproyeksikan (dalam Dolar AS) saat menjalankan tugas satu kali di Wilayah saat ini. Perkiraan tersebut menunjukkan jumlah data terkompresi yang diproyeksikan yang akan dianalisis tugas. Hal ini didasarkan pada ukuran dan tipe objek yang saat ini disimpan dalam bucket yang secara eksplisit dipilih untuk tugas atau hingga 500 bucket yang saat ini cocok dengan kriteria bucket yang Anda tentukan untuk tugas, tergantung pada pengaturan tugas.

Perhatikan bahwa perkiraan ini tidak mencerminkan opsi apa pun yang Anda pilih untuk menyempurnakan dan mengurangi ruang lingkup tugas—misalnya, kedalaman pengambilan sampel yang lebih rendah, atau kriteria yang mengecualikan objek S3 tertentu dari tugas. Hal ini juga tidak mencerminkan [Kuota penemuan data sensitif](#) bulanan Anda, yang mungkin membatasi ruang lingkup dan biaya analisis tugas, atau diskon apa pun yang mungkin berlaku untuk akun Anda.

Selain total perkiraan biaya tugas, perkiraan tersebut menyediakan data yang dikumpulkan yang menawarkan wawasan ke dalam ruang lingkup dan biaya yang diproyeksikan tugas:

- Nilai Ukuran menunjukkan ukuran penyimpanan total objek yang dapat dan tidak dapat dianalisis tugas.
- Nilai Jumlah objek menunjukkan jumlah total objek yang dapat dan tidak dapat dianalisis tugas.

Dalam nilai-nilai ini, Objek yang dapat diklasifikasikan adalah objek S3 yang menggunakan [kelas penyimpanan Amazon S3 didukung](#) dan memiliki ekstensi nama file untuk file atau format penyimpanan yang [didukung](#). Hanya objek yang dapat diklasifikasikan yang disertakan dalam perkiraan biaya. Objek yang tidak dapat diklasifikasikan adalah objek yang tidak menggunakan kelas penyimpanan didukung atau tidak memiliki ekstensi nama file untuk file atau format penyimpanan yang didukung. Objek ini tidak termasuk dalam perkiraan biaya.

Perkiraan menyediakan data agregat tambahan untuk objek S3 yang merupakan file terkompresi atau arsip. Nilai Terkompresi menunjukkan ukuran penyimpanan total objek yang menggunakan kelas penyimpanan Amazon S3 didukung dan memiliki ekstensi nama file untuk tipe file terkompresi atau arsip yang didukung. Nilai Tidak terkompresi menunjukkan ukuran perkiraan objek ini jika didekompresi, berdasarkan rasio kompresi tertentu. Data ini relevan dikarenakan cara Macie menganalisis file terkompresi dan file arsip.

Ketika Macie menganalisis file terkompresi atau arsip, Macie memeriksa keseluruhan file dan isi dari file tersebut. Untuk memeriksa isi file, Macie mendekompresikan file, lalu memeriksa setiap file yang diekstraksi menggunakan format yang didukung. Oleh karena itu, jumlah aktual data yang dianalisis tugas tergantung pada:

- Apakah file menggunakan kompresi dan, jika demikian, rasio kompresi yang digunakan.
- Jumlah, ukuran, dan format file yang diekstraksi.

Secara default, Macie mengasumsikan berikut ini ketika menghitung perkiraan biaya untuk tugas:

- Semua file terkompresi dan arsip menggunakan rasio kompresi 3:1.
- Semua file yang diekstraksi menggunakan format file atau penyimpanan yang didukung.

Asumsi ini dapat menghasilkan perkiraan ukuran yang lebih besar untuk ruang lingkup data yang akan dianalisis tugas, dan, akibatnya, perkiraan biaya menjadi lebih tinggi untuk tugas tersebut.

Anda dapat menghitung ulang total perkiraan biaya tugas berdasarkan rasio kompresi yang berbeda. Untuk melakukan ini, pilih rasio dari daftar Pilih perkiraan rasio kompresi di bagian Perkiraan biaya. Macie kemudian memperbarui perkiraan untuk mencocokkan pilihan Anda.

Untuk informasi selengkapnya tentang bagaimana Macie menghitung perkiraan biaya, lihat [Memahami cara perkiraan biaya penggunaan dihitung](#).

## Memantau perkiraan biaya untuk tugas penemuan data sensitif

Jika Anda sudah menjalankan tugas penemuan data sensitif, halaman Penggunaan pada konsol Amazon Macie dapat membantu Anda memantau perkiraan biaya tugas tersebut. Halaman ini menunjukkan perkiraan biaya Anda (dalam Dolar AS) untuk menggunakan Macie saat ini Wilayah AWS selama bulan kalender saat ini. Untuk informasi selengkapnya tentang cara Macie menghitung perkiraan ini, lihat [Memahami cara perkiraan biaya penggunaan dihitung](#).

Untuk meninjau perkiraan biaya Anda untuk menjalankan tugas

1. Buka konsol Amazon Macie di <https://console.aws.amazon.com/macie/>.
2. Dengan menggunakan pemilih Wilayah AWS di bagian pojok kanan atas halaman, pilih Wilayah tempat Anda ingin meninjau perkiraan biaya.
3. Pada panel navigasi, pilih Penggunaan.
4. Pada halaman Penggunaan, lihat rincian perkiraan biaya untuk akun Anda. Item Tugas penemuan data sensitif melaporkan perkiraan total biaya untuk tugas yang telah Anda jalankan sejauh ini selama bulan saat ini selama bulan saat ini di Wilayah saat ini.

Jika Anda adalah administrator Macie untuk sebuah organisasi, bagian Perkiraan biaya menunjukkan keseluruhan perkiraan biaya untuk organisasi Anda untuk bulan saat ini di Wilayah saat ini. Untuk menampilkan perkiraan total biaya tugas yang dijalankan untuk akun tertentu, pilih akun dalam tabel. Bagian Perkiraan biaya kemudian menunjukkan rincian perkiraan biaya untuk akun, termasuk perkiraan biaya tugas yang dijalankan. Untuk menampilkan data ini untuk akun yang berbeda, pilih akun di tabel. Untuk menghapus pilihan akun Anda, pilih X di samping ID akun.

Untuk meninjau dan memantau biaya aktual Anda, gunakan [AWS Billing and Cost Management](#).

## Pengidentifikasi data terkelola direkomendasikan untuk pekerjaan penemuan data sensitif

Untuk mengoptimalkan hasil pekerjaan penemuan data sensitif, Anda dapat mengonfigurasi tugas individual agar secara otomatis menggunakan kumpulan pengidentifikasi data terkelola yang kami rekomendasikan untuk pekerjaan. SEBUAH pengenal data terkelola adalah seperangkat kriteria dan teknik bawaan yang dirancang untuk mendeteksi jenis data sensitif tertentu—misalnya, AWS kunci akses rahasia, nomor kartu kredit, atau nomor paspor untuk negara atau wilayah tertentu.

Kumpulan pengidentifikasi data terkelola yang direkomendasikan dirancang untuk mendeteksi kategori umum dan jenis data sensitif. Berdasarkan penelitian kami, ini dapat mendeteksi kategori umum dan jenis data sensitif sekaligus mengoptimalkan hasil pekerjaan Anda dengan mengurangi kebisingan. Saat kami merilis pengidentifikasi data terkelola baru, kami menambahkannya ke set ini jika kemungkinan besar akan mengoptimalkan hasil pekerjaan Anda lebih lanjut. Seiring waktu, kami mungkin juga menambahkan atau menghapus pengidentifikasi data terkelola yang ada dari set. Jika kami menambahkan atau menghapus pengenalan data terkelola dari set yang disarankan, kami memperbarui halaman ini untuk menunjukkan sifat dan waktu perubahan. Untuk peringatan otomatis tentang perubahan ini, Anda dapat berlangganan RSS feed di [Riwayat dokumen Macie](#) halaman.

Saat Anda membuat pekerjaan penemuan data sensitif, Anda menentukan pengenalan data terkelola yang ingin digunakan untuk menganalisis objek di bucket Amazon Simple Storage Service (Amazon S3). Untuk mengonfigurasi pekerjaan agar menggunakan kumpulan pengidentifikasi data terkelola yang direkomendasikan, pilih [Direkomendasikan](#) pilihan ketika Anda membuat pekerjaan. Pekerjaan kemudian akan secara otomatis menggunakan semua pengidentifikasi data terkelola yang berada di set yang direkomendasikan ketika pekerjaan mulai berjalan. Jika Anda mengonfigurasi pekerjaan agar berjalan lebih dari satu kali, setiap proses akan secara otomatis menggunakan semua pengidentifikasi data terkelola yang ada di set yang disarankan saat dijalankan.

Topik berikut mencantumkan pengidentifikasi data terkelola yang saat ini berada dalam kumpulan yang direkomendasikan, disusun berdasarkan kategori dan jenis data sensitif. Mereka menentukan pengenalan unik (ID) untuk setiap pengidentifikasi data terkelola di set. ID ini menjelaskan jenis data sensitif yang dirancang untuk dideteksi oleh pengenalan data terkelola, misalnya: `PGP_PRIVATE_KEY` untuk kunci pribadi PGP dan `USA_PASSPORT_NUMBER` untuk nomor paspor AS.

Topik

- [Kredensial](#)
- [Informasi keuangan](#)
- [Informasi yang dapat diidentifikasi secara pribadi \(PII\)](#)
- [Pembaruan ke set yang disarankan](#)

Untuk detail tentang pengidentifikasi data terkelola tertentu atau daftar lengkap semua pengidentifikasi data terkelola yang saat ini disediakan Macie, lihat [Menggunakan pengidentifikasi data terkelola](#).

## Kredensial

Untuk mendeteksi kemunculan data kredensial di objek S3, kumpulan yang disarankan menggunakan pengenal data terkelola berikut.

Tipe data sensitif	ID pengenal data terkelola
AWS secret access key	AWS_CREDENTIALS
Header Otorisasi Dasar HTTP	HTTP_BASIC_AUTH_HEADER
Kunci pribadi OpenSSH	OPENSSSH_PRIVATE_KEY
Kunci pribadi PGP	PGP_PRIVATE_KEY
Kunci pribadi Standar Kriptografi Kunci Publik (PKCS)	PKCS
kunci pribadi PuTTY	PUTTY_PRIVATE_KEY

## Informasi keuangan

Untuk mendeteksi kejadian informasi keuangan di objek S3, kumpulan yang disarankan menggunakan pengidentifikasi data terkelola berikut.

Tipe data sensitif	ID pengenal data terkelola
Data strip magnetik kartu kredit	CREDIT_CARD_MAGNETIC_STRIPE
Nomor kartu kredit	CREDIT_CARD_NUMBER (untuk nomor kartu kredit di dekat kata kunci)

## Informasi yang dapat diidentifikasi secara pribadi (PII)

Untuk mendeteksi kejadian informasi identitas pribadi (PII) di objek S3, kumpulan yang disarankan menggunakan pengidentifikasi data terkelola berikut.

Tipe data sensitif	ID pengenal data terkelola
Nomor identifikasi lisensi	CANADA_DRIVERS_LICENSE, DRIVERS_LICENSE (untuk AS), UK_DRIVERS_LICENSE
Nomor Roll Pemilu	UK_ELECTORAL_ROLL_NUMBER
Nomor identifikasi nasional	FRANCE_NATIONAL_IDENTIFICATION_NUMBER, GERMANY_NATIONAL_IDENTIFICATION_NUMBER, ITALY_NATIONAL_IDENTIFICATION_NUMBER, SPAIN_DNI_NUMBER
Nomor Asuransi Nasional (NINO)	UK_NATIONAL_INSURANCE_NUMBER
Nomor paspor	CANADA_PASSPORT_NUMBER, FRANCE_PASSPORT_NUMBER, GERMANY_PASSPORT_NUMBER, ITALY_PASSPORT_NUMBER, SPAIN_PASSPORT_NUMBER, UK_PASSPORT_NUMBER, USA_PASSPORT_NUMBER
Nomor Pokok Wajib Pajak (SIN)	CANADA_SOCIAL_INSURANCE_NUMBER
Nomor Jaminan Sosial (SSN)	SPAIN_SOCIAL_SECURITY_NUMBER, USA_SOCIAL_SECURITY_NUMBER
Nomor identifikasi wajib pajak atau referensi	AUSTRALIA_TAX_FILE_NUMBER, BRAZIL_CPF_NUMBER, FRANCE_TAX_IDENTIFICATION_NUMBER, GERMANY_TAX_IDENTIFICATION_NUMBER, SPAIN_NIE_NUMBER, SPAIN_NIF_NUMBER, SPAIN_TAX_IDENTIFICATION_NUMBER, USA_INDIVIDUAL_TAX_IDENTIFICATION_NUMBER

## Pembaruan ke set yang disarankan

Tabel berikut menjelaskan perubahan pada kumpulan pengidentifikasi data terkelola yang kami rekomendasikan untuk pekerjaan penemuan data sensitif. Untuk peringatan otomatis tentang perubahan ini, berlangganan RSS feed pada [Riwayat dokumen Macie](#) halaman.

Perubahan	Deskripsi	Tanggal
Ketersediaan umum	Pelepasan awal dari set yang direkomendasikan.	27 Juni 2023

## Menganalisis objek Amazon S3 terenkripsi dengan Amazon Macie

Saat Anda mengaktifkan Amazon Macie untuk Akun AWS, Macie membuat [peran terkait layanan yang memberi](#) Macie izin yang diperlukan untuk memanggil Amazon Simple Storage Service (Amazon S3) dan lainnya atas nama Anda. Layanan AWS Peran terkait layanan menyederhanakan proses penyiapan Layanan AWS karena Anda tidak perlu menambahkan izin secara manual untuk layanan untuk menyelesaikan tindakan atas nama Anda. Untuk mempelajari lebih lanjut tentang jenis peran ini, lihat [Menggunakan peran terkait layanan](#) di AWS Identity and Access Management [Panduan Pengguna](#).

Kebijakan izin untuk peran terkait layanan Macie (`AWSServiceRoleForAmazonMacie`) memungkinkan Macie melakukan tindakan yang mencakup pengambilan informasi tentang bucket dan objek S3 Anda, serta mengambil dan menganalisis objek di bucket S3 Anda. Jika akun Anda adalah akun administrator Macie untuk suatu organisasi, kebijakan tersebut juga memungkinkan Macie untuk melakukan tindakan ini atas nama Anda untuk akun anggota di organisasi Anda.

Jika objek S3 dienkripsi, kebijakan izin untuk peran terkait layanan Macie biasanya memberi Macie izin yang diperlukan untuk mendekripsi objek. Namun, ini tergantung pada jenis enkripsi yang digunakan. Hal ini juga dapat tergantung pada apakah Macie diperbolehkan untuk menggunakan kunci enkripsi yang sesuai.

### Topik

- [Opsional enkripsi untuk objek Amazon S3](#)
- [Mengizinkan Amazon Macie menggunakan pelanggan yang dikelola AWS KMS key](#)



## Opsi enkripsi untuk objek Amazon S3

Amazon S3 mendukung beberapa opsi enkripsi untuk objek S3. Untuk sebagian besar opsi ini, Amazon Macie dapat mendekripsi objek dengan menggunakan peran terkait layanan Macie untuk akun Anda. Namun, hal ini tergantung pada tipe enkripsi yang digunakan untuk mengenkripsi suatu objek.

### Enkripsi sisi server dengan kunci terkelola Amazon S3 (SSE-S3)

Jika objek dienkripsi menggunakan enkripsi sisi server dengan kunci terkelola Amazon S3 (SSE-S3), Macie dapat mendekripsi objek tersebut.

Untuk mempelajari jenis enkripsi ini, lihat [Menggunakan enkripsi sisi server dengan kunci terkelola Amazon S3 di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon](#).

### Enkripsi sisi server dengan AWS KMS keys (DSSE-KMS dan SSE-KMS)

Jika objek dienkripsi menggunakan enkripsi sisi server dua lapisan atau enkripsi sisi server dengan AWS terkelola AWS KMS key (DSSE-KMS atau SSE-KMS), Macie dapat mendekripsi objek tersebut.

[Jika objek dienkripsi menggunakan enkripsi sisi server dua lapis atau enkripsi sisi server dengan pelanggan yang dikelola AWS KMS key \(DSSE-KMS atau SSE-KMS\), Macie dapat mendekripsi objek hanya jika Anda mengizinkan Macie menggunakan kunci tersebut.](#) Ini adalah kasus untuk objek yang dienkripsi dengan kunci KMS dikelola sepenuhnya di dalam AWS KMS dan kunci KMS di penyimpanan kunci eksternal. Jika Macie tidak diizinkan menggunakan kunci KMS yang berlaku, Macie hanya dapat menyimpan dan melaporkan metadata untuk objek tersebut.

Untuk mempelajari jenis enkripsi ini, lihat [Menggunakan enkripsi sisi server dua lapis dengan AWS KMS keys dan Menggunakan enkripsi sisi server dengan Panduan Pengguna Layanan Penyimpanan Sederhana AWS KMS keys](#) Amazon.

#### Tip

Anda dapat secara otomatis membuat daftar semua pelanggan yang dikelola AWS KMS keys yang perlu diakses Macie untuk menganalisis objek di bucket S3 untuk akun Anda. Untuk melakukan ini, jalankan skrip AWS KMS Permission Analyzer, yang tersedia dari repositori [Amazon Macie Scripts](#). GitHub Script juga dapat menghasilkan script tambahan dari AWS Command Line Interface (AWS CLI) perintah. Anda dapat menjalankan perintah

tersebut secara opsional untuk memperbarui pengaturan konfigurasi dan kebijakan yang diperlukan untuk kunci KMS yang Anda tentukan.

### Enkripsi sisi server dengan kunci yang disediakan pelanggan (SSE-C)

Jika objek dienkripsi menggunakan enkripsi sisi server dengan kunci yang disediakan pelanggan (SSE-C), Macie tidak dapat mendekripsi objek tersebut. Macie hanya dapat menyimpan dan melaporkan metadata untuk objek.

Untuk mempelajari jenis enkripsi ini, lihat [Menggunakan enkripsi sisi server dengan kunci yang disediakan pelanggan di Panduan Pengguna](#) Layanan Penyimpanan Sederhana Amazon.

### Enkripsi sisi klien

Jika objek dienkripsi menggunakan enkripsi sisi klien, Macie tidak dapat mendekripsi objek. Macie hanya dapat menyimpan dan melaporkan metadata untuk objek. Misalnya, Macie dapat melaporkan ukuran objek dan tag yang terkait dengan objek tersebut.

Untuk mempelajari jenis enkripsi ini dalam konteks Amazon S3, lihat [Melindungi data dengan menggunakan enkripsi sisi klien di](#) Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

Anda dapat [memfilter inventaris bucket](#) di Macie untuk menentukan bucket S3 mana yang menyimpan objek yang menggunakan jenis enkripsi tertentu. Anda juga dapat menentukan bucket mana yang secara default menggunakan tipe enkripsi sisi server tertentu saat menyimpan objek baru. Tabel berikut memberikan contoh filter yang dapat Anda terapkan ke inventaris bucket Anda untuk menemukan informasi ini.

Untuk menunjukkan bucket yang...	Terapkan filter ini...
Menyimpan objek yang menggunakan enkripsi SSE-C	Jumlah objek dengan enkripsi disediakan Pelanggan dan Dari = 1
Simpan objek yang menggunakan enkripsi DSSE-KMS atau SSE-KMS	Jumlah objek dengan enkripsi AWS KMS dikelola dan Dari = 1
Simpan objek yang menggunakan enkripsi SSE-S3	Jumlah objek dengan enkripsi dikelola Amazon S3 dan Dari = 1

Untuk menunjukkan bucket yang...	Terapkan filter ini...
Menyimpan objek yang menggunakan enkripsi sisi klien (atau tidak dienkripsi)	Jumlah objek berdasarkan enkripsi adalah Tidak ada enkripsi dan Dari = 1
Enkripsi objek baru secara default menggunakan enkripsi DSSE-KMS	Enkripsi default = aws:kms:dsse
Enkripsi objek baru secara default menggunakan enkripsi SSE-KMS	Enkripsi default = aws:kms
Enkripsi objek baru secara default menggunakan enkripsi SSE-S3	Enkripsi default = AES256

Jika bucket dikonfigurasi untuk mengenkripsi objek baru secara default menggunakan enkripsi DSSE-KMS atau SSE-KMS, Anda juga dapat menentukan mana yang digunakan. AWS KMS key Untuk melakukan ini, pilih ember di halaman bucket S3. Di panel detail bucket, di bawah enkripsi sisi server, lihat bidang. AWS KMS key Bidang ini menunjukkan Nama Sumber Daya Amazon (ARN) atau pengenal unik (ID kunci) untuk kunci tersebut.

## Mengizinkan Amazon Macie menggunakan pelanggan yang dikelola AWS KMS key

Jika objek Amazon S3 dienkripsi menggunakan enkripsi sisi server dua lapisan atau enkripsi sisi server dengan pelanggan yang dikelola (DSSE-KMS AWS KMS key atau SSE-KMS), Amazon Macie dapat mendekripsi objek hanya jika diizinkan untuk menggunakan kunci. Cara menyediakan akses ini tergantung pada apakah akun yang memiliki kunci juga memiliki bucket S3 yang menyimpan objek:

- Jika akun yang sama memiliki AWS KMS key dan bucket, pengguna akun harus memperbarui kebijakan kunci.
- Jika satu akun memiliki AWS KMS key dan akun lain memiliki bucket, pengguna akun yang memiliki kunci harus mengizinkan akses lintas akun ke kunci tersebut.

Topik ini menjelaskan cara melakukan tugas-tugas ini dan memberikan contoh untuk kedua skenario tersebut. Untuk mempelajari selengkapnya tentang mengizinkan akses ke pelanggan yang dikelola AWS KMS keys, lihat [Otentikasi dan kontrol akses untuk AWS KMS](#) di Panduan AWS Key Management Service Pengembang.

## Mengizinkan akses akun yang sama ke kunci yang dikelola pelanggan

Jika akun yang sama memiliki bucket AWS KMS key dan S3, pengguna akun harus menambahkan pernyataan ke kebijakan untuk kunci tersebut. Pernyataan tambahan harus mengizinkan peran terkait layanan Macie agar akun dapat mendekripsi data dengan menggunakan kunci. Untuk informasi detail tentang pembaruan kebijakan kunci, lihat [Mengganti kebijakan kunci](#) dalam Panduan Developer AWS Key Management Service.

Dalam pernyataan:

- `PrincipalElement` harus menentukan Nama Sumber Daya Amazon (ARN) dari peran terkait layanan Macie untuk akun yang memiliki bucket dan S3. AWS KMS key

Jika akun dalam opt-inWilayah AWS, ARN juga harus menyertakan kode Wilayah yang sesuai untuk Wilayah tersebut. Misalnya, jika akun tersebut berada di Wilayah Middle East (Bahrain), yang memiliki kode Wilayah `me-south-1`, elemen `Principal` harus menentukan `arn:aws:iam::123456789012:role/aws-service-role/macie.me-south-1.amazonaws.com/AWSServiceRoleForAmazonMacie`, angka `123456789012` adalah ID akun untuk akun tersebut. Untuk daftar kode Wilayah untuk Wilayah di mana Macie saat ini tersedia, lihat [titik akhir dan kuota Amazon Macie](#) di. Referensi Umum AWS

- `Action` harus menentukan tindakan `kms:Decrypt`. Ini adalah satu-satunya AWS KMS tindakan yang Macie harus diizinkan untuk melakukan untuk mendekripsi objek S3 yang dienkripsi dengan kunci.

Berikut ini adalah contoh pernyataan untuk ditambahkan ke kebijakan untuk AWS KMS key.

```
{
  "Sid": "Allow the Macie service-linked role to use the key",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::123456789012:role/aws-service-role/macie.amazonaws.com/AWSServiceRoleForAmazonMacie"
  },
  "Action": [
    "kms:Decrypt"
  ],
  "Resource": "*"
}
```

Dalam contoh sebelumnya:

- `AWSBidang` dalam `Principal` elemen menentukan ARN dari peran `AWSServiceRoleForAmazonMacie` terkait layanan Macie () untuk akun. Hal ini memungkinkan peran terkait layanan Macie untuk melakukan tindakan yang ditentukan oleh pernyataan kebijakan. `123456789012` adalah contoh ID akun. Ganti nilai ini dengan ID akun untuk akun yang memiliki kunci KMS dan bucket S3.
- `ActionArray` menentukan tindakan yang diizinkan untuk dilakukan oleh peran terkait layanan Macie menggunakan kunci KMS — mendekripsi ciphertext yang dienkripsi dengan kunci.

Tempat Anda menambahkan pernyataan ini ke kebijakan kunci bergantung pada struktur dan elemen yang saat ini berisi kebijakan. Ketika Anda menambahkan pernyataan, pastikan bahwa sintaksnya valid. Kebijakan kunci menggunakan format JSON. Ini berarti bahwa Anda juga harus menambahkan koma sebelum atau setelah pernyataan, tergantung pada tempat Anda menambahkan pernyataan ke kebijakan.

## Mengizinkan akses lintas akun ke kunci yang dikelola pelanggan

Jika satu akun memiliki AWS KMS key (pemilik kunci) dan akun lain memiliki bucket S3 (pemilik bucket), pemilik kunci harus memberi pemilik bucket akses lintas akun ke kunci KMS. Untuk melakukan ini, pemilik kunci terlebih dahulu memastikan bahwa kebijakan kunci memungkinkan pemilik bucket untuk menggunakan kunci dan membuat hibah untuk kunci tersebut. Pemilik ember kemudian membuat hibah untuk kunci tersebut. Hibah adalah instrumen kebijakan yang memungkinkan AWS prinsipal untuk menggunakan kunci KMS dalam operasi kriptografi jika kondisi yang ditentukan oleh hibah terpenuhi. Dalam hal ini, hibah mendelegasikan izin yang relevan ke peran terkait layanan Macie untuk akun pemilik bucket.

Untuk informasi detail tentang pembaruan kebijakan kunci, lihat [Mengganti kebijakan kunci](#) dalam Panduan Developer AWS Key Management Service. Untuk mempelajari tentang hibah, lihat [Hibah AWS KMS di Panduan AWS Key Management Service](#) Pengembang.

### Langkah 1: Perbarui kebijakan utama

Dalam kebijakan kunci, pemilik kunci harus memastikan bahwa kebijakan tersebut mencakup dua pernyataan:

- Pernyataan pertama memungkinkan pemilik bucket menggunakan kunci untuk mendekripsi data.
- Pernyataan kedua memungkinkan pemilik bucket untuk membuat hibah untuk peran terkait layanan Macie untuk akun mereka (pemilik bucket).

Dalam pernyataan pertama, elemen `Principal` harus menentukan ARN dari akun pemilik bucket. Array `Action` harus menentukan tindakan `kms:Decrypt`. Ini adalah satu-satunya AWS KMS tindakan yang Macie harus diizinkan untuk melakukan untuk mendekripsi objek yang dienkripsi dengan kunci. Berikut ini adalah contoh pernyataan ini dalam kebijakan untuk AWS KMS key.

```
{
  "Sid": "Allow account 111122223333 to use the key",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:root"
  },
  "Action": [
    "kms:Decrypt"
  ],
  "Resource": "*"
}
```

Dalam contoh sebelumnya:

- Bidang `AWS` di elemen `Principal` menentukan ARN dari akun pemilik bucket ini (`111122223333`). Hal ini memungkinkan pemilik bucket untuk melakukan tindakan yang ditentukan oleh pernyataan kebijakan. `111122223333` adalah contoh ID akun. Ganti nilai ini dengan ID akun untuk akun pemilik bucket.
- `ActionArray` menentukan tindakan yang diizinkan oleh pemilik bucket menggunakan kunci KMS—mendekripsi ciphertext yang dienkripsi dengan kunci.

Pernyataan kedua di kebijakan kunci mengizinkan pemilik bucket membuat hibah untuk peran terkait layanan Macie untuk akun mereka. Dalam pernyataan ini, elemen `Principal` harus menentukan ARN dari akun pemilik bucket. Array `Action` harus menentukan tindakan `kms:CreateGrant`. Elemen `Condition` dapat memfilter akses ke tindakan `kms:CreateGrant` yang ditentukan dalam pernyataan. Berikut ini adalah contoh pernyataan ini dalam kebijakan untuk AWS KMS key.

```
{
  "Sid": "Allow account 111122223333 to create a grant",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:root"
  },
  "Action": [
    "kms:CreateGrant"
  ]
}
```

```
    ],
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "kms:GranteePrincipal": "arn:aws:iam::111122223333:role/aws-service-role/
macie.amazonaws.com/AWSServiceRoleForAmazonMacie"
      }
    }
  }
}
```

Dalam contoh sebelumnya:

- Bidang AWS di elemen `Principal` menentukan ARN dari akun pemilik bucket ini (`111122223333`). Hal ini memungkinkan pemilik bucket untuk melakukan tindakan yang ditentukan oleh pernyataan kebijakan. `111122223333` adalah contoh ID akun. Ganti nilai ini dengan ID akun untuk akun pemilik bucket.
- `ActionArray` menentukan tindakan yang diizinkan dilakukan pemilik bucket pada kunci KMS—buat hibah untuk kunci tersebut.
- Elemen `Condition` menggunakan [operator kondisi](#) `StringEquals` dan [kunci syarat](#) `kms:GranteePrincipal` untuk memfilter akses ke tindakan yang ditentukan oleh pernyataan kebijakan. Dalam hal ini, pemilik bucket hanya dapat membuat hibah untuk yang ditentukan `GranteePrincipal`, yang merupakan ARN dari peran terkait layanan Macie untuk akun mereka. Dalam ARN itu, `111122223333` adalah contoh ID akun. Ganti nilai ini dengan ID akun untuk akun pemilik bucket.

Jika akun pemilik bucket ikut serta Wilayah AWS, sertakan juga kode Wilayah yang sesuai di ARN peran terkait layanan Macie. Misalnya, jika akun berada di Wilayah Middle East (Bahrain), yang memiliki kode Wilayah `me-south-1`, ganti `macie.amazonaws.com` dengan `macie.me-south-1.amazonaws.com` di ARN. Untuk daftar kode Wilayah untuk Wilayah di mana Macie saat ini tersedia, lihat [titik akhir dan kuota Amazon Macie](#) di Referensi Umum AWS

Tempat pemilik kunci menambah pernyataan ke kebijakan kunci bergantung pada struktur dan elemen yang saat ini berisi kebijakan. Ketika pemilik kunci menambahkan pernyataan, mereka harus memastikan bahwa sintaksnya valid. Kebijakan kunci menggunakan format JSON. Ini berarti bahwa pemilik kunci juga harus menambahkan koma sebelum atau sesudah setiap pernyataan, tergantung di mana mereka menambahkan pernyataan ke kebijakan.

## Langkah 2: Buat hibah

Setelah pemilik kunci memperbarui kebijakan kunci seperlunya, pemilik bucket harus membuat hibah untuk kunci tersebut. Pemberian ini mendelegasikan izin yang relevan ke peran terkait layanan Macie untuk akun (pemilik bucket) mereka. Sebelum pemilik bucket membuat hibah, mereka harus memverifikasi bahwa mereka diizinkan untuk melakukan tindakan `kms:CreateGrant` untuk akun mereka. Tindakan ini memungkinkan mereka untuk menambahkan hibah ke pelanggan yang sudah ada dan dikelola AWS KMS key.

Untuk membuat hibah, pemilik bucket dapat menggunakan [CreateGrant](#) pengoperasian AWS Key Management Service API. Ketika pemilik bucket membuat hibah, mereka harus menentukan nilai berikut untuk parameter yang diperlukan:

- `KeyId`— ARN dari kunci KMS. Untuk akses lintas akun ke kunci KMS, nilai ini harus berupa ARN. Tidak bisa menggunakan kunci ID.
- `GranteePrincipal`— ARN dari peran terkait layanan Macie (`AWSServiceRoleForAmazonMacie` untuk akun mereka. Nilai ini harus `arn:aws:iam::111122223333:role/aws-service-role/macie.amazonaws.com/AWSServiceRoleForAmazonMacie`, yang mana `111122223333` adalah ID akun untuk akun pemilik bucket.

Jika akun mereka berada di Wilayah keikutsertaan, ARN harus menyertakan kode Wilayah yang sesuai. Misalnya, jika akun mereka berada di Wilayah Timur Tengah (Bahrain), yang memiliki kode Wilayah `saya-selatan-1`, ARN `arn:aws:iam::111122223333:role/aws-service-role/macie.me-south-1.amazonaws.com/AWSServiceRoleForAmazonMacie` seharusnya, di mana `111122223333` adalah ID akun untuk akun pemilik bucket.

- `Operations`— Tindakan AWS KMS dekripsi (`Decrypt`). Ini adalah satu-satunya AWS KMS tindakan yang Macie harus diizinkan untuk melakukan untuk mendekripsi objek yang dienkripsi dengan kunci KMS.

Untuk membuat hibah untuk kunci KMS yang dikelola pelanggan dengan menggunakan AWS Command Line Interface (AWS CLI), jalankan perintah [create-grant](#). Contoh berikut menunjukkan cara melakukannya. Contoh ini diformat untuk Microsoft Windows dan menggunakan karakter kelanjutan baris caret (^) untuk meningkatkan keterbacaan.

```
C:\> aws kms create-grant ^
--key-id arn:aws:kms:us-east-1:123456789012:key/1234abcd-12ab-34cd-56ef-1234567890ab ^
--grantee-principal arn:aws:iam::111122223333:role/aws-service-role/
macie.amazonaws.com/AWSServiceRoleForAmazonMacie ^
```



**--operations "Decrypt"**

Di mana:

- `key-id` menentukan ARN dari kunci KMS untuk menerapkan hibah ke.
- `grantee-principal` menentukan ARN peran terkait layanan Macie untuk akun yang diizinkan untuk melakukan tindakan yang ditentukan oleh hibah. Nilai ini harus sesuai dengan ARN yang ditentukan oleh `kms:GranteePrincipal` kondisi pernyataan kedua dalam kebijakan kunci.
- `operations` menentukan tindakan bahwa hibah memungkinkan prinsipal yang ditentukan untuk melakukan—mendekripsi ciphertext yang dienkripsi dengan kunci KMS.

Jika perintah berjalan dengan berhasil, Anda menerima output yang mirip dengan berikut ini.

```
{
  "GrantToken": "<grant token>",
  "GrantId": "1a2b3c4d2f5e69f440bae30eaec9570bb1fb7358824f9ddfa1aa5a0dab1a59b2"
}
```

Yang mana `GrantToken` merupakan string yang unik, non-rahasia, variabel-panjang, base64-encoded yang mewakili hibah yang diciptakan, dan `GrantId` adalah pengidentifikasi unik untuk hibah.

## Menyimpan dan mempertahankan hasil penemuan data sensitif dengan Amazon Macie

Saat Anda menjalankan pekerjaan penemuan data sensitif atau Amazon Macie melakukan penemuan data sensitif otomatis, Macie membuat catatan analisis untuk setiap objek Amazon Simple Storage Service (Amazon S3) yang disertakan dalam cakupan analisis. Catatan ini, disebut sebagai hasil penemuan data sensitif, mencatat detail tentang analisis yang dilakukan Macie pada objek S3 individu. Ini termasuk objek yang Macie tidak mendeteksi data sensitif, dan karena itu tidak menghasilkan temuan, dan objek yang tidak dapat dianalisis Macie karena kesalahan atau masalah. Jika Macie mendeteksi data sensitif dalam suatu objek, catatan tersebut mencakup data dari temuan yang sesuai serta informasi tambahan. Hasil penemuan data sensitif memberi Anda catatan analisis yang dapat membantu audit atau investigasi privasi dan perlindungan data.

Macie menyimpan hasil penemuan data sensitif Anda hanya selama 90 hari. Untuk mengakses hasil Anda dan mengaktifkan penyimpanan dan retensi jangka panjang, konfigurasi Macie untuk

mengkripsi hasil dengan kunci AWS Key Management Service (AWS KMS) dan menyimpannya dalam bucket S3. Bucket dapat berfungsi sebagai repositori jangka panjang definitif untuk semua hasil penemuan data sensitif Anda. Anda kemudian dapat secara opsional mengakses dan menanyakan hasil di repositori itu.

Topik ini memandu Anda melalui proses penggunaan AWS Management Console untuk mengonfigurasi repositori untuk hasil penemuan data sensitif Anda. Konfigurasi adalah kombinasi dari AWS KMS key yang mengenkripsi hasil, bucket S3 yang menyimpan hasil, dan pengaturan Macie yang menunjukkan kunci dan bucket mana yang akan digunakan. Jika Anda lebih suka mengonfigurasi pengaturan Macie secara terprogram, Anda dapat menggunakan [PutClassificationExportConfiguration](#) pengoperasian Amazon Macie API.

Ketika Anda mengonfigurasi pengaturan di Macie, pilihan Anda hanya berlaku untuk Wilayah AWS saat ini. Jika Anda administrator Macie untuk suatu organisasi, pilihan Anda hanya berlaku untuk akun Anda. Pilihan tersebut tidak berlaku untuk akun anggota yang terkait.

Jika Anda menggunakan Macie dalam beberapa Wilayah AWS, konfigurasi pengaturan repositori untuk setiap Wilayah tempat Anda menggunakan Macie. Anda dapat secara opsional menyimpan hasil penemuan data sensitif untuk beberapa Wilayah dalam bucket S3 yang sama. Namun, perhatikan persyaratan berikut:

- Untuk menyimpan hasil untuk Wilayah yang AWS diaktifkan secara default Akun AWS, seperti Wilayah AS Timur (Virginia N.), Anda harus memilih bucket di Wilayah yang diaktifkan secara default. Hasilnya tidak dapat disimpan dalam bucket di Wilayah keikutsertaan (Wilayah yang dinonaktifkan secara default).
- Untuk menyimpan hasil untuk Wilayah keikutsertaan, seperti Wilayah Timur Tengah (Bahrain), Anda harus memilih ember di Wilayah yang sama atau Wilayah yang diaktifkan secara default. Hasilnya tidak dapat disimpan dalam ember di Wilayah keikutsertaan yang berbeda.

Untuk menentukan apakah Wilayah diaktifkan secara default, lihat [Wilayah dan titik akhir](#) di Panduan AWS Identity and Access Management Pengguna. Selain persyaratan sebelumnya, pertimbangkan juga apakah Anda ingin [mengambil sampel data sensitif](#) yang dilaporkan Macie dalam temuan individu. Untuk mengambil sampel data sensitif dari objek S3 yang terpengaruh, semua sumber daya dan data berikut harus disimpan di Wilayah yang sama: objek yang terpengaruh, temuan yang berlaku, dan hasil penemuan data sensitif yang sesuai.

## Tugas

- [Gambaran Umum](#)

- [Langkah 1: Verifikasi izin Anda](#)
- [Langkah 2: Konfigurasi AWS KMS key](#)
- [Langkah 3: Pilih ember S3](#)

## Gambaran Umum

Amazon Macie secara otomatis membuat hasil penemuan data sensitif untuk setiap objek Amazon S3 yang dianalisis atau coba dianalisis saat Anda menjalankan pekerjaan penemuan data sensitif atau melakukan penemuan data sensitif otomatis untuk akun atau organisasi Anda. Hal ini mencakup:

- Objek yang Macie mendeteksi data sensitif, dan karena itu juga menghasilkan temuan data sensitif.
- Objek yang Macie tidak mendeteksi data sensitif, dan karenanya tidak menghasilkan temuan data sensitif.
- Objek yang tidak dapat dianalisis Macie karena kesalahan atau masalah seperti pengaturan izin atau penggunaan file atau format penyimpanan yang tidak didukung.

Jika Macie mendeteksi data sensitif dalam objek S3, hasil penemuan data sensitif mencakup data dari temuan data sensitif yang sesuai. Ini memberikan informasi tambahan juga, seperti lokasi tempat terjadinya 1.000 kejadian dari setiap tipe data sensitif yang Macie temukan dalam objek. Sebagai contoh:

- Nomor kolom dan baris untuk sel atau bidang di buku kerja Microsoft Excel, file CSV, atau file TSV
- Jalur ke bidang atau array dalam file JSON atau JSON Lines
- Nomor baris untuk baris dalam file teks non-biner selain file CSV, JSON, JSON Lines, atau TSV, misalnya, file HTML, TXT, atau XML
- Nomor halaman untuk halaman dalam file Format Dokumen Portabel Adobe (PDF)
- Indeks catatan dan jalur ke bidang dalam catatan di kontainer objek Apache Avro atau file Apache Parquet

Jika objek S3 yang terpengaruh adalah file arsip, seperti file.tar atau .zip, hasil penemuan data sensitif juga menyediakan data lokasi terperinci untuk kemunculan data sensitif dalam file individual yang diekstrak Macie dari arsip. Macie tidak menyertakan informasi ini dalam temuan data sensitif untuk file arsip. Untuk melaporkan data lokasi, hasil penemuan data sensitif menggunakan skema [JSON standar](#).

Hasil penemuan data sensitif tidak termasuk data sensitif yang ditemukan Macie. Sebaliknya, ini memberi Anda catatan analisis yang dapat membantu untuk audit atau investigasi.

Macie menyimpan hasil penemuan data sensitif Anda selama 90 hari. Anda tidak dapat mengaksesnya langsung di konsol Amazon Macie atau dengan Amazon Macie API. Sebagai gantinya, ikuti langkah-langkah dalam topik ini untuk mengonfigurasi Macie untuk mengenkripsi hasil Anda dengan AWS KMS key yang Anda tentukan, dan simpan hasilnya dalam bucket S3 yang juga Anda tentukan. Macie kemudian menulis hasilnya ke file JSON Lines (.jsonl), menambahkan file ke bucket sebagai file GNU Zip (.gz), dan mengenkripsi data menggunakan enkripsi SSE-KMS. Pada 8 November 2023, Macie juga menandatangani objek S3 yang dihasilkan dengan Kode Otentikasi Pesan (HMAC) berbasis Hash. AWS KMS key

Setelah Anda mengonfigurasi Macie untuk menyimpan hasil penemuan data sensitif Anda di bucket S3, bucket dapat berfungsi sebagai repositori jangka panjang definitif untuk hasilnya. Anda kemudian dapat secara opsional mengakses dan menanyakan hasil di repositori itu.

#### Tip

Untuk contoh terperinci dan instruksional tentang bagaimana Anda dapat menanyakan dan menggunakan hasil penemuan data sensitif untuk menganalisis dan melaporkan potensi risiko keamanan data, lihat [Cara menanyakan dan memvisualisasikan hasil penemuan data sensitif Macie dengan posting QuickSight blog Amazon Athena dan Amazon](#) di Blog Keamanan.AWS

Untuk contoh kueri Amazon Athena yang dapat Anda gunakan untuk menganalisis hasil penemuan data sensitif, kunjungi repositori [Amazon Macie Results Analytics](#). GitHub Repositori ini juga menyediakan instruksi untuk mengkonfigurasi Athena untuk mengambil dan mendekripsi hasil Anda, dan skrip untuk membuat tabel untuk hasil.

## Langkah 1: Verifikasi izin Anda

Sebelum Anda mengonfigurasi repositori untuk hasil penemuan data sensitif Anda, verifikasi bahwa Anda memiliki izin yang Anda perlukan untuk mengenkripsi dan menyimpan hasilnya. Untuk memverifikasi izin Anda, gunakan AWS Identity and Access Management (IAM) untuk meninjau kebijakan IAM yang dilampirkan pada identitas IAM Anda. Kemudian bandingkan informasi dalam kebijakan tersebut dengan daftar tindakan berikut yang harus Anda lakukan untuk mengonfigurasi repositori.

## Amazon Macie

Untuk Macie, verifikasi bahwa Anda diizinkan untuk melakukan tindakan berikut:

`macie2:PutClassificationExportConfiguration`

Tindakan ini memungkinkan Anda menambahkan atau mengubah pengaturan repositori di Macie.

## Amazon S3

Untuk Amazon S3, verifikasi bahwa Anda diizinkan untuk melakukan tindakan berikut:

- `s3:CreateBucket`
- `s3:GetBucketLocation`
- `s3:ListAllMyBuckets`
- `s3:PutBucketAcl`
- `s3:PutBucketPolicy`
- `s3:PutBucketPublicAccessBlock`
- `s3:PutObject`

Tindakan ini mengizinkan Anda untuk mengakses dan mengonfigurasi bucket S3 yang dapat berfungsi sebagai repositori.

## AWS KMS

Untuk menggunakan konsol Amazon Macie untuk menambah atau mengubah setelan repositori, pastikan juga bahwa Anda diizinkan melakukan tindakan berikut: AWS KMS

- `kms:DescribeKey`
- `kms:ListAliases`

Tindakan ini memungkinkan Anda untuk mengambil dan menampilkan informasi tentang AWS KMS keys untuk akun Anda. Anda kemudian dapat memilih salah satu kunci ini untuk mengenkripsi hasil penemuan data sensitif Anda.

Jika Anda berencana untuk membuat yang baru AWS KMS key untuk mengenkripsi data, Anda juga harus diizinkan untuk melakukan tindakan berikut: `kms:CreateKey`, `kms:GetKeyPolicy`, dan `kms:PutKeyPolicy`.

Jika Anda tidak diizinkan untuk melakukan tindakan yang diperlukan, mintalah bantuan AWS administrator Anda sebelum melanjutkan ke langkah berikutnya.

## Langkah 2: Konfigurasi AWS KMS key

Setelah memverifikasi izin, tentukan Macie mana yang AWS KMS key ingin digunakan Macie untuk mengenkripsi hasil penemuan data sensitif Anda. Kuncinya harus berupa kunci KMS enkripsi simetris yang dikelola pelanggan yang diaktifkan Wilayah AWS sama dengan bucket S3 tempat Anda ingin menyimpan hasilnya.

Kuncinya bisa ada AWS KMS key dari akun Anda sendiri, atau yang sudah ada AWS KMS key yang dimiliki akun lain. Jika Anda ingin menggunakan kunci KMS baru, buat kunci sebelum melanjutkan. Jika Anda ingin menggunakan kunci yang ada yang dimiliki akun lain, dapatkan Nama Sumber Daya Amazon (ARN) dari kunci tersebut. Anda harus memasukkan ARN ini ketika Anda mengonfigurasi pengaturan repositori di Macie. Untuk informasi tentang membuat dan meninjau pengaturan kunci KMS, lihat [Mengelola kunci di Panduan AWS Key Management Service](#) Pengembang.

### Note

Kuncinya bisa berupa AWS KMS key di toko kunci eksternal. Namun, kuncinya mungkin lebih lambat dan kurang dapat diandalkan daripada kunci yang dikelola sepenuhnya di dalamnya AWS KMS. Anda dapat mengurangi risiko ini dengan menyimpan hasil penemuan data sensitif Anda di bucket S3 yang dikonfigurasi untuk menggunakan kunci sebagai Kunci Bucket S3. Melakukannya mengurangi jumlah AWS KMS permintaan yang harus dibuat untuk mengenkripsi hasil penemuan data sensitif Anda.

Untuk informasi tentang penggunaan kunci KMS di penyimpanan kunci eksternal, lihat [Penyimpanan kunci eksternal](#) di Panduan AWS Key Management Service Pengembang.

Untuk informasi tentang menggunakan Kunci Bucket S3, lihat [Mengurangi biaya SSE-KMS dengan Kunci Bucket Amazon S3 di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon](#).

Setelah Anda menentukan kunci KMS mana yang ingin digunakan Macie, berikan izin kepada Macie untuk menggunakan kunci tersebut. Jika tidak, Macie tidak akan dapat mengenkripsi atau menyimpan hasil Anda di repositori. Untuk memberikan izin kepada Macie untuk menggunakan kunci, perbarui kebijakan kunci untuk kunci tersebut. Untuk informasi terperinci tentang kebijakan utama dan mengelola akses ke kunci KMS, lihat [Kebijakan utama AWS KMS di](#) Panduan AWS Key Management Service Pengembang.

## Untuk memperbarui kebijakan utama

1. Buka AWS KMS konsol di <https://console.aws.amazon.com/kms>.
2. Untuk mengubah Wilayah AWS, gunakan pemilih Wilayah di sudut kanan atas halaman.
3. Pilih kunci yang Anda ingin Macie gunakan untuk mengenkripsi hasil penemuan data sensitif Anda.
4. Di tab Kebijakan kunci, pilih Edit.
5. Salin pernyataan berikut ke clipboard Anda dan kemudian tambahkan ke kebijakan:

```
{
  "Sid": "Allow Macie to use the key",
  "Effect": "Allow",
  "Principal": {
    "Service": "macie.amazonaws.com"
  },
  "Action": [
    "kms:GenerateDataKey",
    "kms:Encrypt"
  ],
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "aws:SourceAccount": "111122223333"
    },
    "ArnLike": {
      "aws:SourceArn": [
        "arn:aws:macie2:Region:111122223333:export-configuration:*",
        "arn:aws:macie2:Region:111122223333:classification-job/*"
      ]
    }
  }
}
```

Saat Anda menambahkan pernyataan, pastikan sintaksnya valid. Kebijakan menggunakan format JSON. Ini berarti bahwa Anda juga perlu menambahkan koma sebelum atau sesudah pernyataan, tergantung di tempat Anda menambahkan pernyataan ke kebijakan. Jika Anda menambahkan pernyataan sebagai pernyataan terakhir, tambahkan koma setelah tanda kurung kurawal penutup untuk pernyataan sebelumnya. Jika Anda menemukannya sebagai pernyataan pertama atau di antara dua pernyataan yang ada, tambahkan koma setelah tanda kurung kurawal penutup untuk pernyataan tersebut.

## 6. Perbarui pernyataan dengan nilai yang benar untuk lingkungan Anda:

- Di Condition bidang, ganti nilai placeholder, di mana:
  - **111122223333** adalah ID akun untuk Anda. Akun AWS
  - **Wilayah** adalah Wilayah AWS tempat Anda menggunakan Macie dan Anda ingin mengizinkan Macie menggunakan kuncinya.

Jika Anda menggunakan Macie di beberapa Wilayah dan ingin mengizinkan Macie menggunakan kunci di Wilayah tambahan, tambahkan `aws:SourceArn` ketentuan untuk setiap Wilayah tambahan. Sebagai contoh:

```
"aws:SourceArn": [
  "arn:aws:macie2:us-east-1:111122223333:export-configuration:*",
  "arn:aws:macie2:us-east-1:111122223333:classification-job/*",
  "arn:aws:macie2:us-west-2:111122223333:export-configuration:*",
  "arn:aws:macie2:us-west-2:111122223333:classification-job/*"
]
```

Atau, Anda dapat mengizinkan Macie untuk menggunakan kunci di semua Wilayah. Untuk melakukan ini, ganti nilai placeholder dengan karakter wildcard (\*). Sebagai contoh:

```
"aws:SourceArn": [
  "arn:aws:macie2*:111122223333:export-configuration:*",
  "arn:aws:macie2*:111122223333:classification-job/*"
]
```

- Jika Anda menggunakan Macie di Wilayah keikutsertaan, tambahkan kode Wilayah yang sesuai ke nilai bidang tersebut `Service`. Misalnya, jika Anda menggunakan Macie di Wilayah Middle East (Bahrain), yang memiliki kode Wilayah `me-south-1`, ganti `macie.amazonaws.com` dengan `macie.me-south-1.amazonaws.com`. Untuk daftar Wilayah di mana Macie saat ini tersedia dan kode Wilayah untuk masing-masing wilayah, lihat [titik akhir dan kuota Amazon Macie](#) di Referensi Umum AWS

Perhatikan bahwa Condition bidang menggunakan dua kunci kondisi global IAM:

- [aws:SourceAccount](#) — Kondisi ini memungkinkan Macie untuk melakukan tindakan yang ditentukan hanya untuk akun Anda. Lebih khusus lagi, ini menentukan akun mana yang dapat melakukan tindakan yang ditentukan untuk sumber daya dan tindakan yang ditentukan oleh `aws:SourceArn` kondisi.



Untuk memungkinkan Macie melakukan tindakan yang ditentukan untuk akun tambahan, tambahkan ID akun untuk setiap akun tambahan ke kondisi ini. Sebagai contoh:

```
"aws:SourceAccount": [111122223333,444455556666]
```

- [aws: SourceArn](#) — Kondisi ini mencegah orang lain Layanan AWS melakukan tindakan yang ditentukan. Ini juga mencegah Macie menggunakan kunci saat melakukan tindakan lain untuk akun Anda. Dengan kata lain, ini memungkinkan Macie untuk mengenkripsi objek S3 dengan kunci hanya jika objek adalah hasil penemuan data sensitif, dan hanya jika hasil tersebut untuk penemuan data sensitif otomatis atau pekerjaan penemuan data sensitif yang dibuat oleh akun yang ditentukan di Wilayah yang ditentukan.

Untuk memungkinkan Macie melakukan tindakan yang ditentukan untuk akun tambahan, tambahkan ARN untuk setiap akun tambahan ke kondisi ini. Sebagai contoh:

```
"aws:SourceArn": [  
  "arn:aws:macie2:us-east-1:111122223333:export-configuration:*",  
  "arn:aws:macie2:us-east-1:111122223333:classification-job/*",  
  "arn:aws:macie2:us-east-1:444455556666:export-configuration:*",  
  "arn:aws:macie2:us-east-1:444455556666:classification-job/*"  
]
```

Akun yang ditentukan oleh `aws:SourceAccount` dan `aws:SourceArn` kondisi harus cocok.

Kondisi ini membantu mencegah Macie digunakan sebagai [wakil yang bingung](#) selama transaksi dengan AWS KMS. Meskipun kami tidak merekomendasikannya, Anda dapat menghapus kondisi ini dari pernyataan.

7. Setelah selesai menambahkan dan memperbarui pernyataan, pilih Simpan perubahan.

## Langkah 3: Pilih ember S3

Setelah memverifikasi izin dan mengonfigurasinya AWS KMS key, Anda siap menentukan bucket S3 mana yang ingin Anda gunakan sebagai repositori untuk hasil penemuan data sensitif Anda. Anda memiliki dua opsi:

- Gunakan bucket S3 baru yang dibuat Macie — Jika Anda memilih opsi ini, Macie secara otomatis membuat bucket S3 baru saat ini Wilayah AWS untuk hasil penemuan Anda. Macie juga

menerapkan kebijakan bucket ke bucket. Kebijakan ini memungkinkan Macie menambahkan objek ke bucket. Hal ini juga membutuhkan objek untuk dienkripsi dengan AWS KMS key yang Anda tentukan, menggunakan enkripsi SSE-KMS. Untuk meninjau kebijakan, pilih Lihat kebijakan di konsol Amazon Macie setelah Anda menentukan nama bucket dan kunci KMS yang akan digunakan.

- Gunakan bucket S3 yang ada yang Anda buat – Jika Anda lebih memilih untuk menyimpan hasil penemuan Anda dalam bucket S3 tertentu yang Anda buat, buat bucket sebelum Anda melanjutkan. Kemudian periksa pengaturan bucket dan perbarui kebijakan bucket untuk memastikan bahwa Macie dapat menambahkan objek ke bucket. Topik ini menjelaskan pengaturan mana yang harus diperiksa dan cara memperbarui kebijakan. Topik ini juga memberikan contoh pernyataan untuk menambah kebijakan.

Bagian berikut memberikan instruksi untuk setiap opsi. Pilih bagian untuk opsi yang Anda inginkan.

Gunakan bucket S3 baru yang dibuat Macie

Jika Anda lebih memilih menggunakan bucket S3 baru yang dibuat Macie untuk Anda, langkah terakhir dalam prosesnya adalah mengonfigurasi pengaturan repositori di Macie.

Untuk mengonfigurasi pengaturan repositori di Macie

1. [Buka konsol Amazon Macie di https://console.aws.amazon.com/macie/](https://console.aws.amazon.com/macie/).
2. Di panel navigasi, di bawah Pengaturan, pilih Hasil penemuan.
3. Di bawah Repositori untuk hasil penemuan data sensitif, pilih Buat bucket.
4. Di kotak Buat bucket, masukkan nama untuk bucket.

Nama harus unik di semua bucket S3. Selain itu, nama hanya dapat terdiri dari huruf kecil, angka, titik (.), dan tanda hubung (-). Untuk persyaratan penamaan tambahan, lihat [Aturan penamaan bucket](#) di dalam Panduan Pengguna Amazon Simple Storage Service.

5. Perluas bagian Advanced.
6. (Opsional) Untuk menentukan awalan yang akan digunakan di jalur ke lokasi di bucket, masukkan awalan di kotak awalan hasil penemuan data.

Saat Anda memasukkan nilai, Macie memperbarui contoh di bawah kotak untuk menunjukkan jalur ke lokasi bucket tempat ia akan menyimpan hasil penemuan Anda.

7. Untuk Blokir semua akses publik, pilih Ya untuk mengaktifkan semua pengaturan blokir akses publik untuk bucket.

Untuk informasi tentang pengaturan ini, lihat [Memblokir akses publik ke penyimpanan Amazon S3 Anda](#) di dalam Panduan Pengguna Amazon Simple Storage Service.

8. Di bawah Pengaturan enkripsi, tentukan AWS KMS key yang Anda ingin Macie gunakan untuk mengenkripsi hasil:
  - Untuk menggunakan kunci dari akun Anda sendiri, pilih Pilih kunci dari akun Anda. Kemudian, dalam AWS KMS keydaftar, pilih kunci yang akan digunakan. Daftar ini menampilkan kunci KMS enkripsi simetris yang dikelola pelanggan untuk akun Anda.
  - Untuk menggunakan kunci yang dimiliki akun lain, pilih Masukkan ARN kunci dari akun lain. Kemudian, di kotak AWS KMS key ARN, masukkan Nama Sumber Daya Amazon (ARN) dari kunci yang akan digunakan—misalnya, **arn:aws:kms:us-east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab**
9. Setelah Anda selesai memasukkan pengaturan, pilih Simpan.

Macie menguji pengaturan untuk memverifikasi bahwa mereka benar. Jika pengaturan salah, Macie menampilkan pesan kesalahan untuk membantu Anda mengatasi masalah.

Setelah Anda menyimpan pengaturan repositori, Macie menambahkan hasil penemuan yang ada untuk 90 hari sebelumnya ke repositori. Macie juga mulai menambahkan hasil penemuan baru ke repositori.

Gunakan bucket S3 yang ada yang Anda buat

Jika Anda lebih memilih untuk menyimpan hasil penemuan data sensitif Anda dalam bucket S3 tertentu yang Anda buat, buat dan konfigurasi bucket sebelum Anda mengonfigurasi pengaturan repositori di Macie. Saat Anda membuat bucket, perhatikan persyaratan berikut:

- Jika Anda mengaktifkan Object Lock untuk bucket, Anda harus menonaktifkan pengaturan retensi default untuk fitur tersebut. Jika tidak, Macie tidak akan dapat menambahkan hasil penemuan Anda ke bucket. Untuk informasi tentang pengaturan ini, lihat [Menggunakan Lock Object S3](#) di Panduan Pengguna Amazon Simple Storage Service.
- Untuk menyimpan hasil penemuan Anda untuk Wilayah yang diaktifkan secara default Akun AWS, seperti Wilayah AS Timur (Virginia N.), bucket harus berada di Wilayah yang diaktifkan secara default. Hasilnya tidak dapat disimpan dalam bucket di Wilayah keikutsertaan (Wilayah yang dinonaktifkan secara default).

- Untuk menyimpan hasil penemuan Anda untuk Wilayah keikutsertaan, seperti Wilayah Timur Tengah (Bahrain), bucket harus berada di Wilayah atau Wilayah yang sama yang diaktifkan secara default. Hasilnya tidak dapat disimpan dalam ember di Wilayah keikutsertaan yang berbeda.

Untuk menentukan apakah Wilayah diaktifkan secara default, lihat [Wilayah dan titik akhir](#) di Panduan AWS Identity and Access Management Pengguna.

Setelah Anda membuat bucket, perbarui kebijakan bucket agar Macie dapat mengambil informasi tentang bucket dan menambahkan objek ke bucket. Anda kemudian dapat mengonfigurasi pengaturan repositori di Macie.

Untuk memperbarui kebijakan bucket untuk bucket

1. Buka konsol Amazon S3 di <https://console.aws.amazon.com/s3/>.
2. Pilih bucket yang ingin Anda gunakan untuk menyimpan hasil penemuan Anda.
3. Pilih tab Izin.
4. Di bagian Kebijakan bucket, pilih Edit.
5. Salin kebijakan contoh berikut ke clipboard Anda:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Allow Macie to use the GetBucketLocation operation",
      "Effect": "Allow",
      "Principal": {
        "Service": "macie.amazonaws.com"
      },
      "Action": "s3:GetBucketLocation",
      "Resource": "arn:aws:s3:::myBucketName",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "111122223333"
        },
        "ArnLike": {
          "aws:SourceArn": [
            "arn:aws:macie2:Region:111122223333:export-configuration:*",
            "arn:aws:macie2:Region:111122223333:classification-job/*"
          ]
        }
      }
    }
  ]
}
```

```

    }
  }
},
{
  "Sid": "Allow Macie to add objects to the bucket",
  "Effect": "Allow",
  "Principal": {
    "Service": "macie.amazonaws.com"
  },
  "Action": "s3:PutObject",
  "Resource": "arn:aws:s3:::myBucketName/[optional prefix/*]",
  "Condition": {
    "StringEquals": {
      "aws:SourceAccount": "111122223333"
    },
    "ArnLike": {
      "aws:SourceArn": [
        "arn:aws:macie2:Region:111122223333:export-
configuration:*",
        "arn:aws:macie2:Region:111122223333:classification-job/*"
      ]
    }
  }
},
{
  "Sid": "Deny unencrypted object uploads. This is optional",
  "Effect": "Deny",
  "Principal": {
    "Service": "macie.amazonaws.com"
  },
  "Action": "s3:PutObject",
  "Resource": "arn:aws:s3:::myBucketName/[optional prefix/*]",
  "Condition": {
    "StringNotEquals": {
      "s3:x-amz-server-side-encryption": "aws:kms"
    }
  }
},
{
  "Sid": "Deny incorrect encryption headers. This is optional",
  "Effect": "Deny",
  "Principal": {
    "Service": "macie.amazonaws.com"
  },

```

```

    "Action": "s3:PutObject",
    "Resource": "arn:aws:s3:::myBucketName/[optional prefix/]*",
    "Condition": {
      "StringNotEquals": {
        "s3:x-amz-server-side-encryption-aws-kms-key-id":
"arn:aws:kms:Region:111122223333:key/KMSKeyId"
      }
    }
  },
  {
    "Sid": "Deny non-HTTPS access",
    "Effect": "Deny",
    "Principal": "*",
    "Action": "s3:*",
    "Resource": "arn:aws:s3:::myBucketName/*",
    "Condition": {
      "Bool": {
        "aws:SecureTransport": "false"
      }
    }
  }
]
}

```

6. Tempel kebijakan contoh di editor Kebijakan bucket di konsol Amazon S3.
7. Perbarui kebijakan contoh dengan nilai yang benar untuk lingkungan Anda:
  - Dalam pernyataan opsional yang menyangkal header enkripsi yang salah:
    - Ganti *myBucketName* dengan nama ember.
    - Dalam `StringNotEquals` kondisi tersebut, ganti *ARN:AWS:KMS:Region:111122223333:key/kms KeyId* dengan Amazon Resource Name (ARN) yang akan digunakan untuk enkripsi hasil penemuan Anda. AWS KMS key
  - Dalam semua pernyataan lainnya, ganti nilai placeholder, di mana:
    - *myBucketName* adalah nama ember.
    - *111122223333* adalah ID akun untuk Anda. Akun AWS
    - *Wilayah* adalah Wilayah AWS tempat Anda menggunakan Macie dan ingin mengizinkan Macie menambahkan hasil penemuan ke ember.

Jika Anda menggunakan Macie di beberapa Wilayah dan ingin mengizinkan Macie menambahkan hasil ke bucket untuk Wilayah tambahan, tambahkan `aws:SourceArn` ketentuan untuk setiap Wilayah tambahan. Sebagai contoh:

```
"aws:SourceArn": [
  "arn:aws:macie2:us-east-1:111122223333:export-configuration:*",
  "arn:aws:macie2:us-east-1:111122223333:classification-job/*",
  "arn:aws:macie2:us-west-2:111122223333:export-configuration:*",
  "arn:aws:macie2:us-west-2:111122223333:classification-job/*"
]
```

Atau, Anda dapat mengizinkan Macie untuk menambahkan hasil ke bucket untuk semua Wilayah di mana Anda menggunakan Macie. Untuk melakukan ini, ganti nilai placeholder dengan karakter wildcard (\*). Sebagai contoh:

```
"aws:SourceArn": [
  "arn:aws:macie2*:111122223333:export-configuration:*",
  "arn:aws:macie2*:111122223333:classification-job/*"
]
```

- Jika Anda menggunakan Macie di Region opt-in, tambahkan kode Region yang sesuai ke nilai untuk `Service` bidang di setiap pernyataan yang menentukan prinsip layanan Macie. Misalnya, jika Anda menggunakan Macie di Wilayah Middle East (Bahrain), yang memiliki kode Wilayah `me-south-1`, ganti `macie.amazonaws.com` dengan `macie.me-south-1.amazonaws.com` dalam setiap pernyataan yang berlaku. Untuk daftar Wilayah di mana Macie saat ini tersedia dan kode Wilayah untuk masing-masing wilayah, lihat [titik akhir dan kuota Amazon Macie](#) di. Referensi Umum AWS

Perhatikan bahwa kebijakan contoh menyertakan pernyataan yang memungkinkan Macie menentukan Region mana bucket berada di (`GetBucketLocation`) dan menambahkan objek ke bucket (`PutObject`). Pernyataan ini mendefinisikan kondisi yang menggunakan dua kunci kondisi global IAM:

- [aws: SourceAccount](#) — Kondisi ini memungkinkan Macie untuk menambahkan hasil penemuan data sensitif ke bucket hanya untuk akun Anda. Ini mencegah Macie menambahkan hasil penemuan untuk akun lain ke ember. Lebih khusus lagi, kondisi menentukan akun mana yang dapat menggunakan bucket untuk sumber daya dan tindakan yang ditentukan oleh `aws:SourceArn` kondisi.

Untuk menyimpan hasil akun tambahan di bucket, tambahkan ID akun untuk setiap akun tambahan ke kondisi ini. Sebagai contoh:

```
"aws:SourceAccount": [111122223333,444455556666]
```

- [aws: SourceArn](#) — Kondisi ini membatasi akses ke bucket berdasarkan sumber objek yang ditambahkan ke bucket. Ini mencegah orang lain Layanan AWS menambahkan objek ke ember. Ini juga mencegah Macie menambahkan objek ke bucket saat melakukan tindakan lain untuk akun Anda. Lebih khusus lagi, kondisi ini memungkinkan Macie untuk menambahkan objek ke bucket hanya jika objek adalah hasil penemuan data sensitif, dan hanya jika hasil tersebut untuk penemuan data sensitif otomatis atau pekerjaan penemuan data sensitif yang dibuat oleh akun yang ditentukan di Wilayah yang ditentukan.

Untuk memungkinkan Macie melakukan tindakan yang ditentukan untuk akun tambahan, tambahkan ARN untuk setiap akun tambahan ke kondisi ini. Sebagai contoh:

```
"aws:SourceArn": [  
  "arn:aws:macie2:us-east-1:111122223333:export-configuration:*",  
  "arn:aws:macie2:us-east-1:111122223333:classification-job/*",  
  "arn:aws:macie2:us-east-1:444455556666:export-configuration:*",  
  "arn:aws:macie2:us-east-1:444455556666:classification-job/*"  
]
```

Akun yang ditentukan oleh `aws:SourceAccount` dan `aws:SourceArn` kondisi harus cocok.

Kedua kondisi tersebut membantu mencegah Macie digunakan sebagai [wakil yang bingung](#) selama transaksi dengan Amazon S3. Meskipun kami tidak merekomendasikannya, Anda dapat menghapus kondisi ini dari kebijakan bucket.

8. Setelah Anda selesai memperbarui kebijakan bucket, pilih Simpan perubahan.

Anda sekarang dapat mengonfigurasi pengaturan repositori di Macie.

Untuk mengonfigurasi pengaturan repositori di Macie

1. [Buka konsol Amazon Macie di https://console.aws.amazon.com/macie/](https://console.aws.amazon.com/macie/).
2. Di panel navigasi, di dalam Pengaturan, pilih Hasil penemuan.
3. Di bawah Repositori untuk hasil penemuan data sensitif, pilih Bucket yang ada.



4. Untuk Pilih bucket, pilih bucket yang ingin Anda simpan hasil penemuan Anda.
5. (Opsional) Untuk menentukan awalan yang akan digunakan di jalur ke lokasi di bucket, perluas bagian Advanced. Kemudian, untuk awalan hasil penemuan data, masukkan awalan yang akan digunakan.

Saat Anda memasukkan nilai, Macie memperbarui contoh di bawah kotak untuk menunjukkan jalur ke lokasi bucket tempat ia akan menyimpan hasil penemuan Anda.

6. Di bawah Pengaturan enkripsi, tentukan AWS KMS key yang Anda ingin Macie gunakan untuk mengenkripsi hasil:
  - Untuk menggunakan kunci dari akun Anda sendiri, pilih Pilih kunci dari akun Anda. Kemudian, dalam AWS KMS keydaftar, pilih kunci yang akan digunakan. Daftar ini menampilkan kunci KMS enkripsi simetris yang dikelola pelanggan untuk akun Anda.
  - Untuk menggunakan kunci yang dimiliki akun lain, pilih Masukkan ARN kunci dari akun lain. Kemudian, di kotak AWS KMS key ARN, masukkan ARN dari kunci yang akan digunakan—misalnya, **arn:aws:kms:us-east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab**
7. Setelah Anda selesai memasukkan pengaturan, pilih Simpan.

Macie menguji pengaturan untuk memverifikasi bahwa mereka benar. Jika pengaturan salah, Macie menampilkan pesan kesalahan untuk membantu Anda mengatasi masalah.

Setelah Anda menyimpan pengaturan repositori, Macie menambahkan hasil penemuan yang ada untuk 90 hari sebelumnya ke repositori. Macie juga mulai menambahkan hasil penemuan baru ke repositori.

#### Note

Jika Anda kemudian mengubah setelan awalan hasil penemuan data, perbarui juga kebijakan bucket di Amazon S3. Pernyataan kebijakan yang menentukan jalur sebelumnya harus menentukan jalur baru. Jika tidak, Macie tidak akan diizinkan untuk menambahkan hasil penemuan Anda ke ember.

**i** Tip

Untuk mengurangi biaya enkripsi sisi server, konfigurasi juga bucket S3 untuk menggunakan Kunci Bucket S3, dan tentukan AWS KMS key yang Anda konfigurasi untuk enkripsi hasil penemuan data sensitif Anda. Penggunaan Kunci Bucket S3 mengurangi jumlah panggilan AWS KMS, yang dapat mengurangi biaya AWS KMS permintaan. Jika kunci KMS berada di penyimpanan kunci eksternal, penggunaan S3 Bucket Key juga dapat meminimalkan dampak kinerja penggunaan kunci. Untuk mempelajari lebih lanjut, lihat [Mengurangi biaya SSE-KMS dengan Amazon S3 Bucket Keys di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon](#).

## Kelas dan format penyimpanan yang didukung oleh Amazon Macie

Untuk membantu Anda menemukan data sensitif di kawasan data Amazon Simple Storage Service (Amazon S3), Amazon Macie mendukung sebagian besar kelas penyimpanan Amazon S3 dan berbagai format file dan penyimpanan. Dukungan ini berlaku untuk penggunaan [pengidentifikasi data terkelola](#) dan penggunaan [pengidentifikasi data khusus](#) untuk menganalisis objek S3.

Agar Macie dapat menganalisis objek S3, objek harus disimpan dalam bucket tujuan umum Amazon S3 menggunakan kelas penyimpanan yang didukung. Objek juga harus menggunakan file atau format penyimpanan yang didukung. Topik di bagian ini mencantumkan kelas penyimpanan dan format file dan penyimpanan yang saat ini didukung Macie.

**i** Tip

Meskipun Macie dioptimalkan untuk Amazon S3, Anda dapat menggunakannya untuk menemukan data sensitif dalam sumber daya yang saat ini Anda simpan di tempat lain. Anda dapat melakukan ini dengan memindahkan data ke Amazon S3 sementara atau permanen. Misalnya, ekspor Amazon Relational Database Service atau snapshot Amazon Aurora ke Amazon S3 dalam format Apache Parquet. Atau ekspor tabel Amazon DynamoDB ke Amazon S3. Anda kemudian dapat membuat pekerjaan penemuan data sensitif untuk menganalisis data di Amazon S3.

### Topik

- [Kelas penyimpanan Amazon S3 yang didukung](#)

- [Format file dan penyimpanan yang didukung](#)

## Kelas penyimpanan Amazon S3 yang didukung

Untuk penemuan data sensitif, Amazon Macie mendukung kelas penyimpanan Amazon S3 berikut:

- Redundansi Berkurang (RRS)
- Pengambilan Instan Gletser S3
- Tingkat Cerdas S3
- S3 Satu Zona - Akses Jarang (S3 Satu Zona - Ia)
- S3 Standard
- Akses Standar S3-Jarang (Standar S3-IA)

Macie tidak menganalisis objek S3 yang menggunakan kelas penyimpanan Amazon S3 lainnya, seperti S3 Glacier Deep Archive atau S3 Express One Zone. Selain itu, Macie tidak menganalisis objek yang disimpan di bucket direktori Amazon S3.

Jika Anda mengonfigurasi tugas penemuan data sensitif untuk menganalisis objek S3 yang tidak menggunakan kelas penyimpanan Amazon S3 yang didukung, Macie melewati objek tersebut saat pekerjaan berjalan. Macie tidak mencoba untuk mengambil atau menganalisis data dalam objek — objek diperlakukan sebagai objek yang tidak dapat diklasifikasikan. Objek yang tidak dapat diklasifikasikan adalah objek yang tidak menggunakan kelas penyimpanan yang didukung atau file atau format penyimpanan yang didukung. Macie hanya menganalisis objek yang menggunakan kelas penyimpanan yang didukung dan file atau format penyimpanan yang didukung.

Demikian pula, jika Anda mengonfigurasi Macie untuk melakukan penemuan data sensitif otomatis, objek yang tidak dapat diklasifikasikan tidak memenuhi syarat untuk dipilih dan dianalisis. Macie hanya memilih objek yang menggunakan kelas penyimpanan Amazon S3 yang didukung dan format file atau penyimpanan yang didukung.

Untuk mengidentifikasi bucket S3 yang berisi objek yang tidak dapat diklasifikasikan, Anda dapat [memfilter](#) inventaris bucket S3. Untuk setiap bucket dalam inventaris Anda, ada kolom yang melaporkan jumlah dan ukuran penyimpanan total objek yang tidak dapat diklasifikasikan dalam bucket.

Untuk informasi terperinci tentang kelas penyimpanan yang disediakan Amazon S3, lihat [Menggunakan kelas penyimpanan Amazon S3 di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon](#).

## Format file dan penyimpanan yang didukung

Saat Amazon Macie menganalisis objek S3, Macie mengambil versi terbaru objek dari Amazon S3, dan kemudian melakukan pemeriksaan mendalam terhadap konten objek. Pemeriksaan ini memperhitungkan format file atau penyimpanan data. Macie dapat menganalisis data dalam berbagai format, termasuk format kompresi dan arsip yang umum digunakan.

Ketika Macie menganalisis data dalam file terkompresi atau arsip, Macie memeriksa file lengkap dan isi file. Untuk memeriksa isi file, Macie mendekompresi file, lalu memeriksa setiap file yang diekstraksi menggunakan format yang didukung. Macie dapat melakukan hal ini sebanyak 1.000.000 file dan hingga kedalaman bersarang 10 tingkat. Untuk informasi tentang kuota tambahan yang berlaku untuk penemuan data sensitif, lihat [Kuota Amazon Macie](#).

Tabel berikut mencantumkan dan menjelaskan jenis file dan format penyimpanan yang dapat dianalisis Macie untuk mendeteksi data sensitif. Untuk setiap jenis yang didukung, tabel juga mencantumkan ekstensi nama file yang berlaku.

Jenis file atau penyimpanan	Deskripsi	Ekstensi nama file
Big data	Objek kontainer Apache Avro dan file Apache Parquet	.avro, .parquet
Kompresi atau arsip	Arsip terkompresi GNU Zip, arsip TAR, dan arsip terkompresi ZIP	.gz, .gzip, .tar, .zip
Dokumen	File Adobe Portable Document Format, buku kerja Microsoft Excel, dan dokumen Microsoft Word	.doc, .docx, .pdf, .xls, .xlsx
Pesan email	<a href="#">File surat elektronik yang isinya memenuhi persyaratan yang ditentukan oleh</a>	.eml

Jenis file atau penyimpanan	Deskripsi	Ekstensi nama file
	<a href="#">IETF RFC untuk pesan surat elektronik, seperti RFC 2822</a>	
Teks	File teks non-biner seperti file nilai yang dipisahkan koma (CSV), file Hypertext Markup Language (HTML), file JavaScript Object Notation (JSON), file JSON Lines, dokumen teks biasa, file nilai yang dipisahkan tab (TSV), dan file Extensible Markup Language (XHTML)	.csv, .htm, .html, .json, .jsonl, .tsv, .txt, dan yang lainnya (tergantung pada tipe file teks non-biner)

Macie tidak menganalisis data dalam gambar, atau audio, video, dan jenis konten multimedia lainnya.

Jika Anda mengonfigurasi pekerjaan penemuan data sensitif untuk menganalisis objek S3 yang tidak menggunakan file atau format penyimpanan yang didukung, Macie melewati objek tersebut saat pekerjaan berjalan. Macie tidak mencoba untuk mengambil atau menganalisis data dalam objek — objek diperlakukan sebagai objek yang tidak dapat diklasifikasikan. Objek yang tidak dapat diklasifikasikan adalah objek yang tidak menggunakan kelas penyimpanan Amazon S3 yang didukung atau format file atau penyimpanan yang didukung. Macie hanya menganalisis objek yang menggunakan kelas penyimpanan yang didukung dan file atau format penyimpanan yang didukung.

Demikian pula, jika Anda mengonfigurasi Macie untuk melakukan penemuan data sensitif otomatis, objek yang tidak dapat diklasifikasikan tidak memenuhi syarat untuk dipilih dan dianalisis. Macie hanya memilih objek yang menggunakan kelas penyimpanan Amazon S3 yang didukung dan format file atau penyimpanan yang didukung.

Untuk mengidentifikasi bucket S3 yang berisi objek yang tidak dapat diklasifikasikan, Anda dapat [memfilter](#) inventaris bucket S3. Untuk setiap bucket dalam inventaris Anda, ada kolom yang melaporkan jumlah dan ukuran penyimpanan total objek yang tidak dapat diklasifikasikan dalam bucket.

# Menganalisis temuan Amazon Macie

Amazon Macie membuat temuan saat mendeteksi potensi pelanggaran kebijakan atau masalah terkait keamanan atau privasi bucket Amazon Simple Storage Service (Amazon S3) Anda atau mendeteksi data sensitif dalam objek S3. Temuan adalah laporan detail tentang potensi masalah atau data sensitif yang ditemukan oleh Macie. Setiap temuan memberikan tingkat kepelikan, informasi tentang sumber daya yang terpengaruh, dan detail tambahan, seperti kapan dan bagaimana Macie menemukan masalah atau data. Macie menyimpan temuan kebijakan dan data sensitif Anda selama 90 hari.

Anda dapat meninjau, menganalisis, dan mengelola temuan dengan cara berikut ini.

## Konsol Amazon Macie

Halaman Temuan di konsol Amazon Macie mendaftar temuan Anda dan memberikan informasi detail untuk temuan individu. Halaman ini juga menyediakan opsi untuk pengelompokan, penyaringan, dan pemilahan temuan, serta untuk membuat dan mengelola aturan penekanan. Aturan penekanan dapat membantu Anda menyederhanakan analisis dari temuan Anda.

## API Amazon Macie

Dengan API Amazon Macie, Anda dapat melakukan kueri dan mengambil data temuan dengan menggunakan alat baris AWS perintah atau AWS SDK, atau dengan mengirimkan permintaan HTTPS langsung ke Macie. Untuk mengueri data, Anda mengirimkan permintaan ke API Amazon Macie dan menggunakan parameter yang didukung untuk menentukan temuan yang Anda ingin ambil. Setelah Anda mengirimkan permintaan Anda, Macie mengembalikan hasil dalam respons JSON. Kemudian Anda dapat menyampaikan hasilnya ke layanan atau aplikasi lain untuk analisis yang lebih mendalam, penyimpanan jangka panjang, atau untuk pelaporan. Untuk informasi selengkapnya, lihat [Referensi API Amazon Macie](#).

## Amazon EventBridge

Untuk mendukung integrasi dengan layanan dan sistem lain, seperti pemantauan atau sistem manajemen peristiwa, Macie menerbitkan temuan ke Amazon EventBridge sebagai peristiwa. EventBridge, sebelumnya Amazon CloudWatch Events, adalah layanan bus peristiwa nirserver yang dapat mengirimkan pengaliran data secara waktu nyata dari aplikasi Anda sendiri, aplikasi perangkat lunak sebagai layanan (SaaS), dan seperti Macie. Layanan AWS Hal ini dapat merutekan data yang ke target seperti AWS Lambda fungsi, topik Amazon Simple Notification Service, dan aliran Amazon Kinesis untuk pemrosesan tambahan dan otomatis. Penggunaan

EventBridge juga membantu memastikan retensi data jangka panjang. Untuk mempelajari selengkapnya EventBridge, lihat [Panduan EventBridge Pengguna Amazon](#).

Macie secara otomatis menerbitkan peristiwa EventBridge untuk temuan baru. Hal ini juga menerbitkan peristiwa secara otomatis untuk kejadian berikutnya dari temuan kebijakan yang ada. Karena data temuan disusun sebagai EventBridge peristiwa, Anda dapat lebih mudah memantau, menganalisis, dan bertindak berdasarkan temuan dengan menggunakan layanan dan alat lainnya. Misalnya, Anda dapat menggunakan EventBridge untuk secara otomatis mengirim jenis temuan baru tertentu ke AWS Lambda fungsi yang, pada gilirannya, memproses dan mengirimkan data ke sistem insiden keamanan dan manajemen peristiwa (SIEM) Anda. Jika Anda mengintegrasikan Notifikasi Pengguna AWS dengan Macie, Anda juga dapat menggunakan peristiwa tersebut untuk diberi tahu temuan secara otomatis melalui saluran pengiriman yang Anda tentukan. Untuk mempelajari tentang menggunakan EventBridge peristiwa untuk memantau dan memproses temuan, lihat [Integrasi Amazon Macie dengan Amazon EventBridge](#).

## AWS Security Hub

Untuk analisis tambahan yang lebih luas tentang postur keamanan organisasi Anda, Anda juga dapat mempublikasikan temuan ke AWS Security Hub. Security Hub adalah layanan yang mengumpulkan data keamanan dari Layanan AWS dan mendukung solusi AWS Partner Network keamanan untuk memberi Anda gambaran menyeluruh tentang status keamanan Anda di seluruh AWS lingkungan Anda. Security Hub juga membantu Anda memeriksa lingkungan Anda terkait standar industri dan praktik terbaik terkait keamanan. Untuk mempelajari selengkapnya tentang Security Hub, lihat [Panduan Pengguna AWS Security Hub](#). Untuk mempelajari tentang menggunakan Security Hub untuk memantau dan memproses temuan, lihat [Integrasi Amazon Macie dengan AWS Security Hub](#).

Selain temuan, Macie membuat hasil penemuan data sensitif untuk objek S3 yang dianalisisnya untuk menemukan data sensitif. Hasil temuan data sensitif adalah catatan yang mencatat detail tentang analisis terhadap suatu objek. Ini termasuk objek yang tidak menemukan data sensitif oleh Macie, dan karenanya tidak menghasilkan temuan, dan objek yang tidak dapat dianalisis Macie karena kesalahan atau masalah. Hasil penemuan data sensitif memberi Anda catatan analisis yang dapat membantu untuk audit privasi dan perlindungan data atau investigasi. Anda tidak dapat mengakses hasil penemuan data sensitif langsung di konsol Amazon Macie atau dengan API Amazon Macie secara langsung di konsol Amazon Macie. Sebaliknya, Anda mengonfigurasi Macie untuk menyimpan hasil dalam bucket S3. Kemudian Anda dapat mengakses dan mengueri hasil dalam bucket tersebut. Untuk mempelajari cara mengonfigurasi Macie untuk menyimpan hasil, lihat [Menyimpan dan mempertahankan hasil penemuan data sensitif](#).

## Topik

- [Tipe temuan Amazon Macie](#)
- [Bekerja dengan temuan sampel di Amazon Macie](#)
- [Meninjau temuan di konsol Amazon Macie](#)
- [Memfilter temuan Amazon Macie](#)
- [Menyelidiki data sensitif dengan temuan Amazon Macie](#)
- [Menekan temuan Amazon Macie](#)
- [Penilaian tingkat kepelikan untuk temuan Amazon Macie](#)

## Tipe temuan Amazon Macie

Amazon Macie menghasilkan dua kategori temuan: temuan kebijakan dan temuan data sensitif. Temuan kebijakan adalah laporan terperinci tentang potensi pelanggaran kebijakan atau masalah keamanan atau privasi bucket Amazon Simple Storage Service (Amazon S3). Macie menghasilkan temuan kebijakan sebagai bagian dari aktivitas yang sedang berlangsung untuk mengevaluasi dan memantau bucket S3 Anda untuk keamanan dan kontrol akses. Temuan data sensitif adalah laporan terperinci dari data sensitif yang dideteksi Macie dalam objek S3. Macie menghasilkan temuan data sensitif sebagai bagian dari aktivitas yang dilakukannya saat Anda menjalankan pekerjaan penemuan data sensitif atau melakukan penemuan data sensitif otomatis untuk akun Anda.

Dalam setiap kategori, ada jenis tertentu. Jenis temuan memberikan wawasan tentang sifat masalah atau data sensitif yang ditemukan Macie. Detail temuan memberikan [peringkat keparahan](#), informasi tentang sumber daya yang terpengaruh, dan informasi tambahan, seperti kapan dan bagaimana Macie menemukan masalah atau data sensitif. Tingkat keparahan dan detail setiap temuan bervariasi tergantung pada jenis dan sifat temuan.

## Topik

- [Jenis temuan kebijakan](#)
- [Jenis temuan data sensitif](#)

### Tip

Untuk mengeksplorasi dan mempelajari tentang berbagai kategori dan jenis temuan yang dapat dihasilkan Macie, [buatlah temuan sampel](#). Temuan sampel menggunakan data contoh



dan nilai placeholder untuk menunjukkan jenis informasi yang mungkin terkandung dalam setiap jenis temuan.

## Jenis temuan kebijakan

Amazon Macie menghasilkan temuan kebijakan saat kebijakan atau pengaturan untuk bucket S3 diubah dengan cara yang mengurangi keamanan atau privasi bucket dan objek bucket. Untuk informasi tentang cara Macie mendeteksi perubahan ini, lihat [Cara Macie memantau keamanan data Amazon S3](#)

Macie menghasilkan temuan kebijakan hanya jika perubahan terjadi setelah Anda mengaktifkan Macie untuk Anda. Akun AWS Misalnya, jika setelah akses publik diblokir dinonaktifkan untuk bucket S3 setelah Anda mengaktifkan Macie, Macie akan membuat temuan `BlockPublicAccessDisabledpolicy:IAMuser/S3` untuk bucket. Namun, jika setelah akses publik dinonaktifkan untuk bucket saat Anda mengaktifkan Macie dan setelah tersebut terus dinonaktifkan, Macie tidak akan menghasilkan temuan `BlockPublicAccessDisabledpolicy:iamuser/S3` untuk bucket tersebut.

Jika Macie mendeteksi kejadian berikutnya dari temuan kebijakan yang ada, Macie memperbarui temuan yang ada dengan menambahkan rincian tentang kejadian berikutnya dan menambah jumlah kejadian. Macie menyimpan temuan kebijakan selama 90 hari.

Macie dapat menghasilkan tipe temuan kebijakan berikut untuk bucket S3.

### Policy:IAMUser/S3BlockPublicAccessDisabled

Semua pengaturan akses publik blok tingkat ember dinonaktifkan untuk bucket. Akses ke bucket dikendalikan oleh pengaturan blokir akses publik untuk akun, daftar kontrol akses (ACL), dan kebijakan bucket untuk bucket.

Untuk mempelajari pengaturan blok akses publik untuk bucket S3, lihat [Memblokir akses publik ke penyimpanan Amazon S3 Anda](#) di Panduan Pengguna Amazon Simple Storage Service.

### Policy:IAMUser/S3BucketEncryptionDisabled

Pengaturan enkripsi default untuk bucket disetel ulang ke perilaku enkripsi Amazon S3 default, yaitu mengenkripsi objek baru secara otomatis dengan kunci terkelola Amazon S3.

Mulai 5 Januari 2023, Amazon S3 secara otomatis menerapkan enkripsi sisi server dengan kunci terkelola Amazon S3 (SSE-S3) sebagai tingkat dasar enkripsi untuk objek yang ditambahkan

ke bucket. Anda dapat mengonfigurasi pengaturan enkripsi default bucket untuk menggunakan enkripsi sisi server dengan AWS KMS kunci (SSE-KMS) atau enkripsi sisi server dua lapis dengan kunci (DSSE-KMS). AWS KMS Untuk mempelajari setelan dan opsi enkripsi default untuk bucket S3, lihat [Menyetel perilaku enkripsi sisi server default untuk bucket S3](#) di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

Jika Macie membuat jenis temuan ini sebelum 5 Januari 2023, temuan tersebut menunjukkan bahwa pengaturan enkripsi default dinonaktifkan untuk bucket yang terpengaruh. Ini berarti bahwa pengaturan bucket tidak menentukan perilaku enkripsi sisi server default untuk objek baru. Kemampuan untuk menonaktifkan pengaturan enkripsi default untuk bucket tidak lagi didukung oleh Amazon S3.

Policy:IAMUser/S3BucketPublic

Kebijakan ACL atau bucket untuk bucket diubah untuk mengizinkan akses oleh pengguna anonim atau semua identitas yang diautentikasi AWS Identity and Access Management (IAM).

Untuk mempelajari tentang kebijakan ACL dan bucket untuk bucket S3, lihat [Identity and Access Management di Amazon S3](#) di Panduan Pengguna Amazon Simple Storage Service.

Policy:IAMUser/S3BucketReplicatedExternally

Replikasi diaktifkan dan dikonfigurasi untuk mereplikasi objek dari bucket ke bucket untuk Akun AWS yang eksternal (bukan bagian dari) organisasi Anda. Organisasi adalah kumpulan akun Macie yang dikelola secara terpusat sebagai sekelompok akun terkait melalui AWS Organizations atau dengan undangan Macie.

Dalam kondisi tertentu, Macie mungkin menghasilkan jenis temuan ini untuk bucket yang tidak dikonfigurasi untuk mereplikasi objek ke bucket untuk eksternal. Akun AWS [Hal ini dapat terjadi jika bucket tujuan dibuat berbeda Wilayah AWS selama 24 jam sebelumnya, setelah Macie mengambil bucket dan metadata objek dari Amazon S3 sebagai bagian dari siklus penyegaran harian](#). Untuk menyelidiki temuan, mulailah dengan menyegarkan data inventaris Anda. Kemudian [tinjau detail ember](#). Detailnya menunjukkan apakah bucket dikonfigurasi untuk mereplikasi objek ke bucket lain. Jika bucket dikonfigurasi untuk melakukan ini, detailnya menyertakan ID akun untuk setiap akun yang memiliki bucket tujuan.

Untuk mempelajari tentang pengaturan replikasi untuk bucket S3, lihat [Mereplikasi objek](#) di Panduan Pengguna Amazon Simple Storage Service.

## Policy: IAMUser/S3BucketSharedExternally

Kebijakan ACL atau bucket untuk bucket diubah agar bucket dapat dibagikan dengan Akun AWS yang eksternal (bukan bagian dari) organisasi Anda. Organisasi adalah kumpulan akun Macie yang dikelola secara terpusat sebagai sekelompok akun terkait melalui AWS Organizations atau dengan undangan Macie.

Dalam kasus tertentu, Macie mungkin menghasilkan jenis temuan ini untuk bucket yang tidak dibagikan dengan akun AWS eksternal. Hal ini dapat terjadi jika Macie tidak dapat sepenuhnya mengevaluasi hubungan antara Principal elemen dalam kebijakan bucket dan [kunci konteks kondisi AWS global tertentu atau kunci kondisi Amazon S3](#) dalam Condition elemen kebijakan. Kunci kondisi yang berlaku adalah:aws:PrincipalAccount,aws:PrincipalArn,aws:PrincipalOrgID,aws:PrincipalOrgPath,aws:DataAccessPointArn. Kami menyarankan Anda meninjau kebijakan bucket untuk menentukan apakah akses ini dimaksudkan dan aman.

Untuk mempelajari tentang kebijakan ACL dan bucket untuk bucket S3, lihat [Identity and Access Management di Amazon S3](#) di Panduan Pengguna Amazon Simple Storage Service.

## Policy: IAMUser/S3BucketSharedWithCloudFront

Kebijakan bucket untuk bucket diubah untuk memungkinkan bucket dibagikan dengan identitas akses CloudFront asal Amazon (OAI), kontrol akses CloudFront asal (OAC), atau CloudFront OAI dan OAC. CloudFront OAI atau OAC memungkinkan pengguna untuk mengakses objek bucket melalui satu atau lebih distribusi tertentu CloudFront.

Untuk mempelajari tentang CloudFront OAI dan OAC, lihat [Membatasi akses ke asal Amazon S3 di Panduan Pengembang Amazon. CloudFront](#)

### Note

Dalam kasus tertentu, Macie menghasilkan temuan policy:iamuser/S3 alih-alih BucketSharedExternally temuan policy:iamuser/S3 untuk bucket. BucketSharedWithCloudFront Kasus-kasus ini adalah:

- Bucket dibagikan dengan Akun AWS yang eksternal untuk organisasi Anda, selain CloudFront OAI atau OAC.
- Kebijakan bucket menentukan ID pengguna kanonik, bukan Nama Sumber Daya Amazon (ARN), dari OAI. CloudFront

Ini menghasilkan temuan kebijakan tingkat keparahan yang lebih tinggi untuk ember.

## Jenis temuan data sensitif

Macie menghasilkan temuan data sensitif ketika mendeteksi data sensitif dalam objek S3 yang dianalisis untuk menemukan data sensitif. Ini termasuk analisis yang dilakukan Macie saat Anda menjalankan pekerjaan penemuan data sensitif dan saat melakukan penemuan data sensitif otomatis.

Misalnya, jika Anda membuat dan menjalankan pekerjaan penemuan data sensitif dan Macie mendeteksi nomor rekening bank di objek S3, Macie menghasilkan temuan SensitiveData A:S3Object/Financial untuk objek tersebut. Demikian pula, jika Macie mendeteksi nomor rekening bank dalam objek S3 yang dianalisis selama siklus penemuan data sensitif otomatis, Macie menghasilkan temuan objek/keuangan untuk objek tersebut. SensitiveData

Jika Macie mendeteksi data sensitif dalam objek S3 yang sama selama menjalankan pekerjaan berikutnya atau siklus penemuan data sensitif otomatis, Macie menghasilkan temuan data sensitif baru untuk objek tersebut. Tidak seperti temuan kebijakan, semua temuan data sensitif diperlakukan sebagai baru (unik). Macie menyimpan temuan data sensitif selama 90 hari.

Macie dapat menghasilkan jenis temuan data sensitif berikut untuk objek S3.

### SensitiveData:S3Object/Credentials

Objek berisi data kredensial sensitif, seperti kunci akses AWS rahasia atau kunci pribadi.

### SensitiveData:S3Object/CustomIdentifier

Objek berisi teks yang cocok dengan kriteria deteksi dari satu atau lebih pengidentifikasi data kustom. Objek mungkin berisi lebih dari satu tipe data sensitif.

### SensitiveData:S3Object/Financial

Objek tersebut berisi informasi keuangan yang sensitif, seperti nomor rekening bank atau nomor kartu kredit.

## SensitiveData:S3Object/Multiple

Objek berisi lebih dari satu kategori data sensitif—kombinasi data kredensial, informasi keuangan, informasi pribadi, atau teks yang sesuai dengan kriteria deteksi satu atau lebih pengidentifikasi data kustom.

## SensitiveData:S3Object/Personal

Objek tersebut berisi informasi pribadi yang sensitif — informasi identitas pribadi (PII) seperti nomor paspor atau nomor identifikasi SIM, informasi kesehatan pribadi (PHI) seperti asuransi kesehatan atau nomor identifikasi medis, atau kombinasi PII dan PHI.

Untuk informasi tentang jenis data sensitif yang dapat dideteksi Macie menggunakan kriteria dan teknik bawaan, lihat [Menggunakan pengidentifikasi data terkelola](#). Untuk informasi tentang tipe objek S3 yang dapat dianalisis oleh Macie, lihat [Kelas dan format penyimpanan yang didukung](#).

## Bekerja dengan temuan sampel di Amazon Macie

Untuk mengeksplorasi dan mempelajari berbagai [jenis temuan](#) yang dapat dihasilkan Amazon Macie, Anda dapat membuat temuan sampel. Temuan sampel menggunakan data contoh dan nilai placeholder untuk menunjukkan jenis informasi yang mungkin terkandung dalam setiap jenis temuan.

Misalnya, BucketPublic temuan sampel Policy:iamuser/S3 berisi detail tentang bucket Simple Storage Service Amazon (Amazon S3) fiktif. Detail temuan ini mencakup contoh data tentang aktor dan tindakan yang mengubah daftar kontrol akses (ACL) untuk bucket dan membuat bucket dapat diakses publik. Demikian pula, temuan SensitiveData:sample: S3Object/Multiple berisi detail tentang buku kerja Microsoft Excel fiktif. Detail temuan mencakup contoh data tentang jenis dan lokasi data sensitif di buku kerja.

Selain membiasakan diri dengan informasi yang mungkin terkandung dalam berbagai jenis temuan, Anda dapat menggunakan temuan sampel untuk menguji integrasi dengan aplikasi, layanan, dan sistem lain. Bergantung pada [aturan penindasan](#) untuk akun Anda, Macie dapat mempublikasikan temuan sampel ke Amazon EventBridge sebagai peristiwa. Dengan menggunakan contoh data dalam temuan sampel, Anda dapat mengembangkan dan menguji solusi otomatis untuk memantau dan memproses peristiwa ini. Bergantung pada [pengaturan publikasi](#) untuk akun Anda, Macie juga dapat mempublikasikan temuan sampel ke AWS Security Hub. Ini berarti Anda juga dapat menggunakan temuan sampel untuk mengembangkan dan menguji solusi untuk memantau dan memproses temuan Macie di Security Hub. Untuk informasi tentang mempublikasikan temuan ke layanan ini, lihat [Pemantauan dan pemrosesan temuan](#).

## Topik

- [Membuat temuan sampel](#)
- [Meninjau temuan sampel](#)
- [Menekan temuan sampel](#)

## Membuat temuan sampel

Anda dapat membuat sampel temuan dengan menggunakan konsol Amazon Macie atau Amazon Macie API. Jika Anda menggunakan konsol, Macie secara otomatis menghasilkan satu sampel temuan untuk setiap jenis temuan yang didukung Macie. Jika Anda menggunakan API, Anda dapat membuat sampel untuk setiap jenis atau hanya tipe tertentu yang Anda tentukan.

### Console

Ikuti langkah-langkah berikut untuk membuat temuan sampel dengan menggunakan konsol Amazon Macie.

Untuk membuat temuan sampel

1. [Buka konsol Amazon Macie di https://console.aws.amazon.com/macie/](https://console.aws.amazon.com/macie/).
2. Pada panel navigasi, silakan pilih Pengaturan.
3. Di bawah Temuan sampel, pilih Hasilkan temuan sampel.

### API

Untuk membuat temuan sampel secara terprogram, gunakan [CreateSampleFindings](#) pengoperasian Amazon Macie API. Saat Anda mengirimkan permintaan, gunakan `findingTypes` parameter secara opsional untuk menentukan hanya jenis temuan sampel tertentu yang akan dibuat. Untuk secara otomatis membuat sampel dari semua jenis, jangan sertakan parameter ini dalam permintaan Anda.

Untuk membuat temuan sampel dengan menggunakan [AWS Command Line Interface\(AWS CLI\)](#), jalankan [create-sample-findings](#) perintah. Untuk secara otomatis membuat sampel dari semua jenis temuan, jangan sertakan `finding-types` parameter. Untuk membuat sampel hanya jenis temuan tertentu, sertakan parameter ini dan tentukan jenis temuan sampel yang akan dibuat. Sebagai contoh:

```
C:\> aws macie2 create-sample-findings --finding-types "SensitiveData:S3Object/
Multiple" "Policy:IAMUser/S3BucketPublic"
```

*Dimana:S3Object/Multiple SensitiveData adalah jenis temuan data sensitif untuk dibuat dan kebijakan: iamuser/S3 adalah jenis temuan kebijakan untuk dibuat. BucketPublic*

Jika perintah berjalan dengan sukses, Macie mengembalikan respon kosong.

## Meninjau temuan sampel

Untuk membantu Anda mengidentifikasi temuan sampel yang Anda buat, Macie menetapkan nilai untuk bidang Sampel dari setiap temuan sampel ke Benar. Selain itu, nama bucket S3 yang terpengaruh adalah sama untuk semua temuan sampel: macie-sample-finding-bucket. Jika Anda meninjau temuan sampel menggunakan halaman Temuan di konsol Amazon Macie, Macie juga menampilkan awalan [SAMPEL] di bidang Jenis pencarian untuk setiap temuan sampel.

### Console

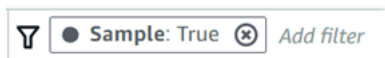
Ikuti langkah-langkah berikut untuk meninjau temuan sampel dengan menggunakan konsol Amazon Macie.

Untuk meninjau temuan sampel

1. [Buka konsol Amazon Macie di https://console.aws.amazon.com/macie/](https://console.aws.amazon.com/macie/).
2. Di panel navigasi, pilih Temuan.
3. Pada halaman Temuan, lakukan salah satu hal berikut:
  - Di kolom tipe Finding, cari temuan yang tipenya dimulai dengan [SAMPLE], seperti yang ditunjukkan pada gambar berikut.

<input type="checkbox"/>	Severity ▾	Finding type ▾	Resources affected
<input type="checkbox"/>	Low	[SAMPLE] Policy:IAMUser/S3BucketEncryptionDisabled	macie-sample-finding-bucket
<input type="checkbox"/>	High	[SAMPLE] SensitiveData:S3Object/CustomIdentifier	macie-sample-finding-bucket/en
<input type="checkbox"/>	Low	[SAMPLE] SensitiveData:S3Object/Personal	macie-sample-finding-bucket/pe
<input type="checkbox"/>	High	[SAMPLE] Policy:IAMUser/S3BucketPublic	macie-sample-finding-bucket
<input type="checkbox"/>	Medium	[SAMPLE] Policy:IAMUser/S3BucketSharedWithCloudFront	macie-sample-finding-bucket
<input type="checkbox"/>	High	[SAMPLE] Policy:IAMUser/S3BucketSharedExternally	macie-sample-finding-bucket
<input type="checkbox"/>	High	[SAMPLE] SensitiveData:S3Object/Financial	macie-sample-finding-bucket/fin
<input type="checkbox"/>	High	[SAMPLE] Policy:IAMUser/S3BucketReplicatedExternally	macie-sample-finding-bucket
<input type="checkbox"/>	High	[SAMPLE] SensitiveData:S3Object/Credentials	macie-sample-finding-bucket/cr
<input type="checkbox"/>	High	[SAMPLE] SensitiveData:S3Object/Multiple	macie-sample-finding-bucket/sa
<input type="checkbox"/>	High	[SAMPLE] Policy:IAMUser/S3BlockPublicAccessDisabled	macie-sample-finding-bucket

- Dengan menggunakan kotak kriteria Filter di atas tabel, filter tabel untuk hanya menampilkan temuan sampel. Untuk melakukan ini, letakkan kursor Anda di dalam kotak. Dalam daftar bidang yang muncul, pilih Contoh. Kemudian pilih Benar, lalu pilih Terapkan. Ini menambahkan kondisi filter berikut ke tabel:



4. Untuk meninjau detail temuan sampel tertentu, pilih temuannya. Panel detail menampilkan informasi untuk temuan.

Anda juga dapat mengunduh dan menyimpan detail dari satu atau lebih temuan sampel sebagai file JSON. Untuk melakukan ini, pilih kotak centang untuk setiap temuan sampel yang ingin Anda unduh dan simpan. Kemudian pilih Ekspor (JSON) pada menu Tindakan di bagian atas halaman Temuan. Di jendela yang muncul, pilih Unduh. Untuk deskripsi terperinci tentang bidang JSON yang dapat disertakan dalam temuan, lihat [Temuan](#) di Referensi API Amazon Macie.

## API

Untuk meninjau temuan sampel secara terprogram, pertama-tama gunakan [ListFindings](#) pengoperasian Amazon Macie API untuk mengambil identifier unik `findingId` ()



untuk setiap temuan sampel yang Anda buat. Kemudian gunakan [GetFindings](#) operasi untuk mengambil rincian temuan tersebut.

Saat Anda mengirimkan ListFindings permintaan, Anda dapat menentukan kriteria filter untuk menyertakan hanya temuan sampel dalam hasil. Untuk melakukan ini, tambahkan kondisi filter di mana nilai untuk sample bidang tersebut true. Jika Anda menggunakan AWS CLI, jalankan perintah [daftar-temuan](#) dan gunakan finding-criteria parameter untuk menentukan kondisi filter. Sebagai contoh:

```
C:\> aws macie2 list-findings --finding-criteria={"criterion":{"sample":{"eq":["true"]}}}
```

Jika permintaan Anda berhasil, Macie mengembalikan array. findingIds Array mencantumkan pengenal unik untuk setiap temuan sampel untuk akun Anda saat ini Wilayah AWS.

Untuk kemudian mengambil rincian temuan sampel, tentukan pengidentifikasi unik ini dalam GetFindings permintaan atau, untuk AWS CLI, saat Anda menjalankan perintah [get-temuan](#).

## Menekan temuan sampel

Seperti temuan lainnya, Macie menyimpan temuan sampel selama 90 hari. Setelah Anda selesai meninjau dan bereksperimen dengan sampel, Anda dapat mengarsipkannya secara opsional dengan [membuat aturan penekanan](#). Jika Anda melakukan ini, temuan sampel berhenti muncul secara default di konsol dan statusnya berubah menjadi diarsipkan.

Untuk mengarsipkan temuan sampel menggunakan konsol Amazon Macie, konfigurasi aturan untuk mengarsipkan temuan di mana nilai untuk bidang Sampel adalah Benar. Untuk mengarsipkan temuan sampel menggunakan Amazon Macie API, konfigurasi aturan untuk mengarsipkan temuan di mana nilai untuk sample bidang tersebut berada. true

## Meninjau temuan di konsol Amazon Macie

Amazon Macie memantau AWS lingkungan Anda dan menghasilkan temuan kebijakan saat mendeteksi potensi pelanggaran kebijakan atau masalah dengan keamanan atau privasi bucket Amazon Simple Storage Service (Amazon S3). Macie menghasilkan temuan data sensitif ketika mendeteksi data sensitif di objek S3. Macie menyimpan kebijakan dan temuan data sensitif Anda selama 90 hari.

Setiap temuan menentukan [jenis temuan](#) dan [peringkat keparahan](#). Rincian tambahan mencakup informasi tentang sumber daya yang terpengaruh dan kapan dan bagaimana Macie menemukan masalah atau data sensitif yang dilaporkan oleh temuan tersebut. Tingkat keparahan dan detail setiap temuan bervariasi tergantung pada jenis dan sifat temuan.

Dengan menggunakan konsol Amazon Macie, Anda dapat meninjau dan menganalisis temuan, serta mengakses detail temuan individu. Anda juga dapat mengekspor satu atau lebih temuan ke file JSON. Untuk membantu Anda menyederhanakan analisis Anda, konsol tersebut menawarkan beberapa opsi untuk membangun tampilan kustom dari temuan.

Gunakan pengelompokan yang telah ditentukan

Gunakan halaman tertentu untuk meninjau temuan yang dikelompokkan berdasarkan kriteria seperti bucket S3 yang terpengaruh, jenis pencarian, atau pekerjaan penemuan data sensitif. Dengan halaman ini, Anda dapat meninjau statistik agregat untuk setiap kelompok, seperti jumlah temuan berdasarkan tingkat keparahan. Anda juga dapat menelusuri untuk meninjau detail temuan individu dalam grup, dan Anda dapat menerapkan filter untuk menyempurnakan analisis Anda.

Misalnya, jika Anda mengelompokkan semua temuan berdasarkan bucket S3 dan perhatikan bahwa bucket tertentu memiliki pelanggaran kebijakan, Anda dapat dengan cepat menentukan apakah ada juga temuan data sensitif untuk bucket tersebut. Untuk melakukannya, pilih Berdasarkan bucket di panel navigasi (di bawah Temuan), lalu pilih bucket. Pada panel detail yang muncul, bagian Temuan berdasarkan jenis mencantumkan jenis temuan yang berlaku untuk ember, seperti yang ditunjukkan pada gambar berikut.

**DOC-EXAMPLE-BUCKET1**

Bucket name: **DOC-EXAMPLE-BUCKET1**

**Findings by severity**

High	42	<a href="#">↗</a>
Medium	12	<a href="#">↗</a>
Low	4	<a href="#">↗</a>

**Findings by type**

SensitiveData:S3Object/Multiple	42	<a href="#">↗</a>
SensitiveData:S3Object/Personal	15	<a href="#">↗</a>
Policy:IAMUser/S3BucketEncryptionDisabled	1	<a href="#">↗</a>

**Findings by job**

93f7246f0a269c32cdbea6a15cce2532	29	<a href="#">↗</a>
----------------------------------	----	-------------------

Untuk menyelidiki tipe tertentu, pilih jumlah tipe untuk. Macie menampilkan tabel semua temuan yang cocok dengan jenis yang dipilih dan berlaku untuk ember. Untuk menyempurnakan hasilnya, filter tabel.

### Buat dan terapkan filter

Gunakan atribut temuan tertentu untuk menyertakan atau mengecualikan temuan tertentu dari tabel Temuan. Atribut temuan adalah bidang yang menyimpan data spesifik untuk temuan, seperti jenis pencarian, tingkat keparahan, atau nama bucket S3 yang terpengaruh. Jika Anda memfilter tabel, Anda dapat lebih mudah mengidentifikasi temuan yang memiliki karakteristik tertentu. Kemudian Anda dapat menelusuri untuk meninjau detail temuan tersebut.

Misalnya, untuk meninjau semua temuan data sensitif Anda, tambahkan kriteria filter untuk bidang Kategori. Untuk menyempurnakan hasil dan hanya menyertakan jenis temuan data sensitif tertentu, tambahkan kriteria filter untuk bidang Jenis pencarian. Sebagai contoh:

**Findings (1)** [Info](#) [↻](#) [Actions](#)

This table lists findings for your organization. Select a finding to show its details. You can also filter, group, and sort findings based on specific fields and field values.

[Suppress findings](#) Saved rules [Choose a rule](#)

**Filter criteria**


Finding status: [Current](#)

Filter criteria: [Category: Classification](#) [Finding type: SensitiveData:S3Object/Personal](#) [Add filter](#) [Save rule](#) [X](#)

Untuk meninjau detail temuan tertentu, pilih temuan. Panel detail menampilkan informasi untuk temuan.

Anda juga dapat mengurutkan temuan dalam urutan naik atau turun menurut bidang tertentu. Untuk melakukan ini, klik judul kolom untuk bidang. Untuk mengubah susunan urutan, klik judul kolom lagi.

Untuk meninjau temuan di konsol

1. [Buka konsol Amazon Macie di https://console.aws.amazon.com/macie/](https://console.aws.amazon.com/macie/).
2. Di panel navigasi, pilih Temuan. Halaman Temuan menampilkan temuan yang dibuat atau diperbarui Macie untuk akun Anda saat ini Wilayah AWS selama 90 hari terakhir. Secara default, ini tidak termasuk temuan yang ditekan oleh [aturan penekanan](#).
3. Untuk memutar dan meninjau temuan berdasarkan grup logis yang telah ditentukan sebelumnya, pilih Berdasarkan bucket, Berdasarkan jenis, atau Menurut pekerjaan di panel navigasi (di bawah Temuan). Kemudian pilih item di tabel. Di panel detail, pilih tautan untuk bidang yang akan diputar.
4. Untuk memfilter temuan berdasarkan kriteria tertentu, gunakan opsi filter di atas tabel:
  - Untuk menampilkan temuan yang ditekan oleh aturan penekanan, gunakan menu Finding status. Pilih Semua untuk menampilkan temuan yang ditekan dan tidak ditekan, atau pilih Diarsipkan untuk menampilkan hanya temuan yang ditekan. Untuk kemudian menyembunyikan temuan yang ditekan lagi, pilih Current.
  - Untuk menampilkan hanya temuan yang memiliki atribut tertentu, gunakan kotak kriteria Filter. Tempatkan kursor Anda di dalam kotak dan tambahkan kondisi filter untuk atribut. Untuk lebih menyempurnakan hasilnya, tambahkan syarat untuk atribut tambahan. Untuk kemudian menghapus kondisi, pilih ikon hapus kondisi  ) untuk kondisi yang akan dihapus.

Untuk informasi lebih lanjut tentang temuan penyaringan, lihat [Membuat dan menerapkan filter untuk temuan](#).

5. Untuk mengurutkan temuan berdasarkan bidang tertentu, klik judul kolom untuk bidang tersebut. Untuk mengubah urutan pengurutan, klik judul kolom lagi.
6. Untuk meninjau detail temuan tertentu, pilih temuannya. Panel detail menampilkan informasi untuk temuan.

 Tip

Anda dapat menggunakan panel detail untuk berputar dan menelusuri bidang tertentu. Untuk menunjukkan temuan yang memiliki nilai yang sama untuk suatu bidang, pilih



di bidang. Atau pilih



untuk menunjukkan temuan yang memiliki nilai lain untuk bidang tersebut.

Untuk menemukan data sensitif, Anda juga dapat menggunakan panel detail untuk menyelidiki data sensitif yang ditemukan Macie di objek S3 yang terpengaruh:

- Untuk menemukan kemunculan jenis data sensitif tertentu, pilih tautan numerik di bidang untuk jenis data tersebut. Macie menampilkan informasi (dalam format JSON) tentang di mana Macie menemukan data. Untuk informasi selengkapnya, lihat [Menemukan data sensitif](#).
- Untuk mengambil sampel data sensitif yang ditemukan Macie, pilih Tinjau di bidang Reveal samples. Untuk informasi selengkapnya, lihat [Mengambil sampel data sensitif](#).
- Untuk mengarahkan ke hasil penemuan data sensitif yang sesuai, pilih tautan di bidang Lokasi hasil mendetail. Macie membuka konsol Amazon S3 dan menampilkan file atau folder yang berisi hasil penemuan. Untuk informasi selengkapnya, lihat [Menyimpan dan mempertahankan hasil penemuan data sensitif](#).

Anda juga dapat mengunduh dan menyimpan detail dari satu atau lebih temuan sebagai file JSON. Untuk melakukannya, centang kotak untuk setiap temuan yang ingin Anda unduh dan simpan. Kemudian pilih Ekspor (JSON) pada menu Tindakan di bagian atas halaman Temuan. Di jendela yang muncul, pilih Unduh. Untuk deskripsi terperinci tentang bidang JSON yang dapat disertakan dalam temuan, lihat [Temuan](#) di Referensi API Amazon Macie.

## Memfilter temuan Amazon Macie

Untuk melakukan analisis yang ditargetkan dan menganalisis temuan dengan lebih efisien, Anda dapat memfilter temuan Amazon Macie. Dengan filter, Anda membangun tampilan khusus dan kueri untuk temuan, yang dapat membantu Anda mengidentifikasi dan fokus pada temuan yang memiliki karakteristik khusus. Gunakan konsol Amazon Macie untuk memfilter temuan, atau kirim kueri secara terprogram menggunakan API Amazon Macie.

Saat Anda membuat filter, Anda menggunakan atribut temuan tertentu untuk menentukan kriteria untuk menyertakan atau mengecualikan temuan dari tampilan atau dari hasil kueri. Temuan atribut adalah bidang yang menyimpan data spesifik untuk temuan, seperti kepelikan, tipe, atau nama bucket S3 bahwa temuan berlaku untuk.

Di Macie, filter terdiri atas satu atau beberapa syarat. Setiap syarat, juga disebut sebagai kriteria, terdiri dari tiga bagian:

- Bidang berbasis atribut, seperti Kepelikan atau Tipe temuan.
- Operator, seperti sama dengan atau tidak sama dengan.
- Satu atau beberapa nilai. Tipe dan jumlah nilai tergantung pada bidang dan operator yang Anda pilih.

Jika Anda membuat filter yang ingin Anda gunakan lagi, Anda dapat menyimpannya sebagai aturan filter. filter aturan adalah set kriteria filter yang Anda buat dan simpan untuk diterapkan kembali ketika Anda meninjau temuan di konsol Amazon Macie.

Anda juga dapat menyimpan filter sebagai aturan penindasan. aturan penekanan adalah set kriteria filter yang Anda buat dan simpan untuk secara otomatis mengarsipkan temuan yang cocok dengan kriteria aturan. Untuk mempelajari tentang aturan penindasan, lihat [Menekan temuan](#).

Topik

- [Hal mendasar pem-filter-an temuan](#)
- [Membuat dan menerapkan filter untuk temuan](#)
- [Membuat dan mengelola aturan filter untuk temuan](#)
- [Bidang untuk memfilter temuan](#)

## Hal mendasar pem-filter-an temuan

Saat Anda membuat filter, ingatlah fitur dan panduan berikut. Perhatikan juga bahwa hasil yang difilter terbatas pada 90 hari sebelumnya dan saat ini. Wilayah AWS Amazon Macie menyimpan temuan Anda hanya selama 90 hari di masing-masing. Wilayah AWS

Topik

- [Menggunakan beberapa syarat dalam filter](#)
- [Menentukan nilai untuk bidang](#)

- [Menentukan beberapa nilai untuk bidang](#)
- [Menggunakan operator dalam syarat](#)

## Menggunakan beberapa syarat dalam filter

Filter dapat mencakup satu atau lebih syarat-syarat. Setiap syarat, juga disebut sebagai kriteria, terdiri dari tiga bagian:

- Bidang berbasis atribut, seperti Kepelikan atau Tipe temuan. Untuk daftar bidang yang dapat Anda gunakan, lihat [Bidang untuk memfilter temuan](#).
- Operator, seperti sama dengan atau tidak sama dengan. Untuk daftar operator yang dapat Anda gunakan, lihat [Menggunakan operator dalam syarat](#).
- Satu atau beberapa nilai. Tipe dan jumlah nilai tergantung pada bidang dan operator yang Anda pilih.

Jika filter berisi beberapa syarat, Macie menggunakan logika AND untuk menggabungkan syarat dan mengevaluasi kriteria filter. Ini berarti bahwa temuan cocok dengan kriteria filter hanya jika cocok dengan semua kondisi dalam filter.

Misalnya, jika Anda menambahkan syarat untuk hanya menyertakan temuan dengan kepelikan tinggi dan menambahkan ketentuan lain untuk menyertakan hanya temuan data sensitif, Macie mengembalikan semua temuan data sensitif dengan kepelikan tinggi. Dengan kata lain, Macie mengecualikan semua temuan kebijakan dan semua temuan data sensitif dengan kepelikan medium dan rendah.

Anda dapat menggunakan bidang hanya sekali dalam filter. Namun, Anda dapat menentukan beberapa nilai untuk banyak bidang.

Misalnya, jika syarat menggunakan bidang Kepelikan untuk menyertakan hanya temuan kepelikan tinggi, Anda tidak dapat menggunakan Kepelikan dalam syarat lain untuk menyertakan temuan kepelikan medium atau kepelikan rendah. Sebaliknya, tentukan beberapa nilai untuk syarat yang ada, atau gunakan operator yang berbeda untuk syarat yang ada. Misalnya, untuk menyertakan semua temuan kepelikan medium dan kepelikan tinggi, tambahkan syarat Kepelikan Sama dengan Medium, Tinggi atau tambahkan syarat Kepelikan tidak sama dengan Rendah.

## Menentukan nilai untuk bidang

Ketika Anda menentukan nilai untuk bidang, nilai tersebut harus sesuai dengan tipe data yang mendasari bidang tersebut. Tergantung pada bidang, Anda dapat menentukan salah satu dari tipe nilai berikut.

### Array teks (string)

Menentukan daftar nilai teks (string) untuk bidang. Setiap string berkorelasi dengan nilai yang telah ditentukan sebelumnya atau yang sudah ada untuk suatu bidang—misalnya, bidang Tinggi untuk Keparahan, `:S3Object/Financial` untuk bidang jenis Finding, atau nama bucket S3 `SensitiveData` untuk bidang nama bucket S3.

Jika Anda menggunakan array, perhatikan hal berikut:

- Nilai peka huruf besar/kecil.
- Anda tidak dapat menentukan nilai parsial atau menggunakan karakter wildcard dalam nilai. Anda harus menentukan nilai yang lengkap dan valid untuk bidang tersebut.

Misalnya, untuk memfilter temuan bucket S3 yang bernama Bucket S3-saya, masukkan **my-S3-bucket** sebagai nilai untuk bidang nama bucket S3. Jika Anda memasukkan nilai lain, seperti **my-s3-bucket** atau **my-S3**, Macie tidak akan mengembalikan temuan untuk bucket.

Untuk daftar nilai yang valid untuk setiap bidang, lihat [Bidang untuk memfilter temuan](#).

Anda dapat menentukan sebanyak 50 nilai dalam array. Cara Anda menentukan nilai-nilai tergantung pada apakah Anda menggunakan konsol Amazon Macie atau API Amazon Macie, seperti yang dibahas dalam [Menentukan beberapa nilai untuk bidang](#).

### Boolean

Menentukan salah satu dari dua nilai yang saling eksklusif untuk bidang.

Jika Anda menggunakan konsol Amazon Macie untuk menentukan tipe nilai, konsol menyediakan daftar nilai untuk memilih dari. Jika Anda menggunakan API Amazon Macie, tentukan `true` atau `false` untuk nilai.

### Tanggal/Waktu (dan rentang waktu)

Menentukan tanggal dan waktu absolut untuk bidang. Jika Anda menentukan tipe nilai, Anda harus menentukan tanggal dan waktu.



Di konsol Amazon Macie, nilai tanggal dan waktu berada di zona waktu lokal Anda dan menggunakan notasi 24 jam. Dalam semua konteks lain, nilai-nilai ini dalam Waktu Universal Terkoordinasi (UTC) dan format ISO 8601 yang diperpanjang—misalnya `2020-09-01T14:31:13Z` untuk 14:31:13 UTC 1 September 2020.

Jika bidang menyimpan nilai tanggal/waktu, Anda dapat menggunakan bidang untuk menentukan rentang waktu tetap atau relatif. Misalnya, Anda hanya dapat menyertakan temuan yang dibuat antara dua tanggal dan waktu tertentu, atau hanya temuan yang dibuat sebelum atau setelah tanggal dan waktu tertentu. Cara Anda menentukan rentang waktu bergantung pada apakah Anda menggunakan konsol Amazon Macie atau API Amazon Macie:

- Pada konsol tersebut, gunakan pemilih tanggal atau masukkan teks secara langsung di kotak Dari dan Untuk.
- Dengan API, tentukan rentang waktu tetap dengan menambahkan syarat yang menentukan tanggal dan waktu pertama dalam rentang, dan tambahkan syarat lain yang menentukan tanggal dan waktu terakhir dalam rentang. Jika Anda melakukan hal ini, Macie menggunakan logika AND untuk menggabungkan syarat. Untuk menentukan rentang waktu relatif, tambahkan satu syarat yang menentukan tanggal dan waktu pertama atau terakhir dalam rentang tersebut. Tentukan nilai sebagai stempel waktu Unix dalam milidetik—misalnya, `1604616572653` untuk 22:49:32 UTC 5 November 2020.

Pada konsol tersebut, rentang waktu inklusif. Dengan API, rentang waktu bisa inklusif atau eksklusif, tergantung operator yang Anda pilih.

## Angka (dan rentang numerik)

Menentukan bilangan bulat panjang untuk bidang.

Jika bidang menyimpan nilai numerik, Anda bisa menggunakan bidang tersebut untuk menentukan rentang numerik tetap atau relatif. Misalnya, Anda hanya dapat menyertakan temuan yang melaporkan 50-90 kemunculan data sensitif dalam objek S3. Cara Anda menentukan rentang numerik bergantung pada apakah Anda menggunakan konsol Amazon Macie atau API Amazon Macie:

- Pada konsol tersebut, gunakan kotak Dari dan Untuk untuk memasukkan angka terendah dan tertinggi dalam rentang, masing-masing.
- Dengan API, tentukan rentang numerik tetap dengan menambahkan syarat yang menentukan angka terendah dalam rentang, dan tambahkan syarat lain yang menetapkan angka tertinggi dalam rentang. Jika Anda melakukan hal ini, Macie menggunakan logika AND untuk

menggabungkan syarat. Untuk menentukan rentang numerik relatif, tambahkan satu syarat yang menentukan angka terendah atau tertinggi dalam rentang tersebut.

Pada konsol tersebut, rentang angka adalah inklusif. Dengan API, rentang numerik dapat inklusif atau eksklusif, tergantung pada operator yang Anda pilih.

## Teks (string)

Menentukan nilai teks tunggal (string) untuk bidang. String berkaitan dengan nilai yang telah ditetapkan sebelumnya atau yang sudah ada untuk bidang-misalnya, Tinggi untuk Kepelikan, nama bucket S3 untuk nama bucket S3, atau pengenal unik untuk tugas penemuan data sensitif untuk bidang ID Tugas.

Jika Anda menentukan string teks tunggal, perhatikan hal berikut ini:

- Nilai peka huruf besar/kecil.
- Anda tidak dapat menggunakan nilai parsial atau menggunakan karakter wildcard dalam nilai-nilai. Anda harus menentukan nilai yang lengkap dan valid untuk bidang tersebut.

Misalnya, untuk memfilter temuan bucket S3 yang bernama Bucket S3-saya, masukkan **my-S3-bucket** sebagai nilai untuk bidang nama bucket S3. Jika Anda memasukkan nilai lain, seperti **my-s3-bucket** atau **my-S3**, Macie tidak akan mengembalikan temuan untuk bucket.

Untuk daftar nilai yang valid untuk setiap bidang, lihat [Bidang untuk memfilter temuan](#).

## Menentukan beberapa nilai untuk bidang

Dengan bidang dan operator tertentu, Anda dapat menentukan beberapa nilai untuk bidang. Jika Anda melakukan ini, Macie menggunakan logika OR untuk menggabungkan nilai dan mengevaluasi kriteria filter. Ini berarti bahwa temuan cocok dengan kriteria jika memiliki salah satu nilai untuk bidang tersebut.

Misalnya, jika Anda menambahkan kondisi untuk menyertakan temuan di mana nilai untuk bidang tipe Finding sama dengan: S3Object/Financial SensitiveData ,:S3Object/Personal, SensitiveData Macie mengembalikan temuan data sensitif untuk objek S3 yang hanya berisi informasi keuangan, dan objek S3 yang hanya berisi informasi pribadi. Dengan kata lain, Macie mengecualikan semua temuan kebijakan. Macie juga mengecualikan semua temuan data sensitif untuk objek yang berisi tipe data sensitif lainnya atau beberapa tipe data sensitif.

Pengecualian adalah kondisi yang menggunakan eqExactMatchoperator. Untuk operator ini, Macie menggunakan logika AND untuk menggabungkan nilai dan mengevaluasi kriteria filter. Ini berarti

bahwa temuan cocok dengan kriteria hanya jika memiliki semua nilai untuk bidang dan hanya nilai-nilai untuk bidang tersebut. Untuk mempelajari selengkapnya tentang operator ini, lihat [Menggunakan operator dalam syarat](#).

Cara Anda menentukan beberapa nilai untuk suatu bidang bergantung pada apakah Anda menggunakan API Amazon Macie atau konsol Amazon Macie. Dengan API, Anda menggunakan array yang mencantumkan nilai.

Pada konsol tersebut, Anda biasanya memilih nilai-nilai dari daftar. Namun, untuk beberapa bidang, Anda harus menambahkan syarat berbeda untuk setiap nilai. Misalnya, untuk menyertakan temuan data yang dideteksi Macie menggunakan pengidentifikasi data khusus tertentu, lakukan hal berikut:

1. Tempatkan kursor Anda di kotak Kriteria filter dan kemudian pilih bidang Nama pengenalan data kustom. Masukkan nama pengenalan data kustom, lalu pilih Terapkan.
2. Ulangi langkah sebelumnya untuk setiap pengenalan data khusus tambahan yang ingin Anda tentukan untuk filter.

Untuk daftar bidang yang perlu Anda lakukan ini, lihat [Bidang untuk memfilter temuan](#).

## Menggunakan operator dalam syarat

Anda dapat menggunakan tipe operator berikut dalam syarat individual.

Sama dengan () eq

Mencocokkan (=) nilai apa pun yang ditentukan untuk bidang. Anda dapat menggunakan operator sama dengan dengan tipe nilai berikut: array teks (string), Boolean, tanggal/waktu, nomor, dan teks (string).

Untuk banyak bidang, Anda dapat menggunakan operator ini dan menentukan sebanyak 50 nilai untuk bidang tersebut. Jika Anda melakukan ini, Macie menggunakan logika OR untuk menggabungkan nilai. Ini berarti bahwa temuan cocok dengan kriteria jika memiliki salah satu nilai yang ditentukan untuk bidang tersebut.

Misalnya:

- Untuk menyertakan temuan yang melaporkan kemunculan informasi keuangan, informasi pribadi, atau informasi keuangan dan pribadi, tambahkan syarat yang menggunakan bidang Kategori data sensitif dan operator ini, serta tentukan Informasi keuangan dan Informasi pribadi sebagai nilai bidang tersebut.

- Untuk menyertakan temuan yang melaporkan kemunculan nomor kartu kredit, alamat surat, atau nomor kartu kredit dan alamat surat, tambahkan kondisi untuk bidang Jenis deteksi data sensitif, gunakan operator ini, CREDIT\_CARD\_NUMBER dan tentukan ADDRESSserta sebagai nilai untuk bidang tersebut.

Jika Anda menggunakan API Amazon Macie untuk menentukan syarat yang menggunakan operator ini dengan nilai tanggal/waktu, tentukan nilainya sebagai stempel waktu Unix dalam milidetik—misalnya, 1604616572653 untuk 22:49:32 UTC 5 November 2020.

Sama persis dengan kecocokan () eqExactMatch

Secara eksklusif cocok dengan semua nilai yang ditentukan untuk bidang. Anda dapat menggunakan operator pencocokan sama persis dengan dengan satu set bidang pilihan.

Jika Anda menggunakan operator ini dan menentukan beberapa nilai untuk bidang, Macie menggunakan logika AND untuk menggabungkan nilai. Ini berarti bahwa temuan cocok dengan kriteria hanya jika memiliki semua nilai yang ditentukan untuk bidang dan hanya nilai-nilai untuk bidang tersebut. Anda dapat menentukan sebanyak 50 nilai untuk bidang.

Misalnya:

- Untuk menyertakan temuan yang melaporkan kemunculan nomor kartu kredit dan tidak ada jenis data sensitif lainnya, tambahkan kondisi untuk bidang Jenis deteksi data sensitif, gunakan operator ini, dan tentukan CREDIT\_CARD\_NUMBER sebagai satu-satunya nilai untuk bidang tersebut.
- Untuk menyertakan temuan yang melaporkan kejadian nomor kartu kredit dan alamat surat (dan tidak ada jenis data sensitif lainnya), tambahkan kondisi untuk bidang Jenis deteksi data sensitif, gunakan operator ini, CREDIT\_CARD\_NUMBER dan tentukan ADDRESSserta sebagai nilai untuk bidang tersebut.

Karena Macie menggunakan logika AND untuk menggabungkan nilai bidang, Anda tidak dapat menggunakan operator ini dalam kombinasi dengan operator lain untuk bidang yang sama. Dengan kata lain, jika Anda menggunakan operator pencocokan sama persis dengan bidang dalam satu syarat, Anda harus menggunakannya di semua syarat lain yang menggunakan bidang yang sama.

Seperti operator lain, Anda dapat menggunakan operator pencocokan sama persis di lebih dari satu syarat dalam filter. Jika Anda melakukan ini, Macie menggunakan logika AND untuk menggabungkan syarat dan mengevaluasi filter. Ini berarti bahwa temuan cocok dengan kriteria filter hanya jika memiliki semua nilai yang ditentukan oleh semua kondisi dalam filter.

Misalnya, untuk menyertakan temuan yang dibuat setelah waktu tertentu, melaporkan kemunculan nomor kartu kredit, dan tidak melaporkan tipe data sensitif lainnya, lakukan hal berikut:

1. Tambahkan syarat yang menggunakan bidang Dibuat di, menggunakan operator yang lebih besar dari, dan menentukan tanggal dan waktu mulai untuk filter.
2. Tambahkan kondisi lain yang menggunakan bidang tipe deteksi data Sensitif, menggunakan operator pencocokan sama persis, dan tentukan CREDIT\_CARD\_NUMBER sebagai satu-satunya nilai untuk bidang tersebut.

Anda dapat menggunakan operator pencocokan sama persis dengan bidang berikut:

- ID pengidentifikasi data kustom (`customDataIdentifiers.detections.arn`)
- Nama pengidentifikasi data kustom (`customDataIdentifiers.detections.name`)
- Kunci tanda bucket S3 (`resourcesAffected.s3Bucket.tags.key`)
- Nilai tanda bucket S3 (`resourcesAffected.s3Bucket.tags.value`)
- Kunci tanda objek S3 (`resourcesAffected.s3Object.tags.key`)
- Nilai tanda objek S3 (`resourcesAffected.s3Object.tags.value`)
- Tipe deteksi data sensitif (`sensitiveData.detections.type`)
- Kategori data sensitif (`sensitiveData.category`)

Dalam daftar sebelumnya, nama kurung menggunakan notasi titik untuk menunjukkan nama bidang dalam representasi temuan JSON dan API Amazon Macie.

Lebih besar dari (gt)

Lebih besar dari (>) nilai yang ditentukan untuk bidang. Anda dapat menggunakan operator lebih besar dari dengan nomor dan tanggal/nilai waktu.

Misalnya, untuk menyertakan hanya temuan yang melaporkan lebih dari 90 kemunculan data sensitif dalam objek S3, tambahkan syarat yang menggunakan bidang Jumlah total data sensitif dan operator ini, dan tentukan 90 sebagai nilai untuk bidang tersebut. Untuk melakukannya di konsol Amazon Macie, masukkan **91** di kotak Dari, jangan masukkan nilai dalam kotak Untuk, lalu pilih Terapkan. Perbandingan numerik dan berbasis waktu sudah termasuk di konsol tersebut.

Jika Anda menggunakan API Amazon Macie untuk menentukan rentang waktu yang menggunakan operator ini, Anda harus menentukan nilai tanggal/waktu sebagai stempel waktu Unix dalam milidetik—misalnya, 1604616572653 untuk 22:49:32 UTC 5 November 2020.

## Lebih besar dari atau sama dengan (gte)

Lebih besar dari atau sama dengan ( $\geq$ ) nilai yang ditentukan untuk bidang. Anda dapat menggunakan lebih besar dari atau sama dengan operator dengan nilai angka dan tanggal/waktu.

Misalnya, untuk menyertakan hanya temuan yang melaporkan 90 atau lebih kemunculan data sensitif dalam objek S3, tambahkan syarat yang menggunakan bidang Jumlah total data sensitif dan operator ini, serta tentukan 90 sebagai nilai untuk bidang tersebut. Untuk melakukannya di konsol Amazon Macie, masukkan **90** di kotak Dari, jangan masukkan nilai dalam kotak Untuk, lalu pilih Terapkan.

Jika Anda menggunakan API Amazon Macie untuk menentukan rentang waktu yang menggunakan operator ini, Anda harus menentukan nilai tanggal/waktu sebagai stempel waktu Unix dalam milidetik—misalnya, 1604616572653 untuk 22:49:32 UTC 5 November 2020.

## Kurang dari (lt)

Kurang dari ( $<$ ) nilai yang ditentukan untuk bidang. Anda dapat menggunakan operator kurang dari dengan nilai angka dan tanggal/waktu.

Misalnya, untuk menyertakan hanya temuan yang melaporkan kurang dari 90 kemunculan data sensitif dalam objek S3, tambahkan syarat yang menggunakan bidang Jumlah total data sensitif dan operator ini, serta tentukan 90 sebagai nilai untuk bidang tersebut. Untuk melakukan ini pada konsol Amazon Macie, masukkan **89** di kotak Untuk, jangan masukkan nilai dalam kotak Dari, lalu pilih Terapkan. Perbandingan numerik dan berbasis waktu sudah termasuk di konsol tersebut.

Jika Anda menggunakan API Amazon Macie untuk menentukan rentang waktu yang menggunakan operator ini, Anda harus menentukan nilai tanggal/waktu sebagai stempel waktu Unix dalam milidetik—misalnya, 1604616572653 untuk 22:49:32 UTC 5 November 2020.

## Kurang dari atau sama dengan (lte)

Kurang dari atau sama dengan ( $\leq$ ) nilai yang ditentukan untuk bidang. Anda dapat menggunakan Kurang dari atau sama dengan operator dengan nilai angka dan tanggal/waktu.

Misalnya, untuk menyertakan hanya temuan yang melaporkan 90 atau lebih sedikit kemunculan data sensitif dalam objek S3, tambahkan syarat yang menggunakan bidang Jumlah total data sensitif dan operator ini, serta tentukan 90 sebagai nilai untuk bidang tersebut. Untuk melakukan ini pada konsol Amazon Macie, masukkan **90** di kotak Untuk, jangan masukkan nilai dalam kotak Dari, lalu pilih Terapkan.

Jika Anda menggunakan API Amazon Macie untuk menentukan rentang waktu yang menggunakan operator ini, Anda harus menentukan nilai tanggal/waktu sebagai stempel waktu Unix dalam milidetik—misalnya, 1604616572653 untuk 22:49:32 UTC 5 November 2020.

Tidak sama dengan () neq

Tidak cocok (≠) nilai apa pun yang ditentukan untuk bidang. Anda dapat menggunakan operator tidak sama dengan tipe nilai berikut: array teks (string), Boolean, tanggal/waktu, angka, dan teks (string).

Untuk banyak bidang, Anda dapat menggunakan operator ini dan menentukan sebanyak 50 nilai untuk bidang tersebut. Jika Anda melakukan ini, Macie menggunakan logika OR untuk menggabungkan nilai. Ini berarti bahwa temuan cocok dengan kriteria jika tidak memiliki nilai yang ditentukan untuk bidang tersebut.

Misalnya:

- Untuk mengecualikan temuan yang melaporkan kemunculan informasi keuangan, informasi pribadi, atau informasi keuangan dan pribadi, tambahkan syarat yang menggunakan bidang Kategori data sensitif dan operator ini, serta menentukan Informasi keuangan dan Informasi pribadi sebagai nilai untuk bidang tersebut.
- Untuk mengecualikan temuan yang melaporkan kemunculan nomor kartu kredit, tambahkan kondisi untuk bidang Jenis deteksi data sensitif, gunakan operator ini, dan tentukan CREDIT\_CARD\_NUMBER sebagai nilai untuk bidang tersebut.
- Untuk mengecualikan temuan yang melaporkan kemunculan nomor kartu kredit, alamat surat, atau nomor kartu kredit dan alamat surat, tambahkan kondisi untuk bidang Jenis deteksi data sensitif, gunakan operator ini, CREDIT\_CARD\_NUMBER dan tentukan ADDRESS serta sebagai nilai untuk bidang tersebut.

Jika Anda menggunakan API Amazon Macie untuk menentukan syarat yang menggunakan operator ini dengan nilai tanggal/waktu, tentukan nilainya sebagai stempel waktu Unix dalam milidetik—misalnya, 1604616572653 untuk 22:49:32 UTC 5 November 2020.

## Membuat dan menerapkan filter untuk temuan

Untuk mengidentifikasi dan fokus pada temuan yang memiliki karakteristik khusus, Anda dapat memfilter temuan di konsol Amazon Macie dan dalam kueri yang Anda kirimkan secara terprogram menggunakan API Amazon Macie. Saat Anda membuat filter, Anda menggunakan atribut temuan tertentu untuk menentukan kriteria untuk menyertakan atau mengecualikan temuan dari tampilan atau

dari hasil kueri. Temuan atribut adalah bidang yang menyimpan data spesifik untuk temuan, seperti kepelikan, tipe, atau nama bucket S3 bahwa temuan berlaku untuk.

Di Macie, filter terdiri atas satu atau beberapa syarat. Setiap syarat, juga disebut sebagai kriteria, terdiri dari tiga bagian:

- Bidang berbasis atribut, seperti Kepelikan atau Tipe temuan.
- Operator, seperti sama dengan atau tidak sama dengan.
- Satu atau beberapa nilai. Tipe dan jumlah nilai tergantung pada bidang dan operator yang Anda pilih.

Bagaimana Anda menentukan dan menerapkan syarat filter tergantung pada apakah Anda menggunakan konsol Amazon Macie atau API Amazon Macie.

Topik

- [Memfilter temuan pada konsol Amazon Macie](#)
- [Memfilter temuan secara terprogram dengan API Amazon Macie](#)

## Memfilter temuan pada konsol Amazon Macie

Jika Anda menggunakan konsol Amazon Macie untuk memfilter temuan, Macie menyediakan opsi untuk membantu Anda memilih bidang, operator, dan nilai untuk masing-masing syarat. Anda mengakses opsi ini dengan menggunakan pengaturan filter pada halaman Temuan, seperti yang ditunjukkan pada gambar berikut.



Dengan menggunakan menu status Finding, Anda dapat menentukan apakah akan menyertakan temuan yang ditekan (diarsipkan secara otomatis) oleh aturan [penekanan](#). Dengan menggunakan kotak kriteria Filter, Anda dapat memasukkan kondisi filter.

Saat Anda menempatkan kursor di kotak kriteria Filter, Macie menampilkan daftar bidang yang dapat Anda gunakan dalam kondisi filter. Bidang disusun berdasarkan kategori logis. Misalnya, kategori

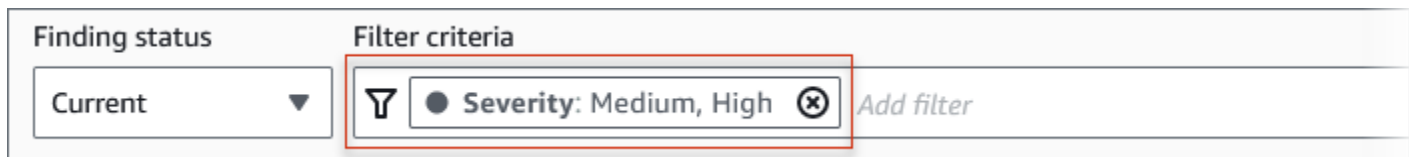


Bidang umum menyertakan bidang yang berlaku untuk semua tipe temuan, dan kategori Bidang klasifikasi menyertakan bidang yang hanya berlaku untuk temuan data sensitif. Bidang diurutkan menurut abjad dalam setiap kategori.

Untuk menambahkan syarat, mulailah dengan memilih bidang dari daftar. Untuk menemukan bidang, jelajahi daftar lengkap, atau memasukkan bagian dari nama bidang untuk mempersempit daftar bidang.

Tergantung pada bidang yang Anda pilih, Macie menampilkan opsi yang berbeda. Opsi mencerminkan tipe dan sifat bidang yang Anda pilih. Misalnya, jika Anda memilih bidang Kepelikan, Macie menampilkan daftar nilai untuk dipilih dari-Rendah,Medium, dan Tinggi. Jika Anda memilih bidang nama bucket S3, Macie menampilkan kotak teks tempat Anda dapat memasukkan nama bucket. Bidang mana pun yang Anda pilih, Macie memandu Anda melalui langkah-langkah untuk menambahkan syarat yang menyertakan pengaturan yang diperlukan untuk bidang tersebut.

Setelah Anda menambahkan kondisi, Macie menerapkan kriteria untuk kondisi dan menambahkan kondisi ke token filter di kotak kriteria Filter, seperti yang ditunjukkan pada gambar berikut.



Dalam contoh ini, syarat dikonfigurasi untuk menyertakan semua temuan dengan kepelikan medium dan tinggi, dan untuk mengecualikan semua temuan dengan kepelikan rendah. Hal ini mengembalikan temuan di mana nilai untuk bidang Kepelikan sama dengan Medium atau Tinggi.

#### Tip

Untuk banyak bidang, Anda dapat mengubah operator kondisi dari sama ke tidak sama dengan dengan memilih ikon sama dengan



di token filter untuk kondisi tersebut. Jika Anda melakukan ini, Macie mengubah operator menjadi tidak sama dan menampilkan ikon tidak sama dengan



di token. Untuk beralih ke operator sama dengan lagi, pilih ikon yang tidak sama.

Saat Anda menambahkan lebih banyak kondisi, Macie menerapkan kriteria mereka dan menambahkannya ke token di kotak kriteria Filter. Anda

dapat merujuk ke kotak kapan saja untuk menentukan kriteria mana yang telah Anda terapkan. Untuk menghapus kondisi, pilih ikon hapus kondisi



di token untuk kondisi tersebut.

Untuk memfilter temuan menggunakan konsol tersebut

1. [Buka konsol Amazon Macie di https://console.aws.amazon.com/macie/.](https://console.aws.amazon.com/macie/)
2. Di panel navigasi, pilih Temuan.
3. (Opsional) Untuk pertama kali melakukan pivot dan meninjau temuan oleh grup logis yang telah ditentukan sebelumnya, pilih Berdasarkan keranjang, Berdasarkan jenis, atau Berdasarkan pekerjaan di panel navigasi (di bawah Temuan). Kemudian pilih item di tabel. Di panel detail, pilih tautan untuk bidang yang akan diputar.
4. (Opsional) Untuk menampilkan temuan yang ditekan oleh [aturan penekanan](#), ubah pengaturan status Filter. Pilih Diarsipkan untuk menampilkan hanya temuan yang ditekan, atau pilih Semua untuk menampilkan temuan yang ditekan dan tidak ditekan. Untuk menyembunyikan temuan yang ditekan, pilih Current.
5. Untuk menambahkan syarat filter:
  - a. Tempatkan kursor Anda di kotak Kriteria filter, lalu pilih bidang yang akan digunakan untuk kondisi tersebut. Untuk informasi tentang bidang yang dapat Anda gunakan, lihat [Bidang untuk memfilter temuan](#).
  - b. Masukkan tipe nilai yang sesuai untuk bidang. Untuk informasi selengkapnya tentang berbagai tipe nilai, lihat [Menentukan nilai untuk bidang](#).

### Array teks (string)

Untuk tipe nilai ini, Macie sering menyediakan daftar nilai untuk dipilih. Jika demikian, pilih setiap nilai yang ingin Anda gunakan dalam syarat.

Jika Macie tidak memberikan daftar nilai, masukkan nilai yang lengkap dan valid untuk bidang tersebut. Untuk menentukan nilai tambahan untuk bidang, pilih Terapkan, lalu tambahkan syarat lain untuk setiap nilai tambahan.

Perhatikan bahwa nilai peka huruf besar dan kecil. Selain itu, Anda tidak dapat menggunakan nilai parsial atau karakter wildcard dalam nilai-nilai. Misalnya, untuk memfilter temuan bucket S3 yang bernama Bucket S3-saya, masukkan **my-S3-bucket**

sebagai nilai untuk bidang nama bucket S3. Jika Anda memasukkan nilai lain, seperti **my-s3-bucket** atau **my-S3**, Macie tidak akan mengembalikan temuan untuk bucket.

## Boolean

Untuk tipe nilai, Macie menyediakan daftar nilai untuk memilih dari. Pilih nilai yang ingin Anda gunakan dalam syarat.

## Tanggal/Waktu (rentang waktu)

Untuk tipe nilai ini, gunakan kotak Dari dan Untuk untuk menentukan rentang waktu inklusif:

- Untuk menentukan rentang waktu tetap, gunakan kotak Dari dan Untuk untuk menentukan tanggal dan waktu pertama serta tanggal dan waktu terakhir dalam rentang tersebut.
- Untuk menentukan rentang waktu relatif yang dimulai pada tanggal dan waktu tertentu dan berakhir pada waktu saat ini, masukkan tanggal dan waktu mulai di kotak Dari, dan menghapus teks apa pun di kotak Untuk.
- Untuk menentukan rentang waktu relatif yang berakhir pada tanggal dan waktu tertentu, masukkan tanggal dan waktu akhir di kotak Untuk, dan menghapus teks apa pun di kotak Dari.

Perhatikan bahwa nilai waktu menggunakan notasi 24 jam. Jika Anda menggunakan pemilih tanggal untuk memilih tanggal, Anda bisa menyaring nilai dengan memasukkan teks secara langsung di kotak Dari dan Untuk.



## Angka (rentang numerik)

Untuk tipe nilai ini, gunakan kotak Dari dan Untuk untuk memasukkan satu atau beberapa bilangan bulat yang menentukan rentang angka inklusif, tetap atau relatif.

## Nilai teks (string)

Untuk tipe nilai ini, masukkan nilai yang lengkap dan valid untuk bidang tersebut.

Perhatikan bahwa nilai peka huruf besar dan kecil. Selain itu, Anda tidak dapat menggunakan nilai parsial atau karakter wildcard dalam nilai-nilai. Misalnya, untuk memfilter temuan bucket S3 yang bernama Bucket S3-saya, masukkan **my-S3-bucket** sebagai nilai untuk bidang nama bucket S3. Jika Anda memasukkan nilai lain, seperti **my-s3-bucket** atau **my-S3**, Macie tidak akan mengembalikan temuan untuk bucket.

- c. Setelah selesai menambahkan nilai untuk bidang, pilih Terapkan. Macie menerapkan kriteria filter dan menambahkan kondisi ke token filter di kotak kriteria Filter.
6. Ulangi langkah 5 untuk setiap syarat tambahan yang ingin Anda tambahkan.
7. Untuk menghapus kondisi, pilih ikon hapus kondisi  di token filter untuk kondisi tersebut.
8. Untuk mengubah kondisi, hapus kondisi dengan memilih ikon hapus kondisi  di token filter untuk kondisi tersebut. Kemudian ulangi langkah 5 untuk menambahkan syarat dengan pengaturan yang benar.

Jika Anda ingin menggunakan set kondisi ini lagi, Anda dapat menyimpan set sebagai aturan filter. Untuk melakukan ini, pilih Simpan aturan di kotak Kriteria filter. Masukkan nama, dan deskripsi secara opsional untuk aturan. Setelah selesai, pilih Simpan.

## Memfilter temuan secara terprogram dengan API Amazon Macie

Untuk memfilter temuan secara terprogram, tentukan kriteria filter dalam kueri yang Anda kirimkan menggunakan [ListFindings](#) atau [GetFindingStatistics](#) pengoperasian Amazon Macie API. `ListFindingsOperasi` mengembalikan array ID pencarian, satu ID untuk setiap temuan yang cocok dengan kriteria filter. `GetFindingStatisticsOperasi` mengembalikan data statistik agregat tentang semua temuan yang cocok dengan kriteria filter, dikelompokkan berdasarkan bidang yang Anda tentukan dalam permintaan Anda.

Perhatikan bahwa `ListFindings` dan `GetFindingStatistics` berbeda dari operasi yang Anda gunakan untuk [menekan temuan](#). Tidak seperti operasi penekanan, yang juga menentukan kriteria filter, operasi `ListFindings` dan `GetFindingStatistics` hanya mengkueri data temuan. Mereka tidak melakukan tindakan apa pun pada temuan yang sesuai dengan kriteria filter. Untuk menekan temuan, gunakan [CreateFindingsFilter](#) pengoperasian Amazon Macie API.

Untuk menentukan kriteria filter dalam kueri, sertakan peta syarat filter dalam permintaan Anda. Untuk setiap syarat, tentukan bidang, operator, dan satu atau beberapa nilai untuk bidang tersebut. Tipe dan jumlah nilai tergantung pada bidang dan operator yang Anda pilih. Untuk informasi tentang bidang, operator, dan tipe nilai yang dapat Anda gunakan dalam syarat, lihat [Bidang untuk memfilter temuan](#), [Menggunakan operator dalam syarat](#), dan [Menentukan nilai untuk bidang](#).

Contoh berikut menunjukkan kepada Anda cara menentukan kriteria filter dalam kueri yang Anda kirimkan menggunakan [AWS Command Line Interface\(AWS CLI\)](#). Anda juga dapat melakukan ini dengan menggunakan versi terbaru dari alat baris AWS perintah lain atau AWS SDK, atau dengan mengirim permintaan HTTPS langsung ke Macie. Untuk informasi tentang alat AWS dan SDK, lihat [Alat untuk Membangun di AWS](#).

#### Contoh

- [Contoh 1: Temuan filter berdasarkan tingkat kepelikan](#)
- [Contoh 2: Temuan filter berdasarkan kategori data sensitif](#)
- [Contoh 3: Temuan filter berdasarkan rentang waktu tetap](#)
- [Contoh 4: Temuan filter berdasarkan status penekanan](#)
- [Contoh 5: Temuan filter berdasarkan beberapa bidang dan tipe nilai](#)

Contoh-contoh menggunakan perintah [daftar temuan](#). Jika sebuah contoh berhasil dijalankan, Macie mengembalikan sebuah array `findingIds`. Array mencantumkan pengenal unik untuk setiap temuan yang cocok dengan kriteria filter, seperti yang ditunjukkan pada contoh berikut.

```
{
  "findingIds": [
    "1f1c2d74db5d8caa76859ec52example",
    "6cfa9ac820dd6d55cad30d851example",
    "702a6fd8750e567d1a3a63138example",
    "826e94e2a820312f9f964cf60example",
    "274511c3fdcd87010a19a3a42example"
  ]
}
```

Jika tidak ada temuan yang cocok dengan kriteria filter, Macie mengembalikan `findingIds` array kosong.

```
{
  "findingIds": []
}
```

#### Contoh 1: Temuan filter berdasarkan tingkat kepelikan

Contoh ini menggunakan perintah [daftar-temuan](#) untuk mengambil ID temuan untuk semua temuan tingkat keparahan tinggi dan tingkat keparahan sedang Anda saat ini. Wilayah AWS

Untuk Linux, macOS, atau Unix:

```
$ aws macie2 list-findings --finding-criteria '{"criterion":{"severity.description":
{"eq":["High","Medium"]}}}'
```

Untuk Microsoft Windows:

```
C:\> aws macie2 list-findings --finding-criteria={"criterion\":
{"severity.description\":{"eq\":["High\","\Medium\"]}}
```

Dengan:

- *kepelikan.description* menentukan nama JSON dari bidang Kepelikan.
- *eq* menentukan operator sama dengan.
- *Tinggi* dan *Medium* adalah array nilai enumerasi untuk bidang Kepelikan.

Contoh 2: Temuan filter berdasarkan kategori data sensitif

Contoh ini menggunakan perintah [daftar-temuan](#) untuk mengambil ID pencarian untuk semua temuan data sensitif Anda yang ada di Wilayah saat ini dan melaporkan kejadian informasi keuangan (dan tidak ada kategori data sensitif lainnya) di objek S3.

Untuk Linux, macOS, atau Unix, menggunakan karakter garis miring terbalik (\) untuk meningkatkan keterbacaan:

```
$ aws macie2 list-findings \
--finding-criteria '{"criterion":
{"classificationDetails.result.sensitiveData.category":{"eqExactMatch":
["FINANCIAL_INFORMATION"]}}}'
```

Untuk Microsoft Windows, menggunakan karakter kelanjutan baris tanda sisipan (^) untuk meningkatkan keterbacaan:

```
C:\> aws macie2 list-findings ^
--finding-criteria={"criterion\":
{"classificationDetails.result.sensitiveData.category\":{"eqExactMatch\":
["FINANCIAL_INFORMATION\"]}}
```

Dengan:

- `classificationDetails.result.sensitiveData.category` menentukan nama JSON dari bidang Kategori data sensitif.
- `eqExactMatch` menentukan sama persis operator pencocokan.
- `FINANCIAL_INFORMATION` adalah nilai enumerasi untuk bidang Kategori data sensitif.

Contoh 3: Temuan filter berdasarkan rentang waktu tetap

Contoh ini menggunakan perintah [daftar temuan](#) untuk mengambil ID temuan untuk semua temuan Anda yang ada di Wilayah saat ini dan dibuat antara pukul 07:00 UTC 5 Oktober 2020, dan 07:00 UTC 5 November 2020 (inklusif).

Untuk Linux, macOS, atau Unix:

```
$ aws macie2 list-findings --finding-criteria '{"criterion":{"createdAt":{"gte":"1601881200000","lte":"1604559600000"}}}'
```

Untuk Microsoft Windows:

```
C:\> aws macie2 list-findings --finding-criteria="{\"criterion\":{\"createdAt\":{\"gte\":\"1601881200000\",\"lte\":\"1604559600000\"}}}"
```

Dengan:

- `createdAt` menentukan nama JSON dari bidang Dibuat di.
- `gte` menentukan operator Lebih besar dari atau sama dengan.
- `1601881200000` adalah tanggal dan waktu pertama (sebagai stempel waktu Unix dalam milidetik) dalam rentang waktu tersebut.
- `lte` menentukan operator kurang dari atau sama dengan.
- `1604559600000` adalah tanggal dan waktu terakhir (sebagai stempel waktu Unix dalam milidetik) dalam rentang waktu tersebut.

Contoh 4: Temuan filter berdasarkan status penekanan

Contoh ini menggunakan perintah [daftar temuan](#) untuk mengambil ID temuan untuk semua temuan Anda yang ada di Wilayah saat ini dan disembunyikan (diarsipkan secara otomatis) oleh aturan penekanan.

Untuk Linux, macOS, atau Unix:

```
$ aws macie2 list-findings --finding-criteria '{"criterion":{"archived":{"eq":["true"]}}}'
```

Untuk Microsoft Windows:

```
C:\> aws macie2 list-findings --finding-criteria="{\"criterion\":{\"archived\":{\"eq\":[\"true\"]}}}"
```

Dengan:

- *Diarsipkan* menentukan nama JSON dari bidang Diarsipkan.
- *eq* menentukan operator sama dengan.
- *benar* adalah nilai Boolean untuk bidang Diarsipkan.

Contoh 5: Temuan filter berdasarkan beberapa bidang dan tipe nilai

Contoh ini menggunakan perintah [daftar-temuan](#) untuk mengambil ID pencarian untuk semua temuan data sensitif Anda yang ada di Wilayah saat ini dan cocok dengan kriteria berikut: dibuat antara 07:00 UTC 5 Oktober 2020, dan 07:00 UTC 5 November 2020 (secara eksklusif); melaporkan kemunculan data keuangan dan tidak ada kategori data sensitif lainnya di objek S3; dan tidak ditekan (diarsipkan secara otomatis) oleh aturan penekanan.

Untuk Linux, macOS, atau Unix, menggunakan karakter garis miring terbalik (\) untuk meningkatkan keterbacaan:

```
$ aws macie2 list-findings \
--finding-criteria '{"criterion":{"createdAt":
{"gt":"1601881200000","lt":"1604559600000"},"classificationDetails.result.sensitiveData.category":
{"eqExactMatch":["FINANCIAL_INFORMATION"]},"archived":{"eq":["false"]}}}'
```

Untuk Microsoft Windows, menggunakan karakter kelanjutan baris tanda sisipan (^) untuk meningkatkan keterbacaan:

```
C:\> aws macie2 list-findings ^
--finding-criteria="{\"criterion\":{\"createdAt\":{\"gt\":1601881200000,
\"lt\":1604559600000},\"classificationDetails.result.sensitiveData.category\":
{\"eqExactMatch\":[\"FINANCIAL_INFORMATION\"]},\"archived\":{\"eq\":[\"false\"]}}}"
```

Dengan:



- *CreatedAt* menentukan nama JSON dari bidang Dibuat di, dan:
  - *gte* menentukan operator lebih besar dari atau sama dengan.
  - *1601881200000* adalah tanggal dan waktu pertama (sebagai stempel waktu Unix dalam milidetik) dalam rentang waktu tersebut.
  - *lt* menentukan operator kurang dari atau sama dengan.
  - *1604559600000* adalah tanggal dan waktu terakhir (sebagai stempel waktu Unix dalam milidetik) dalam rentang waktu tersebut.
- *classificationDetails.result.sensitiveData.category* menentukan nama JSON dari bidang Kategori data sensitif, dan:
  - *eqExactMatch* menentukan sama persis operator pencocokan.
  - *FINANCIAL\_INFORMATION* adalah nilai enumerasi untuk bidang.
- *Diarsipkan* menentukan nama JSON dari bidang Diarsipkan, dan:
  - *eq* menentukan operator sama dengan.
  - *salah* adalah nilai Boolean untuk bidang.

## Membuat dan mengelola aturan filter untuk temuan

Aturan filter adalah serangkaian kriteria filter yang Anda buat dan simpan untuk digunakan kembali saat Anda meninjau temuan di konsol Amazon Macie. Aturan filter dapat membantu Anda melakukan analisis temuan yang konsisten yang memiliki karakteristik tertentu. Misalnya, Anda mungkin membuat satu aturan filter untuk menganalisis semua temuan kebijakan kepelikan tinggi untuk bucket S3 yang berisi objek tidak terenkripsi, dan aturan filter lain untuk menganalisis semua temuan data sensitif kepelikan tinggi yang melaporkan tipe data sensitif tertentu.

Perhatikan bahwa aturan filter berbeda dari aturan penekanan. Aturan penekanan adalah serangkaian kriteria filter yang Anda buat dan simpan untuk mengarsipkan temuan secara otomatis yang sesuai dengan kriteria aturan. Meskipun kedua jenis aturan menyimpan dan menerapkan kriteria filter, aturan filter tidak melakukan tindakan apa pun pada temuan yang sesuai dengan kriteria aturan. Sebaliknya, aturan filter hanya menentukan temuan yang muncul di konsol tersebut setelah Anda menerapkan aturan. Untuk informasi selengkapnya tentang aturan penekanan, lihat [Menekan temuan](#).

Untuk membuat dan mengelola aturan filter, Anda dapat menggunakan konsol Amazon Macie atau API Amazon Macie. Topik berikut menjelaskan caranya. Untuk API, topiknya mencakup contoh cara melakukan tugas ini dengan menggunakan [AWS Command Line Interface\(AWS CLI\)](#). Anda juga

dapat melakukan tugas-tugas ini dengan menggunakan versi terbaru dari alat baris AWS perintah lain atau AWS SDK, atau dengan mengirim permintaan HTTPS langsung ke Macie. Untuk informasi tentang alat AWS dan SDK, lihat [Alat untuk Membangun di AWS](#).

## Topik

- [Membuat aturan filter](#)
- [Menerapkan aturan filter](#)
- [Mengubah aturan filter](#)
- [Menghapus aturan filter](#)

## Membuat aturan filter

Saat Anda membuat aturan filter, Anda menentukan kriteria filter, nama, dan, secara opsional, deskripsi aturan. Anda dapat membuat aturan filter dengan menggunakan konsol Amazon Macie atau Amazon Macie API.

### Console

Ikuti langkah-langkah ini untuk membuat aturan filter menggunakan konsol Amazon Macie.

Untuk membuat aturan filter

1. [Buka konsol Amazon Macie di https://console.aws.amazon.com/macie/](https://console.aws.amazon.com/macie/).
2. Di panel navigasi, pilih Temuan.

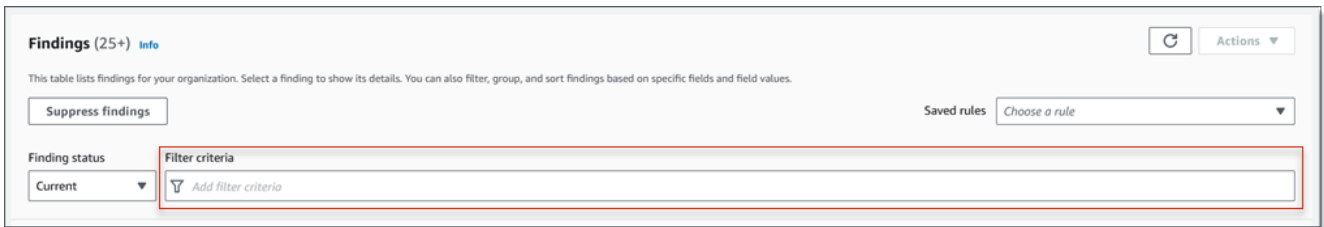
#### Tip

Untuk menggunakan aturan filter yang ada sebagai titik awal, pilih aturan dari daftar Aturan tersimpan.

Anda juga dapat merampingkan pembuatan aturan dengan terlebih dahulu memutar dan menelusuri temuan oleh grup logis yang telah ditentukan sebelumnya. Jika Anda melakukan ini, Macie secara otomatis membuat dan menerapkan syarat filter yang sesuai, yang dapat menjadi titik awal yang berguna untuk membuat aturan.

Untuk melakukan ini, pilih Menurut bucket, Menurut tipe, atau Menurut tugas di panel navigasi (di bawah Temuan), lalu pilih item dalam tabel. Di panel detail, pilih tautan untuk bidang yang akan dialihkan.

3. Dalam kotak kriteria Filter, tambahkan kondisi yang menentukan kriteria filter untuk aturan.



Untuk mempelajari cara menambahkan syarat filter, lihat [Membuat dan menerapkan filter untuk temuan](#).

4. Ketika Anda selesai menentukan kriteria filter untuk aturan, pilih Simpan aturan di kotak Kriteria filter.



5. Di bawah Aturan filter, masukkan nama dan, secara opsional, deskripsi aturan.
6. Pilih Save (Simpan).

## API

Untuk membuat aturan filter secara terprogram, gunakan [CreateFindingsFilter](#) pengoperasian Amazon Macie API dan tentukan nilai yang sesuai untuk parameter yang diperlukan:

- Untuk `action` parameter, tentukan N00P untuk memastikan bahwa Macie tidak menekan (secara otomatis mengarsipkan) temuan yang cocok dengan kriteria aturan.
- Untuk parameter `criterion`, tentukan pemetaan syarat yang menentukan kriteria filter untuk aturan.

Di peta, setiap syarat harus menentukan bidang, operator, dan satu atau beberapa nilai untuk bidang tersebut. Tipe dan jumlah nilai tergantung pada bidang dan operator yang Anda pilih. Untuk informasi tentang bidang, operator, dan tipe nilai yang dapat Anda gunakan dalam syarat, lihat [Bidang untuk memfilter temuan](#), [Menggunakan operator dalam syarat](#), dan [Menentukan nilai untuk bidang](#).

Untuk membuat aturan filter dengan menggunakan AWS CLI, jalankan [create-findings-filter](#) perintah dan tentukan nilai yang sesuai untuk parameter yang diperlukan. Contoh berikut

membuat aturan filter yang mengembalikan semua temuan data sensitif yang ada saat ini Wilayah AWS dan melaporkan kejadian informasi pribadi (dan tidak ada kategori data sensitif lainnya) di objek S3.

Contoh ini diformat untuk Linux, macOS, atau Unix, dan menggunakan karakter garis miring terbalik (\) untuk meningkatkan keterbacaan.

```
$ aws macie2 create-findings-filter \  
--action NOOP \  
--name my_filter_rule \  
--finding-criteria '{"criterion":  
{"classificationDetails.result.sensitiveData.category":{"eqExactMatch":  
["PERSONAL_INFORMATION"]}}}'
```

Contoh ini diformat untuk Microsoft Windows dan menggunakan karakter kelanjutan baris tanda sisipan (^) untuk meningkatkan keterbacaan.

```
C:\> aws macie2 create-findings-filter ^  
--action NOOP ^  
--name my_filter_rule ^  
--finding-criteria={"criterion\  
{\"classificationDetails.result.sensitiveData.category"\:{"\eqExactMatch\":  
[\"PERSONAL_INFORMATION"]}}
```

Dengan:

- *my\_filter\_rule* adalah nama khusus untuk aturan.
- *criterion* adalah pemetaan syarat filter untuk aturan:
  - *classificationDetails.result.sensitiveData.category* adalah nama JSON dari bidang Kategori data sensitif.
  - *eqExactMatch* menentukan sama persis operator kecocokan.
  - *PERSONAL\_INFORMATION* adalah nilai enumerasi untuk bidang Kategori data sensitif.

Jika perintah berjalan dengan berhasil, Anda menerima output yang mirip dengan berikut ini.

```
{  
  "arn": "arn:aws:macie2:us-west-2:123456789012:findings-filter/9b2b4508-  
aa2f-4940-b347-d1451example",  
  "id": "9b2b4508-aa2f-4940-b347-d1451example"
```

```
}
```

Di mana `arn` adalah Amazon Resource Name (ARN) dari aturan filter yang dibuat, dan `id` adalah pengenal unik untuk aturan.

Untuk contoh penambahan kriteria filter, lihat [Memfilter temuan secara terprogram dengan API Amazon Macie](#).

## Menerapkan aturan filter

Saat Anda menerapkan aturan filter, Amazon Macie menggunakan kriteria aturan untuk menentukan temuan mana yang akan disertakan atau dikecualikan dari tampilan temuan Anda di konsol. Macie juga menampilkan kriteria untuk membantu Anda menentukan kriteria yang Anda terapkan.

Perhatikan bahwa aturan filter dirancang untuk digunakan dengan konsol Amazon Macie. Anda tidak dapat menggunakannya secara langsung dalam kueri yang Anda kirimkan secara terprogram menggunakan API Amazon Macie. Namun, jika Anda menggunakan API untuk menanyakan temuan, Anda dapat mengambil kriteria filter untuk aturan dengan menggunakan [GetFindingsFilter](#) operasi. Anda kemudian dapat menambahkan kriteria ke kueri Anda. Untuk informasi tentang menentukan kriteria filter dalam kueri, lihat [Membuat dan menerapkan filter untuk temuan](#).

Ikuti langkah-langkah ini untuk memfilter temuan di konsol tersebut dengan menerapkan aturan filter.

Untuk menerapkan aturan filter

1. [Buka konsol Amazon Macie di https://console.aws.amazon.com/macie/](https://console.aws.amazon.com/macie/).
2. Di panel navigasi, pilih Temuan.
3. Di daftar Aturan tersimpan, pilih aturan filter yang ingin Anda terapkan. Macie menerapkan kriteria aturan dan menampilkan kriteria di kotak kriteria Filter.
4. (Opsional) Untuk menyempurnakan kriteria, gunakan kotak Kriteria filter untuk menambah atau menghapus kondisi filter. Jika Anda melakukannya, perubahan tidak akan memengaruhi pengaturan aturan. Macie tidak akan menyimpan perubahan Anda kecuali Anda secara eksplisit menyimpannya sebagai aturan baru.
5. Untuk menerapkan aturan filter yang berbeda, ulangi langkah 3.

Setelah Anda menerapkan aturan filter, Anda dapat dengan cepat menghapus semua kriteria filter dari tampilan Anda dengan memilih X di kotak kriteria Filter.

## Mengubah aturan filter


Anda dapat mengubah pengaturan untuk aturan filter kapan saja dengan menggunakan konsol Amazon Macie atau Amazon Macie API. Anda juga dapat menetapkan dan mengelola tag untuk aturan tersebut.

Tag adalah label yang Anda tentukan dan tetapkan ke jenis AWS sumber daya tertentu. Setiap tanda terdiri dari kunci tanda yang diperlukan dan nilai tanda opsional. Tag dapat membantu Anda mengidentifikasi, mengkategorikan, dan mengelola sumber daya dengan cara yang berbeda, seperti berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Untuk mempelajari selengkapnya, lihat [Menandai sumber daya Amazon Macie](#).

### Console

Ikuti langkah-langkah ini untuk mengubah pengaturan pada aturan filter yang sudah ada menggunakan konsol Amazon Macie.

Untuk mengubah aturan filter

1. [Buka konsol Amazon Macie di https://console.aws.amazon.com/macie/](https://console.aws.amazon.com/macie/).
2. Di panel navigasi, pilih Temuan.
3. Di daftar Aturan tersimpan, pilih ikon edit  di samping aturan filter yang ingin Anda ubah.
4. Lakukan langkah-langkah berikut:
  - Untuk mengubah kriteria filter aturan, gunakan kotak kriteria Filter untuk memasukkan kondisi untuk kriteria yang Anda inginkan. Untuk mempelajari caranya, lihat [Membuat dan menerapkan filter untuk temuan](#).
  - Untuk mengubah nama aturan, masukkan nama baru di kotak Nama di bawah Aturan filter.
  - Untuk mengubah deskripsi aturan, masukkan deskripsi baru di kotak Deskripsi di bawah Aturan filter.
  - Untuk menetapkan, meninjau, atau mengedit tag untuk aturan, pilih Kelola tag di bawah Aturan filter. Kemudian tinjau dan ubah tag seperlunya. Aturan dapat memiliki sebanyak 50 tag.
5. Setelah selesai membuat perubahan, pilih Simpan.

## API

Untuk mengubah aturan filter secara terprogram, gunakan [UpdateFindingsFilter](#) pengoperasian Amazon Macie API. Saat Anda mengirimkan permintaan, gunakan parameter yang didukung untuk menentukan nilai baru untuk setiap setelan yang ingin Anda ubah.

Untuk parameter `id`, tentukan pengidentifikasi unik untuk aturan yang akan Anda ubah. Anda bisa mendapatkan pengenalan ini dengan menggunakan [ListFindingsFilter](#) operasi untuk mengambil daftar aturan filter dan penekanan untuk akun Anda. Jika Anda menggunakan AWS CLI, jalankan [list-findings-filters](#) perintah untuk mengambil daftar ini.

Untuk mengubah aturan filter dengan menggunakan AWS CLI, jalankan [update-findings-filter](#) perintah dan gunakan parameter yang didukung untuk menentukan nilai baru untuk setiap pengaturan yang ingin Anda ubah. Misalnya, perintah berikut mengubah nama aturan filter yang ada.

```
C:\> aws macie2 update-findings-filter --id 9b2b4508-aa2f-4940-b347-d1451example --name personal_information_only
```

Dengan:

- *9b2b4508-aa2f-4940-b347-d1451example* adalah pengenalan unik untuk aturan.
- *personal\_information\_only* adalah nama baru untuk aturan.

Jika perintah berjalan dengan berhasil, Anda menerima output yang mirip dengan berikut ini.

```
{
  "arn": "arn:aws:macie2:us-west-2:123456789012:findings-filter/9b2b4508-aa2f-4940-b347-d1451example",
  "id": "9b2b4508-aa2f-4940-b347-d1451example"
}
```

Di mana `arn` adalah Amazon Resource Name (ARN) aturan yang diubah, dan `id` adalah pengenalan unik untuk aturan.

Demikian pula, contoh berikut mengonversi aturan filter untuk aturan penekanan dengan mengubah nilai untuk parameter `action` dari `ARCHIVE` ke `NOOP`.

```
C:\> aws macie2 update-findings-filter --id 8a1c3508-aa2f-4940-b347-d1451example --  
action NOOP
```

Dengan:

- **8a1c3508-aa2f-4940-b347-d1451example** adalah pengenal unik untuk aturan.
- **NOOP** adalah tindakan baru yang dilakukan Macie pada temuan yang sesuai dengan kriteria aturan—tidak melakukan tindakan (jangan menekan temuan).

Jika perintah berhasil dijalankan, Anda menerima output yang mirip dengan berikut ini:

```
{  
  "arn": "arn:aws:macie2:us-west-2:123456789012:findings-filter/8a1c3508-  
aa2f-4940-b347-d1451example",  
  "id": "8a1c3508-aa2f-4940-b347-d1451example"  
}
```

Di mana `arn` adalah Amazon Resource Name (ARN) aturan yang diubah, dan `id` adalah pengenal unik untuk aturan.


## Menghapus aturan filter

Anda dapat menghapus aturan filter kapan saja dengan menggunakan konsol Amazon Macie atau Amazon Macie API.

### Console

Ikuti langkah-langkah ini untuk menghapus aturan filter menggunakan konsol Amazon Macie.

Untuk menghapus aturan filter

1. [Buka konsol Amazon Macie di https://console.aws.amazon.com/macie/](https://console.aws.amazon.com/macie/).
2. Di panel navigasi, pilih Temuan.
3. Di daftarAturan tersimpan, pilih ikon edit  
()  
di samping aturan filter yang ingin Anda hapus.
4. Di bawah Aturan filter pilih Hapus.



## API

Untuk menghapus aturan filter secara terprogram, gunakan [DeleteFindingsFilter](#) pengoperasian Amazon Macie API. Untuk parameter `id`, tentukan pengidentifikasi unik untuk aturan filter yang akan Anda hapus. Anda bisa mendapatkan pengenalan ini dengan menggunakan [ListFindingsFilter](#) operasi untuk mengambil daftar aturan filter dan penekanan untuk akun Anda. Jika Anda menggunakan AWS CLI, jalankan [list-findings-filters](#) perintah untuk mengambil daftar ini.

Untuk menghapus aturan filter dengan menggunakan AWS CLI, jalankan [delete-findings-filter](#) perintah. Misalnya:

```
C:\> aws macie2 delete-findings-filter --id 9b2b4508-aa2f-4940-b347-d1451example
```

Di mana *9b2b4508-aa2f-4940-b347-d1451example* adalah pengidentifikasi unik untuk aturan filter yang akan dihapus.

Jika perintah berhasil dijalankan, Macie mengembalikan respons HTTP 200 kosong. Jika tidak, Macie mengembalikan HTTP 4xx atau respons 500 yang menunjukkan alasan operasi gagal.

## Bidang untuk memfilter temuan

Untuk membantu Anda menganalisis temuan dengan lebih efisien, konsol Amazon Macie dan API Amazon Macie menyediakan akses ke beberapa set bidang untuk memfilter temuan:

- Bidang umum— Bidang ini menyimpan data yang berlaku untuk semua tipe temuan. Mereka berkaitan dengan atribut temuan umum seperti kepelikan, tipe temuan, dan ID temuan.
- Bidang sumber daya yang terpengaruh — Bidang ini menyimpan data tentang sumber daya yang diterapkan oleh temuan, seperti nama, tag, dan pengaturan enkripsi untuk bucket atau objek S3 yang terpengaruh.
- Bidang kebijakan— Bidang ini menyimpan data yang spesifik untuk temuan kebijakan, seperti tindakan yang menghasilkan temuan, dan entitas yang melakukan tindakan.
- Bidang klasifikasi data sensitif — Bidang ini menyimpan data yang spesifik untuk temuan data sensitif, seperti kategori dan jenis data sensitif yang ditemukan Macie di objek S3 yang terpengaruh.

Filter dapat menggunakan bidang kombinasi dari salah satu set sebelumnya.

Topik di bagian ini mencantumkan dan menjelaskan masing-masing bidang yang dapat Anda gunakan untuk memfilter temuan. Untuk detail tambahan tentang bidang ini, termasuk hubungan apa pun di antara bidang, lihat [Temuan di Referensi](#) API Amazon Macie.

## Topik

- [Bidang umum](#)
- [Bidang sumber daya terpengaruh](#)
- [Bidang kebijakan](#)
- [Bidang klasifikasi data sensitif](#)

## Bidang umum

Tabel berikut mencantumkan dan menjelaskan bidang yang dapat Anda gunakan untuk memfilter temuan berdasarkan atribut temuan umum. Bidang ini menyimpan data yang berlaku untuk semua tipe temuan.

Pada tabel, kolom Bidang menunjukkan nama bidang pada konsol Amazon Macie. Kolom Bidang JSON menggunakan notasi titik untuk menunjukkan nama bidang dalam temuan representasi JSON dan API Amazon Macie. Kolom Deskripsi menyediakan deskripsi singkat dari data yang disimpan bidang, dan menunjukkan persyaratan untuk nilai filter. Tabel diurutkan dalam urutan abjad berdasarkan bidang, dan kemudian berdasarkan bidang JSON.

Bidang	Bidang JSON	Deskripsi
ID Akun	accountId	Pengidentifikasi unik untuk Akun AWS yang diterapkan oleh temuan tersebut. Hal ini biasanya akun yang memiliki sumber daya yang terpengaruh.
—	archived	Nilai Boolean yang menentukan apakah temuan ditekan (diarsipkan secara otomatis) oleh aturan penekanan.

Bidang	Bidang JSON	Deskripsi
		<p>Untuk menggunakan bidang ini dalam filter di konsol, pilih opsi pada menu Status pencarian: Diarsipkan (hanya ditekan), Saat ini (hanya tidak ditekan), atau Semua (keduanya ditekan dan tidak ditekan).</p>
Kategori	category	<p>Kategori temuan.</p> <p>Konsol tersebut menyediakan daftar nilai untuk memilih dari saat Anda menambahkan bidang ini ke filter. Dalam API, nilai yang valid adalah: CLASSIFICATION , untuk temuan data sensitif; dan, POLICY, untuk temuan kebijakan.</p>
—	count	<p>Jumlah total kemunculan temuan. Untuk temuan data sensitif, nilai ini selalu 1. Semua temuan data sensitif dianggap unik.</p> <p>Bidang ini tidak tersedia sebagai opsi filter pada konsol tersebut. Dengan API, Anda dapat menggunakan bidang ini untuk menentukan rentang numerik untuk filter.</p>

Bidang	Bidang JSON	Deskripsi
Dibuat di	<code>createdAt</code>	<p>Tanggal dan waktu ketika Macie menciptakan temuan.</p> <p>Anda dapat menggunakan bidang ini untuk menentukan rentang waktu untuk filter.</p>
ID Temuan	<code>id</code>	<p>Pengenal unik untuk temuan. Ini adalah string acak yang dihasilkan dan ditetapkan Macie ke sebuah temuan saat membuat temuan tersebut.</p>
Tipe temuan*	<code>type</code>	<p>Tipe temuan-misalnya, <code>SensitiveData:S3object/Personal</code> atau <code>Policy:IAMUser/S3BucketPublic</code>.</p> <p>Konsol tersebut menyediakan daftar nilai untuk memilih dari saat Anda menambahkan bidang ini ke filter. Untuk daftar nilai yang valid di API, lihat <a href="#">FindingType</a> di Referensi API Amazon Macie.</p>
Wilayah	<code>region</code>	<p>Temuan Wilayah AWS yang Macie ciptakan dalam—misalnya, <code>us-east-1</code> atau <code>ca-central-1</code>.</p>

Bidang	Bidang JSON	Deskripsi
Sampel	<code>sample</code>	<p>Nilai Boolean yang menentukan apakah temuan tersebut adalah temuan sampel. Temuan sampel adalah temuan yang menggunakan contoh data dan nilai placeholder untuk menunjukkan apa yang mungkin terkandung dalam temuan.</p> <p>Konsol tersebut menyediakan daftar nilai untuk memilih dari saat Anda menambahkan bidang ini ke filter.</p>
Kepelikan	<code>severity.description</code>	<p>Representasi kualitatif dari kepelikan temuan ini.</p> <p>Konsol tersebut menyediakan daftar nilai untuk memilih dari saat Anda menambahkan bidang ini ke filter. Di API, nilai yang valid adalah: Low, Medium, dan High.</p>
Diperbarui pada	<code>updatedAt</code>	<p>Tanggal dan waktu saat temuan terakhir diperbarui. Untuk temuan data sensitif, nilai ini sama dengan nilai untuk bidang Dibuat di. Semua temuan data sensitif dianggap baru (unik).</p> <p>Anda dapat menggunakan bidang ini untuk menentukan rentang waktu untuk filter.</p>

\* Untuk menentukan beberapa nilai untuk bidang ini pada konsol tersebut, tambahkan syarat yang menggunakan bidang dan tentukan nilai yang berbeda untuk filter, lalu ulangi langkah itu untuk setiap nilai tambahan. Untuk melakukan ini dengan API, gunakan array yang mencantumkan nilai yang akan digunakan untuk filter.

## Bidang sumber daya terpengaruh

Topik berikut mencantumkan dan menjelaskan bidang yang dapat Anda gunakan untuk memfilter temuan berdasarkan sumber daya tempat temuan diterapkan. Topik diatur berdasarkan tipe sumber daya.

### Topik

- [Bucket S3](#)
- [Objek S3](#)

### Bucket S3

Tabel berikut mencantumkan dan menjelaskan bidang yang dapat Anda gunakan untuk memfilter temuan berdasarkan karakteristik bucket S3 tempat temuan diterapkan.

Pada tabel, kolom Bidang menunjukkan nama bidang pada konsol Amazon Macie. Kolom Bidang JSON menggunakan notasi titik untuk menunjukkan nama bidang dalam temuan representasi JSON dan API Amazon Macie. (Nama bidang JSON yang lebih panjang menggunakan urutan karakter baris baru (\n) untuk meningkatkan keterbacaan.) Kolom Deskripsi menyediakan deskripsi singkat dari data yang disimpan bidang, dan menunjukkan persyaratan untuk nilai filter. Tabel diurutkan dalam urutan abjad berdasarkan bidang, dan kemudian berdasarkan bidang JSON.

Bidang	Bidang JSON	Deskripsi
—	<code>resourcesAffected.s3Bucket.createdAt</code>	<p>Tanggal dan waktu saat bucket yang terpengaruh dibuat, atau perubahan seperti pengeditan kebijakan bucket baru-baru ini dilakukan pada bucket yang terpengaruh.</p> <p>Bidang ini tidak tersedia sebagai opsi filter pada konsol</p>

Bidang	Bidang JSON	Deskripsi
		tersebut. Dengan API, Anda dapat menggunakan bidang ini untuk menentukan rentang waktu untuk filter.
Enkripsi default untuk bucket S3	<code>resourcesAffected.s3Bucket.defaultServerSideEncryption.encryptionType</code>	<p>Algoritma enkripsi sisi server yang digunakan secara default untuk mengenkripsi objek yang ditambahkan ke bucket yang terpengaruh.</p> <p>Konsol tersebut menyediakan daftar nilai untuk memilih dari saat Anda menambahkan bidang ini ke filter. Untuk daftar nilai yang valid untuk API, lihat <a href="#">EncryptionType</a> di Referensi API Amazon Macie.</p>
Enkripsi ember S3 ID kunci KMS*	<code>resourcesAffected.s3Bucket.defaultServerSideEncryption.kmsMasterKeyId</code>	Nama Sumber Daya Amazon (ARN) atau pengenal unik (ID kunci) untuk AWS KMS key yang digunakan secara default untuk mengenkripsi objek yang ditambahkan ke bucket yang terpengaruh.

Bidang	Bidang JSON	Deskripsi
Enkripsi bucket S3 diperlukan oleh kebijakan bucket	<code>resourcesAffected.s3Bucket.allowsUnencryptedObjectUploads</code>	<p>Menentukan apakah kebijakan bucket untuk bucket yang terpengaruh memerlukan enkripsi objek di sisi server saat objek ditambahkan ke bucket.</p> <p>Konsol tersebut menyediakan daftar nilai untuk memilih dari saat Anda menambahkan bidang ini ke filter. Untuk daftar nilai yang valid untuk API, lihat <a href="#">S3Bucket</a> di Referensi API Amazon Macie.</p>
Nama bucket S3.	<code>resourcesAffected.s3Bucket.name</code>	Nama lengkap ember yang terkena dampak.
Nama tampilan pemilik bucket S3	<code>resourcesAffected.s3Bucket.owner.displayName</code>	Nama tampilan pengguna AWS yang memiliki bucket yang terpengaruh.



Bidang	Bidang JSON	Deskripsi
Izin akses publik bucket S3	<pre>resourcesAffected. s3Bucket.publicAcc ess.effectivePermi ssion</pre>	<p>Menentukan apakah bucket yang terpengaruh dapat diakses secara publik berdasarkan kombinasi pengaturan izin yang berlaku untuk bucket.</p> <p>Konsol tersebut menyediakan daftar nilai untuk memilih dari saat Anda menambahkan bidang ini ke filter. Untuk daftar nilai yang valid untuk API, lihat <a href="#">BucketPublicAccess</a> di Referensi API Amazon Macie.</p>
—	<pre>resourcesAffected. s3Bucket.publicAcc ess.permissionConf iguration.\n accountLevelPermis sions.blockPublicA ccess.blockPublicA cls</pre>	<p>Nilai Boolean yang menentukan apakah Amazon S3 memblokir daftar kontrol akses (ACL) publik untuk bucket yang terpengaruh dan objek dalam bucket. Ini adalah pengaturan akses publik blokir tingkat akun untuk bucket.</p> <p>Bidang ini tidak tersedia sebagai opsi filter pada konsol tersebut.</p>

Bidang	Bidang JSON	Deskripsi
—	<pre>resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n accountLevelPermissions.blockPublicAccess.blockPublicPolicy</pre>	<p>Nilai Boolean yang menentukan apakah Amazon S3 memblokir kebijakan bucket publik untuk bucket yang terpengaruh. Ini adalah pengaturan akses publik blokir tingkat akun untuk bucket.</p> <p>Bidang ini tidak tersedia sebagai opsi filter pada konsol tersebut.</p>
—	<pre>resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n accountLevelPermissions.blockPublicAccess.ignorePublicAcls</pre>	<p>Nilai Boolean yang menentukan apakah Amazon S3 mengabaikan ACL publik untuk bucket yang terpengaruh dan objek dalam bucket. Ini adalah pengaturan akses publik blokir tingkat akun untuk bucket.</p> <p>Bidang ini tidak tersedia sebagai opsi filter pada konsol tersebut.</p>
—	<pre>resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n accountLevelPermissions.blockPublicAccess.restrictPublicBuckets</pre>	<p>Nilai Boolean yang menentukan apakah Amazon S3 membatasi kebijakan bucket publik untuk bucket yang terpengaruh. Ini adalah pengaturan akses publik blokir tingkat akun untuk bucket.</p> <p>Bidang ini tidak tersedia sebagai opsi filter pada konsol tersebut.</p>

Bidang	Bidang JSON	Deskripsi
—	<pre>resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n bucketLevelPermissions.accessControlList.allowsPublicReadAccess</pre>	<p>Nilai Boolean yang menentukan apakah ACL level bucket untuk bucket yang terpengaruh memberikan izin akses baca untuk bucket kepada publik umum.</p> <p>Bidang ini tidak tersedia sebagai opsi filter pada konsol tersebut.</p>
—	<pre>resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n bucketLevelPermissions.accessControlList.allowsPublicWriteAccess</pre>	<p>Nilai Boolean yang menentukan apakah ACL level bucket untuk bucket yang terpengaruh memberikan izin akses tulis kepada publik umum untuk bucket.</p> <p>Bidang ini tidak tersedia sebagai opsi filter pada konsol tersebut.</p>
—	<pre>resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n bucketLevelPermissions.blockPublicAccess.blockPublicAccess</pre>	<p>Nilai Boolean yang menentukan apakah Amazon S3 memblokir ACL publik untuk bucket yang terpengaruh dan objek dalam bucket. Ini adalah setelan akses publik blokir level bucket untuk bucket.</p> <p>Bidang ini tidak tersedia sebagai opsi filter pada konsol tersebut.</p>

Bidang	Bidang JSON	Deskripsi
—	<pre>resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n bucketLevelPermissions.blockPublicAccess.blockPublicPolicy</pre>	<p>Nilai Boolean yang menentukan apakah Amazon S3 memblokir kebijakan bucket publik untuk bucket yang terpengaruh. Ini adalah pengaturan akses publik blok tingkat bucket untuk bucket.</p> <p>Bidang ini tidak tersedia sebagai opsi filter pada konsol tersebut.</p>
—	<pre>resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n bucketLevelPermissions.blockPublicAccess.ignorePublicAcls</pre>	<p>Nilai Boolean yang menentukan apakah Amazon S3 mengabaikan ACL publik untuk bucket yang terpengaruh dan objek dalam bucket. Ini adalah pengaturan akses publik blok tingkat bucket untuk bucket.</p> <p>Bidang ini tidak tersedia sebagai opsi filter pada konsol tersebut.</p>
—	<pre>resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n bucketLevelPermissions.blockPublicAccess.restrictPublicBuckets</pre>	<p>Nilai Boolean yang menentukan apakah Amazon S3 membatasi kebijakan bucket publik untuk bucket yang terpengaruh. Ini adalah pengaturan akses publik blok tingkat bucket untuk bucket.</p> <p>Bidang ini tidak tersedia sebagai opsi filter pada konsol tersebut.</p>

Bidang	Bidang JSON	Deskripsi
—	<code>resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n</code> <code>bucketLevelPermissions.bucketPolicy.allowsPublicReadAccess</code>	Nilai Boolean yang menentukan apakah kebijakan bucket yang terpengaruh memungkinkan publik umum memiliki akses baca ke bucket.  Bidang ini tidak tersedia sebagai opsi filter pada konsol tersebut.
—	<code>resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n</code> <code>bucketLevelPermissions.bucketPolicy.allowsPublicWriteAccess</code>	Nilai Boolean yang menentukan apakah kebijakan bucket yang terpengaruh memungkinkan publik umum memiliki akses tulis ke bucket.  Bidang ini tidak tersedia sebagai opsi filter pada konsol tersebut.
Kunci tanda bucket S3	<code>resourcesAffected.s3Bucket.tags.key</code>	Kunci tanda yang terkait dengan bucket yang terpengaruh.
Nilai tanda bucket S3	<code>resourcesAffected.s3Bucket.tags.value</code>	nilai tanda yang terkait dengan bucket yang terpengaruh.

\* Untuk menentukan beberapa nilai untuk bidang ini pada konsol tersebut, tambahkan syarat yang menggunakan bidang dan tentukan nilai yang berbeda untuk filter, lalu ulangi langkah itu untuk setiap nilai tambahan. Untuk melakukan ini dengan API, gunakan array yang mencantumkan nilai yang akan digunakan untuk filter.

## Objek S3

Tabel berikut ini mencantumkan dan menjelaskan bidang yang dapat Anda gunakan untuk memfilter temuan berdasarkan karakteristik objek S3 tempat temuan diterapkan.

Pada tabel, kolom Bidang menunjukkan nama bidang pada konsol Amazon Macie. Kolom Bidang JSON menggunakan notasi titik untuk menunjukkan nama bidang dalam temuan representasi JSON dan API Amazon Macie. Kolom Deskripsi menyediakan deskripsi singkat dari data yang disimpan bidang, dan menunjukkan persyaratan untuk nilai filter. Tabel diurutkan dalam urutan abjad berdasarkan bidang, dan kemudian berdasarkan bidang JSON.

Bidang	Bidang JSON	Deskripsi
ID kunci KMS enkripsi objek S3*	<code>resourcesAffected.s3object.serverSideEncryption.kmsMasterKeyId</code>	Nama Sumber Daya Amazon (ARN) atau pengenal unik (ID kunci) untuk AWS KMS key yang digunakan untuk mengenkripsi objek yang terpengaruh.
Tipe enkripsi objek S3	<code>resourcesAffected.s3object.serverSideEncryption.encryptionType</code>	<p>Algoritma enkripsi sisi server yang digunakan untuk mengenkripsi objek yang terpengaruh.</p> <p>Konsol tersebut menyediakan daftar nilai untuk memilih dari saat Anda menambahkan bidang ini ke filter. Untuk daftar nilai yang valid untuk API, lihat <a href="#">EncryptionType</a> di Referensi API Amazon Macie.</p>
—	<code>resourcesAffected.s3object.extension</code>	Ekstensi nama file dari objek yang terpengaruh. Untuk objek yang tidak memiliki ekstensi

Bidang	Bidang JSON	Deskripsi
		<p>nama file, tentukan "" sebagai nilai untuk filter.</p> <p>Bidang ini tidak tersedia sebagai opsi filter pada konsol tersebut.</p>
—	<code>resourcesAffected.s3object.lastModified</code>	<p>Tanggal dan waktu ketika objek terpengaruh dibuat atau terakhir diubah, mana saja yang terbaru.</p> <p>Bidang ini tidak tersedia sebagai opsi filter pada konsol tersebut. Dengan API, Anda dapat menggunakan bidang ini untuk menentukan rentang waktu untuk filter.</p>
Kunci objek S3*	<code>resourcesAffected.s3object.key</code>	<p>Nama lengkap (kunci) dari objek yang terpengaruh, termasuk awalan objek jika berlaku.</p>
—	<code>resourcesAffected.s3object.path</code>	<p>Jalur lengkap ke objek yang terpengaruh, termasuk nama bucket yang terpengaruh dan nama objek (kunci).</p> <p>Bidang ini tidak tersedia sebagai opsi filter pada konsol tersebut.</p>

Bidang	Bidang JSON	Deskripsi
Akses publik objek S3	<code>resourcesAffected.s3object.publicAccess</code>	<p>Nilai Boolean yang menentukan apakah objek yang terpengaruh dapat diakses secara publik berdasarkan kombinasi pengaturan izin yang berlaku untuk objek tersebut.</p> <p>Konsol tersebut menyediakan daftar nilai untuk memilih dari saat Anda menambahkan bidang ini ke filter.</p>
Kunci tanda objek S3*	<code>resourcesAffected.s3object.tags.key</code>	Kunci tanda yang terkait dengan objek yang terpengaruh.
Nilai tanda objek S3*	<code>resourcesAffected.s3object.tags.value</code>	Nilai tanda yang terkait dengan objek yang terpengaruh.

\* Untuk menentukan beberapa nilai untuk bidang ini pada konsol tersebut, tambahkan syarat yang menggunakan bidang dan tentukan nilai yang berbeda untuk filter, lalu ulangi langkah itu untuk setiap nilai tambahan. Untuk melakukan ini dengan API, gunakan array yang mencantumkan nilai yang akan digunakan untuk filter.

## Bidang kebijakan

Tabel berikut mencantumkan dan menjelaskan bidang yang dapat Anda gunakan untuk memfilter temuan kebijakan. Bidang ini menyimpan data yang spesifik untuk temuan kebijakan.

Pada tabel, kolom Bidang menunjukkan nama bidang pada konsol Amazon Macie. Kolom Bidang JSON menggunakan notasi titik untuk menunjukkan nama bidang dalam temuan representasi JSON dan API Amazon Macie. (Nama bidang JSON yang lebih panjang menggunakan urutan karakter baris



baru (\n) untuk meningkatkan keterbacaan.) Kolom Deskripsi menyediakan deskripsi singkat dari data yang disimpan bidang, dan menunjukkan persyaratan untuk nilai filter. Tabel diurutkan dalam urutan abjad berdasarkan bidang, dan kemudian berdasarkan bidang JSON.

Bidang	Bidang JSON	Deskripsi
Tipe tindakan	<code>policyDetails.action.actionType</code>	Tipe tindakan yang menghasilkan temuan. Satu-satunya nilai yang valid untuk bidang ini adalah <code>AWS_API_CALL</code> .
Nama panggilan API*	<code>policyDetails.action.apiCallDetails.api</code>	Nama operasi yang dipanggil paling baru dan menghasilkan temuan—misalnya, <code>PutBucketPublicAccessBlock</code> .
Nama layanan API	<code>policyDetails.action.apiCallDetails.apiServiceName</code>	URL yang menyediakan operasi Layanan AWS yang dipanggil dan menghasilkan penemuan—misalnya, <code>s3.amazonaws.com</code>
—	<code>policyDetails.action.apiCallDetails.firstSeen</code>	Tanggal dan waktu pertama ketika operasi apa pun dipanggil dan menghasilkan temuan.  Bidang ini tidak tersedia sebagai opsi filter pada konsol tersebut. Dengan API, Anda dapat menggunakan bidang ini untuk menentukan rentang waktu untuk filter.
—	<code>policyDetails.action.apiCallDetails.lastSeen</code>	Tanggal dan waktu terbaru saat operasi tertentu (Nama panggilan API atau api)

Bidang	Bidang JSON	Deskripsi
		<p>dipanggil dan menghasilkan temuan.</p> <p>Bidang ini tidak tersedia sebagai opsi filter pada konsol tersebut. Dengan API, Anda dapat menggunakan bidang ini untuk menentukan rentang waktu untuk filter.</p>
—	<code>policyDetails.actor.domainDetails.domainName</code>	<p>Nama domain perangkat yang digunakan untuk melakukan tindakan.</p> <p>Bidang ini tidak tersedia sebagai opsi filter pada konsol tersebut.</p>
IP kota*	<code>policyDetails.actor.ipAddressDetails.ipCity.name</code>	<p>Nama kota asal untuk alamat IP perangkat yang digunakan untuk melakukan tindakan.</p>
IP negara*	<code>policyDetails.actor.ipAddressDetails.ipCountry.name</code>	<p>Nama negara asal untuk alamat IP perangkat yang digunakan untuk melakukan tindakan—misalnya, United States.</p>
—	<code>policyDetails.actor.ipAddressDetails.ipOwner.asn</code>	<p>Nomor Sistem Mandiri (ASN) untuk sistem mandiri yang menyertakan alamat IP perangkat yang digunakan untuk melakukan tindakan.</p> <p>Bidang ini tidak tersedia sebagai opsi filter pada konsol tersebut.</p>

Bidang	Bidang JSON	Deskripsi
Pemilik IP ASN org*	<code>policyDetails.actor.ipAddressDetails.ipOwner.asnOrg</code>	Pengenal organisasi yang terkait dengan ASN untuk sistem mandiri yang termasuk perangkat alamat IP yang digunakan untuk melakukan tindakan.
ISP* pemilik IP	<code>policyDetails.actor.ipAddressDetails.ipOwner.isp</code>	Nama penyedia layanan internet (ISP) yang dimiliki perangkat alamat IP yang digunakan untuk melakukan tindakan.
Alamat V4 IP*	<code>policyDetails.actor.ipAddressDetails.ipAddressV4</code>	Alamat Internet Protocol versi 4 (IPv4) perangkat yang digunakan untuk melakukan tindakan.
—	<code>policyDetails.actor.userIdentity.assumedRole.accessKeyId</code>	<p>Untuk tindakan yang dilakukan dengan kredensial keamanan sementara yang diperoleh menggunakan operasi <code>AssumeRole</code> API AWS STS, access key ID AWS yang mengidentifikasi kredensialnya.</p> <p>Bidang ini tidak tersedia sebagai opsi filter pada konsol tersebut.</p>

Bidang	Bidang JSON	Deskripsi
Identitas pengguna diasumsikan id akun peran*	<code>policyDetails.actor.userIdentity.assumedRole.accountId</code>	Untuk tindakan yang dilakukan dengan kredensial keamanan sementara yang diperoleh dengan menggunakan AssumeRole pengoperasian AWS STS API, pengidentifikasi unik untuk Akun AWS yang memiliki entitas yang digunakan untuk mendapatkan kredensialnya.
Identitas pengguna diasumsikan peran utama id*	<code>policyDetails.actor.userIdentity.assumedRole.principalId</code>	Untuk tindakan yang dilakukan dengan kredensial keamanan sementara yang diperoleh menggunakan operasi API AssumeRole AWS STS, pengenal unik untuk entitas yang digunakan untuk mendapatkan kredensial.
Identitas pengguna diasumsikan sesi peran ARN*	<code>policyDetails.actor.userIdentity.assumedRole.arn</code>	Untuk tindakan yang dilakukan dengan kredensial keamanan sementara yang diperoleh menggunakan operasi AssumeRole API AWS STS, Amazon Resource Name (ARN) akun sumber, pengguna IAM, atau peran yang digunakan untuk mendapatkan kredensial.

Bidang	Bidang JSON	Deskripsi
—	<pre>policyDetails.actor.userIdentity.assumedRole.sessionContext.\n sessionIssuer.type</pre>	<p>Untuk tindakan yang dilakukan dengan kredensial keamanan sementara yang diperoleh menggunakan operasi AssumeRole API AWS STS, sumber kredensial — keamanan sementara misalnya, Root, IAMUser, atau Role.</p> <p>Bidang ini tidak tersedia sebagai opsi filter pada konsol tersebut.</p>
—	<pre>policyDetails.actor.userIdentity.assumedRole.sessionContext.\n sessionIssuer.userName</pre>	<p>Untuk tindakan yang dilakukan dengan kredensial keamanan sementara yang diperoleh menggunakan operasi AssumeRole API AWS STS, nama atau alias pengguna atau peran yang mengeluarkan sesi. Perhatikan bahwa nilai ini nol jika kredensial diperoleh dari akun root yang tidak memiliki alias.</p> <p>Bidang ini tidak tersedia sebagai opsi filter pada konsol tersebut.</p>
Identitas pengguna id akun dari akun AWS*	<pre>policyDetails.actor.userIdentity.awsAccount.accountId</pre>	<p>Untuk tindakan yang dilakukan menggunakan kredensi untuk yang lainAkun AWS, pengenal unik untuk akun.</p>

Bidang	Bidang JSON	Deskripsi
Identitas pengguna id akun utama AWS*	<code>policyDetails.actor.userIdentity.awsAccount.principalId</code>	Untuk tindakan yang dilakukan menggunakan kredensi untuk yang lainAkun AWS, pengenalan unik untuk entitas yang melakukan tindakan.
Identitas pengguna layanan AWS dipanggil oleh	<code>policyDetails.actor.userIdentity.awsService.invokedBy</code>	Untuk tindakan yang dilakukan oleh akun milikLayanan AWS, nama layanan.
—	<code>policyDetails.actor.userIdentity.federatedUser.accessKeyId</code>	<p>Untuk tindakan yang dilakukan dengan kredensial keamanan sementara yang diperoleh menggunakan operasi <code>GetFederationToken</code> API AWS STS, access key ID AWS yang mengidentifikasi kredensialnya.</p> <p>Bidang ini tidak tersedia sebagai opsi filter pada konsol tersebut.</p>
Sesi federasi identitas pengguna ARN*	<code>policyDetails.actor.userIdentity.federatedUser.arn</code>	Untuk tindakan yang dilakukan dengan kredensial keamanan sementara yang diperoleh menggunakan operasi <code>GetFederationToken</code> API AWS STS, ARN entitas yang digunakan untuk mendapatkan kredensial.

Bidang	Bidang JSON	Deskripsi
ID akun pengguna federasi identitas pengguna*	<code>policyDetails.actor.userIdentity.federatedUser.accountId</code>	Untuk tindakan yang dilakukan dengan kredensial keamanan sementara yang diperoleh dengan menggunakan <code>GetFederationToken</code> pengoperasian AWS STS API, pengidentifikasi unik untuk Akun AWS yang memiliki entitas yang digunakan untuk mendapatkan kredensialnya.
ID utama pengguna federasi identitas pengguna*	<code>policyDetails.actor.userIdentity.federatedUser.principalId</code>	Untuk tindakan yang dilakukan dengan kredensial keamanan sementara yang diperoleh menggunakan operasi API <code>GetFederationToken</code> AWS STS, pengenal unik untuk entitas yang digunakan untuk mendapatkan kredensial.
—	<code>policyDetails.actor.userIdentity.federatedUser.sessionContext.\n\nsessionIssuer.type</code>	Untuk tindakan yang dilakukan dengan kredensial keamanan sementara yang diperoleh menggunakan operasi <code>GetFederationToken</code> API AWS STS, sumber kredensial keamanan sementara—misalnya, <code>Root</code> , <code>IAMUser</code> , atau <code>Role</code> .  Bidang ini tidak tersedia sebagai opsi filter pada konsol tersebut.

Bidang	Bidang JSON	Deskripsi
—	<pre>policyDetails.actor.userIdentity.federatedUser.sessionContext.\n sessionIssuer.userName</pre>	<p>Untuk tindakan yang dilakukan dengan kredensial keamanan sementara yang diperoleh menggunakan operasi <code>GetFederationToken</code> API AWS STS, nama atau alias pengguna atau peran yang mengeluarkan sesi. Perhatikan bahwa nilai ini nol jika kredensial diperoleh dari akun root yang tidak memiliki alias.</p> <p>Bidang ini tidak tersedia sebagai opsi filter pada konsol tersebut.</p>
ID akun IAM identitas pengguna*	<pre>policyDetails.actor.userIdentity.iamUser.accountId</pre>	<p>Untuk tindakan yang dilakukan menggunakan kredensi pengguna IAM, pengenal unik untuk Akun AWS yang terkait dengan pengguna IAM yang melakukan tindakan tersebut.</p>
ID utama IAM identitas pengguna*	<pre>policyDetails.actor.userIdentity.iamUser.principalId</pre>	<p>Untuk tindakan yang dilakukan menggunakan kredensial pengguna IAM, pengenal unik untuk pengguna IAM yang melakukan tindakan tersebut.</p>
Identitas pengguna nama pengguna IAM*	<pre>policyDetails.actor.userIdentity.iamUser.userName</pre>	<p>Untuk tindakan yang dilakukan menggunakan kredensi pengguna IAM, nama pengguna IAM yang melakukan tindakan tersebut.</p>



Bidang	Bidang JSON	Deskripsi
ID akun root identitas pengguna*	<code>policyDetails.actor.userIdentity.root.accountId</code>	Untuk tindakan yang dilakukan menggunakan kredensi untuk AndaAkun AWS, pengenal unik untuk akun tersebut.
ID utama root identitas pengguna*	<code>policyDetails.actor.userIdentity.root.principalId</code>	Untuk tindakan yang dilakukan menggunakan kredensial untuk AndaAkun AWS, pengenal unik untuk entitas yang melakukan tindakan.
Tipe Identitas pengguna	<code>policyDetails.actor.userIdentity.type</code>	<p>Tipe entitas yang melakukan tindakan yang menghasilkan temuan tersebut.</p> <p>Konsol tersebut menyediakan daftar nilai untuk memilih dari saat Anda menambahkan bidang ini ke filter. Untuk daftar nilai yang valid untuk API, lihat <a href="#">UserIdentityType</a> di Referensi API Amazon Macie.</p>

\* Untuk menentukan beberapa nilai untuk bidang ini pada konsol tersebut, tambahkan syarat yang menggunakan bidang dan tentukan nilai yang berbeda untuk filter, lalu ulangi langkah itu untuk setiap nilai tambahan. Untuk melakukan ini dengan API, gunakan array yang mencantumkan nilai yang akan digunakan untuk filter.

## Bidang klasifikasi data sensitif

Tabel berikut berisi daftar dan menjelaskan bidang yang dapat Anda gunakan untuk memfilter temuan data sensitif. Bidang ini menyimpan data yang spesifik untuk temuan data sensitif.

Pada tabel, kolom Bidang menunjukkan nama bidang pada konsol Amazon Macie. Kolom Bidang JSON menggunakan notasi titik untuk menunjukkan nama bidang dalam temuan representasi JSON dan API Amazon Macie. Kolom Deskripsi menyediakan deskripsi singkat dari data yang

disimpan bidang, dan menunjukkan persyaratan untuk nilai filter. Tabel diurutkan dalam urutan abjad berdasarkan bidang, dan kemudian berdasarkan bidang JSON.

Bidang	Bidang JSON	Deskripsi
ID pengidentifikasi data kustom*	<code>classificationDetails.result.customDataIdentifiers.detections.arn</code>	Pengidentifikasi unik untuk pengidentifikasi data kustom yang mendeteksi data dan menghasilkan temuan.
Nama pengidentifikasi data kustom*	<code>classificationDetails.result.customDataIdentifiers.detections.name</code>	Nama pengenalan data khusus yang mendeteksi data dan menghasilkan temuan.
Jumlah total pengidentifikasi data kustom	<code>classificationDetails.result.customDataIdentifiers.detections.count</code>	Jumlah total kemunculan data yang terdeteksi oleh pengenalan data khusus dan menghasilkan temuan.  Anda dapat menggunakan bidang ini untuk menentukan rentang numerik untuk filter.
ID Tugas*	<code>classificationDetails.jobId</code>	Pengenalan unik untuk tugas penemuan data sensitif yang menghasilkan temuan.
Jenis asal	<code>classificationDetails.originType</code>	Bagaimana Macie menemukan data sensitif yang menghasilkan temuan: <code>AUTOMATED_SENSITIVE_DATA_DISCOVERY</code> atau <code>SENSITIVE_DATA_DISCOVERY_JOB</code> .

Bidang	Bidang JSON	Deskripsi
—	<code>classificationDetails.result.mimeType</code>	<p>Tipe konten, sebagai tipe MIME, tempat temuan diterapkan—misalnya, <code>text/csv</code> untuk file CSV atau <code>application/pdf</code> untuk file Format Dokumen Portabel Adobe.</p> <p>Bidang ini tidak tersedia sebagai opsi filter pada konsol tersebut.</p>
—	<code>classificationDetails.result.sizeClassified</code>	<p>Ukuran penyimpanan total, dalam byte, dari objek S3 tempat temuan diterapkan.</p> <p>Bidang ini tidak tersedia sebagai opsi filter pada konsol tersebut. Dengan API, Anda dapat menggunakan bidang ini untuk menentukan rentang numerik untuk filter.</p>

Bidang	Bidang JSON	Deskripsi
Kode status hasil*	<code>classificationDetails.result.status.code</code>	<p>Status temuan. Nilai yang valid adalah:</p> <ul style="list-style-type: none"> <li>• COMPLETE— Macie menyelesaikan analisis objek.</li> <li>• PARTIAL— Macie hanya menganalisis sebagian data dalam objek. Misalnya, objek adalah file arsip yang berisi file dalam format yang tidak didukung.</li> <li>• SKIPPED- Macie tidak dapat menganalisis objek. Misalnya, objek adalah file yang salah format.</li> </ul>
Kategori data sensitif	<code>classificationDetails.result.sensitiveData.category</code>	<p>Kategori data sensitif yang terdeteksi dan menghasilkan temuan.</p> <p>Konsol tersebut menyediakan daftar nilai untuk memilih dari saat Anda menambahkan bidang ini ke filter. Di API, nilai yang valid adalah: CREDENTIALS , FINANCIAL_INFORMATION , dan PERSONAL_INFORMATION .</p>

Bidang	Bidang JSON	Deskripsi
Tipe deteksi data sensitif	<code>classificationDetails.result.sensitiveData.detections.type</code>	<p>Tipe data sensitif yang terdeteksi dan menghasilkan temuan.</p> <p>Konsol tersebut menyediakan daftar nilai untuk memilih dari saat Anda menambahkan bidang ini ke filter. Untuk daftar nilai yang valid untuk konsol dan API, lihat <a href="#">Tipe deteksi data sensitif</a>.</p>
Jumlah total data sensitif	<code>classificationDetails.result.sensitiveData.detections.count</code>	<p>Jumlah total kemunculan data sensitif yang terdeteksi dan menghasilkan temuan.</p> <p>Anda dapat menggunakan bidang ini untuk menentukan rentang numerik untuk filter.</p>

\* Untuk menentukan beberapa nilai untuk bidang ini pada konsol tersebut, tambahkan syarat yang menggunakan bidang dan tentukan nilai yang berbeda untuk filter, lalu ulangi langkah itu untuk setiap nilai tambahan. Untuk melakukan ini dengan API, gunakan array yang mencantumkan nilai yang akan digunakan untuk filter.

### Tipe deteksi data sensitif

Topik berikut mencantumkan nilai yang dapat Anda tentukan untuk bidang Tipe deteksi data sensitif dalam sebuah filter. (Nama JSON dari bidang ini adalah `classificationDetails.result.sensitiveData.detections.type`.) Topik diatur menurut kategori data sensitif yang dapat dideteksi Macie menggunakan pengidentifikasi data terkelola.

#### Kategori

- [Kredensial](#)
- [Informasi keuangan](#)

- [Informasi pribadi: Informasi kesehatan pribadi \(PHI\)](#)
- [Informasi pribadi: Informasi identitas pribadi \(PII\)](#)

Untuk mempelajari lebih lanjut tentang pengenalan data terkelola untuk jenis data sensitif tertentu, lihat [Referensi terperinci: Pengidentifikasi data terkelola Amazon Macie](#).

## Kredensial

Anda dapat menentukan nilai-nilai berikut untuk memfilter temuan yang melaporkan kemunculan data kredensial dalam objek S3.

Tipe data sensitif	Nilai filter
AWS secret access key	AWS_CREDENTIALS
Kunci API Google Cloud	GCP_API_KEY
Header Otorisasi Dasar HTTP	HTTP_BASIC_AUTH_HEADER
Token Web JSON (JWT)	JSON_WEB_TOKEN
Kunci pribadi OpenSSH	OPENSSSH_PRIVATE_KEY
Kunci pribadi PGP	PGP_PRIVATE_KEY
Kunci pribadi Standar Kriptografi Kunci Publik (PKCS)	PKCS
Kunci pribadi PuTTY	PUTTY_PRIVATE_KEY
Kunci API Stripe	STRIPE_CREDENTIALS

## Informasi keuangan

Anda dapat menentukan nilai berikut untuk memfilter temuan yang melaporkan kemunculan informasi keuangan di objek S3.

Tipe data sensitif	Nilai filter
Nomor rekening bank	BANK_ACCOUNT_NUMBER (Untuk Kanada dan Amerika Serikat)
Nomor Rekening Bank Dasar (BBAN)	Tergantung pada negara atau wilayah: FRANCE_BANK_ACCOUNT_NUMBER, GERMANY_BANK_ACCOUNT_NUMBER, ITALY_BANK_ACCOUNT_NUMBER, SPAIN_BANK_ACCOUNT_NUMBER, UK_BANK_ACCOUNT_NUMBER
Tanggal kedaluwarsa kartu kredit	CREDIT_CARD_EXPIRATION
Data strip magnetik kartu kredit	CREDIT_CARD_MAGNETIC_STRIPE
Nomor kartu kredit	CREDIT_CARD_NUMBER (untuk nomor kartu kredit yang berdekatan dengan kata kunci), CREDIT_CARD_NUMBER_(NO_KEYWORD) (untuk nomor kartu kredit yang tidak berdekatan dengan kata kunci)
Kode verifikasi kartu kredit	CREDIT_CARD_SECURITY_CODE
Nomor Rekening Bank Internasional (IBAN)	Tergantung pada negara atau wilayah: ALBANIA_BANK_ACCOUNT_NUMBER, ANDORRA_BANK_ACCOUNT_NUMBER, BOSNIA_AND_HERZEGOVINA_BANK_ACCOUNT_NUMBER, BRAZIL_BANK_ACCOUNT_NUMBER, BULGARIA_BANK_ACCOUNT_NUMBER, COSTA_RICA_BANK_ACCOUNT_NUMBER, CROATIA_BANK_ACCOUNT_NUMBER, CYPRUS_BANK_ACCOUNT_NUMBER, CZECH_REPUBLIC_BANK_ACCOUNT_NUMBER, DENMARK_BANK_ACCOUNT_NUMBER, DOMINICAN_REPUBLIC_BANK_ACCOUNT_NUMBER

Tipe data sensitif	Nilai filter
	ER, EGYPT_BANK_ACCOUNT_NUMBER, ESTONIA_BANK_ACCOUNT_NUMBER, FAROE_ISLANDS_BANK_ACCOUNT_NUMBER, FINLAND_BANK_ACCOUNT_NUMBER, FRANCE_BANK_ACCOUNT_NUMBER, GEORGIA_BANK_ACCOUNT_NUMBER, GERMANY_BANK_ACCOUNT_NUMBER, GREECE_BANK_ACCOUNT_NUMBER, GREENLAND_BANK_ACCOUNT_NUMBER, HUNGARY_BANK_ACCOUNT_NUMBER, ICELAND_BANK_ACCOUNT_NUMBER, IRELAND_BANK_ACCOUNT_NUMBER, ITALY_BANK_ACCOUNT_NUMBER, JORDAN_BANK_ACCOUNT_NUMBER, KOSOVO_BANK_ACCOUNT_NUMBER, LIECHTENSTEIN_BANK_ACCOUNT_NUMBER, LITHUANIA_BANK_ACCOUNT_NUMBER, MALTA_BANK_ACCOUNT_NUMBER, MAURITANIA_BANK_ACCOUNT_NUMBER, MAURITIUS_BANK_ACCOUNT_NUMBER, MONACO_BANK_ACCOUNT_NUMBER, MONTENEGRO_BANK_ACCOUNT_NUMBER, NETHERLANDS_BANK_ACCOUNT_NUMBER, NORTH_MACEDONIA_BANK_ACCOUNT_NUMBER, POLAND_BANK_ACCOUNT_NUMBER, PORTUGAL_BANK_ACCOUNT_NUMBER, SAN_MARINO_BANK_ACCOUNT_NUMBER, SENEGAL_BANK_ACCOUNT_NUMBER, SERBIA_BANK_ACCOUNT_NUMBER, SLOVAKIA_BANK_ACCOUNT_NUMBER, SLOVENIA_BANK_ACCOUNT_NUMBER, SPAIN_BANK_ACCOUNT_NUMBER,



Tipe data sensitif	Nilai filter
	SWEDEN_BANK_ACCOUNT_NUMBER , SWITZERLAND_BANK_ACCOUNT_NUMBER, TIMOR_LESTE_BANK_ACCOUNT_NUMBER, TUNISIA_BANK_ACCOUNT_NUMBER, TURKIYE_BANK_ACCOUNT_NUMBER, UK_BANK_ACCOUNT_NUMBER, UKRAINE_BANK_ACCOUNT_NUMBER, UNITED_ARAB_EMIRATES_BANK_ACCOUNT_NUMBER, VIRGIN_ISLANDS_BANK_ACCOUNT_NUMBER (untuk Kepulauan Virgin Inggris)

### Informasi pribadi: Informasi kesehatan pribadi (PHI)

Anda dapat menentukan nilai-nilai berikut untuk memfilter temuan yang melaporkan kemunculan informasi kesehatan pribadi (PHI) di objek S3.

Tipe data sensitif	Nilai filter
Nomor Registrasi Badan Penegakan Narkoba (DEA)	US_DRUG_ENFORCEMENT_AGENCY_NUMBER
Nomor Klaim Asuransi Kesehatan (HICN)	USA_HEALTH_INSURANCE_CLAIM_NUMBER
Nomor asuransi atau identifikasi medis	Tergantung pada negara atau wilayah: CANADA_HEALTH_NUMBER, EUROPEAN_HEALTH_INSURANCE_CARD_NUMBER, FINLAND_EUROPEAN_HEALTH_INSURANCE_NUMBER, FRANCE_HEALTH_INSURANCE_NUMBER, UK_NHS_NUMBER, USA_MEDICARE_BENEFICIARY_IDENTIFIER

Tipe data sensitif	Nilai filter
Kode Sistem Pengkodean Prosedur Umum Kesehatan (HCPCS)	USA_HEALTHCARE_PROCEDURE_CODE
Kode Obat Nasional (NDC)	USA_NATIONAL_DRUG_CODE
Pengidentifikasi Penyedia Nasional (NPI)	USA_NATIONAL_PROVIDER_IDENTIFIER
Pengidentifikasi perangkat unik (UDI)	MEDICAL_DEVICE_UDI

Informasi pribadi: Informasi identitas pribadi (PII)

Anda dapat menentukan nilai berikut untuk memfilter temuan yang melaporkan kemunculan informasi pengenalan pribadi (PII) di objek S3.

Tipe data sensitif	Nilai filter
Tanggal lahir	DATE_OF_BIRTH
Nomor identifikasi lisensi	Tergantung pada negara atau wilayah: AUSTRALIA_DRIVERS_LICENSE, AUSTRIA_DRIVERS_LICENSE, BELGIUM_DRIVERS_LICENSE, BULGARIA_DRIVERS_LICENSE, CANADA_DRIVERS_LICENSE, CR OATIA_DRIVERS_LICENSE, CYPRUS_DR IVERS_LICENSE, CZECHIA_DRI VERS_LICENSE, DENMARK_DRIVERS_LI CENSE, DRIVERS_LICENSE (untuk AS), ESTONIA_DRIVERS_LICENSE, FINLAND_DRIVERS_LICENSE, FRANCE_DRIVERS_LICENSE, GERMANY_DRIVERS_LICENSE, G REECE_DRIVERS_LICENSE, HUNGARY_D RIVERS_LICENSE, INDIA_DRIV ERS_LICENSE, IRELAND_DRIVERS_LI

Tipe data sensitif	Nilai filter
	CENSE, ITALY_DRIVERS_LICENSE, LATVIA_DRIVERS_LICENSE, LITHUANIA_DRIVERS_LICENSE, LUXEMBOURG_DRIVERS_LICENSE, MALTA_DRIVERS_LICENSE, NETHERLANDS_DRIVERS_LICENSE, POLAND_DRIVERS_LICENSE, PORTUGAL_DRIVERS_LICENSE, ROMANIA_DRIVERS_LICENSE, SLOVAKIA_DRIVERS_LICENSE, SLOVENIA_DRIVERS_LICENSE, SPAIN_DRIVERS_LICENSE, SWEDEN_DRIVERS_LICENSE, UK_DRIVERS_LICENSE
Nomor Roll Pemilu	UK_ELECTORAL_ROLL_NUMBER
Nama lengkap	NAME
Koordinat Sistem Pemosisian Global (GPS)	LATITUDE_LONGITUDE
HTTP cookie	HTTP_COOKIE
Alamat surat-menyurat	ADDRESS, BRAZIL_CEP_CODE
Nomor identifikasi nasional	Tergantung pada negara atau wilayah: BRAZIL_RG_NUMBER, FRANCE_NATIONAL_IDENTIFICATION_NUMBER, GERMANY_NATIONAL_IDENTIFICATION_NUMBER, INDIA_AADHAAR_NUMBER, ITALY_NATIONAL_IDENTIFICATION_NUMBER, SPAIN_DNI_NUMBER
Nomor Asuransi Nasional (NINO)	UK_NATIONAL_INSURANCE_NUMBER

Tipe data sensitif	Nilai filter
Nomor paspor	Tergantung pada negara atau wilayah: CANADA_PASSPORT_NUMBER, FRANCE_PASSPORT_NUMBER, GERMANY_PASSPORT_NUMBER, ITALY_PASSPORT_NUMBER, SPAIN_PASSPORT_NUMBER, UK_PASSPORT_NUMBER, USA_PASSPORT_NUMBER
Nomor tempat tinggal permanen	CANADA_NATIONAL_IDENTIFICATION_NUMBER
Nomor telepon	Tergantung pada negara atau wilayah: BRAZIL_PHONE_NUMBER, FRANCE_PHONE_NUMBER, GERMANY_PHONE_NUMBER, ITALY_PHONE_NUMBER, PHONE_NUMBER (untuk Kanada dan AS), SPAIN_PHONE_NUMBER, UK_PHONE_NUMBER
Nomor Asuransi Sosial (SIN)	CANADA_SOCIAL_INSURANCE_NUMBER
Nomor Jaminan Sosial (SSN)	Tergantung pada negara atau wilayah: SPAIN_SOCIAL_SECURITY_NUMBER, USA_SOCIAL_SECURITY_NUMBER

Tipe data sensitif	Nilai filter
Nomor identifikasi wajib pajak atau referensi	Tergantung pada negara atau wilayah: AUSTRALIA_TAX_FILE_NUMBER, BRAZIL_CNPJ_NUMBER, BRAZIL_CPF_NUMBER, FRANCE_TAX_IDENTIFICATION_NUMBER, GERMANY_TAX_IDENTIFICATION_NUMBER, INDIA_PERMANENT_ACCOUNT_NUMBER, SPAIN_NIE_NUMBER, SPAIN_NIF_NUMBER, SPAIN_TAX_IDENTIFICATION_NUMBER, UK_TAX_IDENTIFICATION_NUMBER, USA_INDIVIDUAL_TAX_IDENTIFICATION_NUMBER
Nomor identifikasi kendaraan (VIN)	VEHICLE_IDENTIFICATION_NUMBER

## Menyelidiki data sensitif dengan temuan Amazon Macie

Saat Anda menjalankan pekerjaan penemuan data sensitif atau Amazon Macie melakukan penemuan data sensitif otomatis, Macie menangkap detail tentang lokasi setiap kemunculan data sensitif yang ditemukan di objek Amazon Simple Storage Service (Amazon S3). Ini termasuk data sensitif yang dideteksi Macie menggunakan [pengidentifikasi data terkelola](#), dan data yang cocok dengan kriteria [pengidentifikasi data kustom](#) yang Anda konfigurasi pekerjaan atau Macie untuk digunakan.

Dengan temuan data sensitif, Anda dapat meninjau detail ini untuk sebanyak 15 kemunculan data sensitif yang ditemukan Macie di objek S3 individu. Detailnya memberikan wawasan tentang luasnya kategori dan jenis data sensitif yang mungkin berisi bucket dan objek S3 tertentu. Mereka dapat membantu Anda menemukan kejadian individu dari data sensitif dalam objek, dan menentukan apakah akan melakukan penyelidikan lebih dalam dari ember dan objek tertentu.

Untuk wawasan tambahan, Anda dapat mengonfigurasi dan menggunakan Macie secara opsional untuk mengambil sampel data sensitif yang dilaporkan Macie dalam temuan individu. Sampel dapat membantu Anda memverifikasi sifat data sensitif yang ditemukan Macie. Mereka juga dapat membantu Anda menyesuaikan penyelidikan Anda terhadap ember dan objek S3 yang terpengaruh.

Jika Anda memilih untuk mengambil sampel data sensitif untuk temuan, Macie menggunakan data dalam temuan untuk menemukan 1-10 kejadian dari setiap jenis data sensitif yang dilaporkan oleh temuan tersebut. Macie kemudian mengekstrak kejadian data sensitif tersebut dari objek yang terpengaruh dan menampilkan data untuk Anda tinjau.

Jika objek S3 berisi banyak kemunculan data sensitif, temuan juga dapat membantu Anda menavigasi ke hasil penemuan data sensitif yang sesuai. Tidak seperti temuan data sensitif, hasil penemuan data sensitif memberikan data lokasi terperinci untuk sebanyak 1.000 kejadian dari setiap jenis data sensitif yang ditemukan Macie dalam suatu objek. Macie menggunakan skema yang sama untuk data lokasi dalam temuan data sensitif dan hasil penemuan data sensitif. Untuk mempelajari selengkapnya tentang hasil penemuan data sensitif, lihat [Menyimpan dan mempertahankan hasil penemuan data sensitif](#).

Topik di bagian ini menjelaskan cara menemukan dan secara opsional mengambil kejadian data sensitif yang dilaporkan oleh temuan data sensitif. Mereka juga menjelaskan skema yang digunakan Macie untuk melaporkan lokasi kejadian individu dari data sensitif yang ditemukan Macie.

Topik

- [Menemukan data sensitif dengan temuan Amazon Macie](#)
- [Mengambil sampel data sensitif dengan temuan Amazon Macie](#)
- [Skema JSON untuk lokasi data sensitif](#)

## Menemukan data sensitif dengan temuan Amazon Macie

Ketika Anda menjalankan tugas penemuan data sensitif atau Amazon Macie melakukan penemuan data sensitif otomatis, Macie melakukan pemeriksaan mendalam dari versi terbaru dari setiap objek Amazon Simple Storage Service (Amazon S3) yang dianalisisnya. Untuk setiap tugas yang dijalankan atau siklus analisis, Macie juga menggunakan algoritme pencarian pertama-mendalam untuk mengisi temuan yang dihasilkan dengan detail tentang lokasi dari data sensitif tertentu yang ditemukan Macie dalam objek S3. Kejadian ini memberikan wawasan ke dalam kategori dan tipe data sensitif yang mungkin berisi Bucket S3 dan objek yang terpengaruh. Detail dapat membantu Anda menemukan setiap kejadian data sensitif dalam objek, dan menentukan apakah melakukan investigasi yang lebih dalam terhadap bucket dan objek tertentu.

Dengan temuan data sensitif, Anda dapat menentukan lokasi sebanyak 15 kejadian data sensitif yang ditemukan Macie dalam objek S3 yang terpengaruh. Hal ini mencakup data sensitif yang

dideteksi Macie menggunakan [pengidentifikasi data terkelola](#), dan data yang cocok dengan kriteria [pengidentifikasi data kustom](#) yang tugasnya Anda konfigurasi atau Macie untuk digunakan.

Temuan data sensitif dapat memberikan detail seperti:

- Nomor baris dan kolom untuk sel atau bidang di buku kerja Microsoft Excel, file CSV, atau file TSV.
- Jalur menuju bidang atau array dalam file JSON atau JSON Lines.
- Nomor baris untuk baris di dalam file teks non-biner selain file CSV, JSON, JSON Lines, atau TSV — misalnya, file HTML, TXT, atau XML.
- Nomor halaman untuk halaman dalam file Format Dokumen Portabel Adobe (PDF).
- Indeks catatan dan jalur menuju bidang pada catatan dalam kontainer objek Apache Avro atau file Apache Parquet.

Anda dapat mengakses detail ini dengan menggunakan konsol Amazon Macie atau API Amazon Macie. Anda juga dapat mengakses detail ini dalam temuan bahwa Macie menerbitkan ke layanan lain AWS, Amazon dan EventBridge AWS Security Hub Untuk mempelajari tentang struktur JSON yang digunakan Macie untuk melaporkan detail ini, lihat [Skema JSON untuk lokasi data sensitif](#) Untuk mempelajari cara mengakses detail dalam temuan ketika Macie menerbitkan ke layanan lain AWS, lihat [Pemantauan dan pemrosesan temuan](#)

Jika objek S3 berisi banyak kejadian data sensitif, Anda juga dapat menggunakan temuan untuk menavigasi ke hasil penemuan data sensitif yang sesuai. Tidak seperti temuan data sensitif, hasil penemuan data sensitif memberikan data lokasi rinci sebanyak 1.000 kejadian dari setiap tipe data sensitif yang ditemukan Macie dalam suatu objek. Jika objek S3 merupakan file arsip, seperti file.tar atau .zip, ini mencakup kejadian data sensitif dalam file individu ketika Macie diekstrak dari arsip. (Macie tidak menyertakan informasi ini dalam temuan data sensitif.) Untuk mempelajari selengkapnya tentang hasil penemuan data sensitif, lihat [Menyimpan dan mempertahankan hasil penemuan data sensitif](#). Macie menggunakan skema yang sama untuk data lokasi dalam temuan data sensitif dan hasil penemuan data sensitif.

## Menemukan kejadian data sensitif

Untuk menemukan kejadian data sensitif, Anda dapat menggunakan konsol Amazon Macie atau API Amazon Macie. Langkah-langkah berikut menjelaskan cara menemukan data sensitif dengan menggunakan konsol.

Untuk menemukan data sensitif secara terprogram, gunakan [GetFindings](#) operasi dari API Amazon Macie. Jika temuan mencakup rincian tentang lokasi satu atau lebih kejadian dari jenis data sensitif

tertentu, occurrences objek dalam temuan memberikan rincian ini. Untuk informasi selengkapnya, lihat [Skema JSON untuk lokasi data sensitif](#).

Untuk menemukan kejadian data sensitif

1. Buka konsol Amazon Macie di <https://console.aws.amazon.com/macie/>.
2. Di panel navigasi, pilih Temuan.

 Tip

Anda dapat menggunakan halaman Tugas untuk menampilkan semua temuan dari tugas penemuan data sensitif tertentu. Untuk melakukannya, pilih Tugas pada panel navigasi, lalu pilih nama tugas. Di bagian atas panel detail, pilih Tampilkan hasil, lalu pilih Tampilkan temuan.

3. Pada halaman Temuan, pilih pencarian untuk data sensitif yang ingin Anda temukan. Panel detail menampilkan informasi temuan.
4. Di panel detail, gulir ke bagian Data sensitif. Bagian ini menyediakan informasi tentang kategori dan tipe pada data sensitif saat Macie ditemukan di objek S3 yang terpengaruh. Hal ini juga menunjukkan jumlah kejadian dari setiap tipe data sensitif yang ditemukan Macie.

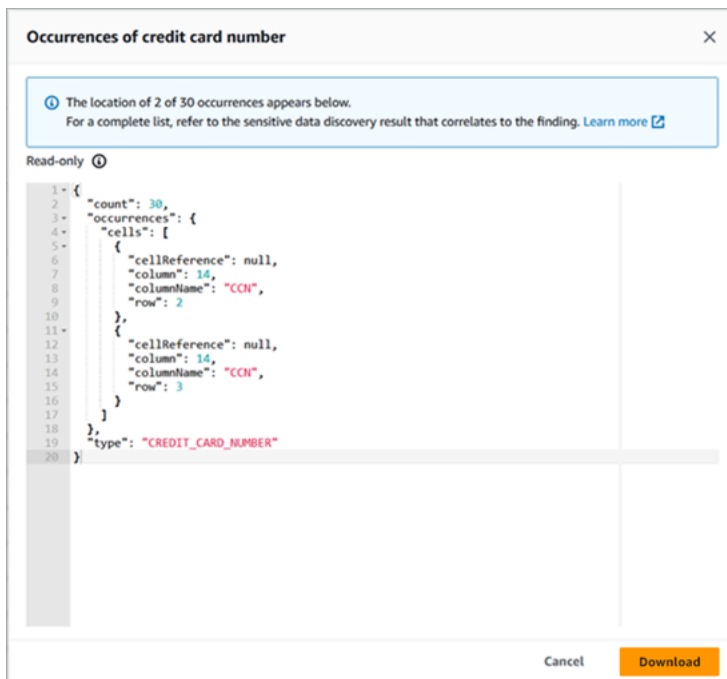
Misalnya, gambar berikut menunjukkan beberapa detail temuan yang melaporkan 30 kejadian nomor kartu kredit, 30 kemunculan nama, dan 30 kejadian nomor Jaminan Sosial AS.

Financial information	
Credit card number	30
Personal information	
Name	30
Usa social security number	30

Jika temuan tersebut berisi detail tentang lokasi dari satu atau beberapa kejadian dari tipe data sensitif tertentu, jumlah kejadian merupakan tautan. Pilih tautan untuk menampilkan detailnya. Macie membuka jendela baru dan menampilkan detail dalam format JSON.

Misalnya, gambar berikut menunjukkan lokasi dua kejadian nomor kartu kredit di objek S3 yang terpengaruh.





Untuk menyimpan detail sebagai file JSON, pilih Unduh, lalu tentukan nama dan lokasi untuk file tersebut.

- (Opsional) Untuk menyimpan semua detail temuan sebagai file JSON, pilih pengidentifikasi temuan dengan (ID Temuan) pada bagian atas panel detail. Macie membuka jendela baru dan menampilkan semua detail dalam format JSON. Pilih Unduh, kemudian tentukan nama dan lokasi untuk file.

Untuk mengakses detail tentang lokasi sebanyak 1.000 kejadian dari setiap tipe data sensitif dalam objek yang terpengaruh, lihat hasil penemuan data sensitif yang sesuai untuk temuan tersebut. Untuk melakukan ini, gulir ke awal bagian Detail panel. Kemudian pilih tautan di bidang Lokasi hasil terperinci. Macie membuka konsol Amazon S3 dan menampilkan file atau folder yang berisi hasil penemuan yang sesuai.

## Mengambil sampel data sensitif dengan temuan Amazon Macie

Untuk memverifikasi sifat data sensitif yang dilaporkan Amazon Macie dalam temuan, Anda dapat mengonfigurasi dan menggunakan Macie secara opsional untuk mengambil dan mengungkapkan sampel data sensitif yang dilaporkan oleh temuan individu. Ini termasuk data sensitif yang dideteksi Macie menggunakan [pengidentifikasi data terkelola](#), dan data yang cocok dengan kriteria pengidentifikasi data [kustom](#). Sampel dapat membantu Anda menyesuaikan penyelidikan objek dan bucket Amazon Simple Storage Service (Amazon S3) yang terpengaruh.

Jika Anda mengambil dan mengungkapkan sampel data sensitif untuk temuan, Macie melakukan tugas umum berikut:

1. Memverifikasi bahwa temuan menentukan lokasi kejadian individu dari data sensitif dan lokasi hasil penemuan [data sensitif](#) yang sesuai.
2. Mengevaluasi hasil penemuan data sensitif yang sesuai, memeriksa validitas metadata untuk objek S3 yang terpengaruh dan data lokasi untuk kejadian data sensitif dalam objek.
3. Dengan menggunakan data dalam hasil penemuan data sensitif, menempatkan 1-10 kejadian pertama dari data sensitif yang dilaporkan oleh temuan, dan mengekstrak 1-128 karakter pertama dari setiap kejadian dari objek S3 yang terpengaruh. Jika temuan melaporkan beberapa jenis data sensitif, Macie melakukan ini hingga 100 jenis.
4. Mengenkripsi data yang diekstrak dengan kunci AWS Key Management Service (AWS KMS) yang Anda tentukan.
5. Menyimpan sementara data terenkripsi dalam cache dan menampilkan data untuk Anda tinjau. Data dienkripsi setiap saat, baik dalam perjalanan maupun saat istirahat.
6. Segera setelah ekstraksi dan enkripsi, secara permanen menghapus data dari cache kecuali retensi tambahan sementara diperlukan untuk menyelesaikan masalah operasional.

Jika Anda memilih untuk mengambil dan mengungkapkan sampel data sensitif untuk temuan lagi, Macie mengulangi tugas-tugas ini untuk mencari, mengekstrak, mengenkripsi, menyimpan, dan akhirnya menghapus sampel.

Macie tidak menggunakan [peran terkait layanan Macie untuk akun Anda untuk melakukan tugas-tugas](#) ini. Sebagai gantinya, Anda menggunakan identitas AWS Identity and Access Management (IAM) Anda atau mengizinkan Macie untuk mengambil peran IAM di akun Anda. Anda dapat mengambil dan mengungkapkan sampel data sensitif untuk temuan jika Anda atau peran diizinkan untuk mengakses sumber daya dan data yang diperlukan, dan melakukan tindakan yang diperlukan. Semua tindakan yang diperlukan [masuk AWS CloudTrail](#).

#### Important

Kami menyarankan Anda membatasi akses ke fungsi ini dengan menggunakan kebijakan [IAM khusus](#). Untuk kontrol akses tambahan, kami menyarankan Anda juga membuat khusus AWS KMS key untuk enkripsi sampel data sensitif yang diambil, dan membatasi penggunaan kunci hanya untuk prinsipal yang harus diizinkan untuk mengambil dan mengungkapkan sampel data sensitif.

Untuk rekomendasi dan contoh kebijakan yang mungkin Anda gunakan untuk mengontrol akses ke fungsionalitas ini, lihat [Cara menggunakan Amazon Macie untuk melihat pratinjau data sensitif di bucket S3](#) postingan blog di Blog Keamanan. AWS

Topik di bagian ini menjelaskan cara mengonfigurasi dan menggunakan Macie untuk mengambil dan mengungkapkan sampel data sensitif untuk temuan. Anda dapat melakukan tugas-tugas ini di semua Wilayah AWS tempat Macie saat ini tersedia kecuali Wilayah Asia Pasifik (Osaka) dan Israel (Tel Aviv).

## Topik

- [Opsi konfigurasi dan persyaratan untuk mengambil sampel data sensitif dengan temuan](#)
- [Mengonfigurasi Amazon Macie untuk mengambil dan mengungkapkan sampel data sensitif dengan temuan](#)
- [Mengambil dan mengungkapkan sampel data sensitif dengan temuan](#)

## Opsi konfigurasi dan persyaratan untuk mengambil sampel data sensitif dengan temuan

Anda dapat mengonfigurasi dan menggunakan Amazon Macie secara opsional untuk mengambil dan mengungkapkan sampel data sensitif yang dilaporkan Macie dalam temuan individual. Jika Anda mengambil dan mengungkapkan sampel data sensitif untuk temuan, Macie menggunakan data dalam [hasil penemuan data sensitif terkait untuk menemukan kejadian data sensitif](#) di objek Amazon Simple Storage Service (Amazon S3) yang terpengaruh. Macie kemudian mengekstrak sampel kejadian tersebut dari objek yang terpengaruh. Macie mengenkripsi data yang diekstrak dengan kunci AWS Key Management Service (AWS KMS) yang Anda tentukan, menyimpan sementara data terenkripsi dalam cache, dan mengembalikan data dalam hasil Anda untuk temuan. Segera setelah ekstraksi dan enkripsi, Macie secara permanen menghapus data dari cache kecuali retensi tambahan sementara diperlukan untuk menyelesaikan masalah operasional.

Macie tidak menggunakan [peran terkait layanan Macie](#) untuk akun Anda untuk menemukan, mengambil, mengenkripsi, atau mengungkapkan sampel data sensitif untuk objek S3 yang terpengaruh. Sebagai gantinya, Macie menggunakan pengaturan dan sumber daya yang Anda konfigurasi untuk akun Anda. Saat Anda mengonfigurasi pengaturan di Macie, Anda menentukan cara mengakses objek S3 yang terpengaruh. Anda juga menentukan mana yang AWS KMS key akan digunakan untuk mengenkripsi sampel. Anda dapat mengonfigurasi pengaturan di semua Wilayah AWS tempat Macie saat ini tersedia kecuali Wilayah Asia Pasifik (Osaka) dan Israel (Tel Aviv).

Untuk mengakses objek S3 yang terpengaruh dan mengambil sampel data sensitif darinya, Anda memiliki dua opsi. Anda dapat mengonfigurasi Macie untuk menggunakan kredensial pengguna AWS Identity and Access Management (IAM) atau mengambil peran IAM:

- **Gunakan kredensial pengguna IAM** — Dengan opsi ini, setiap pengguna akun Anda menggunakan identitas IAM masing-masing untuk mencari, mengambil, mengenkripsi, dan mengungkapkan sampel. Ini berarti bahwa pengguna dapat mengambil dan mengungkapkan sampel data sensitif untuk temuan jika mereka diizinkan untuk mengakses sumber daya dan data yang diperlukan, dan melakukan tindakan yang diperlukan.
- **Asumsikan peran IAM** - Dengan opsi ini, Anda membuat peran IAM yang mendelegasikan akses ke Macie. Anda juga memastikan bahwa kebijakan kepercayaan dan izin untuk peran tersebut memenuhi semua persyaratan bagi Macie untuk mengambil peran tersebut. Macie kemudian mengambil peran ketika pengguna akun Anda memilih untuk mencari, mengambil, mengenkripsi, dan mengungkapkan sampel data sensitif untuk sebuah temuan.

Anda dapat menggunakan konfigurasi dengan semua jenis akun Macie—akun administrator Macie yang didelegasikan untuk organisasi, akun anggota Macie di organisasi, atau akun Macie mandiri.

Topik berikut menjelaskan opsi, persyaratan, dan pertimbangan yang dapat membantu Anda menentukan cara mengonfigurasi pengaturan dan sumber daya untuk akun Anda. Ini termasuk kebijakan kepercayaan dan izin untuk dilampirkan ke peran IAM. Untuk rekomendasi tambahan dan contoh kebijakan yang mungkin Anda gunakan untuk mengambil dan mengungkapkan sampel data sensitif, lihat [Cara menggunakan Amazon Macie untuk melihat pratinjau data sensitif di bucket S3 postingan blog di Blog Keamanan. AWS](#)

## Topik

- [Menentukan metode akses mana yang akan digunakan](#)
- [Menggunakan kredensi pengguna IAM untuk mengakses objek S3 yang terpengaruh](#)
- [Dengan asumsi peran IAM untuk mengakses objek S3 yang terpengaruh](#)
- [Mengkonfigurasi peran IAM untuk mengakses objek S3 yang terpengaruh](#)
- [Mendekripsi objek S3 yang terpengaruh](#)

## Menentukan metode akses mana yang akan digunakan

Saat menentukan konfigurasi mana yang terbaik untuk AWS lingkungan Anda, pertimbangan utama adalah apakah lingkungan Anda menyertakan beberapa akun Amazon Macie yang dikelola

secara terpusat sebagai organisasi. Jika Anda adalah administrator Macie yang didelegasikan untuk organisasi, mengonfigurasi Macie untuk mengambil peran IAM dapat merampingkan pengambilan sampel data sensitif dari objek S3 yang terpengaruh untuk akun di organisasi Anda. Dengan pendekatan ini, Anda membuat peran IAM di akun administrator Anda. Anda juga membuat peran IAM di setiap akun anggota yang berlaku. Peran di akun administrator Anda mendelegasikan akses ke Macie. Peran dalam akun anggota mendelegasikan akses lintas akun ke peran di akun administrator Anda. Jika diterapkan, Anda kemudian dapat menggunakan rantai peran untuk mengakses objek S3 yang terpengaruh untuk akun anggota Anda.

Juga pertimbangkan siapa yang memiliki akses langsung ke temuan individu secara default. Untuk mengambil dan mengungkapkan sampel data sensitif untuk temuan, pengguna harus terlebih dahulu memiliki akses ke temuan:

- Pekerjaan penemuan data sensitif — Hanya akun yang menciptakan pekerjaan yang dapat mengakses temuan yang dihasilkan oleh pekerjaan tersebut. Jika Anda memiliki akun administrator Macie, Anda dapat mengonfigurasi pekerjaan untuk menganalisis objek di bucket S3 untuk akun apa pun di organisasi Anda. Oleh karena itu, pekerjaan Anda dapat menghasilkan temuan untuk objek dalam ember yang dimiliki akun anggota Anda. Jika Anda memiliki akun anggota atau akun Macie mandiri, Anda dapat mengonfigurasi pekerjaan untuk menganalisis objek hanya dalam ember yang dimiliki akun Anda.
- Penemuan data sensitif otomatis — Hanya akun administrator Macie yang dapat mengakses temuan yang dihasilkan penemuan otomatis untuk akun di organisasi mereka. Akun anggota tidak dapat mengakses temuan ini. Jika Anda memiliki akun Macie mandiri, Anda dapat mengakses temuan yang dihasilkan penemuan otomatis hanya untuk akun Anda sendiri.

Jika Anda berencana untuk mengakses objek S3 yang terpengaruh dengan menggunakan peran IAM, pertimbangkan juga hal berikut:

- Untuk menemukan kemunculan data sensitif dalam suatu objek, hasil penemuan data sensitif yang sesuai untuk temuan harus disimpan dalam objek S3 yang ditandatangani Macie dengan Kode Otentikasi Pesan berbasis Hash (HMAC). AWS KMS key Macie harus dapat memverifikasi integritas dan keaslian hasil penemuan data sensitif. Jika tidak, Macie tidak mengambil peran IAM untuk mengambil sampel data sensitif. Ini adalah pagar pembatas tambahan untuk membatasi akses ke data dalam objek S3 untuk akun.
- Untuk mengambil sampel data sensitif dari objek yang dienkripsi dengan pelanggan yang dikelola AWS KMS key, peran IAM harus diizinkan untuk mendekripsi data dengan kunci. Lebih khusus lagi, kebijakan kunci harus memungkinkan peran untuk melakukan `kms:Decrypt`

tindakan. Untuk jenis enkripsi sisi server lainnya, tidak ada izin atau sumber daya tambahan yang diperlukan untuk mendekripsi objek yang terpengaruh. Untuk informasi selengkapnya, lihat [Mendekripsi objek S3 yang terpengaruh](#).

- Untuk mengambil sampel data sensitif dari objek untuk akun lain, saat ini Anda harus menjadi administrator Macie yang didelegasikan untuk akun yang berlaku. Wilayah AWS Selain itu:
  - Macie saat ini harus diaktifkan untuk akun anggota di Wilayah yang berlaku.
  - Akun anggota harus memiliki peran IAM yang mendelegasikan akses lintas akun ke peran IAM di akun administrator Macie Anda. Nama peran harus sama di akun administrator Macie Anda dan akun anggota.
  - Kebijakan kepercayaan untuk peran IAM di akun anggota harus menyertakan kondisi yang menentukan ID eksternal yang benar untuk konfigurasi Anda. ID ini adalah string alfanumerik unik yang dihasilkan Macie secara otomatis setelah Anda mengonfigurasi pengaturan untuk akun administrator Macie Anda. Untuk informasi tentang penggunaan ID eksternal dalam kebijakan kepercayaan, lihat [Cara menggunakan ID eksternal saat memberikan akses ke AWS sumber daya Anda kepada pihak ketiga](#) dalam Panduan AWS Identity and Access Management Pengguna.
  - Jika peran IAM di akun anggota memenuhi semua persyaratan Macie, akun anggota tidak perlu mengonfigurasi dan mengaktifkan pengaturan Macie agar Anda dapat mengambil sampel data sensitif dari objek untuk akun mereka. Macie hanya menggunakan pengaturan dan peran IAM di akun administrator Macie Anda dan peran IAM di akun anggota.

#### Tip

Jika akun Anda adalah bagian dari organisasi besar, pertimbangkan untuk menggunakan AWS CloudFormation templat dan tumpukan yang disetel ke penyediaan dan kelola peran IAM untuk akun anggota di organisasi Anda. Untuk informasi tentang membuat dan menggunakan templat dan kumpulan tumpukan, lihat [Panduan AWS CloudFormation Pengguna](#).

Untuk meninjau dan mengunduh CloudFormation templat yang dapat berfungsi sebagai titik awal, Anda dapat menggunakan konsol Amazon Macie. Di panel navigasi di konsol, di bawah Pengaturan, pilih Reveal samples. Pilih Edit, lalu pilih Lihat izin dan CloudFormation templat peran anggota.

Topik selanjutnya di bagian ini memberikan rincian dan pertimbangan tambahan untuk setiap jenis konfigurasi. Untuk peran IAM, ini termasuk kebijakan kepercayaan dan izin untuk dilampirkan ke

peran. Jika Anda tidak yakin jenis konfigurasi mana yang terbaik untuk lingkungan Anda, mintalah bantuan AWS administrator Anda.

Menggunakan kredensi pengguna IAM untuk mengakses objek S3 yang terpengaruh

Jika Anda mengonfigurasi Amazon Macie untuk mengambil sampel data sensitif dengan menggunakan kredensial pengguna IAM, setiap pengguna akun Macie Anda menggunakan identitas IAM mereka untuk mencari, mengambil, mengenkripsi, dan mengungkapkan sampel untuk temuan individual. Ini berarti bahwa pengguna dapat mengambil dan mengungkapkan sampel data sensitif untuk temuan jika identitas IAM mereka diizinkan untuk mengakses sumber daya dan data yang diperlukan, dan melakukan tindakan yang diperlukan. Semua tindakan yang diperlukan [masuk AWS CloudTrail](#).

Untuk mengambil dan mengungkapkan sampel data sensitif untuk temuan tertentu, pengguna harus diizinkan mengakses data dan sumber daya berikut: temuan, hasil penemuan data sensitif yang sesuai, bucket S3 yang terpengaruh, dan objek S3 yang terpengaruh. Mereka juga harus diizinkan untuk menggunakan AWS KMS key yang digunakan untuk mengenkripsi objek yang terpengaruh, jika berlaku, dan AWS KMS key yang Anda konfigurasi Macie untuk digunakan untuk mengenkripsi sampel data sensitif. Jika ada kebijakan IAM, kebijakan sumber daya, atau setelan izin lainnya yang menolak akses yang diperlukan, pengguna tidak akan dapat mengambil dan mengungkapkan sampel untuk temuan tersebut.

Untuk mengatur jenis konfigurasi ini, selesaikan tugas umum berikut:

1. Verifikasi bahwa Anda mengonfigurasi repositori untuk hasil penemuan data sensitif Anda.
2. AWS KMS keyKonfigurasi yang akan digunakan untuk enkripsi sampel data sensitif.
3. Verifikasi izin Anda untuk mengonfigurasi pengaturan di Macie.
4. Konfigurasi dan aktifkan pengaturan di Macie.

Untuk informasi tentang melakukan tugas-tugas ini, lihat[Mengonfigurasi Amazon Macie untuk mengambil dan mengungkapkan sampel data sensitif dengan temuan](#).

Dengan asumsi peran IAM untuk mengakses objek S3 yang terpengaruh

Untuk mengonfigurasi Amazon Macie untuk mengambil sampel data sensitif dengan mengasumsikan peran IAM, mulailah dengan membuat peran IAM yang mendelegasikan akses ke Macie. Pastikan kebijakan kepercayaan dan izin untuk peran tersebut memenuhi semua persyaratan bagi Macie untuk mengambil peran tersebut. Ketika pengguna akun Macie Anda kemudian memilih untuk



mengambil dan mengungkapkan sampel data sensitif untuk temuan, Macie mengasumsikan peran untuk mengambil sampel dari objek S3 yang terpengaruh. Macie mengasumsikan peran hanya ketika pengguna memilih untuk mengambil dan mengungkapkan sampel untuk temuan. Untuk mengambil peran, Macie menggunakan [AssumeRole](#) operasi AWS Security Token Service (AWS STS) API. Semua tindakan yang diperlukan [masuk AWS CloudTrail](#).

Untuk mengambil dan mengungkapkan sampel data sensitif untuk temuan tertentu, pengguna harus diizinkan mengakses temuan, hasil penemuan data sensitif yang sesuai, dan AWS KMS key yang Anda konfigurasi Macie untuk digunakan untuk mengenkripsi sampel data sensitif. Peran IAM harus memungkinkan Macie mengakses bucket S3 yang terpengaruh dan objek S3 yang terpengaruh. Peran juga harus diizinkan untuk menggunakan AWS KMS key yang digunakan untuk mengenkripsi objek yang terpengaruh, jika berlaku. Jika ada kebijakan IAM, kebijakan sumber daya, atau setelan izin lainnya yang menolak akses yang diperlukan, pengguna tidak akan dapat mengambil dan mengungkapkan sampel untuk temuan tersebut.

Untuk mengatur jenis konfigurasi ini, selesaikan tugas-tugas umum berikut. Jika Anda memiliki akun anggota di suatu organisasi, bekerjalah dengan administrator Macie Anda untuk menentukan apakah dan cara mengonfigurasi pengaturan dan sumber daya untuk akun Anda.

1. Tentukan yang berikut ini:

- Nama peran IAM yang Anda ingin Macie untuk mengambil alih. Jika akun Anda adalah bagian dari organisasi, nama ini harus sama untuk akun administrator Macie yang didelegasikan dan setiap akun anggota yang berlaku di organisasi. Jika tidak, administrator Macie tidak akan dapat mengakses objek S3 yang terpengaruh untuk akun anggota yang berlaku.
- Nama kebijakan izin IAM untuk dilampirkan ke peran IAM. Jika akun Anda adalah bagian dari organisasi, kami sarankan Anda menggunakan nama kebijakan yang sama untuk setiap akun anggota yang berlaku di organisasi. Ini dapat merampingkan penyediaan dan pengelolaan peran dalam akun anggota.

2. Verifikasi bahwa Anda mengonfigurasi repositori untuk hasil penemuan data sensitif Anda.

3. AWS KMS key Konfigurasi yang akan digunakan untuk enkripsi sampel data sensitif.

4. Verifikasi izin Anda untuk membuat peran IAM dan mengonfigurasi pengaturan di Macie.

5. Jika Anda adalah administrator Macie yang didelegasikan untuk suatu organisasi atau Anda memiliki akun Macie mandiri:

- a. Buat dan konfigurasi peran IAM untuk akun Anda. Pastikan kebijakan kepercayaan dan izin untuk peran tersebut memenuhi semua persyaratan bagi Macie untuk mengambil peran tersebut. Untuk detail tentang persyaratan ini, lihat [topik berikutnya](#).



- b. Konfigurasi dan aktifkan pengaturan di Macie. Macie kemudian menghasilkan ID eksternal untuk konfigurasi. Jika Anda administrator Macie untuk suatu organisasi, perhatikan ID ini. Kebijakan kepercayaan untuk peran IAM di setiap akun anggota Anda yang berlaku harus menentukan ID ini.
6. Jika Anda memiliki akun anggota di suatu organisasi:
- a. Minta administrator Macie Anda untuk ID eksternal untuk menentukan dalam kebijakan kepercayaan untuk peran IAM di akun Anda. Juga verifikasi nama peran IAM dan kebijakan izin yang akan dibuat.
  - b. Buat dan konfigurasi peran IAM untuk akun Anda. Pastikan kebijakan kepercayaan dan izin untuk peran tersebut memenuhi semua persyaratan bagi administrator Macie Anda untuk mengambil peran tersebut. Untuk detail tentang persyaratan ini, lihat [topik berikutnya](#).
  - c. (Opsional) Jika Anda ingin mengambil dan mengungkapkan sampel data sensitif dari objek S3 yang terpengaruh untuk akun Anda sendiri, konfigurasi dan aktifkan pengaturan di Macie. Jika Anda ingin Macie mengambil peran IAM untuk mengambil sampel, mulailah dengan membuat dan mengonfigurasi peran IAM tambahan di akun Anda. Pastikan kebijakan kepercayaan dan izin untuk peran tambahan ini memenuhi semua persyaratan bagi Macie untuk mengambil peran tersebut. Kemudian konfigurasi pengaturan di Macie dan tentukan nama peran tambahan ini. Untuk detail tentang persyaratan kebijakan untuk peran tersebut, lihat [topik berikutnya](#).

Untuk informasi tentang melakukan tugas-tugas ini, lihat [Mengonfigurasi Amazon Macie untuk mengambil dan mengungkapkan sampel data sensitif dengan temuan](#).

Mengonfigurasi peran IAM untuk mengakses objek S3 yang terpengaruh

Untuk mengakses objek S3 yang terpengaruh dengan menggunakan peran IAM, mulailah dengan membuat dan mengonfigurasi peran yang mendelegasikan akses ke Amazon Macie. Pastikan kebijakan kepercayaan dan izin untuk peran tersebut memenuhi semua persyaratan bagi Macie untuk mengambil peran tersebut. Bagaimana Anda melakukan ini tergantung pada jenis akun Macie yang Anda miliki.

Bagian berikut memberikan rincian tentang kebijakan kepercayaan dan izin untuk dilampirkan ke peran IAM untuk setiap jenis akun Macie. Pilih bagian untuk jenis akun yang Anda miliki.

**Note**

Jika Anda memiliki akun anggota di organisasi, Anda mungkin perlu membuat dan mengonfigurasi dua peran IAM untuk akun Anda:

- Untuk memungkinkan administrator Macie mengambil dan mengungkapkan sampel data sensitif dari objek S3 yang terpengaruh untuk akun Anda, buat dan konfigurasi peran yang dapat diasumsikan oleh akun administrator Anda. Untuk detail ini, pilih bagian akun anggota Macie.
- Untuk mengambil dan mengungkapkan sampel data sensitif dari objek S3 yang terpengaruh untuk akun Anda sendiri, buat dan konfigurasi peran yang dapat diasumsikan oleh Macie. Untuk detail ini, pilih bagian akun Standalone Macie.

Sebelum Anda membuat dan mengonfigurasi peran IAM, bekerjalah dengan administrator Macie Anda untuk menentukan konfigurasi yang sesuai untuk akun Anda.

Untuk informasi mendetail tentang penggunaan IAM untuk membuat peran, lihat [Membuat peran menggunakan kebijakan kepercayaan khusus](#) di Panduan AWS Identity and Access Management Pengguna.

### Akun administrator Macie

Jika Anda adalah administrator Macie yang didelegasikan untuk organisasi, mulailah dengan menggunakan editor kebijakan IAM untuk membuat kebijakan izin untuk peran IAM. Kebijakan tersebut harus sebagai berikut.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "RetrieveS3Objects",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject"
      ],
      "Resource": [
        "*"
      ]
    }
  ],
}
```

```

    {
      "Sid": "AssumeMacieRevealRoleForCrossAccountAccess",
      "Effect": "Allow",
      "Action": [
        "sts:AssumeRole"
      ],
      "Resource": "arn:aws:iam::*:role/IAMRoleName"
    }
  ]
}

```

Di mana *IAM RoleName* adalah nama peran IAM untuk diasumsikan oleh Macie saat mengambil sampel data sensitif dari objek S3 yang terpengaruh untuk akun organisasi Anda. Ganti nilai ini dengan nama peran yang Anda buat untuk akun Anda, dan rencanakan untuk membuat akun anggota yang berlaku di organisasi Anda. Nama ini harus sama untuk akun administrator Macie Anda dan setiap akun anggota yang berlaku.

#### Note

Dalam kebijakan izin sebelumnya, Resource elemen dalam pernyataan pertama menggunakan karakter wildcard (\*). Hal ini memungkinkan entitas IAM terlampir untuk mengambil objek dari semua bucket S3 yang dimiliki organisasi Anda. Untuk mengizinkan akses ini hanya untuk bucket tertentu, ganti karakter wildcard dengan Amazon Resource Name (ARN) dari setiap bucket. Misalnya, untuk mengizinkan akses hanya ke objek dalam bucket bernama DOC-EXAMPLE-BUCKET, ubah elemen menjadi:

```
"Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
```

Anda juga dapat membatasi akses ke objek dalam bucket S3 tertentu untuk masing-masing akun. Untuk melakukannya, tentukan ARN bucket dalam Resource elemen kebijakan izin untuk peran IAM di setiap akun yang berlaku. Untuk informasi dan contoh selengkapnya, lihat [elemen kebijakan IAM JSON: Sumber daya](#) di AWS Identity and Access ManagementPanduan Pengguna.

Setelah Anda membuat kebijakan izin untuk peran IAM, buat dan konfigurasi peran tersebut. Jika Anda melakukannya dengan menggunakan konsol IAM, pilih Kebijakan kepercayaan khusus sebagai jenis entitas tepercaya untuk peran tersebut. Untuk kebijakan kepercayaan yang mendefinisikan entitas tepercaya untuk peran tersebut, tentukan hal berikut.

```
{
```

```
"Version": "2012-10-17",
"Statement": [
  {
    "Sid": "AllowMacieReveal",
    "Effect": "Allow",
    "Principal": {
      "Service": "reveal-samples.macie.amazonaws.com"
    },
    "Action": "sts:AssumeRole",
    "Condition": {
      "StringEquals": {
        "aws:SourceAccount": "accountID"
      }
    }
  }
]
```

Dimana *AccountID* adalah ID akun untuk Anda. Akun AWS Ganti nilai ini dengan ID akun 12 digit Anda.

Dalam kebijakan kepercayaan sebelumnya:

- **Principal** Elemen menentukan prinsip layanan yang digunakan Macie saat mengambil sampel data sensitif dari objek S3 yang terpengaruh, `reveal-samples.macie.amazonaws.com`
- **Action** Elemen menentukan tindakan yang diizinkan untuk dilakukan oleh prinsipal layanan, [AssumeRole](#) pengoperasian AWS Security Token Service (AWS STS) API.
- **Condition** Elemen mendefinisikan kondisi yang menggunakan [aws: SourceAccount](#) global condition context key. Kondisi ini menentukan akun mana yang dapat melakukan tindakan yang ditentukan. Dalam hal ini, memungkinkan Macie untuk mengambil peran hanya untuk akun yang ditentukan (*accountID*). Kondisi ini membantu mencegah Macie digunakan sebagai [wakil yang bingung](#) selama transaksi dengan AWS STS.

Setelah Anda menentukan kebijakan kepercayaan untuk peran IAM, lampirkan kebijakan izin ke peran tersebut. Ini harus menjadi kebijakan izin yang Anda buat sebelum Anda mulai membuat peran. Kemudian selesaikan langkah-langkah yang tersisa di IAM untuk menyelesaikan pembuatan dan konfigurasi peran. Setelah selesai, [konfigurasi dan aktifkan pengaturan di Macie](#).

## Akun anggota Macie

Jika Anda memiliki akun anggota Macie dan Anda ingin mengizinkan administrator Macie untuk mengambil dan mengungkapkan sampel data sensitif dari objek S3 yang terpengaruh untuk akun Anda, mulailah dengan meminta administrator Macie Anda untuk informasi berikut:

- Nama peran IAM untuk dibuat. Nama harus sama untuk akun Anda dan akun administrator Macie untuk organisasi Anda.
- Nama kebijakan izin IAM untuk dilampirkan ke peran.
- ID eksternal yang akan ditentukan dalam kebijakan kepercayaan untuk peran tersebut. ID ini harus berupa ID eksternal yang dihasilkan Macie untuk konfigurasi administrator Macie Anda.

Setelah Anda menerima informasi ini, gunakan editor kebijakan IAM untuk membuat kebijakan izin untuk peran tersebut. Kebijakan tersebut harus sebagai berikut.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "RetrieveS3Objects",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

Kebijakan izin sebelumnya memungkinkan entitas IAM terlampir untuk mengambil objek dari semua bucket S3 untuk akun Anda. Ini karena Resource elemen dalam kebijakan menggunakan karakter wildcard (\*). Untuk mengizinkan akses ini hanya untuk bucket tertentu, ganti karakter wildcard dengan Amazon Resource Name (ARN) dari setiap bucket. Misalnya, untuk mengizinkan akses hanya ke objek dalam bucket bernama DOC-EXAMPLE-BUCKET2, ubah elemen menjadi:

```
"Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET2/*"
```

Untuk informasi dan contoh selengkapnya, lihat [elemen kebijakan IAM JSON: Sumber daya](#) di AWS Identity and Access Management Panduan Pengguna.

Setelah Anda membuat kebijakan izin untuk peran IAM, buat peran tersebut. Jika Anda membuat peran menggunakan konsol IAM, pilih Kebijakan kepercayaan khusus sebagai jenis entitas tepercaya untuk peran tersebut. Untuk kebijakan kepercayaan yang mendefinisikan entitas tepercaya untuk peran tersebut, tentukan hal berikut.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowMacieAdminRevealRoleForCrossAccountAccess",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::administratorAccountID:role/IAMRoleName"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "sts:ExternalId": "externalID",
          "aws:PrincipalOrgID": "${aws:ResourceOrgID}"
        }
      }
    }
  ]
}
```

Dalam kebijakan sebelumnya, ganti nilai placeholder dengan nilai yang benar untuk lingkungan Anda AWS, di mana:

- *AdministratorAccountID* adalah ID akun 12 digit untuk akun administrator Macie Anda.
- *IAM RoleName* adalah nama peran IAM di akun administrator Macie Anda. Itu harus menjadi nama yang Anda terima dari administrator Macie Anda.
- *ExternalID* adalah ID eksternal yang Anda terima dari administrator Macie Anda.

Secara umum, kebijakan kepercayaan memungkinkan administrator Macie Anda untuk mengambil peran untuk mengambil dan mengungkapkan sampel data sensitif dari objek S3 yang terpengaruh untuk akun Anda. `Principal` Elemen menentukan ARN peran IAM di akun administrator Macie Anda. Ini adalah peran yang digunakan administrator Macie Anda untuk mengambil dan

mengungkapkan sampel data sensitif untuk akun organisasi Anda. `ConditionBlok` mendefinisikan dua kondisi yang selanjutnya menentukan siapa yang dapat mengambil peran:

- Kondisi pertama menentukan ID eksternal yang unik untuk konfigurasi organisasi Anda. Untuk mempelajari lebih lanjut tentang ID eksternal, lihat [Cara menggunakan ID eksternal saat memberikan akses ke AWS sumber daya Anda kepada pihak ketiga](#) dalam Panduan AWS Identity and Access Management Pengguna.
- Kondisi kedua menggunakan kunci konteks kondisi global `aws: PrincipalOrg ID`. Nilai untuk kunci adalah variabel dinamis yang mewakili pengidentifikasi unik untuk organisasi di AWS Organizations (`${aws:ResourceOrgID}`). Kondisi ini membatasi akses hanya ke akun-akun yang merupakan bagian dari organisasi yang sama di AWS Organizations. Jika Anda bergabung dengan organisasi Anda dengan menerima undangan di Macie, hapus ketentuan ini dari kebijakan.

Setelah Anda menentukan kebijakan kepercayaan untuk peran IAM, lampirkan kebijakan izin ke peran tersebut. Ini harus menjadi kebijakan izin yang Anda buat sebelum Anda mulai membuat peran. Kemudian selesaikan langkah-langkah yang tersisa di IAM untuk menyelesaikan pembuatan dan konfigurasi peran. Jangan mengkonfigurasi dan memasukkan pengaturan untuk peran di Macie.

### Akun Macie mandiri

Jika Anda memiliki akun Macie mandiri atau akun anggota Macie dan Anda ingin mengambil dan mengungkapkan sampel data sensitif dari objek S3 yang terpengaruh untuk akun Anda sendiri, mulailah dengan menggunakan editor kebijakan IAM untuk membuat kebijakan izin untuk peran IAM. Kebijakan tersebut harus sebagai berikut.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "RetrieveS3Objects",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

```
}
```

Dalam kebijakan izin sebelumnya, Resource elemen menggunakan karakter wildcard (\*). Hal ini memungkinkan entitas IAM terlampir untuk mengambil objek dari semua bucket S3 untuk akun Anda. Untuk mengizinkan akses ini hanya untuk bucket tertentu, ganti karakter wildcard dengan Amazon Resource Name (ARN) dari setiap bucket. Misalnya, untuk mengizinkan akses hanya ke objek dalam bucket bernama DOC-EXAMPLE-BUCKET3, ubah elemen menjadi:

```
"Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET3/*"
```

Untuk informasi dan contoh selengkapnya, lihat [elemen kebijakan IAM JSON: Sumber daya](#) di AWS Identity and Access Management Panduan Pengguna.

Setelah Anda membuat kebijakan izin untuk peran IAM, buat peran tersebut. Jika Anda membuat peran menggunakan konsol IAM, pilih Kebijakan kepercayaan khusus sebagai jenis entitas tepercaya untuk peran tersebut. Untuk kebijakan kepercayaan yang mendefinisikan entitas tepercaya untuk peran tersebut, tentukan hal berikut.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowMacieReveal",
      "Effect": "Allow",
      "Principal": {
        "Service": "reveal-samples.macie.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "accountID"
        }
      }
    }
  ]
}
```

Dimana *AccountID* adalah ID akun untuk Anda. Akun AWS Ganti nilai ini dengan ID akun 12 digit Anda.

Dalam kebijakan kepercayaan sebelumnya:



- `PrincipalElemen` menentukan prinsip layanan yang digunakan Macie saat mengambil dan mengungkapkan sampel data sensitif dari objek S3 yang terpengaruh, `reveal-samples.macie.amazonaws.com`
- `ActionElemen` menentukan tindakan yang diizinkan untuk dilakukan oleh prinsipal layanan, [AssumeRole](#) pengoperasian AWS Security Token Service (AWS STS) API.
- `ConditionElemen` mendefinisikan kondisi yang menggunakan [aws: SourceAccount](#) global condition context key. Kondisi ini menentukan akun mana yang dapat melakukan tindakan yang ditentukan. Hal ini memungkinkan Macie untuk mengambil peran hanya untuk akun tertentu (`accountID`). Kondisi ini membantu mencegah Macie digunakan sebagai [wakil yang bingung](#) selama transaksi dengan AWS STS.

Setelah Anda menentukan kebijakan kepercayaan untuk peran IAM, lampirkan kebijakan izin ke peran tersebut. Ini harus menjadi kebijakan izin yang Anda buat sebelum Anda mulai membuat peran. Kemudian selesaikan langkah-langkah yang tersisa di IAM untuk menyelesaikan pembuatan dan konfigurasi peran. Setelah selesai, [konfigurasi dan aktifkan pengaturan di Macie](#).

### Mendekripsi objek S3 yang terpengaruh

Amazon S3 mendukung beberapa opsi enkripsi untuk objek S3. Untuk sebagian besar opsi ini, tidak ada sumber daya tambahan atau izin yang diperlukan untuk pengguna IAM atau peran untuk mendekripsi dan mengambil sampel data sensitif dari objek yang terpengaruh. Ini adalah kasus untuk objek yang dienkripsi menggunakan enkripsi sisi server dengan kunci terkelola Amazon S3 atau terkelola. AWS KMS key

Namun, jika objek S3 dienkripsi dengan pelanggan yang dikelola AWS KMS key, izin tambahan diperlukan untuk mendekripsi dan mengambil sampel data sensitif dari objek. Lebih khusus lagi, kebijakan kunci untuk kunci KMS harus memungkinkan pengguna atau peran IAM untuk melakukan tindakan. `kms:Decrypt` Jika tidak, kesalahan terjadi dan Macie tidak mengambil sampel apa pun dari objek. Untuk mempelajari cara menyediakan akses ini bagi pengguna IAM, lihat [Otentikasi dan kontrol akses AWS KMS](#) di Panduan AWS Key Management Service Pengembang.

Cara menyediakan akses ini untuk peran IAM tergantung pada apakah akun yang memiliki AWS KMS key juga memiliki peran tersebut:

- Jika akun yang sama memiliki kunci KMS dan peran, pengguna akun harus memperbarui kebijakan kunci.
- Jika satu akun memiliki kunci KMS dan akun yang berbeda memiliki peran tersebut, pengguna akun yang memiliki kunci harus mengizinkan akses lintas akun ke kunci tersebut.

Topik ini menjelaskan cara melakukan tugas ini untuk peran IAM yang Anda buat untuk mengambil sampel data sensitif dari objek S3. Ini juga memberikan contoh untuk kedua skenario. Untuk informasi tentang mengizinkan akses ke pelanggan yang dikelola AWS KMS keys untuk skenario lain, lihat [Otentikasi dan kontrol akses untuk AWS KMS](#) di Panduan AWS Key Management Service Pengembang.

Mengizinkan akses akun yang sama ke kunci yang dikelola pelanggan

Jika akun yang sama memiliki peran AWS KMS key dan IAM, pengguna akun harus menambahkan pernyataan ke kebijakan kunci. Pernyataan tambahan harus memungkinkan peran IAM untuk mendekripsi data dengan menggunakan kunci. Untuk informasi detail tentang pembaruan kebijakan kunci, lihat [Mengganti kebijakan kunci](#) dalam Panduan Developer AWS Key Management Service.

Dalam pernyataan:

- `PrincipalElement` harus menentukan Nama Sumber Daya Amazon (ARN) dari peran IAM.
- Array `Action` harus menentukan tindakan `kms:Decrypt`. Ini adalah satu-satunya AWS KMS tindakan yang peran IAM harus diizinkan untuk melakukan dekripsi objek yang dienkripsi dengan kunci.

Berikut ini adalah contoh pernyataan untuk ditambahkan ke kebijakan untuk kunci KMS.

```
{
  "Sid": "Allow the Macie reveal role to use the key",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::123456789012:role/IAMRoleName"
  },
  "Action": [
    "kms:Decrypt"
  ],
  "Resource": "*"
}
```

Dalam contoh sebelumnya:

- `AWSBidang` dalam `Principal` elemen menentukan ARN dari peran IAM dalam akun. Hal ini memungkinkan peran untuk melakukan tindakan yang ditentukan oleh pernyataan kebijakan. *123456789012* adalah contoh ID akun. Ganti nilai ini dengan ID akun untuk akun yang memiliki

peran dan kunci KMS. *IAM RoleName* adalah nama contoh. Ganti nilai ini dengan nama peran IAM di akun.

- `ActionArray` menentukan tindakan yang diizinkan untuk dilakukan oleh peran IAM menggunakan kunci KMS — mendekripsi ciphertext yang dienkripsi dengan kunci.

Tempat Anda menambahkan pernyataan ini ke kebijakan kunci bergantung pada struktur dan elemen yang saat ini berisi kebijakan. Ketika Anda menambahkan pernyataan, pastikan bahwa sintaksnya valid. Kebijakan kunci menggunakan format JSON. Ini berarti bahwa Anda juga harus menambahkan koma sebelum atau setelah pernyataan, tergantung pada tempat Anda menambahkan pernyataan ke kebijakan.

Mengizinkan akses lintas akun ke kunci yang dikelola pelanggan

Jika satu akun memiliki AWS KMS key (pemilik kunci) dan akun yang berbeda memiliki peran IAM (pemilik peran), pemilik kunci harus memberi pemilik peran akses lintas akun ke kunci tersebut. Salah satu cara untuk melakukannya adalah dengan menggunakan hibah. Hibah adalah instrumen kebijakan yang memungkinkan AWS prinsipal untuk menggunakan kunci KMS dalam operasi kriptografi jika kondisi yang ditentukan oleh hibah terpenuhi. Untuk mempelajari tentang hibah, lihat [Hibah AWS KMS di Panduan AWS Key Management Service](#) Pengembang.

Dengan pendekatan ini, pemilik kunci pertama-tama memastikan bahwa kebijakan kunci memungkinkan pemilik peran untuk membuat hibah untuk kunci tersebut. Pemilik peran kemudian membuat hibah untuk kunci tersebut. Hibah tersebut mendelegasikan izin yang relevan ke peran IAM di akun mereka. Hal ini memungkinkan peran untuk mendekripsi objek S3 yang dienkripsi dengan kunci.

Langkah 1: Perbarui kebijakan utama

Dalam kebijakan kunci, pemilik kunci harus memastikan bahwa kebijakan tersebut menyertakan pernyataan yang memungkinkan pemilik peran untuk membuat hibah untuk peran IAM di akun mereka (pemilik peran). Dalam pernyataan ini, `Principal` elemen harus menentukan ARN dari akun pemilik peran. Array `Action` harus menentukan tindakan `kms:CreateGrant`. Sebuah `Condition` blok dapat memfilter akses ke tindakan yang ditentukan. Berikut ini adalah contoh pernyataan ini dalam kebijakan untuk kunci KMS.

```
{
  "Sid": "Allow a role in an account to create a grant",
  "Effect": "Allow",
```

```
"Principal": {
  "AWS": "arn:aws:iam::111122223333:root"
},
"Action": [
  "kms:CreateGrant"
],
"Resource": "*",
"Condition": {
  "StringEquals": {
    "kms:GranteePrincipal": "arn:aws:iam::111122223333:role/IAMRoleName"
  },
  "ForAllValues:StringEquals": {
    "kms:GrantOperations": "Decrypt"
  }
}
}
```

Dalam contoh sebelumnya:

- `AWSBidang` dalam `Principal` elemen menentukan ARN dari akun pemilik peran. Ini memungkinkan akun untuk melakukan tindakan yang ditentukan oleh pernyataan kebijakan. **111122223333** adalah contoh ID akun. Ganti nilai ini dengan ID akun untuk akun pemilik peran.
- `ActionArray` menentukan tindakan yang diizinkan oleh pemilik peran pada kunci KMS—buat hibah untuk kunci tersebut.
- `ConditionBlok` menggunakan [operator kondisi](#) dan kunci kondisi berikut untuk memfilter akses ke tindakan yang diizinkan dilakukan oleh pemilik peran pada kunci KMS:
  - [kms: GranteePrincipal](#) — Kondisi ini memungkinkan pemilik peran untuk membuat hibah hanya untuk pokok penerima hibah yang ditentukan, yang merupakan ARN dari peran IAM di akun mereka. Dalam ARN itu, **111122223333** adalah contoh ID akun. Ganti nilai ini dengan ID akun untuk akun pemilik peran. *IAM RoleName* adalah nama contoh. Ganti nilai ini dengan nama peran IAM di akun pemilik peran.
  - [kms: GrantOperations](#) — Kondisi ini memungkinkan pemilik peran untuk membuat hibah hanya untuk mendelegasikan izin untuk melakukan AWS KMS Decrypt tindakan (mendekripsi ciphertext yang dienkripsi dengan kunci). Ini mencegah pemilik peran membuat hibah yang mendelegasikan izin untuk melakukan tindakan lain pada kunci KMS. DecryptTindakan adalah satu-satunya AWS KMS tindakan yang harus diizinkan untuk dilakukan peran IAM untuk mendekripsi objek yang dienkripsi dengan kunci.

Di mana pemilik kunci menambahkan pernyataan ini ke kebijakan kunci tergantung pada struktur dan elemen yang saat ini terkandung dalam kebijakan tersebut. Ketika pemilik kunci menambahkan pernyataan, mereka harus memastikan bahwa sintaksnya valid. Kebijakan kunci menggunakan format JSON. Ini berarti bahwa pemilik kunci juga harus menambahkan koma sebelum atau setelah pernyataan, tergantung pada tempat mereka menambahkan pernyataan ke kebijakan. Untuk informasi detail tentang pembaruan kebijakan kunci, lihat [Mengganti kebijakan kunci](#) dalam Panduan Developer AWS Key Management Service.

## Langkah 2: Buat hibah

Setelah pemilik kunci memperbarui kebijakan kunci seperlunya, pemilik peran membuat hibah untuk kunci tersebut. Hibah mendelegasikan izin yang relevan ke peran IAM di akun mereka (pemilik peran). Sebelum pemilik peran membuat hibah, mereka harus memverifikasi bahwa mereka diizinkan untuk melakukan `kms:CreateGrant` tindakan. Tindakan ini memungkinkan mereka untuk menambahkan hibah ke pelanggan yang sudah ada dan dikelola AWS KMS key.

Untuk membuat hibah, pemilik peran dapat menggunakan [CreateGrant](#) pengoperasian AWS Key Management Service API. Saat pemilik peran membuat hibah, mereka harus menentukan nilai berikut untuk parameter yang diperlukan:

- **KeyId**— ARN dari kunci KMS. Untuk akses lintas akun ke kunci KMS, nilai ini harus berupa ARN. Tidak bisa menggunakan kunci ID.
- **GranteePrincipal**— ARN dari peran IAM dalam akun mereka. Nilai ini seharusnya `arn:aws:iam::111122223333:role/IAMRoleName`, di mana `111122223333` adalah ID akun untuk akun pemilik peran dan `IAM RoleName` adalah nama peran.
- **Operations**— Tindakan AWS KMS dekripsi (`Decrypt`). Ini adalah satu-satunya AWS KMS tindakan yang peran IAM harus diizinkan untuk melakukan dekripsi objek yang dienkripsi dengan kunci KMS.

Jika pemilik peran menggunakan AWS Command Line Interface (AWS CLI), mereka dapat menjalankan perintah [create-grant](#) untuk membuat hibah. Contoh berikut menunjukkan cara melakukannya. Contoh ini diformat untuk Microsoft Windows dan menggunakan karakter kelanjutan baris caret (^) untuk meningkatkan keterbacaan.

```
C:\> aws kms create-grant ^
--key-id arn:aws:kms:us-east-1:123456789012:key/1234abcd-12ab-34cd-56ef-1234567890ab ^
--grantee-principal arn:aws:iam::111122223333:role/IAMRoleName ^
--operations "Decrypt"
```

Di mana:

- `key-id` menentukan ARN dari kunci KMS untuk menerapkan hibah ke.
- `grantee-principal` menentukan ARN dari peran IAM yang diizinkan untuk melakukan tindakan yang ditentukan oleh hibah. Nilai ini harus sesuai dengan ARN yang ditentukan oleh `kms:GranteePrincipal` kondisi dalam kebijakan kunci.
- `operations` menentukan tindakan bahwa hibah memungkinkan prinsipal yang ditentukan untuk melakukan—mendekripsi `ciphertext` yang dienkripsi dengan kunci.

Jika perintah berjalan dengan berhasil, Anda menerima output yang mirip dengan berikut ini.

```
{
  "GrantToken": "<grant token>",
  "GrantId": "1a2b3c4d2f5e69f440bae30eaec9570bb1fb7358824f9ddfa1aa5a0dab1a59b2"
}
```

Yang mana `GrantToken` merupakan string yang unik, non-rahasia, variabel-panjang, base64-encoded yang mewakili hibah yang diciptakan, dan `GrantId` adalah pengidentifikasi unik untuk hibah.

## Mengonfigurasi Amazon Macie untuk mengambil dan mengungkapkan sampel data sensitif dengan temuan

Anda dapat mengonfigurasi dan menggunakan Amazon Macie secara opsional untuk mengambil dan mengungkapkan sampel data sensitif yang dilaporkan Macie dalam temuan data sensitif individual. Sampel dapat membantu Anda memverifikasi sifat data sensitif yang ditemukan Macie. Mereka juga dapat membantu Anda menyesuaikan penyelidikan Anda terhadap objek dan bucket Amazon Simple Storage Service (Amazon S3) yang terpengaruh. Anda dapat mengambil dan mengungkapkan sampel data sensitif di semua Wilayah AWS tempat Macie saat ini tersedia kecuali Wilayah Asia Pasifik (Osaka) dan Israel (Tel Aviv).

Saat Anda mengambil dan mengungkapkan sampel data sensitif untuk sebuah temuan, Macie menggunakan data dalam hasil penemuan data sensitif yang sesuai untuk menemukan kejadian data sensitif di objek S3 yang terpengaruh. Macie kemudian mengekstrak sampel kejadian tersebut dari objek yang terpengaruh. Macie mengenkripsi data yang diekstrak dengan kunci AWS Key Management Service (AWS KMS) yang Anda tentukan, menyimpan sementara data terenkripsi dalam cache, dan mengembalikan data dalam hasil Anda untuk temuan tersebut. Segera setelah

ekstraksi dan enkripsi, Macie secara permanen menghapus data dari cache kecuali retensi tambahan sementara diperlukan untuk menyelesaikan masalah operasional.

Untuk mengambil dan mengungkapkan sampel data sensitif untuk temuan, Anda harus terlebih dahulu mengonfigurasi dan mengaktifkan pengaturan untuk akun Macie Anda. Anda juga perlu mengonfigurasi sumber daya dan izin pendukung untuk akun Anda. Topik di bagian ini memandu Anda melalui proses konfigurasi Macie untuk mengambil dan mengungkapkan sampel data sensitif, dan mengelola status konfigurasi untuk akun Anda.

## Topik

- [Sebelum Anda memulai](#)
- [Mengonfigurasi dan mengaktifkan pengaturan Amazon Macie](#)
- [Menonaktifkan pengaturan Amazon Macie](#)

### Tip

Untuk rekomendasi dan contoh kebijakan yang mungkin Anda gunakan untuk mengontrol akses ke fungsionalitas ini, lihat [Cara menggunakan Amazon Macie untuk melihat pratinjau data sensitif di bucket S3](#) postingan blog di Blog Keamanan. AWS

## Sebelum Anda memulai

Sebelum Anda mengonfigurasi Amazon Macie untuk mengambil dan mengungkapkan sampel data sensitif untuk temuan, selesaikan tugas berikut untuk memastikan bahwa Anda memiliki sumber daya dan izin yang Anda butuhkan.

## Tugas

- [Langkah 1: Konfigurasi repositori untuk hasil penemuan data sensitif](#)
- [Langkah 2: Tentukan cara mengakses objek S3 yang terpengaruh](#)
- [Langkah 3: Konfigurasi AWS KMS key](#)
- [Langkah 4: Verifikasi izin Anda](#)

Tugas-tugas ini bersifat opsional jika Anda sudah mengonfigurasi Macie untuk mengambil dan mengungkapkan sampel data sensitif dan hanya ingin mengubah pengaturan konfigurasi Anda.

## Langkah 1: Konfigurasi repositori untuk hasil penemuan data sensitif

Saat Anda mengambil dan mengungkapkan sampel data sensitif untuk sebuah temuan, Macie menggunakan data dalam hasil penemuan data sensitif yang sesuai untuk menemukan kejadian data sensitif di objek S3 yang terpengaruh. Oleh karena itu, penting untuk memverifikasi bahwa Anda mengonfigurasi repositori untuk hasil penemuan data sensitif Anda. Jika tidak, Macie tidak akan dapat menemukan sampel data sensitif yang ingin Anda ambil dan ungkapkan.

Untuk menentukan apakah Anda telah mengonfigurasi repositori ini untuk akun Anda, Anda dapat menggunakan konsol Amazon Macie: pilih Hasil penemuan (di bawah Pengaturan) di panel navigasi. Untuk melakukan ini secara terprogram, gunakan [GetClassificationExportConfiguration](#) pengoperasian Amazon Macie API. Untuk mempelajari lebih lanjut tentang hasil penemuan data sensitif dan cara mengonfigurasi repositori ini, lihat [Menyimpan dan mempertahankan hasil penemuan data sensitif](#)

## Langkah 2: Tentukan cara mengakses objek S3 yang terpengaruh

Untuk mengakses objek S3 yang terpengaruh dan mengambil sampel data sensitif darinya, Anda memiliki dua opsi. Anda dapat mengonfigurasi Macie untuk menggunakan kredensial pengguna AWS Identity and Access Management (IAM) Anda. Atau Anda dapat mengonfigurasi Macie untuk mengambil peran IAM yang mendelegasikan akses ke Macie. Anda dapat menggunakan konfigurasi dengan semua jenis akun Macie—akun administrator Macie yang didelegasikan untuk organisasi, akun anggota Macie di organisasi, atau akun Macie mandiri. Sebelum Anda mengonfigurasi pengaturan di Macie, tentukan metode akses mana yang ingin Anda gunakan. Untuk detail tentang opsi dan persyaratan untuk setiap metode, lihat [Opsi konfigurasi dan persyaratan untuk mengambil sampel data sensitif dengan temuan](#).

Jika Anda berencana untuk menggunakan peran IAM, buat dan konfigurasi peran tersebut sebelum Anda mengonfigurasi pengaturan di Macie. Pastikan juga bahwa kebijakan kepercayaan dan izin untuk peran tersebut memenuhi semua persyaratan bagi Macie untuk mengambil peran tersebut. Jika akun Anda adalah bagian dari organisasi yang mengelola beberapa akun Macie secara terpusat, bekerjalah dengan administrator Macie Anda untuk terlebih dahulu menentukan apakah dan cara mengonfigurasi peran untuk akun Anda.

## Langkah 3: Konfigurasi AWS KMS key

Saat Anda mengambil dan mengungkapkan sampel data sensitif untuk temuan, Macie mengenkripsi sampel dengan kunci AWS Key Management Service (AWS KMS) yang Anda tentukan. Oleh karena itu, Anda perlu menentukan mana yang ingin AWS KMS key Anda gunakan untuk mengenkripsi sampel. Kuncinya dapat berupa kunci KMS yang ada dari akun Anda sendiri, atau kunci KMS yang



ada yang dimiliki akun lain. Jika Anda ingin menggunakan kunci yang dimiliki akun lain, dapatkan Nama Sumber Daya Amazon (ARN) dari kunci tersebut. Anda harus menentukan ARN ini ketika Anda memasukkan pengaturan konfigurasi di Macie.

Kunci KMS harus berupa kunci enkripsi simetris yang dikelola pelanggan. Ini juga harus berupa kunci wilayah Tunggal yang diaktifkan Wilayah AWS sama dengan akun Macie Anda. Kunci KMS dapat berada di toko kunci eksternal. Namun, kuncinya mungkin lebih lambat dan kurang dapat diandalkan daripada kunci yang dikelola sepenuhnya di dalam AWS KMS. Jika latensi atau masalah ketersediaan mencegah Macie mengenkripsi sampel data sensitif yang ingin Anda ambil dan ungkapkan, kesalahan terjadi dan Macie tidak mengembalikan sampel apa pun untuk temuan tersebut.

Selain itu, kebijakan kunci untuk kunci harus mengizinkan prinsipal yang sesuai (peran IAM, pengguna IAM, atau Akun AWS) untuk melakukan tindakan berikut:

- `kms:Decrypt`
- `kms:DescribeKey`
- `kms:GenerateDataKey`

#### Important

Sebagai lapisan tambahan kontrol akses, kami menyarankan Anda membuat kunci KMS khusus untuk enkripsi sampel data sensitif yang diambil, dan membatasi penggunaan kunci hanya untuk prinsipal yang harus diizinkan untuk mengambil dan mengungkapkan sampel data sensitif. Jika pengguna tidak diizinkan untuk melakukan tindakan sebelumnya untuk kunci, Macie menolak permintaan mereka untuk mengambil dan mengungkapkan sampel data sensitif. Macie tidak mengembalikan sampel apa pun untuk temuan itu.

Untuk informasi tentang membuat dan mengonfigurasi kunci KMS, lihat [Mengelola kunci](#) di Panduan AWS Key Management Service Pengembang. Untuk informasi tentang penggunaan kebijakan utama untuk mengelola akses ke kunci KMS, lihat [Kebijakan utama AWS KMS di](#) Panduan AWS Key Management Service Pengembang.

#### Langkah 4: Verifikasi izin Anda

Sebelum Anda mengonfigurasi pengaturan di Macie, verifikasi juga bahwa Anda memiliki izin yang Anda butuhkan. Untuk memverifikasi izin Anda, gunakan AWS Identity and Access Management

(IAM) untuk meninjau kebijakan IAM yang dilampirkan pada identitas IAM Anda. Kemudian bandingkan informasi dalam kebijakan tersebut dengan daftar tindakan berikut yang harus Anda lakukan.

## Amazon Macie

Untuk Macie, verifikasi bahwa Anda diizinkan untuk melakukan tindakan berikut:

- `macie2:GetMacieSession`
- `macie2:UpdateRevealConfiguration`

Tindakan pertama memungkinkan Anda mengakses akun Macie Anda. Tindakan kedua memungkinkan Anda mengubah pengaturan konfigurasi untuk mengambil dan mengungkapkan sampel data sensitif. Ini termasuk mengaktifkan dan menonaktifkan konfigurasi untuk akun Anda.

Secara opsional, verifikasi bahwa Anda juga diizinkan untuk melakukan `macie2:GetRevealConfiguration` tindakan. Tindakan ini memungkinkan Anda untuk mengambil pengaturan konfigurasi Anda saat ini dan status konfigurasi saat ini untuk akun Anda.

## AWS KMS

Jika Anda berencana menggunakan konsol Amazon Macie untuk masuk ke pengaturan konfigurasi, pastikan juga bahwa Anda diizinkan untuk melakukan tindakan AWS Key Management Service (AWS KMS) berikut:

- `kms:DescribeKey`
- `kms:ListAliases`

Tindakan ini memungkinkan Anda untuk mengambil informasi tentang AWS KMS keys untuk akun Anda. Anda kemudian dapat memilih salah satu tombol ini ketika Anda memasukkan pengaturan.

## IAM

Jika Anda berencana untuk mengkonfigurasi Macie untuk mengambil peran IAM untuk mengambil dan mengungkapkan sampel data sensitif, pastikan juga bahwa Anda diizinkan untuk melakukan tindakan IAM berikut: `iam:PassRole` Tindakan ini memungkinkan Anda untuk meneruskan peran ke Macie, yang pada gilirannya memungkinkan Macie untuk mengambil peran tersebut. Saat Anda memasukkan pengaturan konfigurasi untuk akun Anda, Macie juga dapat memverifikasi bahwa peran tersebut ada di akun Anda dan dikonfigurasi dengan benar.

Jika Anda tidak diizinkan untuk melakukan tindakan yang diperlukan, mintalah bantuan AWS administrator Anda.

## Mengonfigurasi dan mengaktifkan pengaturan Amazon Macie

Setelah Anda memverifikasi bahwa Anda memiliki sumber daya dan izin yang Anda butuhkan, Anda dapat mengonfigurasi pengaturan di Amazon Macie dan mengaktifkan konfigurasi untuk akun Anda.

Jika akun Anda adalah bagian dari organisasi yang mengelola beberapa akun Macie secara terpusat, perhatikan hal berikut sebelum Anda mengonfigurasi atau selanjutnya mengubah pengaturan untuk akun Anda:

- Jika Anda memiliki akun anggota, bekerjalah dengan administrator Macie Anda untuk menentukan apakah dan cara mengonfigurasi pengaturan untuk akun Anda. Administrator Macie Anda dapat membantu Anda menentukan pengaturan konfigurasi yang benar untuk akun Anda.
- Jika Anda memiliki akun administrator Macie dan mengubah setelan untuk mengakses objek S3 yang terpengaruh, perubahan dapat memengaruhi akun dan sumber daya lain untuk organisasi Anda. Ini tergantung pada apakah Macie saat ini dikonfigurasi untuk mengambil peran AWS Identity and Access Management (IAM) untuk mengambil sampel data sensitif. Jika ya dan Anda mengkonfigurasi ulang Macie untuk menggunakan kredensial pengguna IAM, Macie secara permanen menghapus pengaturan yang ada untuk peran IAM—nama peran dan ID eksternal untuk konfigurasi Anda. Jika organisasi Anda kemudian memilih untuk menggunakan peran IAM lagi, Anda harus menentukan ID eksternal baru dalam kebijakan kepercayaan untuk peran di setiap akun anggota yang berlaku.

Untuk detail tentang opsi konfigurasi untuk salah satu jenis akun, lihat [Opsi konfigurasi dan persyaratan untuk mengambil sampel data sensitif dengan temuan](#).

Untuk mengonfigurasi pengaturan di Macie dan mengaktifkan konfigurasi untuk akun Anda, Anda dapat menggunakan konsol Amazon Macie atau Amazon Macie API.

### Console

Ikuti langkah-langkah ini untuk mengonfigurasi dan mengaktifkan pengaturan dengan menggunakan konsol Amazon Macie.

Untuk mengkonfigurasi dan mengaktifkan pengaturan Macie

1. [Buka konsol Amazon Macie di https://console.aws.amazon.com/macie/](https://console.aws.amazon.com/macie/).
2. Dengan menggunakan Wilayah AWS pemilih di sudut kanan atas halaman, pilih Wilayah di mana Anda ingin mengkonfigurasi dan mengaktifkan Macie untuk mengambil dan mengungkapkan sampel data sensitif.

3. Di panel navigasi, di bawah Pengaturan, pilih Reveal samples.
4. Di bagian Pengaturan, pilih Edit.
5. Untuk Status, pilih Aktifkan.
6. Di bawah Access, tentukan metode akses dan pengaturan yang ingin Anda gunakan saat mengambil sampel data sensitif dari objek S3 yang terpengaruh:
  - Untuk menggunakan peran IAM yang mendelegasikan akses ke Macie, pilih Asumsikan peran IAM. Jika Anda memilih opsi ini, Macie mengambil sampel dengan mengasumsikan peran IAM yang Anda buat dan konfigurasi di Anda. Akun AWS Di kotak Nama peran, masukkan nama peran.
  - Untuk menggunakan kredensial pengguna IAM yang meminta sampel, pilih Gunakan kredensial pengguna IAM. Jika Anda memilih opsi ini, setiap pengguna akun Anda menggunakan identitas IAM masing-masing untuk mengambil sampel.
7. Di bawah Enkripsi, tentukan AWS KMS key yang ingin Anda gunakan untuk mengenkripsi sampel data sensitif yang diambil:
  - Untuk menggunakan kunci KMS dari akun Anda sendiri, pilih Pilih kunci dari akun Anda. Kemudian, dalam AWS KMS keydaftar, pilih kunci yang akan digunakan. Daftar ini menampilkan kunci KMS enkripsi simetris yang ada untuk akun Anda.
  - Untuk menggunakan kunci KMS yang dimiliki akun lain, pilih Masukkan ARN kunci dari akun lain. Kemudian, di kotak AWS KMS keyARN, masukkan Nama Sumber Daya Amazon (ARN) dari kunci yang akan digunakan—misalnya, **arn:aws:kms:us-east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab**
8. Setelah Anda selesai memasukkan pengaturan, pilih Simpan.

Macie menguji pengaturan dan memverifikasi bahwa mereka benar. Jika Anda mengonfigurasi Macie untuk mengambil peran IAM, Macie juga memverifikasi bahwa peran tersebut ada di akun Anda dan kebijakan kepercayaan dan izin dikonfigurasi dengan benar. Jika ada masalah, Macie menampilkan pesan yang menjelaskan masalah tersebut.

Untuk mengatasi masalah dengan AWS KMS key, lihat persyaratan dalam [topik sebelumnya](#) dan tentukan kunci KMS yang memenuhi persyaratan. Untuk mengatasi masalah dengan peran IAM, mulailah dengan memverifikasi bahwa Anda memasukkan nama peran yang benar. Jika namanya benar, pastikan bahwa kebijakan peran memenuhi semua persyaratan bagi Macie untuk mengambil peran tersebut. Untuk detail ini, lihat [Mengkonfigurasi peran IAM untuk mengakses](#)

[objek S3 yang terpengaruh](#). Setelah Anda mengatasi masalah apa pun, Anda dapat menyimpan dan mengaktifkan pengaturan.

#### Note

Jika Anda adalah administrator Macie untuk sebuah organisasi dan Anda mengonfigurasi Macie untuk mengambil peran IAM, Macie membuat dan menampilkan ID eksternal setelah Anda menyimpan pengaturan untuk akun Anda. Perhatikan ID ini. Kebijakan kepercayaan untuk peran IAM di setiap akun anggota Anda yang berlaku harus menentukan ID ini. Jika tidak, Anda tidak akan dapat mengambil sampel data sensitif dari objek S3 yang dimiliki akun.

## API

Untuk mengonfigurasi dan mengaktifkan pengaturan secara terprogram, gunakan [UpdateRevealConfiguration](#) pengoperasian Amazon Macie API. Dalam permintaan Anda, tentukan nilai yang sesuai untuk parameter yang didukung:

- Untuk `retrievalConfiguration` parameter, tentukan metode akses dan pengaturan yang ingin Anda gunakan saat mengambil sampel data sensitif dari objek S3 yang terpengaruh:
  - Untuk mengasumsikan peran IAM yang mendelegasikan akses ke Macie, tentukan `ASSUME_ROLE` `retrievalMode` parameter dan tentukan nama peran untuk parameter tersebut. `roleName` Jika Anda menentukan pengaturan ini, Macie akan mengambil sampel dengan mengasumsikan peran IAM yang Anda buat dan konfigurasi dalam pengaturan Anda. Akun AWS
  - Untuk menggunakan kredensial pengguna IAM yang meminta sampel, tentukan `CALLER_CREDENTIALS` parameternya. `retrievalMode` Jika Anda menentukan pengaturan ini, setiap pengguna akun Anda menggunakan identitas IAM masing-masing untuk mengambil sampel.

#### Important

Jika Anda tidak menentukan nilai untuk parameter ini, Macie menetapkan metode akses (`retrievalMode`) ke `CALLER_CREDENTIALS`. Jika Macie saat ini dikonfigurasi untuk menggunakan peran IAM untuk mengambil sampel, Macie juga secara permanen menghapus nama peran saat ini dan ID eksternal untuk konfigurasi Anda. Untuk menyimpan pengaturan ini untuk konfigurasi yang ada, sertakan

`retrievalConfiguration` parameter dalam permintaan Anda dan tentukan pengaturan Anda saat ini untuk parameter tersebut. Untuk mengambil pengaturan Anda saat ini, gunakan [GetRevealConfiguration](#) operasi atau, jika Anda menggunakan AWS Command Line Interface (AWS CLI), jalankan [get-reveal-configuration](#) perintah.

- Untuk `kmsKeyId` parameter, tentukan AWS KMS key yang ingin Anda gunakan untuk mengenkripsi sampel data sensitif yang diambil:
  - Untuk menggunakan kunci KMS dari akun Anda sendiri, tentukan Nama Sumber Daya Amazon (ARN), ID, atau alias untuk kunci tersebut. Jika Anda menentukan alias, sertakan `alias/awalannya`—misalnya, `alias/ExampleAlias`
  - Untuk menggunakan kunci KMS yang dimiliki akun lain, tentukan ARN dari kunci—misalnya, `arn:aws:kms:us-east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`  
Atau tentukan ARN alias untuk kunci—misalnya, `arn:aws:kms:us-east-1:111122223333:alias/ExampleAlias`
- Untuk `status` parameter, tentukan `ENABLED` untuk mengaktifkan konfigurasi untuk akun Macie Anda.

Dalam permintaan Anda, pastikan juga bahwa Anda menentukan Wilayah AWS di mana Anda ingin mengaktifkan dan menggunakan konfigurasi.

Untuk mengkonfigurasi dan mengaktifkan pengaturan dengan menggunakan AWS CLI, jalankan [update-reveal-configuration](#) perintah dan tentukan nilai yang sesuai untuk parameter yang didukung. Misalnya, jika Anda menggunakan Microsoft Windows, jalankan perintah berikut: AWS CLI

```
C:\> aws macie2 update-reveal-configuration ^
--region us-east-1 ^
--configuration={"kmsKeyId\":\"arn:aws:kms:us-east-1:111122223333:alias/
ExampleAlias\", \"status\":\"ENABLED\"} ^
--retrievalConfiguration={"retrievalMode\":\"ASSUME_ROLE\", \"roleName\":
\"MacieRevealRole\"}
```

Di mana:

- `us-east-1` adalah Wilayah untuk mengaktifkan dan menggunakan konfigurasi. Dalam contoh ini, Wilayah AS Timur (Virginia N.).

- `arn:aws:kms:us-east-1:111122223333:alias/` adalah ARN alias untuk digunakan. AWS KMS key Dalam contoh ini, kunci dimiliki oleh akun lain.
- `ENABLED` adalah status konfigurasi.
- `ASSUME_ROLE` adalah metode akses untuk digunakan. Dalam contoh ini, asumsikan peran IAM yang ditentukan.
- `MacieRevealRole` adalah nama peran IAM untuk diasumsikan oleh Macie saat mengambil sampel data sensitif.


Contoh sebelumnya menggunakan karakter kelanjutan baris tanda sisipan (^) untuk meningkatkan keterbacaan.

Saat Anda mengirimkan permintaan Anda, Macie menguji pengaturannya. Jika Anda mengonfigurasi Macie untuk mengambil peran IAM, Macie juga memverifikasi bahwa peran tersebut ada di akun Anda dan kebijakan kepercayaan dan izin dikonfigurasi dengan benar. Jika ada masalah, permintaan Anda gagal dan Macie mengembalikan pesan yang menjelaskan masalah tersebut. Untuk mengatasi masalah dengan AWS KMS key, lihat persyaratan dalam [topik sebelumnya](#) dan tentukan kunci KMS yang memenuhi persyaratan. Untuk mengatasi masalah dengan peran IAM, mulailah dengan memverifikasi bahwa Anda menentukan nama peran yang benar. Jika namanya benar, pastikan bahwa kebijakan peran memenuhi semua persyaratan bagi Macie untuk mengambil peran tersebut. Untuk detail ini, lihat [Mengkonfigurasi peran IAM untuk mengakses objek S3 yang terpengaruh](#). Setelah Anda mengatasi masalah ini, kirimkan permintaan Anda lagi.

Jika permintaan Anda berhasil, Macie mengaktifkan konfigurasi untuk akun Anda di Wilayah yang ditentukan dan Anda menerima output yang serupa dengan berikut ini.

```
{
  "configuration": {
    "kmsKeyId": "arn:aws:kms:us-east-1:111122223333:alias/ExampleAlias",
    "status": "ENABLED"
  },
  "retrievalConfiguration": {
    "externalId": "o2vee30hs31642lexample",
    "retrievalMode": "ASSUME_ROLE",
    "roleName": "MacieRevealRole"
  }
}
```

Di mana `kmsKeyId` menentukan yang AWS KMS key akan digunakan untuk mengenkripsi sampel data sensitif yang diambil, dan `status` merupakan status konfigurasi untuk akun Macie Anda. `retrievalConfigurationNilai` menentukan metode akses dan pengaturan yang akan digunakan saat mengambil sampel.


 Note

Jika Anda adalah administrator Macie untuk organisasi dan Anda mengonfigurasi Macie untuk mengambil peran IAM, perhatikan ID eksternal (`externalId`) dalam respons. Kebijakan kepercayaan untuk peran IAM di setiap akun anggota Anda yang berlaku harus menentukan ID ini. Jika tidak, Anda tidak akan dapat mengambil sampel data sensitif dari objek S3 yang terpengaruh yang dimiliki akun.

Untuk selanjutnya memeriksa pengaturan atau status konfigurasi untuk akun Anda, gunakan [GetRevealConfiguration](#) operasi atau, untuk AWS CLI, jalankan [get-reveal-configuration](#) perintah.

## Menonaktifkan pengaturan Amazon Macie

Anda dapat menonaktifkan pengaturan konfigurasi untuk akun Amazon Macie Anda kapan saja. Jika Anda menonaktifkan konfigurasi, Macie mempertahankan pengaturan yang menentukan mana yang akan digunakan AWS KMS key untuk mengenkripsi sampel data sensitif yang diambil. Macie secara permanen menghapus pengaturan akses Amazon S3 untuk konfigurasi.

 Warning

Saat Anda menonaktifkan pengaturan konfigurasi untuk akun Macie Anda, Anda juga secara permanen menghapus pengaturan saat ini yang menentukan cara mengakses objek S3 yang terpengaruh. Jika Macie saat ini dikonfigurasi untuk mengakses objek yang terpengaruh dengan mengasumsikan peran AWS Identity and Access Management (IAM), ini termasuk: nama peran, dan ID eksternal yang dihasilkan Macie untuk konfigurasi. Pengaturan ini tidak dapat dipulihkan setelah dihapus.

Untuk menonaktifkan pengaturan konfigurasi untuk akun Macie Anda, Anda dapat menggunakan konsol Amazon Macie atau Amazon Macie API.



## Console

Ikuti langkah-langkah ini untuk menonaktifkan pengaturan konfigurasi untuk akun Anda dengan menggunakan konsol Amazon Macie.

Untuk menonaktifkan pengaturan Macie

1. [Buka konsol Amazon Macie di https://console.aws.amazon.com/macie/](https://console.aws.amazon.com/macie/).
2. Dengan menggunakan Wilayah AWS pemilih di sudut kanan atas halaman, pilih Wilayah tempat Anda ingin menonaktifkan pengaturan konfigurasi untuk akun Macie Anda.
3. Di panel navigasi, di bawah Pengaturan, pilih Reveal samples.
4. Di bagian Pengaturan, pilih Edit.
5. Untuk Status, pilih Nonaktifkan.
6. Pilih Simpan.

## API

Untuk menonaktifkan pengaturan konfigurasi secara terprogram, gunakan [UpdateRevealConfiguration](#) pengoperasian Amazon Macie API. Dalam permintaan Anda, pastikan Anda menentukan Wilayah AWS di mana Anda ingin menonaktifkan konfigurasi. Untuk parameter status, tentukan DISABLED.

Untuk menonaktifkan pengaturan konfigurasi dengan menggunakan AWS Command Line Interface (AWS CLI), jalankan [update-reveal-configuration](#) perintah. Gunakan `region` parameter untuk menentukan Wilayah di mana Anda ingin menonaktifkan konfigurasi. Untuk parameter status, tentukan DISABLED. Misalnya, jika Anda menggunakan Microsoft Windows, jalankan perintah berikut: AWS CLI

```
C:\> aws macie2 update-reveal-configuration --region us-east-1 --  
configuration={"status\":\"DISABLED\"}
```

Di mana:

- *us-east-1* adalah Wilayah untuk menonaktifkan konfigurasi. Dalam contoh ini, Wilayah AS Timur (Virginia N.).
- DISABLED adalah status baru dari konfigurasi.

Jika permintaan Anda berhasil, Macie menonaktifkan konfigurasi untuk akun Anda di Wilayah yang ditentukan dan Anda menerima output yang serupa dengan berikut ini.

```
{
  "configuration": {
    "status": "DISABLED"
  }
}
```

Di status mana status baru konfigurasi untuk akun Macie Anda.

Jika Macie dikonfigurasi untuk mengambil peran IAM untuk mengambil sampel data sensitif, Anda dapat menghapus peran dan kebijakan izin peran secara opsional. Macie tidak menghapus sumber daya ini saat Anda menonaktifkan pengaturan konfigurasi untuk akun Anda. Selain itu, Macie tidak menggunakan sumber daya ini untuk melakukan tugas lain untuk akun Anda. Untuk menghapus peran dan kebijakan izinnya, Anda dapat menggunakan konsol IAM atau API IAM. Untuk informasi selengkapnya, lihat [Menghapus peran](#) di Panduan AWS Identity and Access Management Pengguna.

## Mengambil dan mengungkapkan sampel data sensitif dengan temuan

Dengan menggunakan Amazon Macie, Anda dapat mengambil dan mengungkapkan sampel data sensitif yang dilaporkan Macie dalam temuan data sensitif individu. Ini termasuk data sensitif yang dideteksi Macie menggunakan [pengidentifikasi data terkelola](#), dan data yang cocok dengan kriteria pengidentifikasi data [kustom](#). Sampel dapat membantu Anda memverifikasi sifat data sensitif yang ditemukan Macie. Mereka juga dapat membantu Anda menyesuaikan penyelidikan Anda terhadap objek dan bucket Amazon Simple Storage Service (Amazon S3) yang terpengaruh. Anda dapat mengambil dan mengungkapkan sampel data sensitif di semua Wilayah AWS tempat Macie saat ini tersedia kecuali Wilayah Asia Pasifik (Osaka) dan Israel (Tel Aviv).

Jika Anda mengambil dan mengungkapkan sampel data sensitif untuk sebuah temuan, Macie menggunakan data dalam [hasil penemuan data sensitif](#) yang sesuai untuk menemukan 1-10 kejadian pertama dari data sensitif yang dilaporkan oleh temuan tersebut. Macie kemudian mengekstrak 1-128 karakter pertama dari setiap kejadian dari objek S3 yang terpengaruh. Jika sebuah temuan melaporkan beberapa jenis data sensitif, Macie melakukan ini hingga 100 jenis data sensitif yang dilaporkan oleh temuan tersebut.

Saat Macie mengekstrak data sensitif dari objek S3 yang terpengaruh, Macie mengenkripsi data dengan kunci AWS Key Management Service (AWS KMS) yang Anda tentukan, menyimpan

sementara data terenkripsi dalam cache, dan mengembalikan data dalam hasil Anda untuk temuan tersebut. Segera setelah ekstraksi dan enkripsi, Macie secara permanen menghapus data dari cache kecuali retensi tambahan sementara diperlukan untuk menyelesaikan masalah operasional.

Jika Anda memilih untuk mengambil dan mengungkapkan sampel data sensitif untuk temuan lagi, Macie mengulangi proses untuk menemukan, mengekstrak, mengenkripsi, menyimpan, dan akhirnya menghapus sampel.

Untuk demonstrasi bagaimana Anda dapat mengambil dan mengungkapkan sampel data sensitif dengan menggunakan konsol Amazon Macie, tonton video berikut: [Mengambil dan mengungkapkan sampel](#) data sensitif dengan Amazon Macie.

## Topik

- [Sebelum Anda mulai](#)
- [Menentukan apakah sampel data sensitif tersedia untuk temuan](#)
- [Mengambil dan mengungkapkan sampel data sensitif untuk sebuah temuan](#)

## Sebelum Anda mulai

Sebelum Anda dapat mengambil dan mengungkapkan sampel data sensitif untuk temuan, Anda perlu [mengonfigurasi dan mengaktifkan pengaturan untuk akun Amazon Macie Anda](#). Anda juga perlu bekerja dengan AWS administrator Anda untuk memverifikasi bahwa Anda memiliki izin dan sumber daya yang Anda butuhkan.

Saat Anda mengambil dan mengungkapkan sampel data sensitif untuk sebuah temuan, Macie melakukan serangkaian tugas untuk mencari, mengambil, mengenkripsi, dan mengungkapkan sampel. Macie tidak menggunakan [peran terkait layanan Macie untuk akun Anda untuk melakukan tugas-tugas](#) ini. Sebagai gantinya, Anda menggunakan identitas AWS Identity and Access Management (IAM) Anda atau mengizinkan Macie untuk mengambil peran IAM di akun Anda.

Untuk mengambil dan mengungkapkan sampel data sensitif untuk temuan, Anda harus memiliki akses ke temuan, hasil penemuan data sensitif yang sesuai, dan AWS KMS key yang Anda konfigurasi Macie untuk digunakan untuk mengenkripsi sampel data sensitif. Selain itu, Anda atau peran IAM harus diizinkan untuk mengakses bucket S3 yang terpengaruh dan objek S3 yang terpengaruh. Anda atau peran juga harus diizinkan untuk menggunakan AWS KMS key yang digunakan untuk mengenkripsi objek yang terpengaruh, jika berlaku. Jika ada kebijakan IAM,

kebijakan sumber daya, atau setelah izin lainnya yang menolak akses yang diperlukan, kesalahan akan terjadi dan Macie tidak mengembalikan sampel apa pun untuk temuan tersebut.

Anda juga harus diizinkan untuk melakukan tindakan Macie berikut:

- `macie2:GetMacieSession`
- `macie2:GetFindings`
- `macie2:ListFindings`
- `macie2:GetSensitiveDataOccurrences`

Tiga tindakan pertama memungkinkan Anda mengakses akun Macie Anda dan mengambil detail temuan. Tindakan terakhir memungkinkan Anda untuk mengambil dan mengungkapkan sampel data sensitif untuk temuan.

Untuk menggunakan konsol Amazon Macie untuk mengambil dan menampilkan sampel data sensitif, Anda juga harus diizinkan untuk melakukan tindakan berikut:

`macie2:GetSensitiveDataOccurrencesAvailability` Tindakan ini memungkinkan Anda untuk menentukan apakah sampel tersedia untuk temuan individu. Anda tidak memerlukan izin untuk melakukan tindakan ini untuk mengambil dan mengungkapkan sampel secara terprogram. Namun, memiliki izin ini dapat merampingkan pengambilan sampel Anda.

Jika Anda adalah administrator Macie yang didelegasikan untuk organisasi dan Anda mengonfigurasi Macie untuk mengambil peran IAM untuk mengambil sampel data sensitif, Anda juga harus diizinkan untuk melakukan tindakan berikut: `macie2:GetMember` Tindakan ini memungkinkan Anda untuk mengambil informasi tentang hubungan antara akun Anda dan akun yang terpengaruh. Ini memungkinkan Macie untuk memverifikasi bahwa Anda saat ini administrator Macie untuk akun yang terpengaruh.

Jika Anda tidak diizinkan untuk melakukan tindakan yang diperlukan atau mengakses data dan sumber daya yang diperlukan, mintalah bantuan AWS administrator Anda.

Menentukan apakah sampel data sensitif tersedia untuk temuan

Untuk mengambil dan mengungkapkan sampel data sensitif untuk suatu temuan, temuan tersebut harus memenuhi kriteria tertentu. Ini harus menyertakan data lokasi untuk kejadian spesifik dari data sensitif. Selain itu, ia harus menentukan lokasi hasil penemuan data sensitif yang valid dan sesuai. Hasil penemuan data sensitif harus disimpan Wilayah AWS sama dengan temuan. Jika Anda mengonfigurasi Amazon Macie untuk mengakses objek S3 yang terpengaruh dengan

mengasumsikan peran AWS Identity and Access Management (IAM), hasil penemuan data sensitif juga harus disimpan dalam objek S3 yang ditandatangani Macie dengan Kode Otentikasi Pesan (HMAC) berbasis Hash. AWS KMS key

Objek S3 yang terpengaruh juga harus memenuhi kriteria tertentu. Jenis MIME objek harus salah satu dari yang berikut:

- application/avro, untuk file wadah objek Apache Avro (.avro)
- application/gzip, untuk file arsip terkompresi GNU Zip (.gz atau.gzip)
- application/json, untuk file JSON atau JSON Lines (.json atau .jsonl)
- application/parquet, untuk file Apache Parquet (.parquet)
- application/vnd.openxmlformats-officedocument.spreadsheetml.sheet, untuk file buku kerja Microsoft Excel (.xlsx)
- application/zip, untuk file arsip terkompresi ZIP (.zip)
- text/csv, untuk file CSV (.csv)
- text/plain, untuk file teks non-biner selain file CSV, JSON, JSON Lines, atau TSV
- text/tab-separated-values, untuk file TSV (.tsv)

Selain itu, isi objek S3 harus sama dengan saat temuan dibuat. Macie memeriksa tag entitas objek (ETag) untuk menentukan apakah itu cocok dengan ETag yang ditentukan oleh temuan. Selain itu, ukuran penyimpanan objek tidak dapat melebihi kuota ukuran yang berlaku untuk mengambil dan mengungkapkan sampel data sensitif. Untuk daftar kuota yang berlaku, lihat [Kuota Amazon Macie](#).

Jika temuan dan objek S3 yang terpengaruh memenuhi kriteria sebelumnya, sampel data sensitif tersedia untuk temuan tersebut. Anda dapat secara opsional menentukan apakah ini kasus untuk temuan tertentu sebelum Anda mencoba mengambil dan mengungkapkan sampel untuk temuan tersebut.

Untuk menentukan apakah sampel data sensitif tersedia untuk temuan

Anda dapat menggunakan konsol Amazon Macie atau Amazon Macie API untuk menentukan apakah sampel data sensitif tersedia untuk temuan.

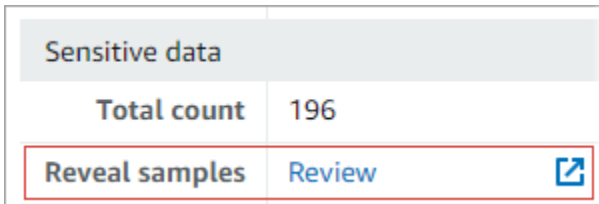
## Console


Ikuti langkah-langkah ini di konsol Amazon Macie untuk menentukan apakah sampel data sensitif tersedia untuk temuan.

Untuk menentukan apakah sampel tersedia untuk temuan

1. [Buka konsol Amazon Macie di https://console.aws.amazon.com/macie/](https://console.aws.amazon.com/macie/).
2. Di panel navigasi, pilih Temuan.
3. Pada halaman Temuan, pilih temuannya. Panel detail menampilkan informasi untuk temuan.
4. Di panel detail, gulir ke bagian Data sensitif. Kemudian lihat bidang Reveal samples.

Jika sampel data sensitif tersedia untuk temuan, tautan Tinjauan akan muncul di bidang, seperti yang ditunjukkan pada gambar berikut.



Sensitive data	
Total count	196
Reveal samples	Review 

Jika sampel data sensitif tidak tersedia untuk temuan, bidang Reveal samples menampilkan teks yang menunjukkan alasannya:

- Akun tidak dalam organisasi — Anda tidak diizinkan mengakses objek S3 yang terpengaruh dengan menggunakan Macie. Akun yang terpengaruh saat ini bukan bagian dari organisasi Anda. Atau akun adalah bagian dari organisasi Anda tetapi Macie saat ini tidak diaktifkan untuk akun saat ini Wilayah AWS.
- Hasil klasifikasi tidak valid - Tidak ada hasil penemuan data sensitif yang sesuai untuk temuan tersebut. Atau hasil penemuan data sensitif terkait tidak tersedia saat ini Wilayah AWS, cacat atau rusak, atau menggunakan format penyimpanan yang tidak didukung. Macie tidak dapat memverifikasi lokasi data sensitif untuk diambil.
- Tanda tangan hasil tidak valid - Hasil penemuan data sensitif terkait disimpan dalam objek S3 yang tidak ditandatangani oleh Macie. Macie tidak dapat memverifikasi integritas dan keaslian hasil penemuan data sensitif. Oleh karena itu, Macie tidak dapat memverifikasi lokasi data sensitif untuk diambil.
- Peran anggota terlalu permisif — Kebijakan kepercayaan atau izin untuk peran IAM di akun anggota yang terpengaruh tidak memenuhi persyaratan Macie untuk membatasi akses ke peran tersebut. Atau kebijakan kepercayaan peran tidak menentukan ID eksternal yang benar untuk organisasi Anda. Macie tidak dapat mengambil peran untuk mengambil data sensitif.
- GetMember Izin hilang — Anda tidak diizinkan untuk mengambil informasi tentang hubungan antara akun Anda dan akun yang terpengaruh. Macie tidak dapat menentukan

apakah Anda diizinkan mengakses objek S3 yang terpengaruh sebagai administrator Macie yang didelegasikan untuk akun yang terpengaruh.

- Objek melebihi kuota ukuran — Ukuran penyimpanan objek S3 yang terpengaruh melebihi kuota ukuran untuk mengambil dan mengungkapkan sampel data sensitif dari jenis file tersebut.
- Objek tidak tersedia - Objek S3 yang terpengaruh tidak tersedia. Objek diubah namanya, dipindahkan, atau dihapus, atau isinya berubah setelah Macie membuat temuan. Atau objek dienkripsi dengan AWS KMS key yang saat ini dinonaktifkan.
- Hasil tidak ditandatangani - Hasil penemuan data sensitif terkait disimpan dalam objek S3 yang belum ditandatangani. Macie tidak dapat memverifikasi integritas dan keaslian hasil penemuan data sensitif. Oleh karena itu, Macie tidak dapat memverifikasi lokasi data sensitif untuk diambil.
- Peran terlalu permisif — Akun Anda dikonfigurasi untuk mengambil kemunculan data sensitif dengan menggunakan peran IAM yang kebijakan kepercayaan atau izinnya tidak memenuhi persyaratan Macie untuk membatasi akses ke peran. Macie tidak dapat mengambil peran untuk mengambil data sensitif.
- Jenis objek yang tidak didukung - Objek S3 yang terpengaruh menggunakan format file atau penyimpanan yang tidak didukung Macie untuk mengambil dan mengungkapkan sampel data sensitif. Tipe MIME dari objek S3 yang terpengaruh bukanlah salah satu nilai dalam daftar [sebelumnya](#).

Jika ada masalah dengan hasil penemuan data sensitif untuk temuan tersebut, informasi di bidang lokasi hasil terperinci dari temuan dapat membantu Anda menyelidiki masalah tersebut. Bidang ini menentukan jalur asli ke hasil di Amazon S3. Untuk menyelidiki masalah dengan peran IAM, pastikan bahwa kebijakan peran memenuhi semua persyaratan bagi Macie untuk mengambil peran tersebut. Untuk detail ini, lihat [Mengkonfigurasi peran IAM untuk mengakses objek S3 yang terpengaruh](#).

## API

Untuk menentukan secara terprogram apakah sampel data sensitif tersedia untuk temuan, gunakan [GetSensitiveDataOccurrencesAvailability](#) pengoperasian Amazon Macie API. Saat Anda mengirimkan permintaan Anda, gunakan `findingId` parameter untuk menentukan pengenal unik untuk temuan tersebut. Untuk mendapatkan pengenal ini, Anda dapat menggunakan [ListFindings](#) operasi ini.

Jika Anda menggunakan AWS Command Line Interface (AWS CLI), jalankan perintah [get-sensitive-data-occurrences-availability](#) dan gunakan `finding-id` parameter untuk menentukan identifier unik untuk temuan. Untuk mendapatkan pengenalan ini, Anda dapat menjalankan perintah [daftar-temuan](#).

Jika permintaan Anda berhasil dan sampel tersedia untuk temuan, Anda menerima output yang mirip dengan berikut ini:

```
{
  "code": "AVAILABLE",
  "reasons": []
}
```

Jika permintaan Anda berhasil dan sampel tidak tersedia untuk temuan, nilai untuk `code` bidang adalah `UNAVAILABLE` dan `reasons` array menentukan alasannya. Sebagai contoh:

```
{
  "code": "UNAVAILABLE",
  "reasons": [
    "UNSUPPORTED_OBJECT_TYPE"
  ]
}
```

Jika ada masalah dengan hasil penemuan data sensitif untuk temuan tersebut, informasi di `classificationDetails.detailedResultsLocation` bidang temuan dapat membantu Anda menyelidiki masalah tersebut. Bidang ini menentukan jalur asli ke hasil di Amazon S3. Untuk menyelidiki masalah dengan peran IAM, pastikan bahwa kebijakan peran memenuhi semua persyaratan bagi Macie untuk mengambil peran tersebut. Untuk detail ini, lihat [Mengkonfigurasi peran IAM untuk mengakses objek S3 yang terpengaruh](#).

## Mengambil dan mengungkapkan sampel data sensitif untuk sebuah temuan

Untuk mengambil dan mengungkapkan sampel data sensitif untuk temuan, Anda dapat menggunakan konsol Amazon Macie atau Amazon Macie API.


### Console


Ikuti langkah-langkah berikut untuk mengambil dan mengungkapkan sampel data sensitif untuk temuan menggunakan konsol Amazon Macie.



Untuk mengambil dan mengungkapkan sampel data sensitif untuk temuan

1. [Buka konsol Amazon Macie di https://console.aws.amazon.com/macie/](https://console.aws.amazon.com/macie/).
2. Di panel navigasi, pilih Temuan.
3. Pada halaman Temuan, pilih temuannya. Panel detail menampilkan informasi untuk temuan.
4. Di panel detail, gulir ke bagian Data sensitif. Kemudian, di bidang Reveal samples, pilih Review:

Sensitive data	
Total count	196
Reveal samples	Review 

 Note

Jika tautan Tinjauan tidak muncul di bidang Reveal samples, sampel data sensitif tidak tersedia untuk temuan tersebut. Untuk informasi tentang mengapa hal ini terjadi, lihat [topik sebelumnya](#).

Setelah Anda memilih Review, Macie menampilkan halaman yang merangkum detail kunci dari temuan tersebut. Detailnya mencakup kategori, jenis, dan jumlah kemunculan data sensitif yang ditemukan Macie di objek S3 yang terpengaruh.

5. Di bagian Data sensitif halaman, pilih Ungkapkan sampel. Macie kemudian mengambil dan mengungkapkan sampel dari 1-10 kejadian pertama dari data sensitif yang dilaporkan oleh temuan tersebut. Setiap sampel berisi 1-128 karakter pertama dari kejadian data sensitif. Diperlukan beberapa menit untuk mengambil dan mengungkapkan sampel.

Jika temuan melaporkan beberapa jenis data sensitif, Macie mengambil dan mengungkapkan sampel hingga 100 jenis. Misalnya, gambar berikut menunjukkan sampel yang mencakup beberapa kategori dan jenis data sensitif—AWS kredensial, nomor telepon AS, dan nama orang.

**Sensitive data**  
Macie found the following types of sensitive data in the S3 object. You can retrieve and reveal samples of the sensitive data that Macie found. Reveal samples

Category	Type	Sample
Credentials	Aws credentials	wJalrXUtnFEMI/K7MDENG/bPxrRfCYEXAMPLEKEY
Credentials	Aws credentials	je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY
Credentials	Aws credentials	wJalrXUtnFEMI/K7MDENG/bPxrRfCYEXAMPLEKEY
Credentials	Aws credentials	je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY
Personal information	Phone number	425-555-0100
Personal information	Phone number	425-555-0101
Personal information	Phone number	425-555-0102
Personal information	Name	John Doe
Personal information	Name	Martha Rivera

Sampel diatur pertama berdasarkan kategori data sensitif, dan kemudian oleh tipe data sensitif.

## API

Untuk mengambil dan mengungkapkan sampel data sensitif untuk temuan secara terprogram, gunakan [GetSensitiveDataOccurrences](#) pengoperasian Amazon Macie API. Saat Anda mengirimkan permintaan Anda, gunakan `findingId` parameter untuk menentukan pengenal unik untuk temuan tersebut. Untuk mendapatkan pengenal ini, Anda dapat menggunakan [ListFindings](#) operasi ini.

Untuk mengambil dan mengungkapkan sampel data sensitif dengan menggunakan AWS Command Line Interface (AWS CLI), jalankan [get-sensitive-data-occurrences](#) perintah dan gunakan `finding-id` parameter untuk menentukan pengidentifikasi unik untuk temuan. Sebagai contoh:

```
C:\> aws macie2 get-sensitive-data-occurrences --finding-id
"1f1c2d74db5d8caa76859ec52example"
```

Dimana *1f1c2d74db5d8caa76859ec52example* adalah *pengidentifikasi unik* untuk temuan ini. Untuk mendapatkan pengenal ini dengan menggunakan AWS CLI, Anda dapat menjalankan perintah [daftar-temuan](#).

Jika permintaan Anda berhasil, Macie mulai memproses permintaan Anda dan Anda menerima output yang serupa dengan berikut ini:

```
{
```

```
"status": "PROCESSING"
}
```

Diperlukan beberapa menit untuk memproses permintaan Anda. Dalam beberapa menit, kirimkan permintaan Anda lagi.

Jika Macie dapat menemukan, mengambil, dan mengenkripsi sampel data sensitif, Macie mengembalikan sampel dalam peta. `sensitiveDataOccurrences` Peta menentukan 1-100 jenis data sensitif yang dilaporkan oleh temuan dan, untuk setiap jenis, 1-10 sampel. Setiap sampel berisi 1-128 karakter pertama dari kejadian data sensitif yang dilaporkan oleh temuan tersebut.

Di peta, setiap kunci adalah ID pengenal data terkelola yang mendeteksi data sensitif, atau nama dan pengidentifikasi unik untuk pengidentifikasi data khusus yang mendeteksi data sensitif. Nilai adalah sampel untuk pengenal data terkelola tertentu atau pengidentifikasi data kustom. Misalnya, respons berikut menyediakan tiga sampel nama orang dan dua sampel kunci akses AWS rahasia yang terdeteksi oleh pengidentifikasi data terkelola (`NAME` dan `AWS_CREDENTIALS`, masing-masing).

```
{
  "sensitiveDataOccurrences": {
    "NAME": [
      {
        "value": "Akua Mansa"
      },
      {
        "value": "John Doe"
      },
      {
        "value": "Martha Rivera"
      }
    ],
    "AWS_CREDENTIALS": [
      {
        "value": "wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY"
      },
      {
        "value": "je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY"
      }
    ]
  },
  "status": "SUCCESS"
}
```

```
}
```

Jika permintaan Anda berhasil tetapi sampel data sensitif tidak tersedia untuk temuan, Anda menerima `UnprocessableEntityException` pesan yang menunjukkan mengapa sampel tidak tersedia. Sebagai contoh:

```
{
  "message": "An error occurred (UnprocessableEntityException) when calling the
  GetSensitiveDataOccurrences operation: OBJECT_UNAVAILABLE"
}
```

Dalam contoh sebelumnya, Macie berusaha mengambil sampel dari objek S3 yang terpengaruh tetapi objek tidak tersedia lagi. Isi objek berubah setelah Macie membuat temuan.

Jika permintaan Anda berhasil tetapi jenis kesalahan lain mencegah Macie mengambil dan mengungkapkan sampel data sensitif untuk temuan tersebut, Anda menerima output yang serupa dengan berikut ini:

```
{
  "error": "Macie can't retrieve the samples. You're not allowed to access the
  affected S3 object or the object is encrypted with a key that you're not allowed to
  use.",
  "status": "ERROR"
}
```

Nilai untuk status bidang adalah `ERROR` dan `error` bidang menjelaskan kesalahan yang terjadi. Informasi dalam [topik sebelumnya](#) dapat membantu Anda menyelidiki kesalahan.

## Skema JSON untuk lokasi data sensitif

Amazon Macie menggunakan struktur JSON standar untuk menyimpan informasi tentang tempat ia menemukan data sensitif di objek Amazon Simple Storage Service (Amazon S3). Struktur digunakan oleh temuan data sensitif dan hasil penemuan data sensitif. Untuk temuan data sensitif, struktur adalah bagian dari skema JSON untuk temuan. Untuk meninjau skema JSON lengkap untuk temuan, lihat Temuan di [Referensi API Amazon Macie](#). Untuk mempelajari selengkapnya tentang hasil penemuan data sensitif, lihat [Menyimpan dan mempertahankan hasil penemuan data sensitif](#).

### Topik

- [Ikhtisar skema JSON untuk lokasi data sensitif](#)

- [Rincian skema JSON dan contoh untuk lokasi data sensitif](#)

## Ikhtisar skema JSON untuk lokasi data sensitif

Untuk melaporkan lokasi data sensitif yang ditemukan Amazon Macie di objek S3 yang terpengaruh, skema JSON untuk temuan data sensitif dan hasil penemuan data sensitif mencakup satu objek dan satu `customDataIdentifiers` objek. `sensitiveData` `customDataIdentifiers` objek memberikan rincian tentang data yang Macie terdeteksi menggunakan [pengidentifikasi data kustom](#). `sensitiveData` objek memberikan rincian tentang data yang Macie terdeteksi menggunakan [pengidentifikasi data yang dikelola](#).

Setiap objek `customDataIdentifiers` dan `sensitiveData` berisi satu `arraydetections` atau lebih:

- Dalam sebuah `customDataIdentifiers` objek, `detections` array menunjukkan pengidentifikasi data kustom mana yang mendeteksi data dan menghasilkan temuan. Untuk setiap pengidentifikasi data kustom, array juga menunjukkan jumlah kejadian data yang dideteksi pengidentifikasi. Array tersebut juga dapat menunjukkan lokasi data yang terdeteksi oleh pengenal.
- Pada objek `sensitiveData`, array `detections` yang menunjukkan tipe data sensitif yang Macie deteksi menggunakan pengidentifikasi data terkelola. Untuk setiap tipe data sensitif, array juga menunjukkan jumlah kejadian dari data, dan dapat menunjukkan lokasi data.

Untuk temuan data sensitif, array `detections` dapat mencakup 1-15 objek `occurrences`. Setiap `occurrences` objek menentukan di mana Macie mendeteksi kejadian individu dari jenis data sensitif tertentu.

Misalnya, `detections` larik berikut menunjukkan lokasi tiga kejadian data sensitif (nomor Jaminan Sosial AS) yang ditemukan Macie dalam file CSV.

```
"sensitiveData": [  
  {  
    "category": "PERSONAL_INFORMATION",  
    "detections": [  
      {  
        "count": 30,  
        "occurrences": {  
          "cells": [  
            {  
              "cellReference": null,  

```

```

        "column": 1,
        "columnName": "SSN",
        "row": 2
    },
    {
        "cellReference": null,
        "column": 1,
        "columnName": "SSN",
        "row": 3
    },
    {
        "cellReference": null,
        "column": 1,
        "columnName": "SSN",
        "row": 4
    }
]
},
"type": "USA_SOCIAL_SECURITY_NUMBER"
}

```

Lokasi dan jumlah occurrences objek dalam detections array bervariasi berdasarkan kategori, jenis, dan jumlah kejadian data sensitif yang dideteksi Macie selama siklus analisis penemuan data sensitif otomatis atau menjalankan pekerjaan penemuan data sensitif. Untuk setiap siklus analisis atau pekerjaan yang dijalankan, Macie menggunakan algoritma penelusuran kedalaman pertama untuk mengisi temuan yang dihasilkan dengan data lokasi selama 1—15 kejadian data sensitif yang dideteksi Macie di objek S3. Kejadian ini menunjukkan kategori dan jenis data sensitif yang mungkin berisi bucket dan objek S3 yang terpengaruh.

occurrencesObjek dapat berisi struktur berikut, tergantung pada jenis file atau format penyimpanan objek S3 yang terpengaruh:

- **Array cells** - Array ini berlaku untuk buku kerja Microsoft Excel, file CSV, dan file TSV. Objek dalam array ini menentukan sel atau bidang yang Macie mendeteksi terjadinya data sensitif di.
- **lineRangesarray** - Array ini berlaku untuk pesan email (EML) file, dan file teks non-biner selain CSV, JSON, JSON Lines, dan file TSV — misalnya, HTML, TXT, dan file XML—misalnya, HTML, TXT, dan XML-file. Objek dalam array ini menentukan garis atau rentang garis inklusif yang Macie mendeteksi terjadinya data sensitif, dan posisi data pada garis atau garis yang ditentukan.

Dalam kasus tertentu, objek dalam lineRanges array menentukan lokasi deteksi data sensitif dalam jenis file atau format penyimpanan yang didukung oleh jenis lain dari array. Kasus-kasus

tersebut adalah: deteksi di bagian tidak terstruktur dari file yang terstruktur lain, seperti komentar dalam file; deteksi dalam file cacat yang dianalisis Macie sebagai plaintext; dan, file CSV atau TSV yang memiliki satu atau lebih nama kolom tempat Macie mendeteksi data sensitif masuk.

- `Array offsetRanges` - Array ini dicadangkan untuk penggunaan di waktu yang akan datang. Jika array ini hadir, nilai untuk itu adalah null.
- `Array pages` - Array ini berlaku untuk file Adobe Portable Document Format (PDF). Objek dalam array ini menentukan halaman yang Macie mendeteksi terjadinya data sensitif di.
- `Array records` - Array ini berlaku untuk kontainer objek Apache Avro, file Apache Parquet, file JSON, dan file JSON Lines. Untuk Avro objek kontainer dan file Parquet, objek dalam array ini menentukan indeks record dan path ke lapangan dalam catatan bahwa Macie mendeteksi terjadinya data sensitif di. Untuk file JSON dan JSON Lines, objek dalam array ini menentukan jalur ke bidang atau array yang Macie mendeteksi terjadinya data sensitif di. Untuk file JSON Lines, hal itu juga menentukan indeks dari baris yang berisi data.

Isi dari susunan ini bervariasi berdasarkan tipe file atau format penyimpanan objek S3 terpengaruh dan isinya.

## Rincian skema JSON dan contoh untuk lokasi data sensitif

Amazon Macie menyesuaikan konten struktur JSON yang digunakannya untuk menunjukkan di mana ia mendeteksi data sensitif dalam jenis file dan konten tertentu. Topik berikut menjelaskan dan memberikan contoh struktur ini.

### Topik

- [Cell array](#)
- [LineRangessusunan](#)
- [Array halaman](#)
- [Array catatan](#)

Untuk daftar lengkap struktur JSON yang dapat disertakan dalam temuan data sensitif, lihat [Temuan di Referensi](#) API Amazon Macie.

### Cell array

Berlaku untuk: Buku kerja Microsoft Excel, file CSV, dan file TSV

Dalam `cells` array, `Cell` objek menentukan sel atau bidang yang Macie mendeteksi terjadinya data sensitif di. Tabel berikut menjelaskan tujuan masing-masing bidang dalam objek `Cell`.

Bidang	Tipe	Deskripsi
<code>cellReference</code>	String	Lokasi sel, sebagai referensi sel absolut, yang berisi kejadian tersebut. Bidang ini hanya berlaku untuk buku kerja Excel. Nilai ini adalah tidak berlaku untuk file CSV dan TSV.
<code>column</code>	Bulat	Jumlah kolom kolom yang berisi kejadian tersebut. Untuk buku kerja Excel, nilai ini berkorelasi dengan karakter abjad (-abjad) untuk pengidentifikasi kolom — misalnya, 1 untuk kolom A, 2 untuk kolom B, dan seterusnya.
<code>columnName</code>	String	Nama kolom yang berisi kejadian, jika tersedia.
<code>row</code>	Bulat	Nomor baris baris yang berisi kejadian tersebut.

Contoh berikut menunjukkan struktur `Cell` objek yang menentukan lokasi terjadinya data sensitif yang Macie terdeteksi dalam file CSV.

```
"cells": [  
  {  
    "cellReference": null,  
    "column": 3,  
    "columnName": "SSN",  
    "row": 5  
  }  
]
```



```
]
```

Dalam contoh sebelumnya, temuan menunjukkan bahwa Macie mendeteksi data sensitif di bidang di baris kelima dari kolom ketiga (bernama SSN) dari file.

Contoh berikut menunjukkan struktur `Cell` objek yang menentukan lokasi terjadinya data sensitif yang Macie terdeteksi dalam buku kerja Excel.

```
"cells": [  
  {  
    "cellReference": "Sheet2!C5",  
    "column": 3,  
    "columnName": "SSN",  
    "row": 5  
  }  
]
```

Pada contoh sebelumnya, temuan menunjukkan bahwa Macie mendeteksi data sensitif di lembar kerja bernama Sheet2 di buku kerja. Di lembar kerja itu, Macie mendeteksi data sensitif di sel di baris kelima kolom ketiga (kolom C, bernama SSN).

### LineRangessusunan

Berlaku untuk: Email message (EML) file, dan file teks non-biner selain CSV, JSON, JSON Lines, dan file TSV — misalnya, HTML, TXT, dan file XML—misalnya, HTML, TXT, dan XML-file

Dalam `lineRanges` array, `Range` objek menentukan garis atau rentang garis inklusif yang Macie mendeteksi terjadinya data sensitif, dan posisi data pada garis atau garis yang ditentukan.

Objek ini sering kosong demi tipe file yang didukung oleh tipe lain dari susunan di objek `occurrences`. Pengecualian nya adalah:

- Data di bagian yang tidak terstruktur dari file lain yang terstruktur, seperti komentar dalam file.
- Data dalam file cacat ketika Macie menganalisisnya sebagai plaintext.
- File CSV atau TSV yang memiliki satu atau beberapa nama kolom tempat Macie mendeteksi data sensitif.

Tabel berikut menjelaskan tujuan masing-masing bidang dalam Objek `Range` dari objek susunan `lineRanges`.

Bidang	Tipe	Deskripsi
end	Bulat	Jumlah baris dari awal file sampai akhir kejadian.
start	Bulat	Jumlah baris dari awal file ke awal terjadinya.
startColumn	Bulat	Jumlah karakter, dengan spasi dan mulai dari 1, dari awal baris pertama yang berisi kejadian (start) hingga awal terjadinya.

Contoh berikut menunjukkan struktur Range objek yang menentukan lokasi terjadinya data sensitif yang Macie terdeteksi pada satu baris dalam file TXT.

```
"lineRanges": [  
  {  
    "end": 1,  
    "start": 1,  
    "startColumn": 119  
  }  
]
```

Dalam contoh sebelumnya, temuan menunjukkan bahwa Macie mendeteksi kejadian lengkap data sensitif (alamat surat) di baris pertama file. Karakter pertama dalam kejadian adalah 119 karakter (dengan spasi) dimulai dari awal baris itu.

Contoh berikut menunjukkan struktur Range objek yang menentukan lokasi terjadinya data sensitif yang mencakup beberapa baris dalam file TXT.

```
"lineRanges": [  
  {  
    "end": 54,  
    "start": 51,  
    "startColumn": 1  
  }  
]
```

Dalam contoh sebelumnya, temuan menunjukkan bahwa Macie mendeteksi terjadinya data sensitif (alamat surat) yang mencakup baris 51 hingga 54 file. Karakter pertama dalam kejadian merupakan karakter pertama di baris 51 dari file.

### Array halaman

Berlaku untuk: File Adobe Portable Dokumen Format (PDF)

Dalam pages array, Page objek menentukan halaman yang Macie mendeteksi terjadinya data sensitif di. Objek berisi bidang pageNumber. pageNumberBidang menyimpan integer yang menentukan nomor halaman halaman yang berisi kejadian tersebut.

Contoh berikut menunjukkan struktur Page objek yang menentukan lokasi terjadinya data sensitif yang Macie terdeteksi dalam file PDF.

```
"pages": [  
  {  
    "pageNumber": 10  
  }  
]
```

Pada contoh sebelumnya, temuan menunjukkan bahwa halaman 10 file berisi kejadian tersebut.

### Array catatan

Berlaku untuk: Kontainer objek Apache Avro, file Apache Parquet, file JSON, dan file JSON Lines

Untuk wadah objek Avro atau file Parquet, Record objek dalam records array menentukan indeks record dan path ke lapangan dalam catatan yang Macie mendeteksi terjadinya data sensitif di. Untuk file JSON dan JSON Lines, Record objek menentukan jalur ke bidang atau larik tempat Macie mendeteksi terjadinya data sensitif. Untuk file JSON Lines, itu juga menentukan indeks baris yang berisi kejadian tersebut.

Tabel berikut menjelaskan tujuan masing-masing bidang dalam objek Record.

Bidang	Tipe	Deskripsi
jsonPath	String	Jalan, sebagai ekspresi JSONPath, untuk terjadinya.

Bidang	Tipe	Deskripsi
		<p>Untuk wadah objek Avro atau file Parquet, ini adalah path ke bidang dalam record (<code>recordIndex</code> ) yang berisi terjadinya. Untuk file JSON atau JSON Lines, ini adalah path ke field atau array yang berisi kejadian tersebut. Jika data adalah nilai dalam array, jalan juga menunjukkan nilai yang berisi kejadian tersebut.</p> <p>Jika Macie mendeteksi data sensitif pada nama elemen apa pun di jalur, Macie menghilangkan bidang <code>jsonPath</code> dari objek <code>Record</code>. Jika nama elemen path melebihi 240 karakter, Macie memotong nama dengan menghapus karakter dari awal nama. Jika jalur penuh yang dihasilkan melebihi 250 karakter, Macie juga akan memotong jalur, dimulai dengan elemen pertama yang ada di jalur, hingga jalur berisi 250 karakter atau lebih sedikit.</p>

Bidang	Tipe	Deskripsi
recordIndex	Bulat	Untuk wadah objek Avro atau file Parquet, indeks record, mulai dari 0, untuk catatan yang berisi kejadian tersebut. Untuk file JSON Lines, indeks baris, mulai dari 0, untuk baris yang berisi kejadian tersebut. Nilai ini selalu 0 untuk file JSON.

Contoh berikut menunjukkan struktur Record objek yang menentukan lokasi terjadinya data sensitif yang Macie terdeteksi dalam file Parquet.

```
"records": [
  {
    "jsonPath": "$['abcdefghijklmnopqrstuvwxy']",
    "recordIndex": 7663
  }
]
```

Dalam contoh sebelumnya, temuan menunjukkan bahwa Macie mendeteksi data sensitif dalam catatan indeks 7663 (catatan nomor 7664). Dalam catatan itu, Macie mendeteksi data sensitif di bidang bernamaabcdefghijklmnopqrstuvwxy. Jalur JSON penuh menuju bidang dalam catatan adalah \$.abcdefghijklmnopqrstuvwxy. Bidang adalah keturunan langsung dari objek root (tingkat luar).

Contoh berikut juga menunjukkan struktur Record objek untuk terjadinya data sensitif yang Macie terdeteksi dalam file Parquet. Namun, dalam contoh ini, Macie dipotong nama bidang yang berisi kejadian karena nama melebihi batas karakter.

```
"records": [
  {
    "jsonPath":
"$['...vwxyzabcdefghijklmnopqrstuvwxyabcdefghijklmnopqrstuvwxyabcde
    "recordIndex": 7663
  }
]
```

```
]
```

Dalam contoh sebelumnya, bidang adalah keturunan langsung dari akar (tingkat luar) objek.

Pada contoh berikut, juga untuk terjadinya data sensitif yang Macie terdeteksi dalam file Parquet, Macie dipotong path penuh ke bidang yang berisi kejadian tersebut. Jalur lengkap melebihi batas karakter.

```
"records": [
  {
    "jsonPath":
"$..usssn2.usssn3.usssn4.usssn5.usssn6.usssn7.usssn8.usssn9.usssn10.usssn11.usssn12.usssn13.us
    "recordIndex": 2335
  }
]
```

Dalam contoh sebelumnya, temuan menunjukkan bahwa Macie mendeteksi data sensitif dalam catatan indeks 2335 (catatan nomor 2336). Dalam catatan itu, Macie mendeteksi data sensitif di bidang bernama `abcdefghijklmnopqrstuvwxyz`. Jalur JSON lengkap ke bidang dalam catatan adalah:

```
$['1234567890']usssn1.usssn2.usssn3.usssn4.usssn5.usssn6.usssn7.usssn8.usssn9.us
```

Contoh berikut menunjukkan struktur `Record` objek yang menentukan lokasi terjadinya data sensitif yang Macie terdeteksi dalam file JSON. Dalam contoh ini, terjadinya adalah nilai tertentu dalam array.

```
"records": [
  {
    "jsonPath": "$.access.key[2]",
    "recordIndex": 0
  }
]
```

Dalam contoh sebelumnya, temuan menunjukkan bahwa Macie mendeteksi data sensitif dalam nilai kedua dari array bernama `key`. Susunan adalah anak dari sebuah objek bernama `access`.

Contoh berikut menunjukkan struktur `Record` objek yang menentukan lokasi terjadinya data sensitif yang Macie terdeteksi dalam file JSON Lines.

```
"records": [
```

```
{
  "jsonPath": "$.access.key",
  "recordIndex": 3
}
]
```

Dalam contoh sebelumnya, temuan menunjukkan bahwa Macie mendeteksi data sensitif dalam nilai ketiga (baris) dalam file. Pada baris itu, terjadinya adalah dalam bidang bernama `key`, yang merupakan anak dari sebuah objek bernama `access`.

## Menekan temuan Amazon Macie

Untuk menyederhanakan analisis temuan Anda, Anda dapat membuat dan menggunakan aturan penekanan. Aturan penekanan adalah seperangkat kriteria filter berbasis atribut yang menentukan kasus saat Anda ingin Amazon Macie untuk mengarsipkan temuan secara otomatis. Aturan penekanan sangat membantu dalam situasi saat Anda telah meninjau kelas temuan dan tidak ingin diberi tahu lagi.

Misalnya, Anda mungkin memutuskan untuk mengizinkan bucket S3 berisi alamat surat, jika bucket tidak mengizinkan akses publik dan mereka mengenkripsi objek baru secara otomatis dengan yang tertentu. AWS KMS key Dalam hal ini, Anda dapat membuat aturan penekanan yang menentukan kriteria filter untuk bidang berikut: Jenis deteksi data sensitif, izin akses publik bucket S3, dan ID kunci KMS enkripsi bucket S3. Aturan tersebut menekan temuan future yang sesuai dengan kriteria filter.

Jika Anda menekan temuan dengan aturan penindasan, Macie terus menghasilkan temuan untuk kejadian berikutnya dari data sensitif dan potensi pelanggaran kebijakan yang sesuai dengan kriteria aturan. Namun, Macie secara otomatis mengubah status temuan menjadi diarsipkan. Ini berarti bahwa temuan tidak muncul secara default pada konsol Amazon Macie, tetapi mereka bertahan di Macie sampai mereka berakhir. Macie menyimpan temuan selama 90 hari.

Selain itu, Macie tidak mempublikasikan temuan yang ditekan ke Amazon EventBridge sebagai peristiwa atau untuk. AWS Security Hub Namun, Macie terus membuat dan menyimpan [hasil penemuan data sensitif](#) yang berhubungan dengan temuan data sensitif yang Anda tekan. Hal ini membantu memastikan bahwa Anda memiliki riwayat temuan data sensitif yang tidak berubah untuk audit privasi dan perlindungan data atau investigasi yang Anda lakukan.

**Note**

Jika akun Anda adalah bagian dari organisasi yang mengelola beberapa akun Macie secara terpusat, aturan penekanan mungkin bekerja secara berbeda untuk akun Anda. Ini tergantung pada kategori temuan yang ingin Anda tekan, dan apakah Anda memiliki administrator Macie atau akun anggota:

- Temuan kebijakan — Hanya administrator Macie yang dapat menekan temuan kebijakan untuk akun organisasi.

Jika Anda memiliki akun administrator Macie dan Anda membuat aturan penindasan, Macie menerapkan aturan tersebut pada temuan kebijakan untuk semua akun di organisasi Anda kecuali Anda mengonfigurasi aturan untuk mengecualikan akun tertentu. Jika Anda memiliki akun anggota Macie dan Anda ingin menekan temuan kebijakan untuk akun Anda, hubungi administrator Macie Anda.

- Temuan data sensitif — Administrator Macie dan anggota individu dapat menekan temuan data sensitif yang dihasilkan oleh pekerjaan penemuan data sensitif mereka. Administrator Macie juga dapat menekan temuan yang dihasilkan Macie saat melakukan penemuan data sensitif otomatis untuk organisasi.

Hanya akun yang menciptakan pekerjaan penemuan data sensitif yang dapat menekan atau mengakses temuan data sensitif yang dihasilkan oleh pekerjaan tersebut. Hanya akun administrator Macie untuk organisasi yang dapat menekan atau mengakses temuan yang dihasilkan oleh penemuan data sensitif otomatis untuk akun di organisasi.

Untuk informasi selengkapnya tentang tugas yang dapat dilakukan oleh administrator dan anggota, lihat [Memahami hubungan antara administrator Amazon Macie dan akun anggota](#).

Untuk membuat dan mengelola aturan penekanan, Anda dapat menggunakan konsol Amazon Macie atau API Amazon Macie. Topik berikut menjelaskan caranya. Untuk API, topiknya mencakup contoh cara melakukan tugas ini dengan menggunakan [AWS Command Line Interface\(AWS CLI\)](#). Anda juga dapat melakukan tugas-tugas ini dengan menggunakan versi terbaru dari alat baris AWS perintah lain atau AWS SDK, atau dengan mengirim permintaan HTTPS langsung ke Macie. Untuk informasi tentang alat dan SDK AWS, lihat [Alat untuk Membangun di AWS](#).

**Topik**



- [Membuat aturan penekanan](#)
- [Meninjau temuan yang ditekan](#)
- [Mengubah aturan penekanan](#)
- [Menghapus aturan penekanan](#)

## Membuat aturan penekanan

Sebelum membuat aturan penekanan, penting untuk dicatat bahwa Anda tidak bisa memulihkan (membuka arsip) temuan yang ditekan menggunakan aturan penekanan. Namun, Anda dapat [meninjau temuan yang ditekan](#) di konsol Amazon Macie dan mengakses temuan yang ditekan dengan API Amazon Macie.

Saat Anda membuat aturan penekanan, Anda menentukan kriteria filter, nama, dan, secara opsional, deskripsi aturan. Anda dapat membuat aturan penindasan dengan menggunakan konsol Amazon Macie atau Amazon Macie API.

### Console

Ikuti langkah-langkah ini untuk membuat aturan penekanan menggunakan konsol Amazon Macie.

Untuk membuat aturan penekanan

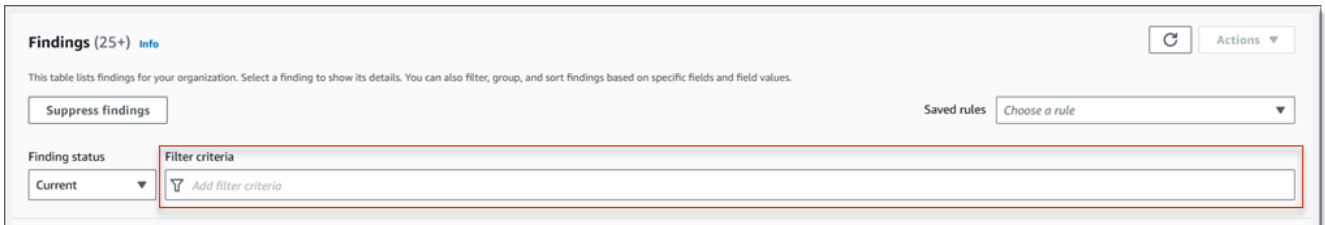
1. [Buka konsol Amazon Macie di https://console.aws.amazon.com/macie/](https://console.aws.amazon.com/macie/).
2. Di panel navigasi, pilih Temuan.

#### Tip

Untuk menggunakan aturan penekanan atau filter yang ada sebagai titik awal, pilih aturan dari daftar Aturan tersimpan.

Anda juga dapat menyederhanakan pembuatan aturan diawali dengan mengubah dan mengerucutkan pada temuan oleh grup logis yang telah ditetapkan. Jika Anda melakukan ini, Macie secara otomatis membuat dan menerapkan syarat filter yang sesuai, yang dapat menjadi titik awal yang berguna untuk membuat aturan. Untuk melakukan ini, pilih Menurut bucket, Menurut tipe, atau Menurut tugas di panel navigasi (di bawah Temuan), lalu pilih item dalam tabel. Di panel detail, pilih tautan untuk bidang yang akan dialihkan.

- Di kotak Kriteria filter, tambahkan kondisi filter yang menentukan atribut temuan yang ingin ditekan oleh aturan.



Untuk mempelajari cara menambahkan syarat filter, lihat [Membuat dan menerapkan filter untuk temuan](#).

- Ketika Anda selesai menambahkan kondisi filter untuk aturan, pilih Menekan temuan.
- Di bawah aturan Suppression, masukkan nama dan, secara opsional, deskripsi aturan.
- Pilih Save (Simpan).

## API

Untuk membuat aturan penekanan secara terprogram, gunakan [CreateFindingsFilter](#) pengoperasian Amazon Macie API dan tentukan nilai yang sesuai untuk parameter yang diperlukan:

- Untuk `action` parameter, tentukan ARCHIVE untuk memastikan bahwa Macie menekan temuan yang sesuai dengan kriteria aturan.
- Untuk parameter `criterion`, tentukan pemetaan syarat yang menentukan kriteria filter untuk aturan.

Di peta, setiap syarat harus menentukan bidang, operator, dan satu atau beberapa nilai untuk bidang tersebut. Tipe dan jumlah nilai tergantung pada bidang dan operator yang Anda pilih. Untuk informasi tentang bidang, operator, dan tipe nilai yang dapat Anda gunakan dalam syarat, lihat [Bidang untuk memfilter temuan](#), [Menggunakan operator dalam syarat](#), dan [Menentukan nilai untuk bidang](#).

Untuk membuat aturan penekanan dengan menggunakan AWS CLI, jalankan [create-findings-filter](#) perintah dan tentukan nilai yang sesuai untuk parameter yang diperlukan. Contoh berikut membuat aturan penekanan yang mengembalikan semua temuan data sensitif yang ada di saat ini Wilayah AWS dan melaporkan kejadian alamat surat (dan tidak ada jenis data sensitif lainnya) di objek S3.

Contoh ini diformat untuk Linux, macOS, atau Unix, dan menggunakan karakter garis miring terbalik (\) untuk meningkatkan keterbacaan.

```
$ aws macie2 create-findings-filter \
--action ARCHIVE \
--name my_suppression_rule \
--finding-criteria '{"criterion":
{"classificationDetails.result.sensitiveData.detections.type":{"eqExactMatch":
["ADDRESS]}}}'
```

Contoh ini diformat untuk Microsoft Windows dan menggunakan karakter kelanjutan baris tanda sisipan (^) untuk meningkatkan keterbacaan.

```
C:\> aws macie2 create-findings-filter ^
--action ARCHIVE ^
--name my_suppression_rule ^
--finding-criteria={"criterion\":
{\ "classificationDetails.result.sensitiveData.detections.type\":{\ "eqExactMatch\":
[\ "ADDRESS\"]}}}
```

Saat:

- *my\_suppression\_rule* adalah nama kustom untuk aturan.
- *criterion* adalah pemetaan syarat filter untuk aturan:
  - *classificationDetails.result.sensitiveData.detections.type* adalah nama JSON dari bidang Tipe deteksi data sensitif.
  - *eqExactMatch* menentukan sama persis operator kecocokan.
  - *ALAMAT* adalah nilai enumerasi untuk bidang Tipe deteksi data sensitif.

Jika berhasil, perintah mengembalikan output yang serupa seperti berikut ini.

```
{
  "arn": "arn:aws:macie2:us-west-2:123456789012:findings-filter/8a3c5608-aa2f-4940-b347-d1451example",
  "id": "8a3c5608-aa2f-4940-b347-d1451example"
}
```

Saat *arn* adalah Amazon Resource Name (ARN) dari aturan penekanan yang dibuat, dan *id* adalah pengidentifikasi unik untuk aturan.

Untuk contoh penambahan kriteria filter, lihat [Memfilter temuan secara terprogram dengan API Amazon Macie](#).

## Meninjau temuan yang ditekan

Secara default, Macie tidak menampilkan temuan yang ditekan pada konsol Amazon Macie. Namun, Anda dapat meninjau temuan ini di konsol dengan mengubah pengaturan filter Anda.

Untuk meninjau temuan yang ditekan di konsol

1. [Buka konsol Amazon Macie di https://console.aws.amazon.com/macie/](https://console.aws.amazon.com/macie/).
2. Di panel navigasi, pilih Temuan. Halaman Temuan menampilkan temuan yang dibuat atau diperbarui Macie untuk akun Anda saat ini Wilayah AWS selama 90 hari terakhir. Secara default, halaman ini tidak termasuk temuan yang ditekan oleh aturan penekanan.
3. Untuk status Finding, lakukan salah satu hal berikut:
  - Untuk hanya menampilkan temuan yang ditekan, pilih Diarsipkan.
  - Untuk menampilkan temuan yang ditekan dan tidak ditekan, pilih Semua.
  - Untuk menyembunyikan temuan yang ditekan lagi, pilih Current.

Anda juga dapat mengakses temuan yang ditekan dengan menggunakan API Amazon Macie. Untuk mengambil daftar temuan yang ditekan, gunakan [ListFindings](#) operasi dan sertakan kondisi filter yang menentukan `true` untuk bidang tersebut. [archived](#) Untuk sebuah contoh terkait cara untuk melakukan operasi ini menggunakan AWS CLI, lihat [Memfilter temuan secara terprogram](#). Untuk kemudian mengambil detail dari satu atau lebih temuan yang ditekan, gunakan [GetFindings](#) operasi dan tentukan pengidentifikasi unik untuk setiap temuan untuk diambil.

## Mengubah aturan penekanan

Anda dapat mengubah pengaturan untuk aturan penekanan kapan saja dengan menggunakan konsol Amazon Macie atau Amazon Macie API. Anda juga dapat menetapkan dan mengelola tag untuk aturan tersebut.


Tag adalah label yang Anda tentukan dan tetapkan ke jenis AWS sumber daya tertentu. Setiap tanda terdiri dari kunci tanda yang diperlukan dan nilai tanda opsional. Tag dapat membantu Anda mengidentifikasi, mengkategorikan, dan mengelola sumber daya dengan cara yang berbeda, seperti

berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Untuk mempelajari selengkapnya, lihat [Menandai sumber daya Amazon Macie](#).

## Console

Ikuti langkah-langkah ini untuk mengubah pengaturan pada aturan penekanan yang sudah ada menggunakan konsol Amazon Macie.

Untuk mengubah aturan penekanan

1. [Buka konsol Amazon Macie di https://console.aws.amazon.com/macie/](https://console.aws.amazon.com/macie/).
2. Di panel navigasi, pilih Temuan.
3. Di daftar Aturan tersimpan, pilih ikon edit  di samping aturan penekanan yang ingin Anda ubah.
4. Lakukan langkah-langkah berikut:
  - Untuk mengubah kriteria aturan, gunakan kotak Filter kriteria untuk memasukkan kondisi yang menentukan atribut temuan yang ingin ditekan oleh aturan. Untuk mempelajari caranya, lihat [Membuat dan menerapkan filter untuk temuan](#).
  - Untuk mengubah nama aturan, masukkan nama baru di kotak Nama di bawah Aturan penekanan.
  - Untuk mengubah deskripsi aturan, masukkan deskripsi baru di kotak Deskripsi di bawah Aturan penekanan.
  - Untuk menetapkan, meninjau, atau mengedit tag untuk aturan, pilih Kelola tag di bawah Aturan penindasan. Kemudian tinjau dan ubah tag seperlunya. Aturan dapat memiliki sebanyak 50 tag.
5. Setelah selesai membuat perubahan, pilih Simpan.

## API

Untuk mengubah aturan penekanan secara terprogram, gunakan [UpdateFindingsFilter](#) pengoperasian Amazon Macie API. Saat Anda mengirimkan permintaan, gunakan parameter yang didukung untuk menentukan nilai baru untuk setiap setelan yang ingin Anda ubah.

Untuk parameter `id`, tentukan pengidentifikasi unik untuk aturan yang akan Anda ubah. Anda bisa mendapatkan pengenalan ini dengan menggunakan [ListFindingsFilter](#) operasi untuk mengambil daftar aturan penekanan dan filter untuk akun Anda. Jika Anda menggunakan AWS CLI, jalankan [list-findings-filters](#) perintah untuk mengambil daftar ini.

Untuk mengubah aturan penekanan dengan menggunakan AWS CLI, jalankan [update-findings-filter](#) perintah dan gunakan parameter yang didukung untuk menentukan nilai baru untuk setiap pengaturan yang ingin Anda ubah. Misalnya, perintah berikut mengubah nama aturan penekanan yang ada.

```
C:\> aws macie2 update-findings-filter --id 8a3c5608-aa2f-4940-b347-d1451example --name mailing_addresses_only
```

Dengan:

- **8a3c5608-aa2f-4940-b347-d1451example** adalah pengidentifikasi unik untuk aturan.
- **mailing\_addresses\_only** adalah nama baru untuk aturan.

Jika berhasil, perintah mengembalikan output yang serupa seperti berikut ini.

```
{
  "arn": "arn:aws:macie2:us-west-2:123456789012:findings-filter/8a3c5608-aa2f-4940-b347-d1451example",
  "id": "8a3c5608-aa2f-4940-b347-d1451example"
}
```

Saat `arn` adalah Amazon Resource Name (ARN) dari aturan yang diubah, dan `id` adalah pengidentifikasi unik untuk aturan.

Demikian pula, contoh berikut mengonversi aturan filter untuk aturan penekanan dengan mengubah nilai untuk parameter `action` dari `N00P` ke `ARCHIVE`.

```
C:\> aws macie2 update-findings-filter --id 8a1c3508-aa2f-4940-b347-d1451example --action ARCHIVE
```

Saat:

- **8a1c3508-aa2f-4940-b347-d1451example** adalah pengenalan unik untuk aturan.

- **ARCHIVE** adalah tindakan baru bagi Macie untuk melakukan temuan yang sesuai dengan kriteria aturan—menekan temuan.

Jika perintah berhasil dijalankan, Anda menerima output yang mirip dengan berikut ini:

```
{
  "arn": "arn:aws:macie2:us-west-2:123456789012:findings-filter/8a1c3508-aa2f-4940-b347-d1451example",
  "id": "8a1c3508-aa2f-4940-b347-d1451example"
}
```

Saat `arn` adalah Amazon Resource Name (ARN) dari aturan yang diubah, dan `id` adalah pengidentifikasi unik untuk aturan.

## Menghapus aturan penekanan

Anda dapat menghapus aturan penindasan kapan saja dengan menggunakan konsol Amazon Macie atau Amazon Macie API. Jika Anda menghapus aturan penekanan, Macie berhenti menekan kemunculan temuan baru dan selanjutnya yang sesuai dengan kriteria aturan dan tidak ditekan oleh aturan lain. Namun, perhatikan bahwa Macie mungkin terus menekan temuan yang saat ini sedang diproses dan sesuai dengan kriteria aturan.


Setelah Anda menghapus aturan penekanan, kemunculan temuan baru dan berikutnya yang cocok dengan kriteria aturan memiliki status saat ini (tidak diarsipkan). Ini berarti bahwa temuan baru muncul secara default di konsol Amazon Macie. Selain itu, Macie menerbitkan temuan ini ke Amazon EventBridge sebagai acara. Bergantung pada [pengaturan publikasi](#) untuk akun Anda, Macie juga menerbitkan temuannya. AWS Security Hub

### Console

Ikuti langkah-langkah ini untuk menghapus aturan penekanan menggunakan konsol Amazon Macie.

Untuk menghapus aturan penekanan

1. [Buka konsol Amazon Macie di https://console.aws.amazon.com/macie/](https://console.aws.amazon.com/macie/).
2. Di panel navigasi, pilih Temuan.

3. Di Aturan tersimpan, pilih ikon edit  di samping aturan penekanan yang ingin Anda hapus.
4. Di bawah Aturan penekanan, pilih Hapus.

## API

Untuk menghapus aturan penekanan secara terprogram, gunakan [DeleteFindingsFilter](#) pengoperasian Amazon Macie API. Untuk parameter `id`, tentukan pengidentifikasi unik untuk aturan penekanan yang akan Anda hapus. Anda bisa mendapatkan pengenal ini dengan menggunakan [ListFindingsFilter](#) operasi untuk mengambil daftar aturan penekanan dan filter untuk akun Anda. Jika Anda menggunakan AWS CLI, jalankan [list-findings-filters](#) perintah untuk mengambil daftar ini.

Untuk menghapus aturan penekanan dengan menggunakan AWS CLI, jalankan [delete-findings-filter](#) perintah. Misalnya:

```
C:\> aws macie2 delete-findings-filter --id 8a3c5608-aa2f-4940-b347-d1451example
```

Di mana *8a3c5608-aa2f-4940-b347-d1451example* adalah pengidentifikasi unik untuk aturan penekanan yang akan dihapus.

Jika perintah berhasil dijalankan, Macie mengembalikan respons HTTP 200 kosong. Jika tidak, Macie mengembalikan HTTP 4xx atau respons 500 yang menunjukkan alasan operasi gagal.

## Penilaian tingkat kepelikan untuk temuan Amazon Macie

Ketika Amazon Macie menghasilkan temuan kebijakan atau data sensitif, secara otomatis memberikan kepelikan kepada temuan. Tingkat keparahan temuan mencerminkan karakteristik utama dari temuan dan dapat membantu Anda menilai dan memprioritaskan temuan Anda. Tingkat kepelikan temuan tidak menyiratkan atau menunjukkan kekritisannya atau kepentingan yang mungkin dimiliki sumber daya yang terpengaruh untuk organisasi Anda.

Untuk temuan kebijakan, tingkat keparahan didasarkan pada sifat potensi masalah dengan keamanan atau privasi data Amazon Simple Storage Service (Amazon S3) Anda. Untuk temuan data sensitif, kepelikan didasarkan pada sifat dan jumlah kejadian data sensitif yang ditemukan Macie dalam objek S3.



Dalam Macie, tingkat kepelikan temuan diwakili dalam dua cara.

### Tingkat keparahan

Ini adalah representasi kualitatif dari kepelikan. Tingkat kepelikan berkisar dari Low, untuk kepelikan rendah, hingga High, untuk kepelikan tinggi.

Tingkat kepelikan muncul secara langsung di konsol Amazon Macie. Mereka juga tersedia dalam representasi temuan JSON di konsol Macie, dari Amazon Macie API, dan dalam hasil penemuan data sensitif yang berkorelasi dengan temuan data sensitif. Tingkat keparahan juga termasuk dalam menemukan peristiwa yang diterbitkan Macie ke Amazon EventBridge dan temuan yang diterbitkan Macie. AWS Security Hub

### Skor keparahan

Ini adalah representasi numerik dari kepelikan. Skor kepelikan berkisar dari 1 hingga 3 dan memetakan langsung ke tingkat kepelikan:

Tingkat kepelikan	Tingkat kepelikan
1	Rendah
2	Sedang
3	Tinggi

Skor kepelikan tidak muncul secara langsung di konsol Amazon Macie. Namun, mereka tersedia dalam representasi temuan JSON di konsol Macie, dari Amazon Macie API, dan dalam hasil penemuan data sensitif yang berkorelasi dengan temuan data sensitif. Skor keparahan juga termasuk dalam menemukan acara yang diterbitkan Macie ke Amazon EventBridge. Mereka tidak termasuk dalam temuan yang diterbitkan Macie. AWS Security Hub

Topik pada bagian ini menunjukkan bagaimana Macie menentukan tingkat kepelikan temuan kebijakan dan temuan data sensitif.

### Topik

- [Penilaian tingkat kepelikan untuk temuan kebijakan](#)
- [Penilaian tingkat kepelikan untuk temuan data sensitif](#)

## Penilaian tingkat kepelikan untuk temuan kebijakan

Tingkat keparahan temuan kebijakan didasarkan pada sifat potensi masalah dengan keamanan atau privasi bucket S3. Tabel berikut mencantumkan tingkat kepelikan yang Macie tetapkan untuk setiap tipe temuan kebijakan. Untuk deskripsi dari setiap tipe, lihat [Tipe temuan](#).

Tipe temuan	Tingkat kepelikan
Policy:IAMUser/S3BlockPublicAccessDisabled	Tinggi
Policy:IAMUser/S3BucketEncryptionDisabled	Rendah
Policy:IAMUser/S3BucketPublic	Tinggi
Policy:IAMUser/S3BucketReplicatedExternally	Tinggi
Policy:IAMUser/S3BucketSharedExternally	Tinggi
Policy:IAMUser/S3BucketSharedWithCloudFront	Sedang

Tingkat kepelikan temuan kebijakan tidak berubah berdasarkan jumlah temuan yang terjadi.

## Penilaian tingkat kepelikan untuk temuan data sensitif

Tingkat kepelikan temuan data sensitif didasarkan pada sifat dan jumlah kejadian data sensitif yang ditemukan Macie dalam objek S3. Topik berikut menunjukkan bagaimana Macie menentukan tingkat kepelikan dari setiap tipe temuan data sensitif:

- [SensitiveData:S3Object/Credentials](#)
- [SensitiveData:S3Object/CustomIdentifier](#)
- [SensitiveData:S3Object/Financial](#)
- [SensitiveData:S3Object/Personal](#)
- [SensitiveData:S3Object/Multiple](#)

Untuk informasi rinci tentang jenis data sensitif yang dapat dideteksi dan dilaporkan Macie dalam temuan data sensitif, lihat [Menggunakan pengidentifikasi data terkelola](#) dan [Membangun pengidentifikasi data kustom](#).

## SensitiveData:S3Object/Credentials

A: SensitiveDataTemuan S3Object/Credentials menunjukkan bahwa objek S3 berisi data kredensial sensitif. Untuk tipe temuan ini, Macie menentukan kepelikan berdasarkan tipe dan jumlah kejadian dari data kredensial yang ditemukan Macie di objek.

Tabel berikut menunjukkan tingkat kepelikan yang Macie tetapkan kepada temuan yang melaporkan kejadian data kredensial dalam objek S3.

Tipe data sensitif	1 kejadian	2-99 kejadian	100 atau lebih kejadian
AWS secret access key	Tinggi	Tinggi	Tinggi
Kunci API Google Cloud	Tinggi	Tinggi	Tinggi
Header Otorisasi Dasar HTTP	Tinggi	Tinggi	Tinggi
Token Web JSON (JWT)	Tinggi	Tinggi	Tinggi
Kunci pribadi OpenSSH	Tinggi	Tinggi	Tinggi
Kunci pribadi PGP	Tinggi	Tinggi	Tinggi
Kunci pribadi Standar Kriptografi Kunci Publik (PKCS)	Tinggi	Tinggi	Tinggi
Kunci pribadi PuTTY	Tinggi	Tinggi	Tinggi
Kunci API Stripe	Tinggi	Tinggi	Tinggi

## SensitiveData:S3Object/CustomIdentifier

A: SensitiveDataS3Object/temuan CustomIdentifier menunjukkan bahwa objek S3 berisi teks yang cocok dengan kriteria deteksi satu atau lebih pengidentifikasi data kustom. Objek mungkin berisi lebih dari satu tipe data sensitif.

Secara default, Macie menetapkan tingkat keparahan Medium untuk jenis penemuan ini—jika objek S3 berisi setidaknya satu kemunculan teks yang cocok dengan kriteria deteksi setidaknya satu pengidentifikasi data kustom, Macie secara otomatis menetapkan tingkat keparahan Medium ke temuan tersebut. Tingkat keparahan temuan tidak berubah berdasarkan jumlah kemunculan teks yang cocok dengan kriteria pengidentifikasi data kustom.

Namun, tingkat keparahan jenis temuan ini dapat bervariasi jika Anda menentukan pengaturan tingkat keparahan khusus untuk pengidentifikasi data khusus yang menghasilkan temuan. Jika ini masalahnya, Macie menentukan tingkat keparahan sebagai berikut:

- Jika objek S3 berisi teks yang cocok dengan kriteria deteksi hanya satu pengidentifikasi data kustom, Macie menentukan tingkat keparahan temuan berdasarkan pengaturan tingkat keparahan untuk pengidentifikasi tersebut.
- Jika objek S3 berisi teks yang cocok dengan kriteria deteksi lebih dari satu pengidentifikasi data kustom, Macie menentukan tingkat keparahan temuan dengan mengevaluasi pengaturan keparahan untuk setiap pengidentifikasi data kustom, menentukan pengaturan mana yang menghasilkan tingkat keparahan tertinggi, dan kemudian menetapkan tingkat keparahan tertinggi untuk temuan tersebut.

Untuk meninjau setelan tingkat keparahan untuk pengenalan data kustom, pilih Pengenal data khusus di panel navigasi di konsol Amazon Macie. Kemudian pilih nama pengidentifikasi data kustom.

Bagian Keparahan menunjukkan pengaturan. Untuk informasi selengkapnya, lihat [Mendefinisikan pengaturan tingkat keparahan temuan untuk pengidentifikasi data kustom](#).

## SensitiveData:S3Object/Financial

J: Temuan SensitiveDataS3Object/Financial menunjukkan bahwa objek S3 berisi informasi keuangan yang sensitif. Untuk tipe temuan ini, Macie menentukan kepelikan berdasarkan tipe dan jumlah kejadian dari informasi keuangan yang ditemukan Macie di objek.

Tabel berikut menunjukkan tingkat kepelikan yang Macie tetapkan kepada temuan yang melaporkan kejadian informasi keuangan dalam objek S3.

Tipe data sensitif	1 kejadian	2-99 kejadian	100 atau lebih kejadian
Nomor rekening bank <sup>1</sup>	Tinggi	Tinggi	Tinggi
Tanggal kedaluwarsa kartu kredit	Rendah	Sedang	Tinggi
Data strip magnetik kartu kredit	Tinggi	Tinggi	Tinggi
Nomor kartu kredit <sup>2</sup>	Tinggi	Tinggi	Tinggi
Kode verifikasi kartu kredit	Sedang	Tinggi	Tinggi

1. Tingkat keparahannya sama untuk semua jenis nomor rekening bank — Nomor Rekening Bank Dasar (BBAN), Nomor Rekening Bank Internasional (IBAN), atau nomor rekening bank Kanada atau AS.
2. Tingkat keparahannya sama untuk nomor kartu kredit yang berada atau tidak berdekatan dengan kata kunci.

Jika temuan melaporkan beberapa tipe informasi keuangan dalam suatu objek, Macie menentukan kepelikan temuan ini dengan menghitung kepelikan untuk setiap tipe informasi keuangan yang Macie temukan, menentukan tipe yang menghasilkan kepelikan tertinggi, dan menetapkan tingkat kepelikan tertinggi tersebut ke temuan. Misalnya, jika Macie mendeteksi 10 tanggal kedaluwarsa kartu kredit (Tingkat keparahan sedang) dan 10 nomor kartu kredit (Tingkat keparahan tinggi) dalam suatu objek, Macie memberikan tingkat keparahan tinggi pada temuan tersebut.

### SensitiveData:S3Object/Personal

J: SensitiveDataTemuan S3Object/Personal menunjukkan bahwa objek S3 berisi informasi pribadi yang sensitif — informasi kesehatan pribadi (PHI), informasi identitas pribadi (PII), atau kombinasi

keduanya. Untuk tipe temuan ini, Macie menentukan kepelikan berdasarkan tipe dan jumlah kejadian dari informasi pribadi yang ditemukan Macie di objek.

Tabel berikut menunjukkan tingkat kepelikan yang Macie tetapkan kepada temuan data sensitif yang melaporkan kejadian PHI dalam objek S3.

Tipe data sensitif	1 kejadian	2-99 kejadian	100 atau lebih kejadian
Nomor Registrasi Badan Penegakan Narkoba (DEA)	Tinggi	Tinggi	Tinggi
Nomor Klaim Asuransi Kesehatan (HICN)	Tinggi	Tinggi	Tinggi
Asuransi kesehatan atau nomor identifikasi medis	Tinggi	Tinggi	Tinggi
Kode Sistem Pengkodean Prosedur Umum Kesehatan (HCPCS)	Tinggi	Tinggi	Tinggi
Kode Obat Nasional (NDC)	Tinggi	Tinggi	Tinggi
Pengidentifikasi Penyedia Nasional (NPI)	Tinggi	Tinggi	Tinggi
Pengidentifikasi perangkat unik (UDI)	Rendah	Sedang	Tinggi

Tabel berikut menunjukkan tingkat kepelikan yang Macie tetapkan kepada temuan data sensitif yang melaporkan kejadian PII dalam objek S3.

Tipe data sensitif	1 kejadian	2-99 kejadian	100 atau lebih kejadian
Tanggal lahir	Rendah	Sedang	Tinggi
Nomor identifikasi SIM	Rendah	Sedang	Tinggi
Nomor Roll Pemilu	Tinggi	Tinggi	Tinggi
Nama lengkap	Rendah	Sedang	Tinggi
Koordinat Sistem Pemosisian Global (GPS)	Rendah	Sedang	Sedang
HTTP cookie	Rendah	Sedang	Tinggi
Alamat surat-men yurat	Rendah	Sedang	Tinggi
Nomor Induk Kependudukan	Tinggi	Tinggi	Tinggi
Nomor Asuransi Nasional (NINO)	Tinggi	Tinggi	Tinggi
Nomor paspor	Sedang	Tinggi	Tinggi
Nomor tempat tinggal permanen	Tinggi	Tinggi	Tinggi
Nomor telepon	Rendah	Sedang	Tinggi
Nomor Asuransi Sosial (SIN)	Tinggi	Tinggi	Tinggi
Nomor Jaminan Sosial (SSN)	Tinggi	Tinggi	Tinggi

Tipe data sensitif	1 kejadian	2-99 kejadian	100 atau lebih kejadian
Nomor Pokok Wajib Pajak	Tinggi	Tinggi	Tinggi
Nomor identifikasi kendaraan (VIN)	Rendah	Rendah	Sedang

Jika sebuah temuan melaporkan beberapa jenis PHI, PII, atau keduanya PHI dan PII dalam suatu objek, Macie menentukan tingkat keparahan temuan dengan menghitung tingkat keparahan untuk setiap jenis, menentukan tipe mana yang menghasilkan tingkat keparahan tertinggi, dan menetapkan tingkat keparahan tertinggi pada temuan tersebut.

Misalnya, jika Macie mendeteksi 10 nama lengkap (tingkat kepelikan Medium) dan 5 nomor paspor (tingkat kepelikan Tinggi) dalam sebuah objek, Macie memberikan tingkat kepelikan Tinggi kepada temuan. Sama seperti kasus sebelumnya, jika Macie mendeteksi 10 nama lengkap (tingkat kepelikan Medium) dan 10 nomor identifikasi asuransi kesehatan (tingkat kepelikan Tinggi) dalam sebuah objek, Macie memberikan tingkat kepelikan Tinggi kepada temuan.

### SensitiveData:S3Object/Multiple

J: SensitiveDataTemuan S3Object/Multiple menunjukkan bahwa objek S3 berisi data yang mencakup beberapa kategori data sensitif—kombinasi data kredensial, informasi keuangan, informasi pribadi, atau teks yang cocok dengan kriteria deteksi satu atau lebih pengidentifikasi data kustom.

Untuk tipe temuan ini, Macie menentukan kepelikan dengan menghitung kepelikan untuk setiap tipe data sensitif yang Macie temukan (seperti yang ditunjukkan dalam topik sebelumnya), menentukan tipe menghasilkan tingkat kepelikan tertinggi, dan menetapkan tingkat kepelikan tertinggi tersebut kepada temuan.

Misalnya, jika Macie mendeteksi 10 nama lengkap (Tingkat keparahan sedang) dan 10 kunci akses AWS rahasia (Tingkat keparahan tinggi) dalam suatu objek, Macie memberikan tingkat keparahan tinggi pada temuan tersebut.



# Pemantauan dan pemrosesan temuan Amazon Macie

Untuk mendukung integrasi dengan aplikasi, layanan, dan sistem lain, seperti pemantauan atau sistem pengelolaan peristiwa, Amazon Macie secara otomatis memublikasikan kebijakan dan temuan data sensitif ke Amazon Macie secara otomatis memublikasikan kebijakan dan temuan data sensitif ke Amazon EventBridge Macie Untuk dukungan tambahan dan analisis yang lebih luas mengenai postur keamanan organisasi Anda, Anda dapat mengonfigurasi Macie untuk juga memublikasikan kebijakan dan temuan data sensitif ke. AWS Security Hub

## Amazon EventBridge

Amazon EventsEventBridge, yang sebelumnya Amazon CloudWatch Events, merupakan layanan bus peristiwa nirserver yang mengirimkan pengaliran data secara langsung dari aplikasi dan layanan, serta merutekan data tersebut ke target seperti AWS Lambda fungsi, topik Amazon Simple Notification Service, dan aliran Amazon Kinesis. DenganEventBridge, Anda dapat mengotomatisasi pemantauan dan pengolahan beberapa tipe peristiwa tertentu, termasuk peristiwa yang Macie terbitkan temuan. Untuk mempelajari selengkapnyaEventBridge, lihat [Panduan EventBridge Pengguna Amazon](#).

Jika Anda mengintegrasikan Notifikasi Pengguna AWS dengan Macie, Anda juga dapat menggunakan EventBridge peristiwa untuk secara otomatis menghasilkan notifikasi tentang peristiwa yang diterbitkan Macie untuk temuan. Dengan Pemberitahuan Pengguna, Anda membuat aturan khusus dan mengonfigurasi saluran pengiriman untuk menerima pemberitahuan tentang EventBridge peristiwa yang menarik. Saluran pengiriman termasuk email, notifikasi AWS Chatbot obrolan, dan notifikasi AWS Console Mobile Application push. Anda juga dapat meninjau pemberitahuan di lokasi pusat padaAWS Management Console. Untuk mempelajari lebih lanjut tentang Pemberitahuan Pengguna, lihat [Panduan Pengguna Notifikasi Pengguna AWS](#).

## AWS Security Hub

AWS Security Hubadalah layanan keamanan yang memberi Anda gambaran menyeluruh tentang status keamanan Anda di AWS lingkungan Anda. Ini mengumpulkan data keamanan dari Layanan AWS dan mendukung solusi AWS Partner Network keamanan, dan membantu Anda memeriksa lingkungan Anda sesuai standar industri keamanan dan praktik terbaik. Ini juga membantu Anda menganalisis tren keamanan dan mengidentifikasi masalah keamanan prioritas tertinggi tertinggi. Dengan Security Hub, Anda dapat meninjau temuan Macie sebagai bagian dari analisis yang lebih luas tentang postur keamanan organisasi Anda. Anda juga dapat

mengumpulkan temuan dari beberapa Wilayah AWS, dan memantau serta memproses data temuan gabungan dari satu Wilayah. Untuk mempelajari selengkapnya tentang Security Hub, lihat [Panduan Pengguna AWS Security Hub](#).

Ketika Macie membuat temuan, secara otomatis menerbitkan temuan untuk EventBridge sebagai peristiwa baru. Tergantung pada pengaturan publikasi yang Anda pilih untuk akun Anda, Macie juga dapat mempublikasikan temuan ke Security Hub. Macie menerbitkan setiap temuan baru secepatnya setelah selesai memproses temuan. Jika Macie mendeteksi kejadian berikutnya dari temuan kebijakan yang ada, Macie menerbitkan pembaruan untuk EventBridge peristiwa yang ada untuk temuan. Tergantung pada pengaturan publikasi Anda, Macie juga dapat mempublikasikan pembaruan ke Security Hub. Macie menerbitkan pembaruan ini secara berulang, menggunakan frekuensi publikasi yang Anda tentukan dalam pengaturan publikasi untuk akun Anda.

### Topik

- [Mengonfigurasi pengaturan publikasi untuk temuan Amazon Macie](#)
- [Integrasi Amazon Macie dengan Amazon EventBridge](#)
- [Integrasi Amazon Macie dengan AWS Security Hub](#)
- [Integrasi Amazon Macie dengan Notifikasi Pengguna AWS](#)
- [Skema EventBridge acara Amazon untuk temuan Amazon Macie](#)

## Mengonfigurasi pengaturan publikasi untuk temuan Amazon Macie

Untuk mendukung integrasi dengan aplikasi, layanan, dan sistem lain, Amazon Macie secara otomatis menerbitkan temuan kebijakan dan temuan data sensitif ke Amazon EventBridge sebagai peristiwa. Untuk informasi tentang bagaimana Anda dapat menggunakan EventBridge untuk memantau dan memproses temuan, lihat [Integrasi Amazon Macie dengan Amazon EventBridge](#).

Anda dapat mengonfigurasi Macie untuk mempublikasikan temuan secara otomatis AWS Security Hub juga, menggunakan opsi tujuan yang Anda tentukan dalam pengaturan publikasi untuk akun Anda. Dengan opsi ini, Anda dapat mengonfigurasi Macie untuk hanya memublikasikan temuan kebijakan dan temuan data sensitif, atau memublikasikan kedua temuan data kebijakan dan sensitif ke Security Hub. Anda juga dapat mengonfigurasi Macie untuk menghentikan penerbitan temuan ke Security Hub. Untuk informasi tentang bagaimana Anda dapat menggunakan Security Hub untuk memantau dan memproses temuan, lihat [Integrasi Amazon Macie dengan AWS Security Hub](#).

Untuk temuan kebijakan, waktu Macie menerbitkan temuan ke yang lain Layanan AWS tergantung pada apakah temuan itu baru dan frekuensi publikasi yang Anda tentukan untuk akun Anda. Untuk temuan data sensitif, waktu temuan selalu berada pada status segera—Macie segera menerbitkan temuan data sensitif setelah selesai memproses temuan. Tidak seperti temuan kebijakan, Macie memperlakukan semua temuan data sensitif sebagai baru (unik).

Perhatikan bahwa Macie tidak memublikasikan kebijakan atau temuan data sensitif yang diarsipkan secara otomatis oleh [aturan penekanan](#). Dengan kata lain, Macie tidak memublikasikan temuan yang ditekan kepada orang lain. Layanan AWS

## Topik

- [Memilih tujuan publikasi untuk temuan](#)
- [Menentukan frekuensi publikasi untuk temuan](#)
- [Mengubah frekuensi publikasi untuk temuan](#)

## Memilih tujuan publikasi untuk temuan

Anda dapat mengonfigurasi Amazon Macie untuk secara otomatis memublikasikan kebijakan dan temuan data sensitif AWS Security Hub selain Amazon. EventBridge Secara default, Macie hanya memublikasikan temuan kebijakan baru dan diperbarui ke Security Hub. Untuk mengubah atau memperluas konfigurasi default, sesuaikan pengaturan tujuan publikasi untuk akun Anda.

Saat menyesuaikan pengaturan tujuan, Anda memilih kategori temuan yang ingin dipublikasikan oleh Macie ke Security Hub—hanya temuan kebijakan, hanya temuan data sensitif, atau temuan data sensitif dan kebijakan. Anda juga dapat memilih untuk berhenti memublikasikan kategori penemuan untuk Security Hub.

Jika Anda mengubah pengaturan tujuan, perubahan Anda hanya berlaku untuk saat ini Wilayah AWS. Jika Anda adalah administrator Macie untuk sebuah organisasi, perubahan yang Anda lakukan hanya berlaku untuk akun Anda. Hal ini tidak berlaku untuk akun anggota terkait. Untuk informasi selengkapnya, lihat [Mengelola beberapa akun](#).

Untuk memilih tujuan publikasi untuk temuan

1. [Buka konsol Amazon Macie di https://console.aws.amazon.com/macie/](https://console.aws.amazon.com/macie/).
2. Pada panel navigasi, silakan pilih Pengaturan.
3. Di bagian Publikasi temuan, di bagian bawah Tujuan pilih salah satu opsi berikut:

- Publikasikan temuan kebijakan ke Security Hub — Pilih kotak centang ini untuk mulai menerbitkan temuan kebijakan baru dan yang diperbarui ke Security Hub secara otomatis. Untuk menghentikan penerbitan temuan kebijakan yang baru dan diperbarui ke Security Hub, Hapus kotak centang ini.

Jika Anda memilih kotak centang ini dan memiliki temuan kebijakan yang ada, Macie tidak mempublikasikannya ke Security Hub secara otomatis. Sebagai gantinya, Macie hanya menerbitkan temuan kebijakan yang dibuatnya atau diperbarui setelah Anda menyimpan perubahan.

- Publikasikan temuan data sensitif ke Security Hub — Pilih kotak centang ini untuk mulai menerbitkan temuan data sensitif baru ke Security Hub secara otomatis. Untuk menghentikan penerbitan temuan data sensitif baru ke Security Hub, kosongkan kotak centang ini.

Jika Anda memilih kotak centang ini dan Anda memiliki temuan data sensitif yang ada, Macie tidak mempublikasikannya ke Security Hub secara otomatis. Sebagai gantinya, Macie hanya menerbitkan temuan data sensitif yang dibuatnya setelah Anda menyimpan perubahan Anda.

#### 4. Pilih Simpan.

Jika Anda memilih untuk mempublikasikan kategori temuan apa pun ke Security Hub, pastikan Anda juga mengaktifkan Security Hub di Wilayah saat ini dan mengonfigurasinya untuk menerima temuan dari Macie. Jika tidak, Anda tidak akan dapat mengakses temuan di Security Hub. Untuk mempelajari cara menerima temuan di Security Hub, lihat [Mengelola integrasi produk](#) di Panduan Pengguna AWS Security Hub .

## Menentukan frekuensi publikasi untuk temuan

Di Amazon Macie, setiap temuan memiliki pengenal unik. Macie menggunakan pengenal ini untuk menentukan kapan harus mempublikasikan temuan ke yang lain: Layanan AWS

- Temuan baru — Ketika Macie membuat temuan kebijakan baru atau data sensitif, Macie memberikan pengenal yang unik untuk temuan sebagai bagian dari pengolahan temuan. Segera setelah Macie selesai memproses temuan tersebut, ia menerbitkan temuan tersebut sebagai acara Amazon baru. EventBridge Bergantung pada pengaturan publikasi untuk akun Anda, Macie juga menerbitkan temuan tersebut sebagai temuan baru. AWS Security Hub
- Memutakhirkan temuan — Ketika Macie mendeteksi kejadian berikutnya dari temuan kebijakan yang sudah ada, Macie melakukan pembaruan pada temuan yang sudah ada dengan

menambahkan detail tentang kejadian berikutnya dan tambahan hitungan dari kejadian. Macie juga menerbitkan pembaruan ini ke EventBridge acara yang ada dan, tergantung pada pengaturan publikasi untuk akun Anda, temuan Security Hub yang ada. Macie melakukan ini hanya demi temuan kebijakan. Temuan data sensitif, tidak seperti temuan kebijakan, semuanya diperlakukan sebagai baru (unik).

Secara default, Macie menerbitkan temuan terbaru setiap 15 menit sebagai bagian dari siklus publikasi berulang. Hal ini berarti bahwa setiap temuan kebijakan yang diperbarui setelah siklus publikasi terbaru akan diadakan, pembaruan lagi pada temuan kebijakan seperlunya, dan termasuk dalam siklus publikasi berikutnya (sekitar 15 menit kemudian). Anda dapat mengubah jadwal ini dengan memilih frekuensi publikasi yang berbeda. Misalnya, jika Anda mengonfigurasi Macie untuk mempublikasikan temuan yang diperbarui setiap jam dan publikasi terjadi pada pukul 12:00, pembaruan apa pun yang terjadi setelah pukul 12:00 akan diterbitkan pada pukul 13:00.

Mohon untuk memperhatikan bahwa tidak satu pun dari kasus ini berlaku untuk temuan yang diarsipkan secara otomatis oleh [aturan penekanan](#). Macie tidak mempublikasikan temuan yang ditekan ke orang lain. Layanan AWS

## Mengubah frekuensi publikasi untuk temuan

Anda dapat mengubah jadwal yang digunakan Amazon Macie untuk mempublikasikan pembaruan temuan kebijakan yang ada di situs lain. Layanan AWS Secara default, Macie memublikasikan temuan terbaru setiap 15 menit. Jika Anda mengubah jadwal ini, perubahan Anda hanya berlaku untuk saat ini Wilayah AWS. Jika Anda adalah administrator Macie untuk sebuah organisasi, perubahan yang Anda lakukan juga berlaku untuk semua akun milik anggota yang berkaitan di Wilayah. Untuk informasi selengkapnya, lihat [Mengelola beberapa akun](#).

Untuk mengubah frekuensi publikasi untuk temuan terbaru

1. [Buka konsol Amazon Macie di https://console.aws.amazon.com/macie/](https://console.aws.amazon.com/macie/).
2. Pada panel navigasi, silakan pilih Pengaturan.
3. Di bagian Publikasi temuan, di bawah Frekuensi pembaruan untuk temuan kebijakan, pilih seberapa sering Anda ingin Macie mempublikasikan temuan kebijakan yang diperbarui ke yang lain Layanan AWS.
4. Pilih Simpan.

## Integrasi Amazon Macie dengan Amazon EventBridge

Amazon EventBridge, sebelumnya Amazon CloudWatch Events, adalah layanan bus peristiwa nonserver. EventBridge mengirimkan pengaliran data secara langsung dari aplikasi dan layanan, dan merutekan data tersebut ke target seperti AWS Lambda fungsi, topik Amazon Simple Notification Service (Amazon SNS), dan aliran Amazon Kinesis. Untuk mempelajari selengkapnya EventBridge, lihat [Panduan EventBridge Pengguna Amazon](#).

Dengan EventBridge, Anda dapat mengotomatisasi pemantauan dan pemrosesan tipe peristiwa tertentu. Ini termasuk peristiwa yang Amazon Macie publikasikan secara otomatis untuk temuan kebijakan baru dan temuan data sensitif. Ini juga mencakup peristiwa yang dipublikasikan oleh Macie secara otomatis untuk kejadian berikutnya dari temuan kebijakan yang ada. Untuk detail tentang cara dan waktu Macie memublikasikan peristiwa ini, lihat [Mengonfigurasi pengaturan publikasi untuk temuan](#).

Dengan menggunakan EventBridge dan peristiwa yang dipublikasikan Macie untuk temuan, Anda dapat memantau dan memproses temuan dalam waktu dekat. Anda kemudian dapat bertindak berdasarkan temuan dengan menggunakan aplikasi dan layanan lain. Misalnya, Anda mungkin menggunakan EventBridge untuk mengirim tipe temuan baru tertentu ke AWS Lambda fungsi. Fungsi Lambda kemudian dapat memproses dan mengirim data ke sistem insiden keamanan dan manajemen kejadian (SIEM) Anda. Jika Anda [mengintegrasikan Notifikasi Pengguna AWS dengan Macie](#), Anda juga dapat menggunakan peristiwa tersebut untuk diberi tahu temuan secara otomatis melalui saluran pengiriman yang Anda tentukan.

Selain pemantauan dan pemrosesan otomatis, penggunaan EventBridge memungkinkan penyimpanan data temuan Anda dalam jangka panjang. Macie menyimpan temuan selama 90 hari. Dengan EventBridge demikian, Anda dapat mengirim data temuan ke platform penyimpanan pilihan Anda dan menyimpan data tersebut selama yang Anda inginkan.

### Note

Untuk penyimpanan jangka panjang, konfigurasi juga Macie untuk menyimpan hasil penemuan data sensitif Anda dalam bucket S3. Hasil penemuan data sensitif adalah catatan detail log tentang analisis yang Macie lakukan pada objek S3 untuk menentukan apakah objek tersebut berisi data sensitif. Untuk mempelajari selengkapnya, lihat [Menyimpan dan mempertahankan hasil penemuan data sensitif](#).

## Topik

- [Bekerja dengan Amazon EventBridge](#)
- [Membuat EventBridge aturan Amazon untuk temuan](#)

## Bekerja dengan Amazon EventBridge

Dengan Amazon EventBridge, Anda membuat aturan untuk menentukan peristiwa yang ingin Anda pantau dan target yang ingin Anda lakukan untuk tindakan otomatis peristiwa tersebut. Target adalah tujuan yang EventBridge mengirimkan peristiwa ke.

Untuk mengotomatisasi pemantauan dan pemrosesan tugas untuk temuan, Anda dapat membuat EventBridge aturan yang secara otomatis mendeteksi peristiwa temuan Amazon Macie dan mengirimkan peristiwa tersebut ke aplikasi atau layanan lain untuk pemrosesan atau tindakan lainnya. Anda dapat menyesuaikan aturan untuk mengirim hanya peristiwa yang memenuhi kriteria tertentu. Untuk melakukan hal ini, tentukan kriteria yang berasal dari [EventBridge skema acara untuk temuan](#)

Misalnya, Anda dapat membuat aturan yang mengirimkan tipe temuan baru tertentu ke fungsi AWS Lambda. Fungsi Lambda kemudian dapat melakukan tugas-tugas seperti: memproses dan mengirim data ke sistem SIEM Anda; secara otomatis menerapkan tipe enkripsi sisi server tertentu ke objek S3; atau, membatasi akses ke objek. Atau Anda dapat membuat aturan yang secara otomatis mengirimkan temuan tingkat kepelikan tinggi baru ke topik Amazon SNS, yang kemudian memberi tahu tim respons insiden Anda tentang temuan tersebut.

Selain memanggil fungsi Lambda dan memberitahukan topik Amazon SNS, EventBridge mendukung tipe target dan tindakan lainnya, seperti menyampaikan peristiwa ke aliran Amazon Kinesis, mengaktifkan AWS Step Functions mesin status, dan memanggil perintah run. AWS Systems Manager Untuk informasi tentang target yang didukung, lihat [EventBridge target Amazon](#) di EventBridge Panduan Pengguna Amazon.

## Membuat EventBridge aturan Amazon untuk temuan

Prosedur berikut menjelaskan cara menggunakan EventBridge konsol Amazon dan [AWS Command Line Interface\(AWS CLI\)](#) untuk membuat EventBridge aturan temuan Amazon Macie. Aturan mendeteksi EventBridge peristiwa yang menggunakan skema dan pola peristiwa untuk temuan Macie, dan mengirimkan peristiwa tersebut ke fungsi untuk diproses. AWS Lambda

AWS Lambda adalah layanan komputasi yang dapat Anda gunakan untuk menjalankan kode tanpa perlu menyediakan atau mengelola server. Anda mengemas kode Anda dan mengunggahnya ke AWS Lambda sebagai Fungsi Lambda. AWS Lambda kemudian menjalankan fungsi saat fungsi tersebut dipanggil. Fungsi dapat dipanggil secara manual oleh Anda, secara otomatis dalam respons terhadap peristiwa, atau dalam merespons atas permintaan dari aplikasi atau layanan. Untuk informasi tentang membuat dan memanggil fungsi Lambda, lihat [Panduan Developer AWS Lambda](#).

## Console

Prosedur ini menjelaskan cara menggunakan EventBridge konsol Amazon untuk membuat aturan yang secara otomatis mengirimkan semua peristiwa temuan Macie ke fungsi Lambda untuk diproses. Aturan menggunakan pengaturan default untuk aturan yang berjalan saat peristiwa tertentu diterima. Untuk detail tentang pengaturan aturan atau untuk mempelajari cara membuat aturan yang menggunakan pengaturan khusus, lihat [Membuat aturan yang bereaksi terhadap peristiwa](#) di Panduan EventBridge Pengguna Amazon.

### Tip

Anda juga dapat membuat aturan yang menggunakan pola kustom untuk mendeteksi dan hanya bertindak atas subset dari peristiwa temuan Macie. Subset ini dapat didasarkan pada bidang tertentu yang Macie sertakan dalam peristiwa temuan. Untuk mempelajari bidang yang tersedia, lihat [EventBridge skema acara untuk temuan](#). Untuk mempelajari cara membuat aturan tipe ini, lihat [Penyaringan konten dalam pola peristiwa](#) dalam Panduan EventBridge Pengguna Amazon.

Sebelum Anda membuat aturan ini, buat fungsi Lambda yang Anda inginkan aturan tersebut digunakan sebagai target. Saat Anda membuat aturan tersebut, Anda harus menentukan fungsi ini sebagai target aturan.

Untuk membuat aturan peristiwa dengan menggunakan konsol tersebut

1. Buka konsol Amazon EventBridge di <https://console.aws.amazon.com/events/>.
2. Di panel navigasi, di dalam Peristiwa, pilih Aturan.
3. Di bagian Aturan, pilih Buat aturan.
4. Pada halaman Tentukan detail aturan, lakukan langkah-langkah berikut:
  - Untuk Nama, masukkan nama untuk aturan.



- (Opsional) Untuk Deskripsi, masukkan deskripsi singkat aturan.
  - Untuk Bus peristiwa, pastikan default dipilih dan Aktifkan aturan pada bus peristiwa yang dipilih diaktifkan.
  - Untuk jenis Aturan, pilih Aturan dengan pola peristiwa.
5. Setelah selesai, pilih Selanjutnya.
  6. Pada halaman Build tindakan, lakukan langkah-langkah berikut:
    - Untuk Sumber acara, pilih AWSacara atau EventBridge mitra.
    - (Opsional) Untuk kejadian Contoh, tinjau contoh peristiwa temuan untuk Macie untuk mempelajari apa yang mungkin berisi peristiwa. Untuk melakukan ini, pilih AWSacara. Kemudian, untuk acara Contoh, pilih Macie Finding.
    - Untuk Event pattern, pilih Event pattern form. Kemudian masukkan pengaturan berikut:
      - Untuk sumber Event, pilih Layanan AWS.
      - Untuk Layanan AWS, masukkan Macie.
      - Untuk jenis Event, masukkan Macie Finding.
  7. Setelah selesai, pilih Selanjutnya.
  8. Pada halaman Pilih target, lakukan langkah-langkah berikut:
    - Untuk jenis Target, pilih Layanan AWS.
    - Untuk Pilih target, masukkan fungsi Lambda. Kemudian, untuk Fungsi, pilih fungsi Lambda yang Anda inginkan untuk dikirimkan ke peristiwa temuan.
    - Untuk Konfigurasi versi/alias, masukkan pengaturan versi dan alias untuk fungsi Lambda target.
    - (Opsional) Untuk Pengaturan tambahan, masukkan pengaturan khusus untuk menentukan data peristiwa yang ingin Anda kirimkan ke fungsi Lambda. Anda juga dapat menentukan cara menangani peristiwa yang tidak dikirim ke fungsi dengan berhasil.
  9. Setelah selesai, pilih Selanjutnya.
  10. Pada halaman Konfigurasikan tag, masukkan satu atau beberapa tag untuk ditetapkan ke aturan. Kemudian pilih Selanjutnya.
  11. Pada halaman Tinjau dan buat, tinjau pengaturan aturan dan verifikasi bahwa pengaturan aturan sudah benar.

Untuk mengubah pengaturan, pilih Edit di bagian yang berisi pengaturan, lalu masukkan pengaturan yang benar. Anda juga dapat menggunakan tab navigasi untuk membuka halaman yang berisi pengaturan.

12. Setelah selesai memverifikasi pengaturan, pilih Buat aturan.

## AWS CLI

Prosedur ini menjelaskan cara menggunakan AWS CLI untuk membuat EventBridge aturan yang mengirimkan semua peristiwa temuan Macie ke fungsi Lambda untuk diproses. Aturan menggunakan pengaturan default untuk aturan yang berjalan saat peristiwa tertentu diterima. Dalam prosedur, perintah diformat untuk Microsoft Windows. Untuk Linux, macOS, atau Unix, ganti karakter kelanjutan baris tanda sisipan (^) dengan garis miring terbalik (\).

Sebelum Anda membuat aturan ini, buat fungsi Lambda yang Anda inginkan aturannya untuk digunakan sebagai target. Ketika Anda membuat fungsi, perhatikan Amazon Resource Name (ARN) dari fungsi tersebut. Anda harus memasukkan ARN ini ketika Anda menentukan target untuk aturan.

Untuk membuat aturan peristiwa dengan menggunakan AWS CLI

1. Buat aturan yang mendeteksi peristiwa untuk semua temuan yang dipublikasikan Macie. EventBridge Untuk melakukan ini, gunakan perintah EventBridge [put-rule](#). Misalnya:

```
C:\> aws events put-rule ^  
--name MacieFindings ^  
--event-pattern "{\"source\":[\"aws.macie\"]}"
```

Di *MacieFindings* mana nama yang Anda inginkan untuk aturan.

Jika perintah berhasil berjalan, EventBridge merespons dengan ARN dari aturan. Perhatikan ARN ini. Anda harus memasukkannya pada langkah 3.

### Tip

Anda juga dapat membuat aturan yang menggunakan pola kustom untuk mendeteksi dan hanya bertindak atas subset dari peristiwa temuan Macie. Subset ini dapat didasarkan pada bidang tertentu yang Macie sertakan dalam peristiwa temuan. Untuk mempelajari bidang yang tersedia, lihat [EventBridge skema acara untuk temuan](#).

Untuk mempelajari cara membuat aturan tipe ini, lihat [Penyaringan konten dalam pola peristiwa](#) dalam Panduan EventBridge Pengguna Amazon.

2. Tentukan fungsi Lambda yang akan digunakan sebagai target aturan. Untuk melakukan ini, gunakan perintah EventBridge [put-targets](#). Misalnya:

```
C:\> aws events put-targets ^
--rule MacieFindings ^
--targets Id=1,Arn=arn:aws:lambda:regionalEndpoint:accountID:function:my-
findings-function
```

Nama *MacieFindings* yang Anda tentukan untuk aturan di langkah 1, dan nilai untuk Arn parameter tersebut adalah ARN dari fungsi yang ingin Anda gunakan aturannya sebagai target.

3. Tambahkan izin yang mengizinkan aturan untuk memanggil target fungsi Lambda. Untuk melakukan ini, gunakan perintah [add-permission](#) Lambda. Misalnya:

```
C:\> aws lambda add-permission ^
--function-name my-findings-function ^
--statement-id Sid ^
--action lambda:InvokeFunction ^
--principal events.amazonaws.com ^
--source-arn arn:aws:events:regionalEndpoint:accountId:rule:MacieFindings
```

Dengan:

- *my-findings-function* adalah nama fungsi Lambda yang Anda inginkan aturan tersebut digunakan sebagai target.
- *Sid* adalah pengidentifikasi pernyataan yang Anda tetapkan untuk menjelaskan pernyataan dalam kebijakan fungsi Lambda.
- *source-arn* adalah ARN EventBridge aturan.

Jika perintah berhasil berjalan, Anda akan menerima output yang sama dengan yang berikut ini:

```
{
  "Statement": "{\"Sid\":\"sid\",
    \"Effect\":\"Allow\",
```

```
\\"Principal\\":{\\"Service\\":\\"events.amazonaws.com\\"},
\\"Action\\":\\"lambda:InvokeFunction\\",
\\"Resource\\":\\"arn:aws:lambda:us-east-1:111122223333:function:my-findings-
function\\",
\\"Condition\\":
  {\\"ArnLike\\":
    {\\"AWS:SourceArn\\":
      \\"arn:aws:events:us-east-1:111122223333:rule/MacieFindings\\"}}}"}
}
```

Nilai Statement adalah versi string JSON dari pernyataan yang ditambahkan ke kebijakan fungsi Lambda.

## Integrasi Amazon Macie dengan AWS Security Hub

AWS Security Hub adalah layanan yang memberi Anda pandangan komprehensif tentang postur keamanan Anda ke seluruh lingkungan AWS dan membantu memeriksa lingkungan Anda terhadap standar industri keamanan dan praktik terbaik. Hal ini dilakukan sebagian dengan mengonsumsi, menggabungkan, mengatur, dan memprioritaskan temuan dari berbagai Layanan AWS solusi keamanan yang didukung. AWS Partner Network Security Hub membantu Anda menganalisis tren keamanan dan mengidentifikasi masalah keamanan dengan prioritas tertinggi. Dengan Security Hub, Anda juga dapat mengumpulkan temuan dari beberapa Wilayah AWS, lalu memantau dan memproses semua data temuan agregat dari satu Wilayah. Untuk mempelajari selengkapnya tentang Security Hub, lihat [Panduan Pengguna AWS Security Hub](#).

Amazon Macie terintegrasi dengan Security Hub, yang berarti Anda dapat mempublikasikan temuan dari Macie ke Security Hub secara otomatis. Security Hub kemudian dapat menyertakan temuan tersebut dalam analisis postur keamanan Anda. Selain itu, Anda dapat menggunakan Security Hub untuk memantau dan memproses kebijakan dan temuan data sensitif sebagai bagian dari kumpulan data temuan yang lebih besar dan teragregat untuk AWS lingkungan Anda. Dengan kata lain, Anda dapat menganalisis temuan Macie sambil melakukan analisis yang lebih luas tentang postur keamanan organisasi Anda, dan memulihkan temuan seperlunya. Security Hub mengurangi kompleksitas penanganan temuan volume besar dari beberapa penyedia. Selain itu, ia menggunakan format standar untuk semua temuan, termasuk temuan dari Macie. Penggunaan format ini, AWS Security Finding Format (ASFF), menghilangkan kebutuhan Anda untuk melakukan konversi data yang memakan waktu.

### Topik

- [Bagaimana Amazon Macie menerbitkan temuan ke AWS Security Hub](#)
- [Contoh temuan Amazon Macie di AWS Security Hub](#)
- [Mengaktifkan dan mengonfigurasi integrasi AWS Security Hub](#)
- [Menghentikan publikasi temuan untuk AWS Security Hub](#)

## Bagaimana Amazon Macie menerbitkan temuan ke AWS Security Hub

Di AWS Security Hub, masalah keamanan dilacak sebagai temuan. Beberapa temuan berasal dari masalah yang terdeteksi oleh Layanan AWS, seperti Amazon Macie, atau dengan solusi AWS Partner Network keamanan yang didukung. Security Hub juga memiliki seperangkat aturan yang digunakan untuk mendeteksi masalah keamanan dan membuat temuan.

Security Hub menyediakan peralatan untuk mengelola temuan dari semua sumber tersebut. Anda dapat meninjau dan memfilter daftar temuan dan meninjau detail temuan individu. Untuk mempelajari caranya, lihat [Melihat daftar dan detail pencarian](#) di Panduan AWS Security Hub Pengguna. Anda juga dapat melacak status investigasi menjadi temuan. Untuk mempelajari cara melakukannya, lihat [Mengambil tindakan pada temuan](#) di Panduan Pengguna AWS Security Hub.

Semua temuan di Security Hub menggunakan format standar JSON yang disebut AWS Security Finding Format (ASFF). ASFF mencakup detail tentang sumber masalah, sumber daya yang terpengaruh, dan status temuan saat ini. Untuk informasi selengkapnya, lihat [AWS Security Finding Format \(ASFF\)](#) di Panduan Pengguna AWS Security Hub.

### Tipe temuan yang dipublikasikan oleh Macie

Tergantung pada pengaturan publikasi yang Anda pilih untuk akun Macie Anda, Macie dapat memublikasikan semua temuan yang dibuatnya ke Security Hub, baik temuan data sensitif maupun temuan kebijakan. Untuk informasi tentang pengaturan ini dan cara mengubahnya, lihat [Mengonfigurasi pengaturan publikasi untuk temuan](#). Secara default, Macie hanya memublikasikan temuan kebijakan yang baru dan terbaru ke Security Hub. Macie tidak memublikasikan temuan data sensitif ke Security Hub.

#### Temuan data sensitif

Jika Anda mengonfigurasi Macie untuk memublikasikan [Temuan data sensitif](#) ke Security Hub, Macie secara otomatis menerbitkan setiap temuan data sensitif yang dibuatnya untuk akun Anda dan melakukannya segera setelah selesai memproses temuan. Macie melakukan ini untuk semua temuan data sensitif yang tidak diarsipkan secara otomatis oleh [Aturan penekan](#).

Jika Anda administrator Macie untuk suatu organisasi, publikasi terbatas pada temuan dari pekerjaan penemuan data sensitif yang Anda jalankan dan aktivitas penemuan data sensitif otomatis yang dilakukan Macie untuk organisasi Anda. Hanya akun yang membuat tugas dapat memublikasikan temuan data sensitif yang dihasilkan oleh tugas. Hanya akun administrator Macie yang dapat memublikasikan temuan data sensitif yang dihasilkan oleh penemuan data sensitif otomatis untuk organisasi mereka.

Ketika Macie memublikasikan temuan data sensitif ke Security Hub, Macie menggunakan [AWS Security Finding Format \(ASFF\)](#), yang merupakan format standar untuk semua temuan di Security Hub. Dalam ASFF, bidang Types menunjukkan tipe temuan. Bidang ini menggunakan taksonomi yang sedikit berbeda dari tipe temuan taksonomi di Macie.

Tabel berikut mencantumkan daftar tipe temuan ASFF untuk setiap tipe temuan data sensitif ketika Macie dapat membuatnya.

Tipe temuan Macie	Tipe temuan ASFF
SensitiveData:S3Object/Credentials	Sensitive Data Identifications/Passwords/SensitiveData:S3Object-Credentials
SensitiveData:S3Object/CustomIdentifier	Sensitive Data Identifications/PII/SensitiveData:S3Object-CustomIdentifier
SensitiveData:S3Object/Financial	Sensitive Data Identifications/Financial/SensitiveData:S3Object-Financial
SensitiveData:S3Object/Multiple	Sensitive Data Identifications/PII/SensitiveData:S3Object-Multiple
SensitiveData:S3Object/Personal	Sensitive Data Identifications/PII/SensitiveData:S3Object-Personal

## Temuan kebijakan

Jika Anda mengonfigurasi Macie untuk memublikasikan [temuan kebijakan](#) ke Security Hub, Macie secara otomatis menerbitkan setiap temuan kebijakan baru yang dibuat dan melakukannya segera setelah Macie selesai memproses temuan. Jika Macie mendeteksi kejadian berikutnya dari temuan kebijakan yang ada, Macie secara otomatis menerbitkan pembaruan untuk temuan yang ada di Security Hub, menggunakan frekuensi publikasi yang Anda tentukan untuk akun Anda. Macie melakukan tugas ini untuk semua temuan kebijakan yang tidak diarsipkan secara otomatis oleh [Aturan penekanan](#).

Jika Anda administrator Macie untuk suatu organisasi, publikasi terbatas pada temuan kebijakan untuk bucket S3 yang dimiliki langsung oleh akun Anda. Macie tidak memublikasikan temuan kebijakan yang dibuat atau diperbarui untuk akun anggota di organisasi Anda. Hal ini membantu untuk memastikan bahwa Anda tidak memiliki data temuan duplikat di Security Hub.

Sama halnya dengan temuan data sensitif, Macie menggunakan AWS Security Finding Format (ASFF) ketika Macie memublikasikan temuan kebijakan yang baru dan diperbarui untuk Security Hub. Dalam ASFF, bidang Types menggunakan taksonomi yang sedikit berbeda dari tipe temuan taksonomi di Macie.

Tabel berikut mencantumkan tipe temuan ASFF untuk setiap tipe temuan kebijakan ketika Macie dapat membuatnya. Jika Macie membuat atau memperbarui temuan kebijakan di Security Hub pada atau setelah 28 Januari 2021, temuan memiliki salah satu nilai berikut untuk bidang Types ASFF di Security Hub.

Tipe temuan Macie	Tipe temuan ASFF
Policy:IAMUser/S3BlockPublicAccessDisabled	Software and Configuration Checks/AWS Security Best Practices/Policy:IAMUser-S3BlockPublicAccessDisabled
Policy:IAMUser/S3BucketEncryptionDisabled	Software and Configuration Checks/AWS Security Best Practices/Policy:IAMUser-S3BucketEncryptionDisabled
Policy:IAMUser/S3BucketPublic	Effects/Data Exposure/Policy:IAMUser-S3BucketPublic

Tipe temuan Macie	Tipe temuan ASFF
Policy:IAMUser/S3BucketReplicatedExternally	Software and Configuration Checks/AWS Security Best Practices/Policy:IAMUser-S3BucketReplicatedExternally
Policy:IAMUser/S3BucketSharedExternally	Software and Configuration Checks/AWS Security Best Practices/Policy:IAMUser-S3BucketSharedExternally
Policy:IAMUser/S3BucketSharedWithCloudFront	Software and Configuration Checks/AWS Security Best Practices/Policy:IAMUser-S3BucketSharedWithCloudFront

Jika Macie membuat atau terakhir memperbarui temuan kebijakan sebelum 28 Januari 2021, temuan tersebut memiliki salah satu nilai berikut untuk bidang Types ASFF di Security Hub:

- Policy:IAMUser/S3BlockPublicAccessDisabled
- Policy:IAMUser/S3BucketEncryptionDisabled
- Policy:IAMUser/S3BucketPublic
- Policy:IAMUser/S3BucketReplicatedExternally
- Policy:IAMUser/S3BucketSharedExternally

Nilai-nilai dalam daftar peta langsung sebelumnya ke nilai-nilai untuk bidang Tipe temuan (type) di Macie.

#### Note

Ketika Anda meninjau dan memproses temuan kebijakan di Security Hub, perhatikan pengecualian berikut ini:

- Secara pastiWilayah AWS, Macie mulai menggunakan tipe temuan ASFF untuk temuan baru dan yang diperbarui pada awal 25 Januari 2021.



- Jika Anda menindaklanjuti temuan kebijakan di Security Hub sebelum Macie mulai menggunakan tipe pencarian ASFF di AndaWilayah AWS, nilai untuk Types bidang ASFF dari temuan tersebut akan menjadi salah satu jenis temuan Macie di daftar sebelumnya. Hal ini tidak akan menjadi salah satu tipe temuan ASFF pada tabel sebelumnya. Hal ini berlaku untuk temuan kebijakan ketika Anda menjalankannya dengan menggunakan konsol AWS Security Hub atau operasi BatchUpdateFindings dari AWS Security Hub API.

## Latensi untuk penerbitan temuan

Ketika Macie membuat kebijakan baru atau temuan data sensitif, Macie akan memublikasikan temuan ke Security Hub dengan segera setelah selesai memproses temuan.

Ketika Macie mendeteksi kejadian berikutnya dari temuan kebijakan yang ada, Macie menerbitkan pembaruan untuk temuan Security Hub yang ada. Waktu pembaruan tergantung pada frekuensi publikasi yang Anda pilih untuk akun Macie Anda. Secara default, Macie memublikasikan pembaruan setiap 15 menit. Untuk informasi selengkapnya, termasuk bagaimana mengubah pengaturan akun, lihat [Mengonfigurasi pengaturan publikasi untuk temuan](#).

## Mencoba kembali publikasi ketika Security Hub tidak tersedia

Jika Security Hub tidak tersedia, Macie membuat antrian temuan yang belum diterima oleh Security Hub. Ketika sistem dipulihkan, Macie mencoba lagi publikasi hingga temuan diterima oleh Security Hub.

## Memperbarui temuan yang ada di Security Hub

Setelah Macie menerbitkan temuan kebijakan ke Security Hub, Macie memperbarui temuan untuk menggambarkan kejadian tambahan dari temuan atau aktivitas temuan. Macie melakukan ini hanya demi temuan kebijakan. Temuan data sensitif, tidak seperti temuan kebijakan, semuanya diperlakukan sebagai baru (unik).

Ketika Macie memublikasikan pembaruan untuk temuan kebijakan, Macie memperbarui nilai untuk bidang temuan Diperbarui Pada (UpdatedAt). Anda dapat menggunakan nilai ini untuk menentukan kapan Macie baru-baru ini mendeteksi terjadinya potensi pelanggaran kebijakan atau masalah berikutnya yang menghasilkan temuan tersebut.

Macie mungkin juga memperbarui nilai untuk bidang temuan Tipe (Types) jika nilai yang ada untuk bidang tersebut bukan merupakan [Tipe temuan ASFF](#). Hal ini tergantung pada apakah Anda telah bertindak berdasarkan temuan di Security Hub. Jika Anda belum bertindak berdasarkan

temuan, Macie mengubah nilai bidang untuk tipe temuan ASFF yang sesuai. Jika Anda telah menjalankan temuan tersebut, menggunakan salah satu konsol AWS Security Hub atau operasi `BatchUpdateFindings` dari AWS Security Hub API, Macie tidak mengubah nilai bidang.

## Contoh temuan Amazon Macie di AWS Security Hub

Saat Amazon Macie menerbitkan temuannya AWS Security Hub, Amazon Macie menggunakan [AWS Security Finding Format \(ASFF\)](#). Ini merupakan format standar untuk semua temuan di Security Hub. Contoh berikut menggunakan data sampel untuk mendemonstrasikan struktur dan sifat data temuan yang diterbitkan Macie ke Security Hub dalam format ini:

- [Contoh penemuan data sensitif](#)
- [Contoh temuan kebijakan](#)

### Contoh temuan data sensitif di Security Hub

Berikut merupakan contoh temuan data sensitif yang diterbitkan Macie ke Security Hub dengan menggunakan ASFF.

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "5be50fce24526e670df77bc00example",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/macie",
  "ProductName": "Macie",
  "CompanyName": "Amazon",
  "Region": "us-east-1",
  "GeneratorId": "aws/macie",
  "AwsAccountId": "111122223333",
  "Types": [
    "Sensitive Data Identifications/PII/SensitiveData:S3Object-Personal"
  ],
  "CreatedAt": "2022-05-11T10:23:49.667Z",
  "UpdatedAt": "2022-05-11T10:23:49.667Z",
  "Severity": {
    "Label": "HIGH",
    "Normalized": 70
  },
  "Title": "The S3 object contains personal information.",
  "Description": "The object contains personal information such as first or last names, addresses, or identification numbers.",
  "ProductFields": {
```

```

    "JobArn": "arn:aws:macie2:us-east-1:111122223333:classification-
job/698e99c283a255bb2c992feceexample",
    "S3Object.Path": "DOC-EXAMPLE-BUCKET1/2022 Sourcing.tsv",
    "S3Object.Extension": ".tsv",
    "S3Bucket.effectivePermission": "NOT_PUBLIC",
    "OriginType": "SENSITIVE_DATA_DISCOVERY_JOB",
    "S3Object.PublicAccess": "false",
    "S3Object.Size": "14",
    "S3Object.StorageClass": "STANDARD",
    "S3Bucket.allowsUnencryptedObjectUploads": "TRUE",
    "JobId": "698e99c283a255bb2c992feceexample",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/
macie/5be50fce24526e670df77bc00example",
    "aws/securityhub/ProductName": "Macie",
    "aws/securityhub/CompanyName": "Amazon"
  },
  "Resources": [
    {
      "Type": "AwsS3Bucket",
      "Id": "arn:aws:s3:::DOC-EXAMPLE-BUCKET1",
      "Partition": "aws",
      "Region": "us-east-1",
      "Details": {
        "AwsS3Bucket": {
          "OwnerId":
"7009a8971cd538e11f6b6606438875e7c86c5b672f46db45460ddcd08example",
          "OwnerName": "johndoe",
          "OwnerAccountId": "444455556666",
          "CreatedAt": "2020-12-30T18:16:25.000Z",
          "ServerSideEncryptionConfiguration": {
            "Rules": [
              {
                "ApplyServerSideEncryptionByDefault": {
                  "SSEAlgorithm": "aws:kms",
                  "KMSMasterKeyID": "arn:aws:kms:us-
east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
                }
              }
            ]
          },
          "PublicAccessBlockConfiguration": {
            "BlockPublicAcls": true,
            "BlockPublicPolicy": true,
            "IgnorePublicAcls": true,

```

```

        "RestrictPublicBuckets": true
      }
    }
  },
  {
    "Type": "AwsS3Object",
    "Id": "arn:aws:s3:::DOC-EXAMPLE-BUCKET1/2022 Sourcing.tsv",
    "Partition": "aws",
    "Region": "us-east-1",
    "DataClassification": {
      "DetailedResultsLocation": "s3://macie-data-discovery-results/
AWSLogs/111122223333/Macie/us-east-1/
698e99c283a255bb2c992feceexample/111122223333/32b8485d-4f3a-3aa1-be33-
aa3f0example.jsonl.gz",
      "Result": {
        "MimeType": "text/tsv",
        "SizeClassified": 14,
        "AdditionalOccurrences": false,
        "Status": {
          "Code": "COMPLETE"
        },
        "SensitiveData": [
          {
            "Category": "PERSONAL_INFORMATION",
            "Detections": [
              {
                "Count": 1,
                "Type": "USA_SOCIAL_SECURITY_NUMBER",
                "Occurrences": {
                  "Cells": [
                    {
                      "Column": 10,
                      "Row": 1,
                      "ColumnName": "Other"
                    }
                  ]
                }
              }
            ]
          }
        ],
        "TotalCount": 1
      }
    },
    "CustomDataIdentifiers": {

```

```

        "Detections": [
          ],
          "TotalCount": 0
        }
      ],
      "Details": {
        "AwsS3Object": {
          "LastModified": "2022-04-22T18:16:46.000Z",
          "ETag": "ebe1ca03ee8d006d457444445example",
          "VersionId": "S1BC72z5hArgex0Jifxw_IN57example",
          "ServerSideEncryption": "aws:kms",
          "SSEKMSKeyId": "arn:aws:kms:us-
east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
      }
    ],
    "WorkflowState": "NEW",
    "Workflow": {
      "Status": "NEW"
    },
    "RecordState": "ACTIVE",
    "FindingProviderFields": {
      "Severity": {
        "Label": "HIGH"
      },
      "Types": [
        "Sensitive Data Identifications/PII/SensitiveData:S3Object-Personal"
      ]
    },
    "Sample": false,
    "ProcessedAt": "2022-05-11T10:23:49.667Z"
  }
}

```

## Contoh temuan kebijakan di Security Hub

Berikut merupakan contoh temuan kebijakan baru yang diterbitkan Macie ke Security Hub di ASFF.

```

{
  "SchemaVersion": "2018-10-08",
  "Id": "36ca8ba0-caf1-4fee-875c-37760example",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/macie",

```

```
"ProductName": "Macie",
"CompanyName": "Amazon",
"Region": "us-east-1",
"GeneratorId": "aws/macie",
"AwsAccountId": "111122223333",
"Types": [
  "Software and Configuration Checks/AWS Security Best Practices/Policy:IAMUser-
S3BlockPublicAccessDisabled"
],
"CreatedAt": "2022-04-24T09:27:43.313Z",
"UpdatedAt": "2022-04-24T09:27:43.313Z",
"Severity": {
  "Label": "HIGH",
  "Normalized": 70
},
"Title": "Block Public Access settings are disabled for the S3 bucket",
"Description": "All Amazon S3 block public access settings are disabled for the
Amazon S3 bucket. Access to the bucket is
controlled only by access control lists (ACLs) or bucket policies.",
"ProductFields": {
  "S3Bucket.effectivePermission": "NOT_PUBLIC",
  "S3Bucket.allowsUnencryptedObjectUploads": "FALSE",
  "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/
macie/36ca8ba0-caf1-4fee-875c-37760example",
  "aws/securityhub/ProductName": "Macie",
  "aws/securityhub/CompanyName": "Amazon"
},
"Resources": [
  {
    "Type": "AwsS3Bucket",
    "Id": "arn:aws:s3::DOC-EXAMPLE-BUCKET2",
    "Partition": "aws",
    "Region": "us-east-1",
    "Tags": {
      "Team": "Recruiting",
      "Division": "HR"
    }
  },
  "Details": {
    "AwsS3Bucket": {
      "OwnerId":
"7009a8971cd538e11f6b6606438875e7c86c5b672f46db45460ddcd08example",
      "OwnerName": "johndoe",
      "OwnerAccountId": "444455556666",
      "CreatedAt": "2020-11-25T18:24:38.000Z",
```

```

    "ServerSideEncryptionConfiguration": {
      "Rules": [
        {
          "ApplyServerSideEncryptionByDefault": {
            "SSEAlgorithm": "aws:kms",
            "KMSEMasterKeyID": "arn:aws:kms:us-
east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
          }
        }
      ],
    },
    "PublicAccessBlockConfiguration": {
      "BlockPublicAcls": false,
      "BlockPublicPolicy": false,
      "IgnorePublicAcls": false,
      "RestrictPublicBuckets": false
    }
  }
}
],
"WorkflowState": "NEW",
"Workflow": {
  "Status": "NEW"
},
"RecordState": "ACTIVE",
"FindingProviderFields": {
  "Severity": {
    "Label": "HIGH"
  },
  "Types": [
    "Software and Configuration Checks/AWS Security Best Practices/
Policy:IAMUser-S3BlockPublicAccessDisabled"
  ]
},
"Sample": false
}

```

## Mengaktifkan dan mengonfigurasi integrasi AWS Security Hub

Untuk mengintegrasikan Amazon Macie dengan AWS Security Hub, aktifkan Security Hub untuk Anda. Akun AWS Untuk mempelajari caranya, lihat [Mengaktifkan Security Hub](#) di Panduan AWS Security Hub Pengguna.

Integrasi akan diaktifkan secara otomatis, ketika Anda mengaktifkan Macie dan Security Hub, . Secara default, Macie mulai mempublikasikan temuan kebijakan baru dan diperbarui ke Security Hub secara otomatis. Anda tidak perlu mengambil langkah tambahan untuk mengonfigurasi integrasi. Jika Anda memiliki temuan kebijakan saat integrasi diaktifkan, Macie tidak mempublikasikannya ke Security Hub. Sebagai gantinya, Macie hanya menerbitkan temuan kebijakan yang dibuat atau diperbarui setelah integrasi diaktifkan.

Secara opsional Anda dapat menyesuaikan konfigurasi Anda dengan memilih frekuensi ketika Macie menerbitkan pembaruan untuk temuan kebijakan di Security Hub. Anda juga dapat memilih untuk mempublikasikan temuan data sensitif ke Security Hub. Untuk mempelajari caranya, lihat [Mengonfigurasi pengaturan publikasi untuk temuan](#).

## Menghentikan publikasi temuan untuk AWS Security Hub

Untuk menghentikan publikasi temuan AWS Security Hub, Anda dapat mengubah pengaturan publikasi untuk akun Amazon Macie Anda. Untuk mempelajari caranya, lihat [Memilih tujuan publikasi untuk temuan](#). Anda juga dapat melakukan ini dengan menggunakan konsol Security Hub atau API Security Hub. Untuk mempelajari cara melakukannya, lihat [Menonaktifkan dan memungkinkan aliran temuan dari integrasi \(konsol\)](#) atau [Menonaktifkan aliran temuan dari integrasi \(Security Hub API, AWS CLI\)](#) di Panduan Pengguna AWS Security Hub.

## Integrasi Amazon Macie dengan Notifikasi Pengguna AWS

AWS User Notifications adalah layanan yang bertindak sebagai lokasi sentral untuk AWS notifikasi Anda di AWS Management Console. Ini termasuk pemberitahuan seperti CloudWatch alarm Amazon, AWS Support kasus, dan komunikasi dari lainnya Layanan AWS. Dengan Pemberitahuan Pengguna, Anda dapat mengonfigurasi aturan khusus dan saluran pengiriman untuk menerima pemberitahuan tentang jenis EventBridge peristiwa Amazon tertentu. Saluran pengiriman termasuk email, notifikasi AWS Chatbot obrolan, dan notifikasi AWS Console Mobile Application push. Anda juga dapat meninjau notifikasi di konsol Pemberitahuan Pengguna AWS. Untuk mempelajari lebih lanjut tentang Pemberitahuan Pengguna, lihat [Panduan Pengguna Notifikasi Pengguna AWS](#).

Macie terintegrasi dengan Notifikasi Pengguna AWS, yang berarti Anda dapat mengonfigurasi Pemberitahuan Pengguna untuk memberi tahu Anda tentang peristiwa yang dipublikasikan Macie EventBridge untuk kebijakan dan temuan data sensitif. Jika peristiwa temuan cocok dengan kriteria yang Anda tentukan, Pemberitahuan Pengguna akan menghasilkan notifikasi. Notifikasi mencakup detail utama dari temuan terkait, seperti jenis dan tingkat keparahan temuan, dan nama sumber daya



yang terpengaruh. Notifikasi Pengguna juga dapat mengirim notifikasi ke satu atau beberapa saluran pengiriman yang Anda tentukan. Anda dapat menyesuaikan pilihan saluran pengiriman agar selaras dengan alur kerja keamanan dan kepatuhan Anda.

Misalnya, Anda dapat mengonfigurasi Pemberitahuan Pengguna untuk menghasilkan notifikasi untuk jenis temuan baru dengan tingkat keparahan tinggi tertentu. Anda juga dapat menentukan AWS Chatbot sebagai saluran pengiriman untuk notifikasi tersebut. Pemberitahuan Pengguna kemudian mendeteksi EventBridge peristiwa untuk temuan, menghasilkan notifikasi yang menyertakan data dari temuan, dan mengirimkan notifikasi ke AWS Chatbot. AWS Chatbot kemudian dapat merutekan notifikasi ke saluran Slack atau ruang obrolan Amazon Chime untuk memberi tahu tim respons insiden Anda.

## Topik

- [Bekerja dengan Notifikasi Pengguna AWS](#)
- [Mengaktifkan dan mengonfigurasi Notifikasi Pengguna AWS untuk temuan Amazon Macie](#)
- [Memetakan bidang Pemberitahuan Pengguna AWS ke bidang pencarian Amazon Macie](#)
- [Mengubah pengaturan Notifikasi Pengguna AWS untuk temuan Amazon Macie](#)
- [Menonaktifkan Notifikasi Pengguna AWS untuk temuan Amazon Macie](#)

## Bekerja dengan Notifikasi Pengguna AWS

Dengan Notifikasi Pengguna AWS, Anda membuat aturan untuk menentukan jenis peristiwa Amazon yang ingin Anda lakukan untuk menentukan jenis peristiwa Amazon yang ingin Anda lakukan untuk menentukan jenis EventBridge peristiwa Amazon yang ingin Anda lakukan untuk menentukan jenis peristiwa Amazon yang ingin Anda lakukan untuk menentukan jenis peristiwa Amazon. Aturan mendefinisikan kriteria bahwa suatu EventBridge peristiwa harus cocok untuk menghasilkan notifikasi. Anda juga dapat memilih satu atau lebih saluran pengiriman untuk aturan. Saluran pengiriman menentukan tempat Anda ingin menerima notifikasi untuk peristiwa yang sesuai dengan kriteria aturan.

Jika Notifikasi Pengguna mendeteksi EventBridge peristiwa yang cocok dengan kriteria aturan, Notifikasi Pengguna akan melakukan tugas umum berikut:

1. Mengekstrak subset data dari peristiwa.
2. Menghasilkan pemberitahuan yang berisi data yang diekstrak.
3. Mengirimkan notifikasi ke saluran pengiriman yang Anda tentukan untuk jenis acara tersebut.

Desain dan struktur notifikasi dioptimalkan untuk setiap saluran pengiriman yang dikirimnya.

Untuk mengontrol frekuensi atau jumlah notifikasi yang Anda terima, Anda dapat mengonfigurasi pengaturan agregasi untuk aturan. Jika Anda mengaktifkan pengaturan ini, Pemberitahuan Pengguna menggabungkan data untuk beberapa peristiwa menjadi satu notifikasi. Anda dapat memilih untuk mengirim pemberitahuan peristiwa agregat dengan cepat dan sering, yang mungkin ingin Anda lakukan untuk kejadian menemukan tingkat keparahan tinggi. Atau kirim mereka lebih jarang untuk menerima lebih sedikit notifikasi, yang mungkin ingin Anda lakukan untuk kejadian menemukan tingkat keparahan rendah. Jika Anda menggabungkan data peristiwa, Anda dapat menelusuri untuk meninjau detail setiap peristiwa agregat dengan menggunakan konsol Notifikasi Pengguna AWS. Dari sana, Anda juga dapat menavigasi ke setiap temuan terkait di konsol Amazon Macie.

## Mengaktifkan dan mengonfigurasi Notifikasi Pengguna AWS untuk temuan Amazon Macie

Untuk mengaktifkan Notifikasi Pengguna AWS untuk menghasilkan notifikasi untuk temuan Amazon Macie, buat konfigurasi notifikasi untuk Macie di Notifikasi Pengguna. Konfigurasi notifikasi menentukan kriteria untuk aturan. Ini juga menentukan saluran pengiriman dan pengaturan lain untuk memantau dan mengirim pemberitahuan tentang EventBridge peristiwa Amazon yang sesuai dengan kriteria aturan. Untuk informasi terperinci tentang membuat konfigurasi notifikasi, lihat [Memulai Pemberitahuan Pengguna AWS](#) di Panduan Pengguna Notifikasi Pengguna AWS.

Untuk membuat konfigurasi notifikasi untuk temuan Macie, pilih opsi berikut untuk aturan peristiwa:

- Untuk Layanan AWS nama, pilih Macie.
- Untuk Tipe kejadian, pilih Temuan Macie.
- Untuk Wilayah, pilih masing-masing Wilayah AWS tempat Anda menggunakan Macie dan ingin diberi tahu tentang temuan.

Dengan konfigurasi ini, Pemberitahuan Pengguna memantau EventBridge peristiwa untuk Anda Akun AWS dan menghasilkan pemberitahuan untuk semua Macie menemukan peristiwa di Wilayah yang Anda pilih. Peristiwa sesuai dengan kriteria berikut:

- `sourcesamaaws.macie`
- `detail-typesamaMacie Finding`

Pola JSON yang mendasari untuk aturan acara adalah:

```
{
  "source": ["aws.macie"],
  "detail-type": ["Macie Finding"]
}
```

Untuk menyempurnakan aturan dan menghasilkan notifikasi hanya untuk sebagian temuan, Anda dapat menyesuaikan pola JSON untuk aturan tersebut. Untuk melakukan hal ini, tentukan kriteria tambahan yang berasal dari [SkemaEventBridge peristiwa untuk temuan Macie](#).

Jika Anda membuat aturan yang menggunakan pola JSON kustom, Anda dapat membuat beberapa konfigurasi notifikasi untuk temuan Macie. Anda kemudian dapat menyesuaikan saluran pengiriman dan pengaturan lainnya untuk setiap konfigurasi agar selaras dengan alur kerja keamanan dan kepatuhan Anda untuk jenis temuan tertentu.

Misalnya, Anda dapat membuat satu aturan yang memberi tahu Anda jika Macie menghasilkan atau memperbarui Policy:IAMUser/S3BucketPublictemuan. Dalam hal ini, pola untuk aturan mungkin:

```
{
  "source": ["aws.macie"],
  "detail-type": ["Macie Finding"],
  "detail": {
    "type": ["Policy:IAMUser/S3BucketPublic"]
  }
}
```

Dan Anda mungkin membuat aturan lain yang memberi tahu Anda jika Macie menghasilkan temuan data sensitif untuk bucket S3 yang dapat diakses publik. Dalam hal ini, pola untuk aturan mungkin:

```
{
  "source": ["aws.macie"],
  "detail-type": ["Macie Finding"],
  "detail": {
    "type": [ { "prefix": "SensitiveData" } ],
    "resourcesAffected": {
      "effectivePermission": ["PUBLIC"]
    }
  }
}
```

Jika Anda membuat beberapa konfigurasi notifikasi untuk temuan Macie, sebaiknya pastikan aturan untuk setiap konfigurasi unik. Jika tidak, Anda mungkin menerima pemberitahuan duplikat untuk temuan individual.

Untuk mempelajari selengkapnya tentang menyesuaikan pola peristiwa untuk aturan, lihat [Menggunakan pola peristiwa JSON yang disesuaikan](#) dalam Panduan Pengguna Notifikasi Pengguna AWS.

## Memetakan bidang Pemberitahuan Pengguna AWS ke bidang pencarian Amazon Macie

Saat Notifikasi Pengguna AWS menghasilkan notifikasi untuk temuan Amazon Macie, Notifikasi tersebut akan mengisi notifikasi dengan data dari subset bidang dalam EventBridge peristiwa Amazon yang sesuai. Bidang ini memberikan detail kunci dari temuan terkait, seperti jenis dan tingkat keparahan temuan, dan nama sumber daya yang terpengaruh.

Jika Anda meninjau notifikasi di konsol Notifikasi Pengguna AWS, notifikasi tersebut mencakup semua data untuk subset bidang ini. Ini juga menyediakan tautan ke temuan terkait di konsol Amazon Macie. Jika Anda meninjau notifikasi di saluran pengiriman lain, pemberitahuan tersebut mungkin berisi data hanya untuk beberapa bidang. Ini karena Pemberitahuan Pengguna menyesuaikan desain dan struktur notifikasi untuk bekerja dengan setiap jenis saluran pengiriman yang didukungnya.

Tabel berikut mencantumkan bidang yang mungkin disertakan dalam pemberitahuan untuk temuan. Dalam tabel, kolom kolom Pemberitahuan menjelaskan (dalam huruf miring) atau menunjukkan nama bidang dalam pemberitahuan. Kolom Bidang Finding menggunakan notasi titik untuk menunjukkan nama bidang bidang Finding EventBridge event menggunakan notasi titik untuk menunjukkan nama bidang. Kolom Deskripsi menjelaskan data yang disimpan di bidang.

Bidang notifikasi	Bidang temuan	Deskripsi
Judul pesan	<code>detail.type</code>	Tipe temuan itu.  Misalnya: <code>Policy:IAMUser/S3BucketPublic</code> atau <code>SensitiveData:S3object/Financial</code> .

Bidang notifikasi	Bidang temuan	Deskripsi
Ringkasan	<code>detail.title</code>	<p>Deskripsi singkat tentang temuan.</p> <p>Misalnya: The S3 object contains financial information.</p>
Deskripsi	<code>detail.description</code>	<p>Deskripsi lengkap tentang temuan.</p> <p>Misalnya: The S3 object contains financial information such as bank account numbers or credit card numbers.</p>
Kepelikan	<code>detail.severity.description</code>	Representasi kualitatif dari kepelikan temuan ini: Low, Medium, atau High.
ID Temuan	<code>detail.id</code>	Pengenal unik untuk temuan.
Dibuat	<code>detail.createdAt</code>	Tanggal dan waktu ketika Macie menciptakan temuan.
Diperbarui	<code>detail.updatedAt</code>	<p>Tanggal dan waktu ketika Macie baru-baru ini memperbarui temuan.</p> <p>Untuk temuan data sensitif, nilai ini sama dengan nilai untuk bidang Dibuat (<code>detail.createdAt</code> ). Semua temuan data sensitif dianggap baru (unik).</p>

Bidang notifikasi	Bidang temuan	Deskripsi
Bucket S3 yang terkena	<code>detail.resourcesAffected.s3Bucket.arn</code>	Amazon Resource Name (ARN) dari Bucket S3 yang terpengaruh.
objek S3 yang terkena	<code>detail.resourcesAffected.s3Object.path</code>	Nama (key) dari objek S3 yang terpengaruh, termasuk nama bucket yang menyimpan objek dan, jika berlaku, awalan objek.  Bidang ini tidak disertakan dalam notifikasi untuk temuan kebijakan.

Bidang notifikasi	Bidang temuan	Deskripsi
<p>Deteksi data sensitif</p>	<p><code>detail.classificationDetails.result.sensitiveData.detections...</code></p> <p>Dan/Atau</p> <p><code>detail.classificationDetails.result.customDataIdentifiers.detections...</code></p>	<p>Ini adalah gabungan dari beberapa bidang dalam suatu peristiwa untuk menemukan data sensitif. Bidang ini tidak disertakan dalam notifikasi untuk temuan kebijakan.</p> <p>Jika pengidentifikasi data terkelola mendeteksi data sensitif, bidang ini menentukan kategori, jenis, dan nomor (count) kejadian data sensitif yang terdeteksi. Misalnya: <code>PERSONAL_INFORMATION: USA_SOCIAL_SECURITY_NUMBER 100 occurrences</code> .</p> <p>Jika pengidentifikasi data kustom mendeteksi data sensitif, bidang ini menentukan nama pengidentifikasi data kustom dan nomor (count) kemunculan data sensitif yang terdeteksi. Misalnya: <code>Employee ID 20 occurrences</code> .</p> <p>Jika temuan melaporkan beberapa jenis data sensitif, notifikasi tersebut menyertakan data hingga empat jenis. Data diisi terlebih dahulu oleh pengidentifikasi data kustom yang berlaku dan kemudian</p>

Bidang notifikasi	Bidang temuan	Deskripsi
		oleh pengidentifikasi data terkelola yang berlaku.

## Mengubah pengaturan Notifikasi Pengguna AWS untuk temuan Amazon Macie

Anda dapat mengubah pengaturan Notifikasi Pengguna AWS untuk temuan Amazon Macie kapan saja. Untuk melakukan ini, edit konfigurasi notifikasi di Pemberitahuan Pengguna. Untuk mempelajari caranya, lihat [Mengelola konfigurasi notifikasi](#) di Panduan Pengguna Notifikasi Pengguna AWS.

Jika Anda memiliki beberapa konfigurasi notifikasi untuk temuan Macie, mengubah pengaturan untuk satu konfigurasi tidak memengaruhi pengaturan untuk konfigurasi Anda yang lain. Anda dapat mengedit semua atau hanya beberapa konfigurasi Anda.

## Menonaktifkan Notifikasi Pengguna AWS untuk temuan Amazon Macie

Untuk berhenti membuat dan menerima notifikasi dari Pemberitahuan Pengguna AWS untuk temuan Amazon Macie, hapus konfigurasi notifikasi di Pemberitahuan Pengguna. Untuk mempelajari caranya, lihat [Mengelola konfigurasi notifikasi](#) di Panduan Pengguna Notifikasi Pengguna AWS.

Jika Anda memiliki beberapa konfigurasi notifikasi untuk temuan Macie, penghapusan satu konfigurasi tidak akan memengaruhi konfigurasi Anda yang lain. Anda dapat menghapus semua atau hanya beberapa konfigurasi Anda.

## Skema EventBridge acara Amazon untuk temuan Amazon Macie

Untuk mendukung integrasi dengan aplikasi, layanan, dan sistem lain, seperti pemantauan atau sistem manajemen acara, Amazon Macie secara otomatis menerbitkan temuan ke Amazon EventBridge sebagai peristiwa. EventBridge, sebelumnya Amazon CloudWatch Events, adalah layanan bus acara tanpa server yang mengirimkan aliran data real-time dari aplikasi dan lainnya Layanan AWS ke target seperti fungsiAWS Lambda, topik Layanan Pemberitahuan Sederhana Amazon, dan aliran Amazon Kinesis. Untuk mempelajari selengkapnya EventBridge, lihat [Panduan EventBridge Pengguna Amazon](#).



**Note**

Jika saat ini Anda menggunakan CloudWatch Peristiwa, perhatikan bahwa EventBridge dan CloudWatch Peristiwa adalah layanan dan API dasar yang sama. Namun, EventBridge termasuk fitur tambahan yang memungkinkan Anda menerima acara dari aplikasi perangkat lunak sebagai layanan (SaaS) dan aplikasi Anda sendiri. Karena dasar layanan dan API adalah sama, skema peristiwa untuk temuan Macie juga sama.

Macie secara otomatis menerbitkan peristiwa untuk semua temuan baru dan kejadian berikutnya dari temuan kebijakan yang ada, kecuali temuan yang diarsipkan secara otomatis oleh aturan penindasan. Peristiwa adalah objek JSON yang sesuai dengan EventBridge skema untuk acara. AWS Setiap acara berisi representasi JSON dari temuan tertentu. Karena data terstruktur sebagai suatu EventBridge peristiwa, Anda dapat lebih mudah memantau, memproses, dan bertindak berdasarkan temuan dengan menggunakan aplikasi, layanan, dan alat lain. Untuk detail tentang bagaimana dan kapan Macie menerbitkan acara untuk temuan, lihat [Mengonfigurasi pengaturan publikasi untuk temuan](#)

## Topik

- [Skema peristiwa](#)
- [Contoh peristiwa untuk temuan kebijakan](#)
- [Contoh peristiwa untuk temuan data sensitif](#)

## Skema peristiwa

Contoh berikut menunjukkan skema [EventBridge acara Amazon untuk temuan Amazon Macie](#). Untuk deskripsi terperinci tentang bidang yang dapat disertakan dalam peristiwa temuan, lihat [Temuan](#) di Referensi API Amazon Macie. Struktur dan bidang peta peristiwa temuan dekat dengan objek Finding dari Amazon Macie API.

```
{
  "version": "0",
  "id": "event ID",
  "detail-type": "Macie Finding",
  "source": "aws.macie",
  "account": "Akun AWS ID (string)",
  "time": "event timestamp (string)",
  "region": "Wilayah AWS (string)",
```

```
"resources": [
  <-- ARNs of the resources involved in the event -->
],
"detail": {
  <-- Details of a policy or sensitive data finding -->
},
"policyDetails": null, <-- Additional details of a policy finding or null for a
sensitive data finding -->
"sample": Boolean,
"archived": Boolean
}
```

## Contoh peristiwa untuk temuan kebijakan

Contoh berikut menggunakan data sampel untuk mendemonstrasikan struktur dan sifat objek dan bidang dalam EventBridge acara Amazon untuk penemuan kebijakan.

Dalam contoh ini, peristiwa melaporkan kejadian berikutnya dari temuan kebijakan yang ada: setelah blokir akses publik dinonaktifkan untuk bucket S3. Bidang dan nilai berikut dapat membantu Anda menentukan bahwa memang hal ini terjadi:

- Bidang `type` diatur ke `Policy:IAMUser/S3BlockPublicAccessDisabled`.
- Bidang `createdAt` dan `updatedAt` memiliki nilai yang berbeda. Ini adalah salah satu indikator bahwa peristiwa tersebut melaporkan kejadian berikutnya dari temuan kebijakan yang ada. Nilai-nilai untuk bidang ini akan sama jika peristiwa melaporkan temuan baru.
- Bidang `count` diatur ke 2, yang menunjukkan bahwa ini merupakan peristiwa kedua dari temuan tersebut.
- Bidang `category` diatur ke `POLICY`.
- Nilai untuk bidang `classificationDetails` adalah `null`, yang membantu membedakan peristiwa ini untuk menemukan kebijakan dari peristiwa yang diperlukan penemuan data sensitif. Untuk temuan data sensitif, nilai ini akan menjadi sekumpulan objek dan bidang yang memberikan informasi bagaimana dan apa yang ditemukan pada data sensitif.

Perhatikan juga bahwa nilai untuk bidang `sample` adalah `true`. Nilai ini menekankan bahwa ini adalah contoh peristiwa yang digunakan dalam dokumentasi.

```
{
  "version": "0",
  "id": "0948ba87-d3b8-c6d4-f2da-732a1example",
```

```
"detail-type": "Macie Finding",
"source": "aws.macie",
"account": "123456789012",
"time": "2021-04-30T23:12:15Z",
"region": "us-east-1",
"resources": [],
"detail": {
  "schemaVersion": "1.0",
  "id": "64b917aa-3843-014c-91d8-937ffexample",
  "accountId": "123456789012",
  "partition": "aws",
  "region": "us-east-1",
  "type": "Policy:IAMUser/S3BlockPublicAccessDisabled",
  "title": "Block public access settings are disabled for the S3 bucket",
  "description": "All bucket-level block public access settings were disabled for
the S3 bucket. Access to the bucket is controlled by account-level block public access
settings, access control lists (ACLs), and the bucket's bucket policy.",
  "severity": {
    "score": 3,
    "description": "High"
  },
  "createdAt": "2021-04-29T15:46:02Z",
  "updatedAt": "2021-04-30T23:12:15Z",
  "count": 2,
  "resourcesAffected": {
    "s3Bucket": {
      "arn": "arn:aws:s3:::DOC-EXAMPLE-BUCKET1",
      "name": "DOC-EXAMPLE-BUCKET1",
      "createdAt": "2020-04-03T20:46:56.000Z",
      "owner": {
        "displayName": "johndoe",
        "id":
"7009a8971cd538e11f6b6606438875e7c86c5b672f46db45460ddcd08example"
      },
      "tags": [
        {
          "key": "Division",
          "value": "HR"
        },
        {
          "key": "Team",
          "value": "Recruiting"
        }
      ]
    }
  }
},
```

```

        "defaultServerSideEncryption": {
            "encryptionType": "aws:kms",
            "kmsMasterKeyId": "arn:aws:kms:us-
east-1:123456789012:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        },
        "publicAccess": {
            "permissionConfiguration": {
                "bucketLevelPermissions": {
                    "accessControlList": {
                        "allowsPublicReadAccess": false,
                        "allowsPublicWriteAccess": false
                    },
                    "bucketPolicy": {
                        "allowsPublicReadAccess": false,
                        "allowsPublicWriteAccess": false
                    },
                    "blockPublicAccess": {
                        "ignorePublicAcls": false,
                        "restrictPublicBuckets": false,
                        "blockPublicAcls": false,
                        "blockPublicPolicy": false
                    }
                },
                "accountLevelPermissions": {
                    "blockPublicAccess": {
                        "ignorePublicAcls": true,
                        "restrictPublicBuckets": true,
                        "blockPublicAcls": true,
                        "blockPublicPolicy": true
                    }
                }
            },
            "effectivePermission": "NOT_PUBLIC"
        },
        "allowsUnencryptedObjectUploads": "FALSE"
    },
    "s3object": null
},
"category": "POLICY",
"classificationDetails": null,
"policyDetails": {
    "action": {
        "actionType": "AWS_API_CALL",
        "apiCallDetails": {

```

```

        "api": "PutBucketPublicAccessBlock",
        "apiServiceName": "s3.amazonaws.com",
        "firstSeen": "2021-04-29T15:46:02.401Z",
        "lastSeen": "2021-04-30T23:12:15.401Z"
    }
},
"actor": {
    "userIdentity": {
        "type": "AssumedRole",
        "assumedRole": {
            "principalId": "AROAI234567890EXAMPLE:AssumedRoleSessionName",
            "arn": "arn:aws:sts::123456789012:assumed-role/RoleToBeAssumed/MySessionName",
            "accountId": "111122223333",
            "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
            "sessionContext": {
                "attributes": {
                    "mfaAuthenticated": false,
                    "creationDate": "2021-04-29T10:25:43.511Z"
                },
                "sessionIssuer": {
                    "type": "Role",
                    "principalId": "AROAI234567890EXAMPLE",
                    "arn": "arn:aws:iam::123456789012:role/RoleToBeAssumed",
                    "accountId": "123456789012",
                    "userName": "RoleToBeAssumed"
                }
            }
        }
    },
    "root": null,
    "iamUser": null,
    "federatedUser": null,
    "awsAccount": null,
    "awsService": null
},
"ipAddressDetails":{
    "ipAddressV4": "192.0.2.0",
    "ipOwner": {
        "asn": "-1",
        "asnOrg": "ExampleFindingASN0rg",
        "isp": "ExampleFindingISP",
        "org": "ExampleFindingORG"
    }
},

```

```
        "ipCountry": {
            "code": "US",
            "name": "United States"
        },
        "ipCity": {
            "name": "Ashburn"
        },
        "ipGeoLocation": {
            "lat": 39.0481,
            "lon": -77.4728
        }
    },
    "domainDetails": null
}
},
"sample": true,
"archived": false
}
}
```

## Contoh peristiwa untuk temuan data sensitif

Contoh berikut menggunakan data sampel untuk menunjukkan struktur dan sifat objek dan bidang dalam EventBridge acara Amazon untuk menemukan data sensitif.

Dalam contoh ini, acara melaporkan temuan data sensitif baru: Amazon Macie menemukan lebih dari satu kategori data sensitif dalam objek S3. Bidang dan nilai-nilai berikut dapat membantu Anda untuk menentukan bahwa hal ini memang terjadi:

- Bidang `type` diatur ke `SensitiveData:S3Object/Multiple`.
- Bidang `createdAt` dan `updatedAt` memiliki nilai yang sama. Tidak seperti temuan kebijakan, hal ini memang terjadi untuk temuan data sensitif. Semua temuan data sensitif dianggap baru.
- Bidang `count` diatur ke `1`, yang menunjukkan bahwa ini adalah temuan baru. Tidak seperti temuan kebijakan, hal ini memang terjadi untuk temuan data sensitif. Semua temuan data sensitif dianggap unik (baru).
- Bidang `category` diatur ke `CLASSIFICATION`.
- Nilai untuk bidang `policyDetails` adalah `null`, yang membantu membedakan peristiwa ini untuk menemukan data sensitif dari suatu peristiwa untuk temuan kebijakan. Untuk temuan kebijakan, nilai ini akan berupa sekumpulan objek dan bidang yang memberikan informasi tentang potensi pelanggaran kebijakan atau masalah dengan keamanan atau privasi bucket S3.

Perhatikan juga bahwa nilai untuk bidang `sample` diatur ke `true`. Nilai ini menekankan bahwa nilai tersebut adalah contoh peristiwa yang digunakan dalam dokumentasi.

```
{
  "version": "0",
  "id": "14ddd0b1-7c90-b9e3-8a68-6a408example",
  "detail-type": "Macie Finding",
  "source": "aws.macie",
  "account": "123456789012",
  "time": "2022-04-20T08:19:10Z",
  "region": "us-east-1",
  "resources": [],
  "detail": {
    "schemaVersion": "1.0",
    "id": "4ed45d06-c9b9-4506-ab7f-18a57example",
    "accountId": "123456789012",
    "partition": "aws",
    "region": "us-east-1",
    "type": "SensitiveData:S3Object/Multiple",
    "title": "The S3 object contains multiple categories of sensitive data",
    "description": "The S3 object contains more than one category of sensitive
data.",
    "severity": {
      "score": 3,
      "description": "High"
    },
    "createdAt": "2022-04-20T18:19:10Z",
    "updatedAt": "2022-04-20T18:19:10Z",
    "count": 1,
    "resourcesAffected": {
      "s3Bucket": {
        "arn": "arn:aws:s3:::DOC-EXAMPLE-BUCKET2",
        "name": "DOC-EXAMPLE-BUCKET2",
        "createdAt": "2020-05-15T20:46:56.000Z",
        "owner": {
          "displayName": "johndoe",
          "id":
"7009a8971cd538e11f6b6606438875e7c86c5b672f46db45460ddcd08example"
        },
        "tags": [
          {
            "key": "Division",
            "value": "HR"
          }
        ]
      }
    }
  }
}
```

```
    },
    {
      "key": "Team",
      "value": "Recruiting"
    }
  ],
  "defaultServerSideEncryption": {
    "encryptionType": "aws:kms",
    "kmsMasterKeyId": "arn:aws:kms:us-
east-1:123456789012:key/1234abcd-12ab-34cd-56ef-1234567890ab"
  },
  "publicAccess": {
    "permissionConfiguration": {
      "bucketLevelPermissions": {
        "accessControlList": {
          "allowsPublicReadAccess": false,
          "allowsPublicWriteAccess": false
        },
        "bucketPolicy": {
          "allowsPublicReadAccess": false,
          "allowsPublicWriteAccess": false
        },
        "blockPublicAccess": {
          "ignorePublicAcls": true,
          "restrictPublicBuckets": true,
          "blockPublicAcls": true,
          "blockPublicPolicy": true
        }
      },
      "accountLevelPermissions": {
        "blockPublicAccess": {
          "ignorePublicAcls": false,
          "restrictPublicBuckets": false,
          "blockPublicAcls": false,
          "blockPublicPolicy": false
        }
      }
    },
    "effectivePermission": "NOT_PUBLIC"
  },
  "allowsUnencryptedObjectUploads": "TRUE"
},
"s3object": {
  "bucketArn": "arn:aws:s3:::DOC-EXAMPLE-BUCKET2",
```



```
    "key": "2022 Sourcing.csv",
    "path": "DOC-EXAMPLE-BUCKET2/2022 Sourcing.csv",
    "extension": "csv",
    "lastModified": "2022-04-19T22:08:25.000Z",
    "versionId": "",
    "serverSideEncryption": {
      "encryptionType": "aws:kms",
      "kmsMasterKeyId": "arn:aws:kms:us-
east-1:123456789012:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    "size": 4750,
    "storageClass": "STANDARD",
    "tags": [
      {
        "key": "Division",
        "value": "HR"
      },
      {
        "key": "Team",
        "value": "Recruiting"
      }
    ],
    "publicAccess": false,
    "etag": "6bb7fd4fa9d36d6b8fb8882caexample"
  }
},
"category": "CLASSIFICATION",
"classificationDetails": {
  "jobArn": "arn:aws:macie2:us-east-1:123456789012:classification-
job/3ce05dbb7ec5505def334104bexample",
  "jobId": "3ce05dbb7ec5505def334104bexample",
  "result": {
    "status": {
      "code": "COMPLETE",
      "reason": null
    },
    "sizeClassified": 4750,
    "mimeType": "text/csv",
    "additionalOccurrences": true,
    "sensitiveData": [
      {
        "category": "PERSONAL_INFORMATION",
        "totalCount": 65,
        "detections": [
```

```
{
  "type": "USA_SOCIAL_SECURITY_NUMBER",
  "count": 30,
  "occurrences": {
    "lineRanges": null,
    "offsetRanges": null,
    "pages": null,
    "records": null,
    "cells": [
      {
        "row": 2,
        "column": 1,
        "columnName": "SSN",
        "cellReference": null
      },
      {
        "row": 3,
        "column": 1,
        "columnName": "SSN",
        "cellReference": null
      },
      {
        "row": 4,
        "column": 1,
        "columnName": "SSN",
        "cellReference": null
      }
    ]
  }
},
{
  "type": "NAME",
  "count": 35,
  "occurrences": {
    "lineRanges": null,
    "offsetRanges": null,
    "pages": null,
    "records": null,
    "cells": [
      {
        "row": 2,
        "column": 3,
        "columnName": "Name",
        "cellReference": null
      }
    ]
  }
}
```

```

    },
    {
      "row": 3,
      "column": 3,
      "columnName": "Name",
      "cellReference": null
    }
  ]
}
],
},
{
  "category": "FINANCIAL_INFORMATION",
  "totalCount": 30,
  "detections": [
    {
      "type": "CREDIT_CARD_NUMBER",
      "count": 30,
      "occurrences": {
        "lineRanges": null,
        "offsetRanges": null,
        "pages": null,
        "records": null,
        "cells": [
          {
            "row": 2,
            "column": 14,
            "columnName": "CCN",
            "cellReference": null
          },
          {
            "row": 3,
            "column": 14,
            "columnName": "CCN",
            "cellReference": null
          }
        ]
      }
    }
  ]
}
],
},
"customDataIdentifiers": {

```

```
        "totalCount": 0,  
        "detections": []  
      }  
    },  
    "detailedResultsLocation": "s3://macie-data-discovery-results/  
AWSLogs/123456789012/Macie/us-east-1/3ce05dbb7ec5505def334104bexample/  
d48bf16d-0deb-3e49-9d8c-d407cexample.jsonl.gz",  
    "originType": "SENSITIVE_DATA_DISCOVERY_JOB"  
  },  
  "policyDetails": null,  
  "sample": true,  
  "archived": false  
}  
}
```

## Prakiraan dan pemantauan biaya Amazon Macie

Untuk membantu Anda memprakirakan dan memantau biaya Anda untuk menggunakan Amazon Macie, Macie menghitung dan menyediakan perkiraan biaya penggunaan untuk akun Anda. Dengan data ini, Anda dapat menentukan akan menyesuaikan penggunaan layanan atau kuota akun Anda. Jika saat ini Anda berpartisipasi dalam uji coba gratis 30 hari Macie, Anda dapat menggunakan data ini untuk memperkirakan biaya penggunaan Macie setelah uji coba gratis berakhir. Anda juga dapat memeriksa status uji coba Anda.

Anda dapat meninjau perkiraan biaya penggunaan Anda pada konsol Amazon Macie dan mengakses secara terprogram dengan API Amazon Macie. Jika Anda administrator Macie untuk suatu organisasi, Anda dapat meninjau dan mengakses kumpulan data untuk organisasi dan rincian data untuk akun di organisasi Anda.

Selain perkiraan biaya penggunaan yang disediakan oleh Macie, Anda dapat meninjau dan memantau biaya aktual Anda dengan menggunakan AWS Billing and Cost Management. AWS Billing and Cost Management menyediakan fitur yang dirancang untuk membantu Anda melacak dan menganalisis biaya Layanan AWS, dan mengelola anggaran untuk akun atau organisasi Anda. Ini juga menyediakan fitur yang dapat membantu Anda memprakirakan biaya penggunaan berdasarkan data historis. Untuk mempelajari selengkapnya, lihat [Panduan Pengguna AWS Billing](#).

### Topik

- [Memahami cara perkiraan biaya penggunaan dihitung untuk Amazon Macie](#)
- [Meninjau perkiraan biaya penggunaan untuk Amazon Macie](#)
- [Berpartisipasi Amazon Macie gratis](#)

## Memahami cara perkiraan biaya penggunaan dihitung untuk Amazon Macie

Penetapan harga Amazon Macie berdasarkan pada dimensi berikut.

### Pemantauan kendali

Biaya ini diperoleh dari mempertahankan inventaris bucket Amazon Simple Storage Service (Amazon S3) Anda serta mengevaluasi dan memantau bucket untuk keamanan dan kontrol akses. Untuk informasi selengkapnya, lihat [Cara Macie memantau keamanan data Amazon S3](#).

Anda dikenakan biaya berdasarkan jumlah total bucket S3 yang dipantau Macie untuk akun Anda. Biaya prorata per hari.

#### Pemantauan objek untuk penemuan data sensitif otomatis

Biaya ini berasal dari pemantauan dan evaluasi inventaris bucket S3 Anda untuk mengidentifikasi objek S3 yang memenuhi syarat untuk dianalisis dengan penemuan data sensitif otomatis. Untuk informasi selengkapnya, lihat [Cara kerja penemuan data sensitif otomatis](#).

Anda dikenakan biaya berdasarkan jumlah total objek S3 yang dimonitor Macie untuk akun Anda. Biaya prorata per hari.

#### Analisis objek dengan pekerjaan penemuan data sensitif dan penemuan data sensitif otomatis

Biaya ini berasal dari menganalisis objek S3 dan melaporkan data sensitif yang ditemukan Macie di objek. Ini termasuk analisis dan pelaporan oleh pekerjaan penemuan data sensitif dan dengan penemuan data sensitif otomatis.

Anda dikenakan biaya berdasarkan jumlah data yang tidak terkompresi yang dianalisis Macie dalam objek S3. Biaya tidak akan dikenakan pada objek yang tidak dapat dianalisis Macie karena alasan seperti penggunaan kelas penyimpanan Amazon S3 yang tidak didukung, penggunaan format file atau penyimpanan yang tidak didukung, atau pengaturan izin. Untuk informasi selengkapnya, lihat [Menemukan data sensitif](#). Selain itu, biaya ini tidak bervariasi berdasarkan jumlah temuan data sensitif yang dihasilkan oleh pekerjaan Anda atau dengan penemuan data sensitif otomatis.

Untuk mengelola biaya penemuan data sensitif otomatis, Anda dapat mengecualikan bucket S3 individual dari analisis. Misalnya, Anda dapat mengecualikan bucket yang diketahui memenuhi persyaratan keamanan dan kepatuhan organisasi Anda. Untuk mengecualikan bucket, Anda dapat [memperbarui pengaturan konfigurasi](#) untuk akun Anda. Anda juga dapat [mengecualikan bucket case-by-case secara tertentu](#) sambil meninjau detail masing-masing bucket dalam inventaris bucket Anda.

Biaya untuk tugas penemuan data sensitif dibatasi oleh Kuota penemuan data sensitif dibatasi oleh Kuota penemuan data sensitif dibatasi oleh [Kuota penemuan data sensitif dibatasi oleh Kuota penemuan data sensitif](#) bulanan untuk akun Anda. (Kuota default adalah data sebesar 5 TB.) Jika tugas berjalan dan analisis objek yang memenuhi syarat mencapai kuota ini, Macie secara otomatis akan menghentikan tugas hingga saat bulan kalender berikutnya dimulai (dan kuota bulanan diatur ulang untuk akun Anda) atau Anda meningkatkan kuota untuk akun Anda.

Jika Anda adalah administrator Macie untuk suatu organisasi, biaya untuk pekerjaan pencarian data sensitif dibatasi oleh kuota penemuan data sensitif bulanan untuk setiap akun yang Anda analisis datanya. Kuota untuk akun anggota menentukan jumlah maksimum data yang dapat dianalisis oleh pekerjaan Anda dan pekerjaan akun anggota untuk akun tersebut selama satu bulan kalender. Jika tugas berjalan dan analisis objek yang memenuhi syarat mencapai kuota ini untuk akun anggota, Macie berhenti menganalisis objek yang dimiliki oleh akun. Ketika Macie selesai menganalisis objek untuk semua akun lain yang belum memenuhi kuota, Macie secara otomatis menghentikan pekerjaan. Jika tugas satu kali, Macie secara otomatis melanjutkan tugas saat bulan kalender berikutnya dimulai atau kuota ditingkatkan untuk semua akun terdampak, mana yang terjadi lebih dulu. Jika ini adalah pekerjaan berkala, Macie secara otomatis melanjutkan pekerjaan ketika proses berikutnya dijadwalkan untuk memulai atau bulan kalender berikutnya dimulai, mana pun yang terjadi lebih dulu. Jika dijalankan terjadwal dimulai sebelum bulan kalender berikutnya dimulai atau kuota ditingkatkan untuk akun yang terpengaruh, Macie tidak menganalisis objek yang dimiliki oleh akun.

 Tip

Untuk tips bermanfaat tentang mengelola atau mengurangi biaya penemuan data sensitif, lihat [Cara menggunakan Amazon Macie untuk mengurangi biaya menemukan posting blog data sensitif](#) di Blog AWSKeamanan.

Untuk informasi detail dan contoh biaya penggunaan, lihat [Harga Amazon Macie](#).

Ketika Anda menggunakan Macie untuk meninjau perkiraan biaya penggunaan Anda, penting untuk memahami cara perkiraan biaya dihitung. Pertimbangkan hal berikut:

- Perkiraan dilaporkan dalam Dolar AS dan Wilayah AWS hanya untuk saat ini. Jika Anda menggunakan Macie di beberapa Wilayah, data tidak dikumpulkan untuk semua Wilayah tempat Anda menggunakan Macie.
- Di konsol tersebut, perkiraan sudah termasuk untuk bulan kalender saat ini hingga saat ini. Jika Anda melakukan kueri pada data secara terprogram dengan API Amazon Macie, Anda dapat memilih rentang waktu inklusif untuk perkiraan. Rentang waktu ini dapat berupa rentang waktu bergulir dari 30 hari sebelumnya atau bulan kalender saat ini hingga saat ini.
- Perkiraan tidak mencerminkan semua diskon yang mungkin berlaku untuk akun Anda. Pengecualiannya adalah diskon yang diperoleh dari tingkat harga volume Wilayah, seperti yang

dijelaskan dalam [Harga Amazon Macie](#). Jika akun Anda memenuhi syarat untuk tipe diskon ini, perkiraan tersebut menunjukkan diskon tersebut.

- Jika Anda administrator Macie untuk suatu organisasi, perkiraan tidak menunjukkan diskon volume penggunaan gabungan untuk organisasi Anda. Untuk informasi tentang diskon ini, lihat [Diskon volume](#) di Panduan Pengguna AWS Billing.
- Untuk pemantauan kendali pencegahan, perkiraan didasarkan pada biaya harian rata-rata untuk rentang waktu yang berlaku. Biaya prorata per hari.
- Untuk penemuan data sensitif otomatis, perkiraan keseluruhan didasarkan pada biaya harian rata-rata untuk pemantauan objek (prorata per hari) dan jumlah data yang tidak terkompresi yang telah dianalisis oleh Macie sejauh ini selama rentang waktu yang berlaku. Jika Anda administrator Macie untuk suatu organisasi dan menganalisis data untuk akun anggota, perkiraan biaya kegiatan tersebut termasuk dalam perkiraan untuk setiap akun yang berlaku.
- Untuk tugas penemuan data sensitif, perkiraan didasarkan pada jumlah data yang tidak terkompresi yang telah dianalisis oleh tugas Anda sejauh ini selama rentang waktu yang berlaku. Jika Anda administrator Macie untuk suatu organisasi dan menjalankan tugas yang menganalisis data untuk akun anggota, perkiraan biaya tugas tersebut termasuk dalam perkiraan untuk akun anggota yang berlaku.
- Jika akun Anda adalah akun anggota di organisasi dan administrator Macie Anda melakukan penemuan data sensitif yang menganalisis data Anda, perkiraan biaya aktivitas tersebut termasuk dalam perkiraan akun Anda.
- Perkiraan tidak termasuk biaya yang Anda keluarkan untuk menggunakan yang lain Layanan AWS dengan fitur Macie. Misalnya, menggunakan pelanggan yang dikelola AWS KMS keys untuk mendekripsi objek S3 yang ingin Anda periksa untuk data sensitif.

Perhatikan juga Macie menyediakan tingkat gratis bulanan untuk analisis objek S3 berdasarkan tugas penemuan data sensitif dan penemuan data sensitif otomatis. Setiap bulan, tidak dikenakan biaya untuk menganalisis data hingga 1 GB untuk menemukan dan melaporkan data sensitif dalam objek S3. Jika data sensitif dianalisis selama bulan tertentu, biaya penemuan data sensitif mulai bertambah untuk akun Anda setelah 1 GB pertama data. Jika data kurang dari 1 GB dianalisis selama bulan tertentu, alokasi yang tersisa tidak akan dialihkan ke bulan berikutnya. Jika akun Anda adalah bagian dari organisasi dengan penagihan gabungan, tingkat gratis berlaku untuk jumlah gabungan data yang dianalisis untuk organisasi Anda. Dengan kata lain, tidak dikenakan biaya untuk menganalisis data hingga 1 GB setiap bulannya untuk semua akun di organisasi Anda.



## Meninjau perkiraan biaya penggunaan untuk Amazon Macie

Untuk meninjau perkiraan biaya penggunaan Anda saat ini untuk Amazon Macie. Konsol dan API menyediakan perkiraan biaya untuk dimensi harga Macie. Jika saat ini Anda berpartisipasi dalam uji coba gratis 30 hari, Anda dapat menggunakan data ini untuk memperkirakan biaya penggunaan Macie setelah uji coba gratis berakhir. Untuk informasi tentang dimensi dan pertimbangan harga Macie, lihat [Memahami cara perkiraan biaya penggunaan dihitung](#) Untuk informasi detail dan contoh biaya penggunaan, lihat [Harga Amazon Macie](#).

Di Macie, perkiraan biaya penggunaan dilaporkan dalam Dolar AS dan hanya berlaku untuk saat iniWilayah AWS. Jika Anda menggunakan konsol tersebut untuk meninjau data, perkiraan biayanya adalah untuk bulan kalender saat ini hingga hari ini (inklusif). Jika Anda melakukan kueri data secara terprogram dengan API Amazon Macie, Anda dapat menentukan rentang waktu inklusif untuk perkiraan, baik rentang waktu bergulir dari 30 hari sebelumnya atau bulan kalender saat ini hingga hari ini.

### Topik

- [Meninjau perkiraan biaya penggunaan pada konsol Amazon Macie](#)
- [Melakukan kueri pada perkiraan biaya penggunaan dengan API Amazon Macie](#)

## Meninjau perkiraan biaya penggunaan pada konsol Amazon Macie

Di konsol Amazon Macie, perkiraan biaya diatur sebagai berikut:

- Pemantauan kendali pencegahan — Ini adalah perkiraan biaya untuk mempertahankan inventaris bucket Amazon Simple Storage Service (Amazon S3) Anda serta mengevaluasi dan memantau bucket untuk keamanan dan kontrol akses.
- Tugas penemuan data sensitif — Ini adalah perkiraan biaya tugas penemuan data sensitif yang Anda jalankan.
- Penemuan data sensitif otomatis — Ini adalah perkiraan biaya untuk melakukan penemuan data sensitif otomatis. Ini termasuk memantau dan mengevaluasi inventaris bucket S3 Anda untuk mengidentifikasi objek S3 yang memenuhi syarat untuk dianalisis. Ini juga mencakup menganalisis objek yang memenuhi syarat dan melaporkan statistik data sensitif, temuan, dan jenis hasil lainnya.

Ikuti langkah-langkah berikut ini untuk meninjau perkiraan biaya penggunaan Anda dengan menggunakan konsol Amazon Macie.

Untuk meninjau perkiraan biaya penggunaan di konsol tersebut

1. Buka konsol Amazon Macie di <https://console.aws.amazon.com/macie/>.
2. Dengan menggunakan pemilih Wilayah AWS di bagian pojok kanan atas halaman, pilih Wilayah tempat Anda ingin meninjau perkiraan biaya.
3. Pada panel navigasi, pilih Penggunaan.

Jika Anda memiliki akun Macie mandiri atau akun Anda adalah akun anggota di organisasi, halaman Penggunaan menampilkan rincian perkiraan biaya penggunaan untuk akun Anda.

Jika Anda administrator Macie untuk suatu organisasi, halaman Penggunaan mencantumkan akun di organisasi Anda:

- Pada tabel, bidang Total menunjukkan total perkiraan biaya untuk setiap akun.
- Bagian Perkiraan biaya menunjukkan total perkiraan biaya untuk organisasi Anda serta rincian biaya tersebut.

Untuk meninjau rincian perkiraan biaya untuk akun tertentu di organisasi Anda, pilih akun dalam tabel. Bagian Perkiraan biaya kemudian menunjukkan rincian ini. Untuk menampilkan data ini untuk akun lain, pilih akun di tabel. Untuk menghapus pilihan akun Anda, pilih X di samping ID akun.

## Melakukan kueri pada perkiraan biaya penggunaan dengan API Amazon Macie

Untuk melakukan kueri pada perkiraan biaya penggunaan secara terprogram, Anda dapat menggunakan operasi API Amazon Macie berikut:

- `GetUsageTotals` – Operasi ini mengembalikan total perkiraan biaya penggunaan akun Anda, dikelompokkan berdasarkan metrik penggunaan. Jika Anda administrator Macie untuk suatu organisasi, operasi ini akan mengembalikan perkiraan biaya gabungan untuk semua akun di organisasi Anda. Untuk mempelajari selengkapnya tentang operasi ini, lihat [Total Penggunaan](#) di Referensi API Amazon Macie.
- `GetUsageStatistics` – Operasi ini mengembalikan statistik penggunaan dan data terkait untuk akun Anda, dikelompokkan berdasarkan akun dan metrik penggunaan. Data tersebut mencakup total perkiraan biaya penggunaan dan kuota rekening giro. Sebagaimana berlaku, ini juga menunjukkan kapan uji coba gratis 30 hari Anda dimulai untuk Macie dan untuk penemuan data sensitif otomatis. Jika Anda administrator Macie untuk suatu organisasi, operasi ini akan mengembalikan rincian data

untuk semua akun di organisasi Anda. Anda dapat menyesuaikan kueri Anda dengan mengurutkan dan memfilter hasil kueri. Untuk mempelajari selengkapnya tentang operasi ini, lihat [Statistik Penggunaan](#) di Referensi API Amazon Macie.

Bila Anda menggunakan salah satu operasi, Anda secara opsional dapat menentukan rentang waktu inklusif untuk data. Rentang waktu ini dapat berupa rentang waktu bergulir dari 30 hari sebelumnya (PAST\_30\_DAYS) atau bulan kalender saat ini hingga hari ini (MONTH\_TO\_DATE). Jika Anda tidak menentukan rentang waktu, Macie mengembalikan data 30 hari sebelumnya.

Contoh berikut menunjukkan cara melakukan kueri pada perkiraan biaya penggunaan dan statistik menggunakan [AWS Command Line Interface\(AWS CLI\)](#). Anda juga dapat melakukan kueri data dengan menggunakan versi saat ini dari alat baris AWS perintah atau AWS SDK, atau dengan mengirimkan permintaan HTTPS langsung ke Macie. Untuk informasi tentang alat AWS dan SDK, lihat [Alat untuk Membangun di AWS](#).

Contoh

- [Contoh 1: Melakukan kueri pada total perkiraan biaya penggunaan](#)
- [Contoh 2: Melakukan kueri pada statistik penggunaan](#)

### Contoh 1: Melakukan kueri pada total perkiraan biaya penggunaan

Untuk melakukan kueri pada total perkiraan biaya penggunaan menggunakan AWS CLI, jalankan [get-usage-totals](#) perintah dan secara opsional tentukan rentang waktu untuk data. Misalnya:

```
C:\> aws macie2 get-usage-totals --time-range MONTH_TO_DATE
```

Ketika **MONTH\_TO\_DATE** menentukan bulan kalender saat ini hingga hari ini sebagai rentang waktu untuk data.

Jika perintah berhasil berjalan, Anda menerima output yang serupa seperti berikut ini.

```
{
  "timeRange": "MONTH_TO_DATE",
  "usageTotals": [
    {
      "currency": "USD",
      "estimatedCost": "153.45",
      "type": "SENSITIVE_DATA_DISCOVERY"
```

```
    },
    {
      "currency": "USD",
      "estimatedCost": "65.18",
      "type": "AUTOMATED_SENSITIVE_DATA_DISCOVERY"
    },
    {
      "currency": "USD",
      "estimatedCost": "1.51",
      "type": "DATA_INVENTORY_EVALUATION"
    },
    {
      "currency": "USD",
      "estimatedCost": "0.98",
      "type": "AUTOMATED_OBJECT_MONITORING"
    }
  ]
}
```

Di `estimatedCost` mana total perkiraan biaya penggunaan untuk metrik penggunaan terkait (`type`):

- `SENSITIVE_DATA_DISCOVERY`, untuk menganalisis objek S3 dengan pekerjaan penemuan data sensitif.
- `AUTOMATED_SENSITIVE_DATA_DISCOVERY`, untuk menganalisis objek S3 dengan penemuan data sensitif otomatis.
- `DATA_INVENTORY_EVALUATION`, untuk memantau dan mengevaluasi bucket S3 untuk keamanan dan kontrol akses.
- `AUTOMATED_OBJECT_MONITORING`, untuk mengevaluasi dan memantau inventaris bucket S3. Anda bisa menggunakan ini untuk mengidentifikasi objek S3 yang memenuhi syarat untuk dianalisis dengan penemuan data sensitif otomatis.

## Contoh 2: Melakukan kueri pada statistik penggunaan

Untuk melakukan kueri pada statistik penggunaan dengan menggunakan AWS CLI, jalankan [get-usage-statistics](#) perintah. Anda secara opsional dapat mengurutkan, memfilter, dan menentukan rentang waktu untuk hasil kueri. Contoh berikut mengambil statistik penggunaan untuk akun administrator Macie selama 30 hari sebelumnya. Hasilnya diurutkan dalam urutan naik berdasarkan ID. Akun AWS

Untuk Linux, macOS, atau Unix, menggunakan karakter garis miring terbalik (\) untuk meningkatkan keterbacaan:

```
$ aws macie2 get-usage-statistics \  
--sort-by '{"key":"accountId","orderBy":"ASC"}' \  
--time-range PAST_30_DAYS
```

Untuk Microsoft Windows, menggunakan karakter kelanjutan baris tanda sisipan (^) untuk meningkatkan keterbacaan:

```
C:\> aws macie2 get-usage-statistics ^  
--sort-by={"key\":"accountId\","orderBy\":"ASC\"} ^  
--time-range PAST_30_DAYS
```

Dengan:

- *accountId* menentukan bidang yang akan digunakan untuk mengurutkan hasil.
- *ASC* adalah urutan untuk diterapkan pada hasil, berdasarkan nilai untuk bidang tertentu (*accountId*).
- *PAST\_30\_DAYS* menentukan 30 hari sebelumnya sebagai rentang waktu untuk data.

Jika perintah berhasil berjalan, Macie mengembalikan array `records`. Array berisi objek untuk setiap akun yang termasuk dalam hasil kueri. Misalnya:

```
{  
  "records": [  
    {  
      "accountId": "111122223333",  
      "automatedDiscoveryFreeTrialStartDate": "2022-11-28T16:00:00+00:00",  
      "freeTrialStartDate": "2020-05-20T12:26:36.917000+00:00",  
      "usage": [  
        {  
          "currency": "USD",  
          "estimatedCost": "1.51",  
          "type": "DATA_INVENTORY_EVALUATION"  
        },  
        {  
          "currency": "USD",  
          "estimatedCost": "65.18",  
          "type": "AUTOMATED_SENSITIVE_DATA_DISCOVERY"  
        }  
      ]  
    }  
  ]  
}
```

```
    },
    {
      "currency": "USD",
      "estimatedCost": "153.45",
      "serviceLimit": {
        "isServiceLimited": false,
        "unit": "TERABYTES",
        "value": 50
      },
      "type": "SENSITIVE_DATA_DISCOVERY"
    },
    {
      "currency": "USD",
      "estimatedCost": "0.98",
      "type": "AUTOMATED_OBJECT_MONITORING"
    }
  ]
},
{
  "accountId": "444455556666",
  "automatedDiscoveryFreeTrialStartDate": "2022-11-28T16:00:00+00:00",
  "freeTrialStartDate": "2020-05-18T16:26:36.917000+00:00",
  "usage": [
    {
      "currency": "USD",
      "estimatedCost": "1.58",
      "type": "DATA_INVENTORY_EVALUATION"
    },
    {
      "currency": "USD",
      "estimatedCost": "63.13",
      "type": "AUTOMATED_SENSITIVE_DATA_DISCOVERY"
    },
    {
      "currency": "USD",
      "estimatedCost": "145.12",
      "serviceLimit": {
        "isServiceLimited": false,
        "unit": "TERABYTES",
        "value": 50
      },
      "type": "SENSITIVE_DATA_DISCOVERY"
    }
  ]
}
```

```
        "currency": "USD",
        "estimatedCost": "1.02",
        "type": "AUTOMATED_OBJECT_MONITORING"
    }
  ]
},
"timeRange": "PAST_30_DAYS"
}
```

Di `estimatedCost` mana total perkiraan biaya penggunaan untuk metrik penggunaan terkait (`type`) untuk akun:

- `DATA_INVENTORY_EVALUATION`, untuk memantau dan mengevaluasi bucket S3 untuk keamanan dan kontrol akses.
- `AUTOMATED_SENSITIVE_DATA_DISCOVERY`, untuk menganalisis objek S3 dengan penemuan data sensitif otomatis.
- `SENSITIVE_DATA_DISCOVERY`, untuk menganalisis objek S3 dengan pekerjaan penemuan data sensitif.
- `AUTOMATED_OBJECT_MONITORING`, untuk mengevaluasi dan memantau inventaris bucket S3 akun untuk mengidentifikasi objek S3 yang memenuhi syarat untuk dianalisis dengan penemuan data sensitif otomatis.

## Berpartisipasi Amazon Macie gratis

Ketika Anda mengaktifkan Amazon Macie untuk pertama kalinya, Anda Akun AWS secara otomatis terdaftar dalam uji coba gratis 30 hari Macie. Ini termasuk akun anggota individu dalam suatu AWS Organizations organisasi.

Selama uji coba gratis, penggunaan Macie tidak dikenakan biaya Wilayah AWS untuk:

- Lakukan pemantauan kendali pencegahan — Ini termasuk menghasilkan dan memelihara inventaris bucket Amazon Simple Storage Service (Amazon S3) Anda di Wilayah. Ini juga termasuk mengevaluasi dan memantau bucket untuk keamanan dan kontrol akses. Untuk informasi selengkapnya, lihat [Cara Macie memantau keamanan data Amazon S3](#).
- Lakukan penemuan data sensitif otomatis — Ini termasuk memantau dan mengevaluasi inventaris bucket S3 Anda di Wilayah untuk mengidentifikasi objek S3 yang memenuhi syarat untuk dianalisis. Ini juga mencakup menganalisis objek yang memenuhi syarat dan melaporkan statistik

data sensitif, temuan, dan jenis hasil lainnya. Untuk informasi selengkapnya, lihat [Cara kerja penemuan data sensitif otomatis](#).

Penemuan data sensitif otomatis hanya tersedia untuk akun administrator Macie dan akun Macie mandiri. Jika Anda memiliki akun administrator Macie, Anda dapat menggunakan fitur ini untuk menganalisis objek dalam bucket S3 yang dimiliki akun anggota Anda.

Untuk daftar Wilayah tempat Macie yang saat ini tersedia, lihat [Kuota dan titik akhir Amazon Macie](#) di bagian. Referensi Umum AWS

Uji coba gratis berjalan selama 30 hari berturut-turut. Anda tidak dapat menjeda setelah dimulai. Setelah uji coba gratis berakhir, biaya mulai bertambah untuk melakukan pemantauan kontrol pencegahan. Biaya juga mulai bertambah untuk melakukan penemuan data sensitif otomatis. Jika Anda administrator Macie untuk suatu organisasi, biaya dikenakan biaya yang berlaku untuk setiap akun di organisasi Anda. Anda dapat menggunakan Macie untuk meninjau rincian perkiraan biaya penggunaan untuk akun individual di organisasi Anda.

#### Note

Uji coba gratis tidak termasuk analisis objek S3 berdasarkan tugas penemuan data sensitif. Anda akan dikenakan biaya jika Anda membuat dan menjalankan tugas penemuan data sensitif yang menganalisis data yang tidak terkompresi selama uji coba gratis berlangsung. (Macie menyediakan tingkat gratis bulanan untuk penemuan data sensitif. Setiap bulan, tidak dikenakan biaya untuk menganalisis data hingga 1 GB yang tidak terkompresi dalam objek S3. Setelah 1 GB data pertama, biaya bertambah.) Anda mungkin juga akan dikenakan biaya untuk Layanan AWS yang Anda gunakan dengan fitur Macie tertentu—misalnya, menggunakan pelanggan yang dikelola AWS KMS keys untuk mendekripsi objek S3 yang data sensitifnya ingin Anda periksa.

Untuk memeriksa status Anda dan perkiraan biaya selama uji coba gratis

Selama uji coba gratis, Anda dapat memeriksa status uji coba dan meninjau perkiraan biaya penggunaan untuk akun Anda. Perkiraan biaya didasarkan pada penggunaan Macie sejauh ini selama uji coba gratis. Perkiraan biaya tersebut dapat membantu Anda memahami jumlah biaya penggunaan Anda setelah uji coba berakhir. Untuk detail tentang cara Macie menghitung nilai-nilai ini, lihat [Memahami cara perkiraan biaya penggunaan dihitung](#).



Ikuti langkah-langkah berikut ini untuk memeriksa status uji coba Anda dan meninjau perkiraan biaya penggunaan di konsol Amazon Macie. Anda juga dapat mengakses data ini secara terprogram dengan menggunakan [GetUsageStatistics](#) operasi API Amazon Macie.

1. Buka konsol Amazon Macie di <https://console.aws.amazon.com/macie/>.
2. Dengan menggunakan Wilayah AWS pemilih di bagian pojok kanan atas halaman, pilih Wilayah tempat Anda ingin memeriksa status uji coba gratis dan perkiraan biaya penggunaan Anda.
3. Di panel navigasi, pilih Penggunaan.

Halaman Penggunaan menunjukkan jumlah hari yang tersisa di uji coba gratis Anda. Hal ini juga menunjukkan rincian perkiraan biaya penggunaan Anda dalam Dolar AS:

- Pemantauan kendali pencegahan — Ini adalah total biaya yang diproyeksikan untuk mempertahankan inventaris bucket S3 Anda serta mengevaluasi dan memantau bucket untuk keamanan dan kendali akses setelah uji coba gratis berakhir.
- Tugas penemuan data sensitif — Ini adalah total perkiraan biaya perkiraan biaya tugas penemuan data sensitif yang Anda jalankan. Tugas penemuan data sensitif tidak disertakan dalam uji coba gratis.
- Penemuan data sensitif otomatis — Ini adalah total biaya yang diproyeksikan untuk melakukan penemuan data sensitif otomatis setelah uji coba gratis berakhir, diuraikan berdasarkan dimensi penetapan harga—pemantauan objek dan analisis objek.

Jika Anda administrator Macie untuk suatu organisasi, halaman Penggunaan memberikan detail tentang akun Macie di organisasi Anda:

- Di tabel, bidang Uji coba gratis menunjukkan apakah akun saat ini sedang berpartisipasi dalam uji coba gratis untuk pemantauan kendali pencegahan atau penemuan data sensitif otomatis. Bidang uji coba gratis kosong jika uji coba gratis yang berlaku telah berakhir. Bidang Total menunjukkan total perkiraan biaya untuk setiap akun.
- Bagian Perkiraan biaya menunjukkan perkiraan biaya untuk organisasi Anda secara keseluruhan.

Untuk meninjau rincian perkiraan biaya untuk akun tertentu di organisasi Anda, pilih akun dalam tabel. Bagian Perkiraan biaya kemudian menunjukkan rincian ini. Untuk menampilkan data ini untuk akun lain, pilih akun di tabel. Untuk menghapus pilihan akun Anda, pilih X di samping ID akun.

**Note**

Jika akun menyimpan lebih dari 150 TB data di Amazon S3, perkiraan dan biaya aktual akun untuk penemuan data sensitif otomatis mungkin lebih tinggi daripada proyeksi biaya yang disediakan Macie selama uji coba gratis 30 hari. Ini karena analisis objek dengan penemuan data sensitif otomatis dijeda ketika 150 GB data yang tidak dikompresi telah dianalisis untuk akun yang terdaftar dalam uji coba gratis. Analisis objek dilanjutkan untuk akun setelah uji coba gratis berakhir.

Untuk biaya perkiraan bantuan untuk akun yang menyimpan lebih dari 150 TB data di Amazon S3, hubungi AWS Support. Untuk mengelola biaya penemuan data sensitif otomatis setelah uji coba gratis berakhir, Anda dapat mengecualikan bucket S3 individual dari analisis berikutnya. Untuk mengecualikan bucket, Anda dapat [memperbarui pengaturan konfigurasi](#) untuk akun Anda. Anda juga dapat [mengecualikan bucket case-by-case secara tertentu](#) sambil meninjau detail masing-masing bucket dalam inventaris bucket Anda.

# Mengelola beberapa akun Amazon Macie

Jika AWS lingkungan Anda memiliki beberapa akun, Anda dapat mengaitkan akun Amazon Macie di lingkungan Anda dan mengelolanya secara terpusat sebagai organisasi di Macie. Dengan konfigurasi ini, administrator Macie yang ditunjuk dapat menilai dan memantau keseluruhan postur keamanan data estat Amazon Simple Storage Service (Amazon S3) organisasi Anda, dan menemukan data sensitif pada bucket S3 organisasi Anda. Administrator juga dapat melakukan berbagai tugas manajemen akun dan administrasi dalam skala besar, seperti memantau perkiraan biaya penggunaan dan menilai kuota akun.

Di Macie, organisasi terdiri dari akun administrator Macie yang ditunjuk dan satu atau lebih akun anggota terkait. Anda dapat mengaitkan akun dengan dua cara, dengan mengintegrasikan Macie dengan AWS Organizations atau dengan mengirim dan menerima undangan keanggotaan di Macie. Kami menyarankan Anda mengintegrasikan Macie dengan AWS Organizations

AWS Organizations adalah layanan manajemen akun global yang memungkinkan AWS administrator untuk mengkonsolidasikan dan mengelola beberapa secara terpusat. Akun AWS Ini menyediakan pengelolaan akun dan fitur tagihan terkonsolidasi yang dirancang untuk mendukung kebutuhan anggaran, keamanan, dan kepatuhan akan. Ini ditawarkan tanpa biaya tambahan dan terintegrasi dengan beberapa Layanan AWS, termasuk Macie, AWS Security Hub, dan Amazon GuardDuty Untuk mempelajari selengkapnya, lihat [Panduan Pengguna AWS Organizations](#).

Jika Anda lebih suka mengelola beberapa akun Macie secara terpusat tanpa menggunakan AWS Organizations, Anda dapat menggunakan undangan keanggotaan sebagai gantinya. Jika Anda mengirim undangan dan diterima oleh akun lain, akun Anda menjadi akun administrator Macie untuk akun lainnya. Jika Anda menerima dan menerima undangan, akun Anda menjadi akun anggota Macie dan akun administrator Macie dapat mengakses dan mengelola pengaturan, data, dan sumber daya tertentu untuk akun Macie Anda.

## Topik

- [Memahami hubungan antara administrator Amazon Macie dan akun anggota](#)
- [Mengelola akun Amazon Macie dengan AWS Organizations](#)
- [Mengelola akun Amazon Macie dengan undangan](#)

## Memahami hubungan antara administrator Amazon Macie dan akun anggota

Jika Anda mengelola beberapa akun Amazon Macie secara terpusat sebagai organisasi, administrator Macie memiliki akses ke data inventaris Amazon Simple Storage Service (Amazon S3), temuan kebijakan, serta setelan serta sumber daya Macie tertentu untuk akun anggota terkait. Administrator juga dapat melakukan penemuan data sensitif otomatis dan menjalankan pekerjaan penemuan data sensitif untuk mendeteksi data sensitif di bucket S3 yang dimiliki akun anggota. Support untuk tugas-tugas tertentu bervariasi berdasarkan apakah akun administrator Macie dikaitkan dengan akun anggota melalui AWS Organizations atau melalui undangan.

Tabel berikut memberikan detail tentang hubungan antara akun administrator Macie dengan anggota. Ini menunjukkan izin default untuk setiap jenis akun. Untuk lebih membatasi akses ke fitur dan operasi Macie, Anda dapat menggunakan kebijakan kustom [AWS Identity and Access Management\(IAM\)](#).

Di tabel:

- Self menunjukkan bahwa akun tidak dapat melakukan tugas untuk akun terkait apa pun.
- Setiap menunjukkan bahwa akun dapat melakukan tugas untuk akun terkait individu.
- Semua menunjukkan bahwa akun dapat melakukan tugas dan tugas berlaku untuk semua akun terkait.

Tanda hubung (-) menunjukkan bahwa akun tidak dapat melakukan tugas.

Tugas	Melalui AWS Organizations		Dengan undangan	
	Administrator	Anggota	Administrator	Anggota
Enable Macie	Any	–	Self	Self
Review the organization's account inventory <sup>1</sup>	All	–	All	–

Add a member account	Any	–	Any	–
Review statistics and metadata for S3 buckets	All	Self	All	Self
Review policy findings	All	Self	All	Self
Suppress (archive) policy findings <sup>2</sup>	All	–	All	–
Publish policy findings <sup>3</sup>	Self	Self	Self	Self
Configure a repository for sensitive data discovery results	Self	Self	Self	Self
Create and use allow lists	Self	Self	Self	Self
Create and use custom data identifiers	Self	Self	Self	Self
Configure and perform automated sensitive data discovery	All	–	All	–

Review automated sensitive data discovery statistics, data, and results	All	–	All	–
Create and run sensitive data discovery jobs <a href="#">4</a>	Any	Self	Any	Self
Review the details of sensitive data discovery jobs <a href="#">5</a>	Self	Self	Self	Self
Review sensitive data findings <a href="#">6</a>	Self	Self	Self	Self
Suppress (archive) sensitive data findings <a href="#">6</a>	Self	Self	Self	Self
Publish sensitive data findings <a href="#">6</a>	Self	Self	Self	Self
Configure Macie to retrieve sensitive data samples for findings	Self	Self	Self	Self
Retrieve sensitive data samples for findings <a href="#">7</a>	Self	Self	Self	Self

Configure publication destinations for findings	Self	Self	Self	Self
Set the publication frequency for findings	All	Self	All	Self
Create sample findings	Self	Self	Self	Self
Review account quotas and estimated usage costs	All	Self	All	Self
Suspend Macie <a href="#">8</a>	Any	–	Any	Self
Disable Macie <a href="#">9</a>	Self	Self	Self	Self
Remove (disassociate) a member account	Any	–	Any	–
Disassociate from an administrator account	–	–	–	Self
Delete an association with another account <a href="#">10</a>	Any	–	Any	Self

1. Administrator untuk organisasi AWS Organizations dapat meninjau semua akun di organisasi, termasuk akun yang belum mengaktifkan Macie. Administrator untuk organisasi berbasis undangan hanya dapat meninjau akun yang mereka tambahkan ke inventaris mereka.

2. Hanya administrator yang dapat menekan temuan kebijakan. Jika administrator membuat aturan penindasan, Macie menerapkan aturan tersebut pada temuan kebijakan untuk semua akun di organisasi kecuali aturan tersebut dikonfigurasi untuk mengecualikan akun tertentu. Jika anggota membuat aturan penindasan, Macie tidak menerapkan aturan tersebut pada temuan kebijakan untuk akun anggota tersebut.
3. Hanya akun yang memiliki sumber daya yang terpengaruh yang dapat mempublikasikan temuan kebijakan untuk AWS Security Hub sumber daya tersebut. Akun administrator dan anggota secara otomatis mempublikasikan temuan kebijakan untuk sumber daya yang terpengaruh ke Amazon EventBridge.
4. Anggota dapat mengonfigurasi pekerjaan untuk menganalisis objek hanya di bucket S3 yang dimiliki akun mereka. Administrator dapat mengonfigurasi pekerjaan untuk menganalisis objek dalam ember yang dimiliki akun mereka atau akun anggota. Untuk informasi tentang bagaimana kuota diterapkan dan biaya dihitung untuk pekerjaan multi-akun, lihat [Memahami cara perkiraan biaya penggunaan dihitung](#)
5. Hanya akun yang membuat pekerjaan yang dapat mengakses detail pekerjaan. Hal ini mencakup detail terkait tugas dalam inventaris bucket S3.
6. Hanya akun yang menciptakan pekerjaan yang dapat mengakses, menekan, atau mempublikasikan temuan data sensitif yang dihasilkan pekerjaan tersebut. Hanya administrator yang dapat mengakses, menekan, atau mempublikasikan temuan data sensitif yang dihasilkan oleh penemuan data sensitif otomatis.
7. Jika temuan data sensitif berlaku untuk objek S3 yang dimiliki akun anggota, administrator mungkin dapat mengambil sampel data sensitif yang dilaporkan oleh temuan tersebut. Ini tergantung pada sumber temuan, dan pengaturan konfigurasi dan sumber daya di akun administrator dan akun anggota. Untuk informasi selengkapnya, lihat [Opsi konfigurasi dan persyaratan untuk mengambil sampel data sensitif](#).
8. Agar administrator menanggihkan Macie untuk akun mereka sendiri, administrator harus terlebih dahulu memisahkan akun mereka dari semua akun anggota.
9. Agar administrator menonaktifkan Macie untuk akun mereka sendiri, administrator harus terlebih dahulu memisahkan akun mereka dari semua akun anggota, dan menghapus asosiasi antara akun mereka dan semua akun tersebut. Administrator untuk organisasi AWS Organizations dapat



melakukan ini dengan bekerja dengan akun manajemen organisasi untuk menunjuk akun yang berbeda sebagai akun administrator.

Agar anggota AWS Organizations organisasi dapat menonaktifkan Macie, administrator harus terlebih dahulu memisahkan akun anggota dari akun administrator mereka. Dalam organisasi berbasis undangan, anggota dapat memisahkan akun mereka dari akun administrator, dan kemudian menonaktifkan Macie.

10. Administrator untuk organisasi AWS Organizations dapat menghapus asosiasi dengan akun anggota setelah mereka memisahkan akun dari akun administrator mereka. Akun terus muncul di inventaris akun administrator, tetapi statusnya menunjukkan bahwa itu bukan akun anggota. Dalam organisasi berbasis undangan, administrator dan anggota dapat menghapus asosiasi dengan akun lain setelah mereka memisahkan akun mereka dari akun lain. Akun lain kemudian berhenti muncul di inventaris akun mereka.

## Mengelola akun Amazon Macie dengan AWS Organizations

Jika Anda menggunakan AWS Organizations untuk mengelola beberapa secara terpusat Akun AWS, Anda dapat mengintegrasikan Amazon Macie dengan AWS Organizations, dan kemudian mengelola Macie untuk akun secara terpusat di organisasi Anda. Dengan konfigurasi ini, administrator Macie yang ditunjuk dapat mengaktifkan dan mengelola Macie untuk sebanyak 10.000 akun. Administrator juga dapat mengakses data inventaris Amazon Simple Storage Service (Amazon S3) dan menemukan data sensitif dalam bucket S3 yang dimiliki akun tersebut. Untuk detail tentang tugas yang dapat dilakukan administrator, lihat [Memahami hubungan antara administrator Amazon Macie dan akun anggota](#).

Untuk mengintegrasikan Macie AWS Organizations, Anda mulai dengan menunjuk akun sebagai akun administrator Macie yang didelegasikan untuk organisasi. Administrator Macie kemudian memungkinkan Macie untuk akun lain dalam organisasi, menambahkan akun tersebut sebagai akun anggota Macie, dan mengkonfigurasi pengaturan Macie dan sumber daya untuk akun.

### Tip

Jika Anda telah mengaitkan akun administrator Macie dengan akun anggota dengan menggunakan undangan, Anda dapat menetapkan akun tersebut sebagai akun administrator Macie yang didelegasikan untuk organisasi Anda. AWS Organizations Jika Anda melakukan ini, semua akun anggota yang terkait saat ini tetap menjadi anggota dan Anda dapat memanfaatkan sepenuhnya manfaat mengelola akun dengan menggunakan AWS

Organizations. Untuk informasi selengkapnya, lihat [Transisi dari organisasi berbasis undangan](#).

Topik di bagian ini menjelaskan cara mengintegrasikan Macie dengan AWS Organizations dan cara mengelola dan mengelola Macie untuk akun dalam suatu organisasi.

Topik

- [Pertimbangan dan rekomendasi untuk menggunakan Amazon Macie dengan AWS Organizations](#)
- [Mengintegrasikan dan mengonfigurasi organisasi di Amazon Macie](#)
- [Meninjau akun Amazon Macie untuk suatu organisasi](#)
- [Mengelola akun anggota Amazon Macie untuk suatu organisasi](#)
- [Menunjuk akun administrator Amazon Macie yang berbeda untuk suatu organisasi](#)
- [Menonaktifkan integrasi Amazon Macie dengan AWS Organizations](#)

## Pertimbangan dan rekomendasi untuk menggunakan Amazon Macie dengan AWS Organizations

Sebelum Anda mengintegrasikan Amazon Macie dengan AWS Organizations dan mengonfigurasi organisasi Anda di Macie, pertimbangkan persyaratan dan rekomendasi berikut. Pastikan juga bahwa Anda memahami [hubungan antara administrator Macie dan akun anggota](#).

Topik

- [Menunjuk akun administrator Macie](#)
- [Mengubah atau menghapus penunjukan akun administrator Macie](#)
- [Menambahkan dan menghapus akun anggota Macie](#)
- [Transisi dari organisasi berbasis undangan](#)

### Menunjuk akun administrator Macie

Saat Anda menentukan akun mana yang harus menjadi akun administrator Macie yang didelegasikan untuk organisasi Anda, ingatlah hal berikut:

- Sebuah organisasi hanya dapat memiliki satu akun administrator Macie yang didelegasikan.
- Akun tidak dapat menjadi administrator Macie dan akun anggota secara bersamaan.

- Hanya akun AWS Organizations manajemen untuk organisasi yang dapat menunjuk akun administrator Macie yang didelegasikan untuk organisasi, dan hanya akun manajemen yang selanjutnya dapat mengubah atau menghapus penunjukan itu.
- Akun AWS Organizations manajemen untuk organisasi juga dapat menjadi akun administrator Macie yang didelegasikan untuk organisasi. Namun, kami tidak merekomendasikan konfigurasi ini berdasarkan praktik terbaik AWS keamanan dan prinsip hak istimewa paling sedikit. Pengguna yang memiliki akses ke akun manajemen untuk tujuan penagihan cenderung berbeda dari pengguna yang membutuhkan akses ke Macie untuk tujuan keamanan informasi.

Jika Anda lebih suka konfigurasi ini, Anda harus mengaktifkan Macie untuk akun manajemen organisasi di setidaknya satu Wilayah AWS sebelum Anda menetapkan akun sebagai akun administrator Macie yang didelegasikan. Jika tidak, akun tidak akan dapat mengakses dan mengelola pengaturan dan sumber daya Macie untuk akun anggota.

- Tidak seperti AWS Organizations, Macie adalah layanan Regional. Ini berarti bahwa penunjukan akun administrator Macie adalah sebutan Regional. Ini juga berarti bahwa asosiasi antara administrator Macie dan akun anggota bersifat Regional. Misalnya, jika akun manajemen menunjuk akun administrator Macie di Wilayah AS Timur (Virginia N.), administrator Macie dapat mengelola Macie untuk akun anggota hanya di Wilayah tersebut.

Untuk mengelola akun Macie secara terpusat dalam beberapa Wilayah AWS, akun manajemen harus masuk ke setiap Wilayah tempat organisasi saat ini menggunakan atau akan menggunakan Macie, lalu menunjuk akun administrator Macie di masing-masing Wilayah tersebut. Administrator Macie kemudian dapat mengonfigurasi organisasi di masing-masing Wilayah tersebut. Untuk daftar Wilayah di mana Macie saat ini tersedia, lihat [titik akhir dan kuota Amazon Macie](#) di Referensi Umum AWS

- Akun hanya dapat dikaitkan dengan satu akun administrator Macie pada satu waktu. Jika organisasi Anda menggunakan Macie di beberapa Wilayah, akun administrator Macie yang ditunjuk harus sama di semua Wilayah tersebut. Namun, akun manajemen organisasi Anda harus menunjuk akun administrator secara terpisah di setiap Wilayah.
- Akun dapat berupa akun administrator Macie yang didelegasikan hanya untuk satu organisasi pada satu waktu. Jika Anda mengelola beberapa organisasi di AWS Organizations, Anda harus menunjuk akun administrator Macie yang berbeda untuk setiap organisasi. Ini karena AWS Organizations persyaratan — akun dapat menjadi anggota hanya satu organisasi pada satu waktu.
- Jika administrator Macie ditangguhkan, diisolasi, atau ditutup, semua akun anggota Macie yang terkait secara otomatis dihapus sebagai akun anggota Macie tetapi Macie tidak dinonaktifkan untuk akun tersebut. Akun AWS

## Mengubah atau menghapus penunjukan akun administrator Macie

Hanya akun AWS Organizations manajemen untuk organisasi yang dapat mengubah atau menghapus penunjukan akun administrator Macie yang didelegasikan untuk organisasi.

Jika akun manajemen menghapus penunjukan, semua akun anggota terkait akan dihapus sebagai akun anggota Macie tetapi Macie tidak dinonaktifkan untuk akun tersebut. Agar akun juga menjeda atau berhenti menggunakan Macie, pengguna akun harus menangguhkan (menjeda) atau menonaktifkan (menghentikan) Macie untuk akun tersebut.

## Menambahkan dan menghapus akun anggota Macie

Saat Anda menambahkan, menghapus, dan mengelola akun anggota untuk organisasi Anda, ingatlah hal berikut:

- Akun administrator Macie dapat dikaitkan dengan tidak lebih dari 10.000 akun anggota Macie yang aktif (diaktifkan) di masing-masing akun. Wilayah AWS Jika organisasi Anda melebihi kuota ini, administrator Macie tidak akan dapat menambahkan akun anggota hingga mereka menghapus jumlah akun anggota yang diperlukan di Wilayah.

Saat organisasi memenuhi kuota ini, kami memberi tahu administrator Macie dengan membuat dan CloudWatch acara AWS Health Amazon untuk akun mereka. Kami juga mengirim email ke alamat yang terkait dengan akun mereka.

Jika Anda administrator Macie untuk suatu organisasi, Anda dapat menentukan berapa banyak akun anggota aktif yang saat ini dikaitkan dengan akun Anda dengan menggunakan halaman Akun di konsol Amazon Macie atau [DescribeOrganizationConfiguration](#) pengoperasian API Amazon Macie. Untuk informasi selengkapnya, lihat [Meninjau akun Amazon Macie untuk suatu organisasi](#).

- Akun hanya dapat dikaitkan dengan satu akun administrator Macie pada satu waktu. Ini berarti bahwa akun tidak dapat menerima undangan Macie dari akun lain jika sudah dikaitkan dengan akun administrator Macie untuk organisasi di AWS Organizations

Demikian pula, jika akun sudah menerima undangan, administrator Macie untuk organisasi di tidak AWS Organizations dapat menambahkan akun sebagai akun anggota Macie. Akun harus terlebih dahulu memisahkan diri dari akun administrator berbasis undangan saat ini.

- Untuk menambahkan akun AWS Organizations manajemen sebagai akun anggota Macie, pengguna akun manajemen harus terlebih dahulu mengaktifkan Macie untuk akun tersebut. Administrator Macie tidak diizinkan untuk mengaktifkan Macie untuk akun manajemen.

- Akun anggota tidak dapat memisahkan diri dari akun administrator Macie-nya. Hanya administrator Macie yang dapat menghapus akun sebagai akun anggota Macie.
- Jika administrator Macie menghapus akun anggota Macie, Macie terus diaktifkan untuk akun tersebut. Untuk juga menjeda atau berhenti menggunakan Macie, pengguna akun harus menanggihkan (menjeda) atau menonaktifkan (menghentikan) Macie untuk akun tersebut.

## Transisi dari organisasi berbasis undangan

Jika Anda telah mengaitkan akun administrator Macie dengan akun anggota menggunakan undangan keanggotaan Macie, sebaiknya Anda menetapkan akun tersebut sebagai akun administrator Macie yang didelegasikan untuk organisasi Anda di AWS Organizations. Ini menyederhanakan transisi dari organisasi berbasis undangan.

Jika Anda melakukan ini, semua akun anggota yang saat ini terkait terus menjadi anggota. Jika akun anggota merupakan bagian dari organisasi Anda AWS Organizations, asosiasi akun secara otomatis berubah dari Melalui undangan menjadi Via AWS Organizations di Macie. Jika akun anggota bukan bagian dari organisasi Anda AWS Organizations, asosiasi akun tetap menjadi Undangan. Dalam kedua kasus, akun terus dikaitkan dengan akun administrator Macie yang didelegasikan sebagai akun anggota.

Kami merekomendasikan pendekatan ini karena akun tidak dapat dikaitkan dengan lebih dari satu akun administrator Macie secara bersamaan. Jika Anda menetapkan akun lain sebagai akun administrator Macie untuk organisasi Anda AWS Organizations, administrator yang ditunjuk tidak akan dapat mengelola akun yang sudah dikaitkan dengan akun administrator Macie lain dengan undangan. Setiap akun anggota harus terlebih dahulu memisahkan diri dari akun administrator berbasis undangan saat ini. Administrator Macie untuk organisasi Anda kemudian AWS Organizations dapat menambahkan akun sebagai akun anggota Macie dan mulai mengelola akun.

Setelah Anda mengintegrasikan Macie dengan AWS Organizations dan Anda mengonfigurasi organisasi Anda di Macie, Anda dapat secara opsional menunjuk akun administrator Macie yang berbeda untuk organisasi tersebut. Anda juga dapat terus menggunakan undangan untuk mengaitkan dan mengelola akun anggota yang bukan bagian dari organisasi Anda. AWS Organizations

## Mengintegrasikan dan mengonfigurasi organisasi di Amazon Macie

Untuk mulai menggunakan Amazon Macie dengan AWS Organizations, akun AWS Organizations manajemen untuk organisasi menetapkan akun sebagai akun administrator Macie yang didelegasikan untuk organisasi. Ini memungkinkan Macie sebagai layanan tepercaya di AWS

Organizations. Ini juga memungkinkan Macie saat ini Wilayah AWS untuk akun administrator yang ditunjuk, dan memungkinkan akun administrator yang ditunjuk untuk mengaktifkan dan mengelola Macie untuk akun lain di organisasi di Wilayah itu. Untuk informasi tentang cara izin ini diberikan, lihat [Menggunakan AWS Organizations dengan yang lain Layanan AWS](#) di Panduan AWS Organizations Pengguna.

Administrator Macie yang didelegasikan kemudian mengonfigurasi organisasi di Macie, terutama dengan menambahkan akun organisasi sebagai akun anggota Macie di Wilayah. Administrator kemudian dapat mengakses pengaturan, data, dan sumber daya Macie tertentu untuk akun tersebut di Wilayah tersebut.

Topik ini menjelaskan cara menunjuk administrator Macie yang didelegasikan untuk organisasi dan cara menambahkan akun organisasi sebagai akun anggota Macie. Sebelum Anda melakukan tugas-tugas ini, pastikan bahwa Anda memahami [hubungan antara administrator dan akun anggota](#). Ini juga merupakan ide yang baik untuk meninjau [pertimbangan dan rekomendasi](#) untuk menggunakan Macie dengan AWS Organizations

## Tugas

- [Langkah 1: Verifikasi izin Anda](#)
- [Langkah 2: Tentukan akun administrator Macie yang didelegasikan untuk organisasi](#)
- [Langkah 3: Secara otomatis mengaktifkan dan menambahkan akun organisasi baru sebagai akun anggota Macie](#)
- [Langkah 4: Aktifkan dan tambahkan akun organisasi yang ada sebagai akun anggota Macie](#)

Untuk mengintegrasikan dan mengonfigurasi organisasi di beberapa Wilayah, akun AWS Organizations manajemen dan administrator Macie yang didelegasikan mengulangi langkah-langkah ini di setiap Wilayah tambahan.

## Langkah 1: Verifikasi izin Anda

Sebelum Anda menetapkan akun administrator Macie yang didelegasikan untuk organisasi Anda, verifikasi bahwa Anda (sebagai pengguna akun AWS Organizations manajemen) diizinkan untuk melakukan tindakan Macie berikut: `macie2:EnableOrganizationAdminAccount` Tindakan ini memungkinkan Anda untuk menunjuk akun administrator Macie yang didelegasikan untuk organisasi Anda dengan menggunakan Macie.

Juga verifikasi bahwa Anda diizinkan untuk melakukan AWS Organizations tindakan berikut:

- `organizations:DescribeOrganization`
- `organizations:EnableAWSServiceAccess`
- `organizations:ListAWSServiceAccessForOrganization`
- `organizations:RegisterDelegatedAdministrator`

Tindakan ini memungkinkan Anda untuk: mengambil informasi tentang organisasi Anda; mengintegrasikan Macie dengan AWS Organizations; mengambil informasi tentang mana Layanan AWS Anda telah terintegrasi dengan AWS Organizations; dan, menunjuk akun administrator Macie yang didelegasikan untuk organisasi Anda.

Untuk memberikan izin ini, sertakan pernyataan berikut dalam kebijakan AWS Identity and Access Management (IAM) untuk akun Anda:

```
{
  "Sid": "Grant permissions to designate a delegated Macie administrator",
  "Effect": "Allow",
  "Action": [
    "macie2:EnableOrganizationAdminAccount",
    "organizations:DescribeOrganization",
    "organizations:EnableAWSServiceAccess",
    "organizations:ListAWSServiceAccessForOrganization",
    "organizations:RegisterDelegatedAdministrator"
  ],
  "Resource": "*"
}
```

Jika Anda ingin menetapkan akun AWS Organizations manajemen Anda sebagai akun administrator Macie yang didelegasikan untuk organisasi, akun Anda juga memerlukan izin untuk melakukan tindakan IAM berikut: `CreateServiceLinkedRole`. Tindakan ini memungkinkan Anda mengaktifkan Macie untuk akun manajemen. Namun, berdasarkan praktik terbaik AWS keamanan dan prinsip hak istimewa terkecil, kami tidak menyarankan Anda melakukan ini.

Jika Anda memutuskan untuk memberikan izin ini, tambahkan pernyataan berikut ke kebijakan IAM untuk akun AWS Organizations manajemen Anda:

```
{
  "Sid": "Grant permissions to enable Macie",
  "Effect": "Allow",
```

```

"Action": [
  "iam:CreateServiceLinkedRole"
],
"Resource": "arn:aws:iam::111122223333:role/aws-service-role/maciek.amazonaws.com/
AWSServiceRoleForAmazonMacie",
"Condition": {
  "StringLike": {
    "iam:AWSServiceName": "maciek.amazonaws.com"
  }
}
}

```

Dalam pernyataan itu, ganti **111122223333** dengan ID akun untuk akun manajemen.

Jika Anda ingin mengelola Macie dalam opt-in Wilayah AWS (Wilayah yang dinonaktifkan secara default), perbarui juga nilai untuk prinsipal layanan Macie di Resource elemen dan kondisi. iam:AWSServiceName Nilai harus menentukan kode Wilayah untuk Wilayah. Misalnya, untuk mengelola Macie di Wilayah Timur Tengah (Bahrain), yang memiliki kode Wilayah saya-selatan-1, lakukan hal berikut:

- Dalam Resource elemen, ganti

```
arn:aws:iam::111122223333:role/aws-service-role/maciek.amazonaws.com/
AWSServiceRoleForAmazonMacie
```

dengan

```
arn:aws:iam::111122223333:role/aws-service-role/maciek.me-
south-1.amazonaws.com/AWSServiceRoleForAmazonMacie
```

Di mana **111122223333** menentukan ID akun untuk akun manajemen dan **me-south-1** menentukan kode Wilayah untuk Wilayah.

- Dalam iam:AWSServiceName kondisi tersebut, ganti maciek.amazonaws.com dengan maciek.me-south-1.amazonaws.com, di mana **me-south-1** menentukan kode Wilayah untuk Wilayah.

Untuk daftar Wilayah di mana Macie saat ini tersedia dan kode Wilayah untuk masing-masing wilayah, lihat [titik akhir dan kuota Amazon Macie](#) di. Referensi Umum AWS Untuk informasi tentang Wilayah keikutsertaan, lihat [Menentukan Wilayah AWS akun mana yang dapat digunakan dalam Panduan AWS Account Management](#) Referensi.



## Langkah 2: Tentukan akun administrator Macie yang didelegasikan untuk organisasi

Setelah memverifikasi izin, Anda (sebagai pengguna akun AWS Organizations manajemen) dapat menunjuk akun administrator Macie yang didelegasikan untuk organisasi Anda.

Untuk menunjuk akun administrator Macie yang didelegasikan untuk sebuah organisasi

Untuk menetapkan akun administrator Macie yang didelegasikan untuk organisasi Anda, Anda dapat menggunakan konsol Amazon Macie atau Amazon Macie API. Hanya pengguna akun AWS Organizations manajemen yang dapat melakukan tugas ini.

### Console

Ikuti langkah-langkah ini untuk menunjuk akun administrator Macie yang didelegasikan dengan menggunakan konsol Amazon Macie.

Untuk menunjuk akun administrator Macie yang didelegasikan

1. Masuk ke AWS Management Console menggunakan akun AWS Organizations manajemen Anda.
2. Dengan menggunakan Wilayah AWS pemilih di sudut kanan atas halaman, pilih Wilayah tempat Anda ingin menunjuk akun administrator Macie yang didelegasikan untuk organisasi Anda.
3. [Buka konsol Amazon Macie di https://console.aws.amazon.com/macie/](https://console.aws.amazon.com/macie/).
4. Lakukan salah satu hal berikut, tergantung pada apakah Macie diaktifkan untuk akun manajemen Anda di Wilayah saat ini:
  - Jika Macie tidak diaktifkan, pilih Mulai di halaman selamat datang.
  - Jika Macie diaktifkan, pilih Pengaturan di panel navigasi.
5. Di bawah Administrator yang didelegasikan, masukkan ID akun 12 digit untuk Akun AWS yang ingin Anda tetapkan sebagai akun administrator Macie.
6. Pilih Delegasikan.

Ulangi langkah sebelumnya di setiap Wilayah tambahan di mana Anda ingin mengintegrasikan organisasi Anda dengan Macie. Anda harus menunjuk akun administrator Macie yang sama di masing-masing Wilayah tersebut.

## API

Untuk menunjuk akun administrator Macie yang didelegasikan secara terprogram, gunakan pengoperasian API Amazon Macie. [EnableOrganizationAdminAccount](#) Untuk menetapkan akun di beberapa Wilayah, kirimkan penunjukan untuk setiap Wilayah tempat Anda ingin mengintegrasikan organisasi Anda dengan Macie. Anda harus menunjuk akun administrator Macie yang sama di masing-masing Wilayah tersebut.

Saat Anda mengirimkan penunjukan, gunakan `adminAccountId` parameter yang diperlukan untuk menentukan ID akun 12 digit Akun AWS untuk ditunjuk sebagai akun administrator Macie untuk organisasi. Pastikan juga bahwa Anda menentukan Wilayah tempat penunjukan berlaku.

Untuk menunjuk akun administrator Macie dengan menggunakan [AWS Command Line Interface\(AWS CLI\)](#), jalankan perintah. [enable-organization-admin-account](#) Untuk `admin-account-id` parameter, tentukan ID akun 12 digit Akun AWS untuk ditunjuk. Gunakan `region` parameter untuk menentukan Wilayah tempat penunjukan berlaku. Sebagai contoh:

```
C:\> aws macie2 enable-organization-admin-account --region us-east-1 --admin-account-id 111122223333
```

Dimana ***us-east-1*** adalah Wilayah yang penunjukannya berlaku untuk (Wilayah AS Timur (Virginia N.)) dan ***111122223333*** adalah ID akun untuk akun yang akan ditunjuk.

Setelah Anda menunjuk akun administrator Macie untuk organisasi Anda, administrator Macie dapat mulai mengonfigurasi organisasi di Macie.

### Langkah 3: Secara otomatis mengaktifkan dan menambahkan akun organisasi baru sebagai akun anggota Macie

Secara default, Macie tidak diaktifkan secara otomatis untuk akun baru saat akun ditambahkan ke organisasi Anda. AWS Organizations Selain itu, akun tidak ditambahkan secara otomatis sebagai akun anggota Macie. Akun muncul di inventaris akun administrator Macie. Namun, Macie belum tentu diaktifkan untuk akun dan administrator Macie tidak dapat mengakses pengaturan, data, dan sumber daya Macie untuk akun tersebut.

Jika Anda adalah administrator Macie yang didelegasikan untuk organisasi, Anda dapat mengubah pengaturan konfigurasi ini untuk organisasi Anda. Jika Anda mengaktifkan pengaturan Aktifkan otomatis, Macie secara otomatis diaktifkan untuk akun baru saat akun ditambahkan ke organisasi Anda AWS Organizations, dan akun tersebut secara otomatis dikaitkan dengan akun administrator

Macie Anda sebagai akun anggota. Mengaktifkan setelan ini tidak memengaruhi akun yang ada di organisasi Anda. Untuk mengaktifkan dan mengelola Macie untuk akun yang ada, Anda harus menambahkan akun secara manual sebagai akun anggota Macie. [Langkah selanjutnya](#) menjelaskan bagaimana melakukan ini.

#### Note

Jika Anda mengaktifkan pengaturan Auto-enable, perhatikan pengecualian berikut:

- Jika akun baru sudah dikaitkan dengan akun administrator Macie yang berbeda, Macie tidak secara otomatis menambahkan akun sebagai akun anggota di organisasi Anda.

Akun harus dipisahkan dari akun administrator Macie saat ini sebelum dapat menjadi bagian dari organisasi Anda di Macie. Anda kemudian dapat menambahkan akun secara manual. Untuk mengidentifikasi akun di mana hal ini terjadi, Anda dapat [meninjau inventaris akun](#) untuk organisasi Anda.

- Jika organisasi Anda mencapai kuota 10.000 akun anggota Macie dalam satu Wilayah AWS, Macie secara otomatis mematikan pengaturan ini di Wilayah.

Jika ini terjadi, kami memberi tahu Anda dengan membuat AWS Health dan CloudWatch acara Amazon untuk akun administrator Macie Anda. Kami juga mengirim email ke alamat yang terkait dengan akun tersebut. Jika jumlah total akun kemudian berkurang menjadi kurang dari 10.000 akun, Macie secara otomatis mengaktifkan pengaturan lagi.

Untuk mengaktifkan dan menambahkan akun organisasi baru secara otomatis sebagai akun anggota Macie

Untuk mengaktifkan dan menambahkan akun baru secara otomatis sebagai akun anggota Macie, Anda dapat menggunakan konsol Amazon Macie atau Amazon Macie API. Hanya administrator Macie yang didelegasikan untuk organisasi yang dapat melakukan tugas ini.

#### Console

Untuk melakukan tugas ini dengan menggunakan konsol, Anda harus diizinkan untuk melakukan AWS Organizations tindakan berikut: `organizations:ListAccounts`. Tindakan ini memungkinkan Anda untuk mengambil dan menampilkan informasi tentang akun di organisasi Anda. Jika Anda memiliki izin ini, ikuti langkah-langkah berikut untuk mengaktifkan dan menambahkan akun organisasi baru secara otomatis sebagai akun anggota Macie.

Untuk mengaktifkan dan menambahkan akun organisasi baru secara otomatis

1. [Buka konsol Amazon Macie di https://console.aws.amazon.com/macie/](https://console.aws.amazon.com/macie/).
2. Dengan menggunakan Wilayah AWS pemilih di sudut kanan atas halaman, pilih Wilayah di mana Anda ingin mengaktifkan secara otomatis dan menambahkan akun baru sebagai akun anggota Macie.
3. Di panel navigasi, di bagian Pengaturan, pilih Akun.
4. Pada halaman Akun, di samping Tambahkan akun, aktifkan pengaturan Aktifkan otomatis.

Ulangi langkah sebelumnya di setiap Wilayah tambahan tempat Anda ingin mengonfigurasi organisasi Anda di Macie.

Untuk selanjutnya mengubah pengaturan ini dan berhenti mengaktifkan dan menambahkan akun baru secara otomatis, ulangi langkah-langkah sebelumnya dan matikan pengaturan Aktifkan otomatis.

## API

Untuk mengaktifkan dan menambahkan akun anggota Macie baru secara otomatis secara terprogram, gunakan [UpdateOrganizationConfiguration](#) pengoperasian API Amazon Macie. Saat Anda mengirimkan permintaan, tetapkan nilai untuk `autoEnable` parameter tersebut `true`. (Nilai default adalah `false`.) Pastikan juga bahwa Anda menentukan Wilayah tempat permintaan Anda berlaku. Untuk mengaktifkan dan menambahkan akun baru secara otomatis di Wilayah tambahan, kirimkan permintaan untuk setiap Wilayah tambahan.

Jika Anda menggunakan AWS CLI untuk mengirimkan permintaan, jalankan [update-organization-configuration](#) perintah dan tentukan `auto-enable` parameter untuk mengaktifkan dan menambahkan akun baru secara otomatis. Sebagai contoh:

```
$ aws macie2 update-organization-configuration --region us-east-1 --auto-enable
```

Di mana `us-east-1` adalah Wilayah di mana untuk secara otomatis mengaktifkan dan menambahkan akun baru, Wilayah AS Timur (Virginia N.).

Untuk selanjutnya mengubah pengaturan ini dan berhenti mengaktifkan dan menambahkan akun baru secara otomatis, jalankan perintah yang sama lagi dan gunakan `no-auto-enable` parameter, bukan `auto-enable` parameter, di setiap Wilayah yang berlaku.

## Langkah 4: Aktifkan dan tambahkan akun organisasi yang ada sebagai akun anggota Macie

Saat Anda mengintegrasikan MacieAWS Organizations, Macie tidak diaktifkan secara otomatis untuk semua akun yang ada di organisasi Anda. Selain itu, akun tidak secara otomatis dikaitkan dengan akun administrator Macie yang didelegasikan sebagai akun anggota Macie.

Oleh karena itu, langkah terakhir untuk mengintegrasikan dan mengonfigurasi organisasi Anda di Macie adalah menambahkan akun organisasi yang ada sebagai akun anggota Macie. Saat Anda menambahkan akun yang ada sebagai akun anggota Macie, Macie secara otomatis diaktifkan untuk akun tersebut dan Anda (sebagai administrator Macie yang didelegasikan) mendapatkan akses ke pengaturan, data, dan sumber daya Macie tertentu untuk akun tersebut.

Perhatikan bahwa Anda tidak dapat menambahkan akun yang saat ini dikaitkan dengan akun administrator Macie lainnya. Untuk menambahkan akun, bekerja dengan pemilik akun untuk terlebih dahulu memisahkan akun dari akun administrator saat ini. Selain itu, Anda tidak dapat menambahkan akun yang ada jika Macie saat ini ditangguhkan untuk akun tersebut. Pemilik akun harus mengaktifkan kembali Macie terlebih dahulu untuk akun tersebut. Terakhir, jika Anda ingin menambahkan akun AWS Organizations manajemen sebagai akun anggota, pengguna akun itu harus mengaktifkan Macie terlebih dahulu untuk akun tersebut.

Untuk mengaktifkan dan menambahkan akun organisasi yang ada sebagai akun anggota Macie

Untuk mengaktifkan dan menambahkan akun organisasi yang ada sebagai akun anggota Macie, Anda dapat menggunakan konsol Amazon Macie atau Amazon Macie API. Hanya administrator Macie yang didelegasikan untuk organisasi yang dapat melakukan tugas ini.

### Console

Untuk melakukan tugas ini dengan menggunakan konsol, Anda harus diizinkan untuk melakukan AWS Organizations tindakan berikut: `organizations:ListAccounts`. Tindakan ini memungkinkan Anda untuk mengambil dan menampilkan informasi tentang akun di organisasi Anda. Jika Anda memiliki izin ini, ikuti langkah-langkah berikut untuk mengaktifkan dan menambahkan akun yang ada sebagai akun anggota Macie.

Untuk mengaktifkan dan menambahkan akun organisasi yang ada

1. [Buka konsol Amazon Macie di https://console.aws.amazon.com/macie/](https://console.aws.amazon.com/macie/).
2. Dengan menggunakan Wilayah AWS pilih di sudut kanan atas halaman, pilih Wilayah yang ingin Anda aktifkan dan tambahkan akun yang ada sebagai akun anggota Macie.

3. Di panel navigasi, di bagian Pengaturan, pilih Akun.

Halaman Akun membuka dan menampilkan tabel akun yang terkait dengan akun Macie Anda. Jika akun adalah bagian dari organisasi Anda AWS Organizations, Jenisnya adalah Via AWS Organizations. Jika akun bukan akun anggota Macie, Statusnya Bukan anggota.

4. Di tabel Akun, pilih kotak centang untuk setiap akun yang ingin Anda tambahkan sebagai akun anggota Macie.

 Tip

Untuk lebih mudah mengidentifikasi akun untuk ditambahkan, Anda dapat memfilter tabel. Untuk melakukan ini, letakkan kursor Anda di kotak filter di atas tabel, lalu pilih Status. Kemudian pilih Status = Bukan Anggota.

5. Pada menu Tindakan, pilih Tambahkan anggota.
6. Konfirmasikan bahwa Anda ingin menambahkan akun yang dipilih sebagai akun anggota.

Setelah Anda mengonfirmasi penambahan akun yang dipilih, status akun berubah menjadi Pembuatan/Pengaktifan, dan kemudian Diaktifkan.

Ulangi langkah sebelumnya di setiap Wilayah tambahan tempat Anda ingin mengonfigurasi organisasi Anda di Macie.

## API

Untuk mengaktifkan dan menambahkan satu atau beberapa akun yang ada secara terprogram sebagai akun anggota Macie, gunakan [CreateMember](#) pengoperasian API Amazon Macie. Saat Anda mengirimkan permintaan, gunakan parameter yang didukung untuk menentukan 12 digit ID akun dan alamat email masing-masing Akun AWS untuk mengaktifkan dan menambahkan. Tentukan juga Wilayah tempat permintaan tersebut berlaku. Untuk mengaktifkan dan menambahkan akun yang ada di Wilayah tambahan, kirimkan permintaan untuk setiap Wilayah tambahan.

Untuk mengambil ID akun dan alamat email Akun AWS untuk mengaktifkan dan menambahkan, Anda dapat menggunakan [ListMembers](#) operasi Amazon Macie API secara opsional. Operasi ini memberikan detail tentang akun yang terkait dengan akun Macie Anda, termasuk akun yang bukan akun anggota Macie. Jika nilai `relationshipStatus` properti akun tidak `Enabled`, akun tersebut bukan akun anggota Macie.

Untuk mengaktifkan dan menambahkan satu atau beberapa akun yang ada dengan menggunakan AWS CLI, jalankan perintah [create-member](#). Gunakan `region` parameter untuk menentukan Wilayah untuk mengaktifkan dan menambahkan akun. Gunakan `account` parameter untuk menentukan ID akun dan alamat email untuk masing-masing Akun AWS untuk ditambahkan. Sebagai contoh:

```
C:\> aws macie2 create-member --region us-east-1 --account="{\"accountId\":  
\"123456789012\",\"email\": \"janedoe@example.com\"}"
```

*Dimana `us-east-1` adalah Wilayah untuk mengaktifkan dan menambahkan akun sebagai akun anggota Macie (Wilayah AS Timur (Virginia N.)), dan `account` parameter menentukan ID akun (123456789012) dan alamat email (`janedoe@example.com`) untuk akun tersebut.*

Jika permintaan Anda berhasil, status (`relationshipStatus`) akun yang ditentukan berubah menjadi `Enabled` inventaris akun Anda.

## Meninjau akun Amazon Macie untuk suatu organisasi

Setelah AWS Organizations organisasi [terintegrasi dan dikonfigurasi](#) di Amazon Macie, administrator Macie yang didelegasikan organisasi dapat mengakses inventaris akun organisasi di Macie. Sebagai administrator Macie untuk organisasi, Anda dapat menggunakan inventaris ini untuk meninjau statistik dan detail akun Macie organisasi Anda di file. Wilayah AWS Anda juga dapat menggunakan inventaris ini untuk [mengelola akun anggota Macie](#) di Wilayah.

Untuk meninjau akun Macie untuk suatu organisasi

Untuk meninjau akun organisasi Anda, Anda dapat menggunakan konsol Amazon Macie atau Amazon Macie API.

### Console

Ikuti langkah-langkah berikut untuk meninjau akun Macie organisasi Anda dengan menggunakan konsol Amazon Macie.

Untuk meninjau akun organisasi Anda

1. [Buka konsol Amazon Macie di https://console.aws.amazon.com/macie/.](https://console.aws.amazon.com/macie/)

2. Dengan menggunakan Wilayah AWS pilih di sudut kanan atas halaman, pilih Wilayah tempat Anda ingin meninjau akun organisasi Anda.
3. Di panel navigasi, di bagian Pengaturan, pilih Akun.

Halaman Akun membuka dan menampilkan statistik agregat dan tabel akun yang terkait dengan akun Macie Anda saat ini. Wilayah AWS

Di bagian atas halaman Akun, Anda akan menemukan statistik agregat berikut.

#### Melalui AWS Organizations

Aktif melaporkan jumlah total akun yang terkait dengan akun Anda melalui AWS Organizations dan saat ini merupakan akun anggota Macie di organisasi Anda. Macie diaktifkan untuk akun-akun ini dan Anda adalah administrator akun Macie.

Semua melaporkan jumlah total akun yang terkait dengan akun Anda AWS Organizations, termasuk akun yang saat ini bukan akun anggota Macie.

#### Dengan undangan

Aktif melaporkan jumlah total akun yang terkait dengan akun Anda oleh undangan Macie dan saat ini merupakan akun anggota Macie. (Akun ini tidak terkait dengan akun Anda melalui AWS Organizations.) Macie diaktifkan untuk akun dan Anda adalah administrator akun Macie karena mereka menerima undangan keanggotaan Macie dari Anda.

Semua melaporkan jumlah total akun yang terkait dengan akun Anda oleh undangan Macie, termasuk akun yang belum menanggapi undangan dari Anda.

#### Aktif/Semua

Aktif melaporkan jumlah total akun yang saat ini merupakan akun anggota Macie untuk akun Anda, baik melalui AWS Organizations atau melalui undangan Macie. Macie diaktifkan untuk akun-akun ini dan Anda adalah administrator akun Macie.

Semua melaporkan jumlah total akun yang terkait dengan akun Anda, baik melalui AWS Organizations atau melalui undangan Macie. Ini termasuk akun yang merupakan bagian dari organisasi Anda di AWS Organizations dan saat ini bukan akun anggota Macie, dan akun apa pun yang belum menanggapi undangan keanggotaan Macie dari Anda.



Dalam tabel, Anda akan menemukan detail tentang setiap akun di Wilayah saat ini. Tabel ini mencakup semua akun yang terkait dengan akun Macie Anda, baik melalui AWS Organizations atau dengan undangan Macie.

### ID Akun

ID akun dan alamat email untuk Akun AWS.

### Nama

Nama akun untuk Akun AWS. Nilai ini biasanya N/A untuk akun yang terkait dengan akun Anda oleh undangan Macie.

### Tipe

Bagaimana akun dikaitkan dengan akun Anda, melalui AWS Organizations atau dengan undangan Macie.

### Status

Status hubungan antara akun Anda dan akun. Untuk akun dalam AWS Organizations organisasi (Type is Via AWS Organizations), nilai yang mungkin adalah:

- Akun ditangguhkan - Akun AWS Ditangguhkan.
- Dibuat/Diaktifkan - Macie sedang memproses permintaan untuk mengaktifkan dan menambahkan akun sebagai akun anggota Macie.
- Diaktifkan - Akun ini adalah akun anggota Macie. Macie diaktifkan untuk akun dan Anda adalah administrator Macie untuk akun tersebut.
- Bukan anggota — Akun ini adalah bagian dari organisasi Anda AWS Organizations tetapi bukan akun anggota Macie.
- Dijeda (ditangguhkan) — Akun tersebut adalah akun anggota Macie tetapi Macie saat ini ditangguhkan untuk akun tersebut.
- Wilayah dinonaktifkan — Akun adalah bagian dari organisasi Anda AWS Organizations tetapi Wilayah saat ini dinonaktifkan untuk Akun AWS.
- Dihapus (dipisahkan) — Akun tersebut sebelumnya merupakan akun anggota Macie tetapi kemudian dihapus sebagai akun anggota. Anda melepaskan akun dari akun administrator Macie Anda. Macie terus diaktifkan untuk akun tersebut.

### Tindakan terakhir

Saat Anda atau akun terkait baru-baru ini melakukan tindakan yang memengaruhi hubungan antar akun Anda.

Untuk mengurutkan tabel berdasarkan bidang tertentu, klik judul kolom untuk bidang. Untuk mengubah urutan pengurutan, klik judul kolom lagi. Untuk memfilter tabel, letakkan kursor Anda di kotak filter, lalu tambahkan kondisi filter untuk bidang. Untuk lebih menyempurnakan hasilnya, tambahkan syarat filter untuk bidang tambahan.

## API

Untuk meninjau akun organisasi Anda secara terprogram, gunakan [ListMembers](#) pengoperasian Amazon Macie API dan pastikan untuk menentukan Wilayah tempat permintaan Anda berlaku. Untuk meninjau akun di Wilayah tambahan, kirimkan permintaan Anda di setiap Wilayah tambahan.

Saat Anda mengirimkan permintaan, gunakan `onlyAssociated` parameter untuk menentukan akun mana yang akan disertakan dalam respons. Secara default, Macie mengembalikan detail tentang hanya akun yang merupakan akun anggota Macie di Wilayah tertentu, baik melalui AWS Organizations atau melalui undangan Macie. Untuk mengambil detail ini untuk semua akun yang terkait dengan akun Macie Anda, termasuk akun yang bukan akun anggota, sertakan `onlyAssociated` parameter dalam permintaan Anda dan tetapkan nilai parameter ke `false`.

Untuk meninjau akun organisasi Anda menggunakan [AWS Command Line Interface\(AWS CLI\)](#), jalankan perintah [list-member](#). Untuk `only-associated` parameter, tentukan apakah akan menyertakan semua akun terkait atau hanya akun anggota Macie. Untuk menyertakan hanya akun anggota, hilangkan parameter ini atau setel nilai parameter ke `true`. Untuk menyertakan semua akun, tetapkan nilai ini ke `false`. Misalnya:

```
C:\> aws macie2 list-members --region us-east-1 --only-associated false
```

Di mana *us-timur-1* adalah Wilayah tempat permintaan tersebut berlaku, Wilayah AS Timur (Virginia N.).

Jika permintaan Anda berhasil, Macie mengembalikan array. `members` Array berisi `member` objek untuk setiap akun yang memenuhi kriteria yang ditentukan dalam permintaan. Dalam objek itu, `relationshipStatus` bidang menunjukkan status hubungan saat ini antara akun Anda dan akun lain di Wilayah yang ditentukan. Untuk akun dalam suatu AWS Organizations organisasi, nilai yang mungkin adalah:

- `AccountSuspended`- Akun AWS Ditangguhkan.
- `Created`— Macie sedang memproses permintaan untuk mengaktifkan dan menambahkan akun sebagai akun anggota Macie.

- **Enabled**— Akun tersebut adalah akun anggota Macie. Macie diaktifkan untuk akun dan Anda adalah administrator Macie untuk akun tersebut.
- **Paused**— Akun tersebut adalah akun anggota Macie tetapi Macie saat ini ditangguhkan (dijeda) untuk akun tersebut.
- **RegionDisabled**— Akun adalah bagian dari organisasi Anda AWS Organizations tetapi Wilayah saat ini dinonaktifkan untuk Akun AWS.
- **Removed**— Akun tersebut sebelumnya merupakan akun anggota Macie tetapi kemudian dihapus sebagai akun anggota. Anda melepaskan akun dari akun administrator Macie Anda. Macie terus diaktifkan untuk akun tersebut.

Untuk informasi tentang bidang lain di member objek, lihat [Anggota di Referensi](#) API Amazon Macie.

## Mengelola akun anggota Amazon Macie untuk suatu organisasi

Setelah AWS Organizations organisasi [terintegrasi dan dikonfigurasi](#) di Amazon Macie, administrator Macie yang didelegasikan organisasi dapat mengakses pengaturan, data, dan sumber daya Macie tertentu untuk akun anggota.

Sebagai administrator Macie untuk suatu organisasi, Anda dapat secara terpusat melakukan tugas manajemen dan administrasi akun tertentu di Macie. Misalnya:

- Menambahkan dan menghapus akun anggota Macie
- Mengelola status Macie untuk akun individual, seperti mengaktifkan atau menangguhkan Macie untuk akun
- Pantau kuota Macie dan perkiraan biaya penggunaan untuk akun individu dan organisasi secara keseluruhan

Anda juga dapat meninjau data inventaris Amazon Simple Storage Service (Amazon S3) dan temuan kebijakan untuk akun anggota Macie. Dan Anda dapat menemukan data sensitif di bucket S3 yang dimiliki akun tersebut. Untuk daftar tugas terperinci yang dapat Anda lakukan, lihat [Memahami hubungan antara administrator Amazon Macie dan akun anggota](#).

Secara default, Macie memberi Anda visibilitas ke data dan sumber daya yang relevan untuk semua akun anggota Macie di organisasi Anda. Anda juga dapat menelusuri untuk meninjau data dan

sumber daya untuk masing-masing akun. Misalnya, jika Anda [menggunakan dasbor Ringkasan](#) untuk menilai postur keamanan Amazon S3 organisasi Anda, Anda dapat memfilter data berdasarkan akun. Demikian pula, jika Anda [memantau perkiraan biaya penggunaan](#), Anda dapat mengakses rincian perkiraan biaya untuk akun anggota individu.

Selain tugas yang umum untuk akun administrator dan anggota, Anda dapat melakukan berbagai tugas administratif untuk organisasi Anda.

## Tugas

- [Menambahkan akun anggota Amazon Macie ke organisasi](#)
- [Menangguhkan Amazon Macie untuk akun anggota dalam suatu organisasi](#)
- [Menghapus akun anggota Amazon Macie dari organisasi](#)

Sebagai administrator Macie untuk organisasi, Anda dapat melakukan tugas-tugas ini dengan menggunakan konsol Amazon Macie atau Amazon Macie API. Jika Anda lebih suka menggunakan konsol, perhatikan bahwa Anda harus diizinkan untuk melakukan AWS Organizations tindakan berikut: `organizations:ListAccounts`. Tindakan ini memungkinkan Anda untuk mengambil dan menampilkan informasi tentang akun yang merupakan bagian dari organisasi Anda. AWS Organizations

## Menambahkan akun anggota Amazon Macie ke organisasi

Dalam beberapa kasus, Anda mungkin perlu menambahkan akun secara manual sebagai akun anggota Macie. Ini adalah kasus untuk akun yang sebelumnya Anda hapus (dipisahkan) sebagai akun anggota. Ini juga terjadi jika Anda tidak mengonfigurasi Macie untuk [mengaktifkan dan menambahkan akun baru secara otomatis sebagai akun anggota](#) saat akun ditambahkan ke organisasi Anda. AWS Organizations

Saat Anda menambahkan akun sebagai akun anggota Macie, Macie diaktifkan untuk akun saat ini Wilayah AWS, jika akun tersebut belum diaktifkan di Wilayah tersebut, dan akun tersebut dikaitkan dengan akun administrator Macie Anda sebagai akun anggota di Wilayah. Akun anggota tidak menerima undangan atau pemberitahuan lain bahwa Anda membuat hubungan ini antara akun Anda.

Perhatikan bahwa Anda tidak dapat menambahkan akun yang sudah dikaitkan dengan akun administrator Macie lainnya. Akun harus terlebih dahulu memisahkan diri dari akun administrator saat ini. Selain itu, Anda tidak dapat menambahkan akun AWS Organizations manajemen sebagai akun anggota kecuali akun manajemen telah mengaktifkan Macie untuk akun tersebut. Untuk mempelajari

tentang persyaratan tambahan, lihat [Pertimbangan dan rekomendasi untuk menggunakan Amazon Macie dengan AWS Organizations](#).

Untuk menambahkan akun anggota Macie ke organisasi

Untuk menambahkan satu atau beberapa akun anggota Macie ke organisasi Anda, Anda dapat menggunakan konsol Amazon Macie atau Amazon Macie API.

## Console

Ikuti langkah-langkah ini untuk menambahkan satu atau beberapa akun anggota Macie dengan menggunakan konsol Amazon Macie.

Untuk menambahkan akun anggota Macie

1. [Buka konsol Amazon Macie di https://console.aws.amazon.com/macie/](https://console.aws.amazon.com/macie/).
2. Dengan menggunakan Wilayah AWS pemilih di sudut kanan atas halaman, pilih Wilayah tempat Anda ingin menambahkan akun anggota.
3. Di panel navigasi, di bagian Pengaturan, pilih Akun. Halaman Akun membuka dan menampilkan tabel akun yang terkait dengan akun Anda.
4. (Opsional) Untuk lebih mudah mengidentifikasi akun yang merupakan bagian dari organisasi Anda AWS Organizations dan bukan akun anggota Macie, gunakan kotak filter di atas tabel untuk menambahkan kondisi filter berikut:
  - Jenis = Organisasi
  - Status = Bukan Anggota

Untuk juga menampilkan akun yang sebelumnya Anda hapus dan mungkin ingin ditambahkan sebagai akun anggota, tambahkan juga kondisi filter Status = Dihapus.

5. Di tabel Akun, pilih kotak centang untuk setiap akun yang ingin Anda tambahkan sebagai akun anggota.
6. Pada menu Tindakan, pilih Tambahkan anggota.
7. Konfirmasikan bahwa Anda ingin menambahkan jumlah akun yang dipilih sebagai akun anggota.

Setelah Anda mengonfirmasi pilihan Anda, status akun yang dipilih berubah menjadi Created/Enabling, dan kemudian Diaktifkan di inventaris akun Anda.

Ulangi langkah sebelumnya di setiap Wilayah tambahan di mana Anda ingin menambahkan akun anggota.

## API

Untuk menambahkan satu atau beberapa akun anggota Macie secara terprogram, gunakan [CreateMember](#) pengoperasian API Amazon Macie.

Saat Anda mengirimkan permintaan, gunakan parameter yang didukung untuk menentukan 12 digit ID akun dan alamat email untuk setiap Akun AWS yang ingin Anda tambahkan. Tentukan juga Wilayah tempat permintaan tersebut berlaku. Untuk menambahkan akun di Wilayah tambahan, kirimkan permintaan Anda di setiap Wilayah tambahan.

Untuk mengambil ID akun dan alamat email akun yang akan ditambahkan, Anda dapat menghubungkan output [ListAccounts](#) pengoperasian AWS Organizations API dan pengoperasian API Amazon Macie. [ListMembers](#) Untuk ListMembers pengoperasian API Macie, sertakan `onlyAssociated` parameter dalam permintaan Anda dan atur nilai parameter ke `false`. Jika operasi berhasil, Macie mengembalikan `members` larik yang memberikan detail tentang semua akun yang terkait dengan akun administrator Macie Anda di Wilayah tertentu, termasuk akun yang saat ini bukan akun anggota. Perhatikan hal berikut dalam array:

- Jika nilai `relationshipStatus` properti akun tidak `Enabled`, akun tersebut dikaitkan dengan akun Anda tetapi bukan akun anggota Macie.
- Jika akun tidak disertakan dalam array tetapi disertakan dalam output ListAccounts operasi AWS Organizations API, akun tersebut adalah bagian dari organisasi Anda AWS Organizations tetapi tidak terkait dengan akun Anda dan, oleh karena itu, bukan akun anggota Macie.

Untuk menambahkan akun anggota dengan menggunakan AWS CLI, jalankan perintah [create-member](#). Gunakan `region` parameter untuk menentukan Wilayah untuk menambahkan akun. Gunakan `account` parameter untuk menentukan ID akun dan alamat email untuk setiap akun yang akan ditambahkan. Misalnya:

```
C:\> aws macie2 create-member --region us-east-1 --account="{\"accountId\":  
\"123456789012\", \"email\": \"janedoe@example.com\"}"
```

*Dimana `us-east-1` adalah Wilayah di mana untuk menambahkan akun sebagai akun anggota (Wilayah AS Timur (Virginia N.)), dan `account` parameter menentukan ID akun (123456789012) dan alamat email (`janedoe@example.com`) untuk akun tersebut.*

Jika permintaan Anda berhasil, status (`relationshipStatus`) akun yang ditentukan berubah menjadi `Enabled` inventaris akun Anda.

## Menangguhkan Amazon Macie untuk akun anggota dalam suatu organisasi

Sebagai administrator Macie untuk organisasi di AWS Organizations, Anda dapat menangguhkan Macie untuk akun anggota di organisasi Anda. Jika Anda melakukan ini, Anda juga dapat mengaktifkan kembali Macie untuk akun di lain waktu.

Saat Anda menangguhkan Macie untuk akun anggota:

- Macie kehilangan akses dan berhenti memberikan metadata tentang data Amazon S3 akun saat ini. Wilayah AWS
- Macie berhenti melakukan semua aktivitas untuk akun di Wilayah. Ini termasuk memantau bucket S3 untuk keamanan dan kontrol akses, melakukan penemuan data sensitif otomatis, dan menjalankan pekerjaan penemuan data sensitif yang saat ini sedang berlangsung.
- Macie membatalkan semua pekerjaan penemuan data sensitif yang dibuat oleh akun di Wilayah. Pekerjaan tidak dapat dilanjutkan atau dimulai kembali setelah dibatalkan.

Jika Anda membuat lowongan untuk menganalisis data yang dimiliki akun anggota, Macie tidak membatalkan pekerjaan Anda. Sebaliknya, pekerjaan melewati sumber daya yang dimiliki oleh akun.

Saat akun ditangguhkan, Macie mempertahankan pengenalan sesi Macie, pengaturan, dan sumber daya untuk akun di Wilayah yang berlaku. Misalnya, temuan akun tetap utuh dan tidak terpengaruh hingga 90 hari. Organisasi Anda tidak dikenakan biaya Macie untuk akun di Wilayah yang berlaku saat Macie ditangguhkan untuk akun di Wilayah tersebut.

Untuk menangguhkan Macie untuk akun anggota di organisasi

Untuk menangguhkan Macie untuk akun anggota di organisasi, Anda dapat menggunakan konsol Amazon Macie atau Amazon Macie API.

### Console

Ikuti langkah-langkah berikut untuk menangguhkan Macie untuk akun anggota dengan menggunakan konsol Amazon Macie.

Untuk menanggihkan Macie untuk akun anggota

1. [Buka konsol Amazon Macie di https://console.aws.amazon.com/macie/](https://console.aws.amazon.com/macie/).
2. Dengan menggunakan Wilayah AWS pemilih di sudut kanan atas halaman, pilih Wilayah tempat Anda ingin menanggihkan Macie untuk akun anggota.
3. Di panel navigasi, di bagian Pengaturan, pilih Akun.
4. Di tabel Akun, pilih kotak centang agar akun ditanggihkan.
5. Pada menu Tindakan, pilih Tangguhkan Macie.
6. Konfirmasikan bahwa Anda ingin menanggihkan Macie untuk akun tersebut.

Setelah Anda mengonfirmasi penanggihan, status akun berubah menjadi Dijeda (ditanggihkan) di inventaris akun Anda.

Ulangi langkah sebelumnya di setiap Wilayah tambahan di mana Anda ingin menanggihkan Macie untuk akun tersebut.

## API

Untuk menanggihkan Macie untuk akun anggota secara terprogram, gunakan [UpdateMemberSession](#) pengoperasian Amazon Macie API.

Saat Anda mengirimkan permintaan, gunakan `id` parameter untuk menentukan ID akun 12 digit untuk Akun AWS yang ingin Anda tangguhkan Macie. Untuk `status` parameter, tentukan `PAUSED` sebagai status baru untuk akun Macie. Tentukan juga Wilayah tempat permintaan tersebut berlaku. Untuk menanggihkan akun di Wilayah tambahan, kirimkan permintaan Anda di setiap Wilayah tambahan.

Untuk mengambil ID akun agar akun ditanggihkan, Anda dapat menggunakan [ListMembers](#) pengoperasian API Amazon Macie. Jika Anda melakukan ini, pertimbangkan untuk memfilter hasil dengan memasukkan `onlyAssociated` parameter dalam permintaan Anda. Jika Anda menetapkan nilai parameter `inittrue`, Macie mengembalikan `members` array yang memberikan rincian hanya tentang akun yang saat ini menjadi akun anggota.

Untuk menanggihkan Macie untuk akun anggota dengan menggunakan AWS CLI, jalankan perintah. [update-member-session](#) Gunakan `region` parameter untuk menentukan Wilayah di mana untuk menanggihkan Macie dan menggunakan `id` parameter untuk menentukan ID akun untuk menanggihkan Macie Akun AWS untuk. Untuk `status` parameter, tentukan `PAUSED`. Misalnya:



```
C:\> aws macie2 update-member-session --region us-east-1 --id 123456789012 --status PAUSED
```

Di mana *us-east-1* adalah Wilayah untuk menanggihkan Macie (Wilayah AS Timur (Virginia N.)), *123456789012* adalah ID akun untuk akun untuk menanggihkan Macie, dan merupakan status baru Macie untuk akun tersebut. PAUSED

Jika permintaan Anda berhasil, Macie mengembalikan respons kosong dan status akun yang ditentukan berubah Paused dalam inventaris akun Anda.

## Menghapus akun anggota Amazon Macie dari organisasi

Jika Anda ingin berhenti mengakses pengaturan, data, dan sumber daya Macie untuk akun anggota, Anda dapat menghapus akun tersebut sebagai akun anggota Macie. Anda melakukan ini dengan memisahkan akun dari akun administrator Macie Anda. Perhatikan bahwa hanya Anda yang dapat melakukan ini untuk akun anggota. Akun AWS Organizations anggota tidak dapat memisahkan diri dari akun administrator Macie-nya.

Saat Anda menghapus akun anggota Macie, Macie tetap diaktifkan untuk akun saat ini. Wilayah AWS Namun, akun tersebut dipisahkan dari akun administrator Macie Anda dan menjadi akun Macie mandiri. Ini berarti Anda kehilangan akses ke semua pengaturan, data, dan sumber daya Macie untuk akun, termasuk metadata dan temuan kebijakan untuk data Amazon S3 akun. Ini juga berarti bahwa Anda tidak dapat lagi menggunakan Macie untuk menemukan data sensitif di bucket S3 yang dimiliki akun tersebut. Jika Anda sudah membuat pekerjaan penemuan sensitif untuk melakukan ini, pekerjaan tersebut melewati bucket yang dimiliki akun tersebut.

Setelah Anda menghapus akun anggota Macie, akun tersebut terus muncul di inventaris akun Anda. Macie tidak memberi tahu pemilik akun bahwa Anda menghapus akun tersebut.

Untuk menghapus akun anggota Macie dari organisasi

Untuk menghapus akun anggota Macie dari organisasi Anda, Anda dapat menggunakan konsol Amazon Macie atau Amazon Macie API.

### Console

Ikuti langkah-langkah ini untuk menghapus akun anggota Macie dengan menggunakan konsol Amazon Macie.

Untuk menghapus akun anggota Macie

1. [Buka konsol Amazon Macie di https://console.aws.amazon.com/macie/](https://console.aws.amazon.com/macie/).
2. Dengan menggunakan Wilayah AWS pemilih di sudut kanan atas halaman, pilih Wilayah tempat Anda ingin menghapus akun anggota.
3. Di panel navigasi, di bagian Pengaturan, pilih Akun.
4. Di tabel Akun, pilih kotak centang untuk akun yang ingin Anda hapus sebagai akun anggota.
5. Pada menu Tindakan, pilih Disassociate account.
6. Konfirmasikan bahwa Anda ingin menghapus akun yang dipilih sebagai akun anggota.

Setelah Anda mengonfirmasi pilihan Anda, status akun berubah menjadi Dihapus (terputus) di inventaris akun Anda.

Ulangi langkah sebelumnya di setiap Wilayah tambahan di mana Anda ingin menghapus akun anggota.

## API

Untuk menghapus akun anggota Macie secara terprogram, gunakan [DisassociateMember](#) pengoperasian Amazon Macie API.

Saat Anda mengirimkan permintaan Anda, gunakan `id` parameter untuk menentukan Akun AWS ID 12 digit untuk dihapus oleh akun anggota. Tentukan juga Wilayah tempat permintaan tersebut berlaku. Untuk menghapus akun di Wilayah tambahan, kirimkan permintaan Anda di setiap Wilayah tambahan.

Untuk mengambil ID akun untuk menghapus akun anggota, Anda dapat menggunakan [ListMembers](#) pengoperasian Amazon Macie API. Jika Anda melakukan ini, pertimbangkan untuk memfilter hasil dengan memasukkan `onlyAssociated` parameter dalam permintaan Anda. Jika Anda menetapkan nilai parameter `inittrue`, Macie mengembalikan `members` array yang memberikan rincian hanya tentang akun yang saat ini merupakan akun anggota Macie.

Untuk menghapus akun anggota Macie dengan menggunakan AWS CLI, jalankan perintah [disassociate-member](#). Gunakan `region` parameter untuk menentukan wilayah tempat menghapus akun. Gunakan `id` parameter untuk menentukan ID akun untuk menghapus akun anggota. Misalnya:

```
C:\> aws macie2 disassociate-member --region us-east-1 --id 123456789012
```

Dimana *us-east-1* adalah Wilayah untuk menghapus akun (Wilayah AS Timur (Virginia N.)) dan *123456789012* adalah ID akun untuk menghapus akun tersebut.

Jika permintaan Anda berhasil, Macie mengembalikan respons kosong dan status akun yang ditentukan berubah *Removed* dalam inventaris akun Anda.

## Menunjuk akun administrator Amazon Macie yang berbeda untuk suatu organisasi

Setelah AWS Organizations organisasi [terintegrasi dan dikonfigurasi](#) di Amazon Macie, akun AWS Organizations manajemen dapat menunjuk akun yang berbeda sebagai akun administrator Macie yang didelegasikan untuk organisasi tersebut.

Sebagai pengguna akun AWS Organizations manajemen untuk organisasi, verifikasi bahwa Anda memenuhi persyaratan izin berikut sebelum Anda menetapkan akun administrator Macie yang berbeda untuk organisasi Anda:

- Anda harus memiliki [izin yang sama](#) yang diperlukan untuk awalnya menunjuk akun administrator Macie untuk organisasi Anda. Anda juga harus diizinkan untuk melakukan AWS Organizations tindakan berikut: `organizations:DeregisterDelegatedAdministrator`. Tindakan tambahan ini memungkinkan Anda untuk menghapus penunjukan saat ini.
- Jika akun Anda saat ini adalah akun anggota Macie, administrator Macie saat ini harus menghapus akun Anda sebagai akun anggota Macie. Jika tidak, Anda tidak akan diizinkan mengakses operasi Macie untuk menunjuk akun administrator yang berbeda. Setelah Anda menetapkan akun administrator baru, administrator Macie baru dapat menambahkan akun Anda sebagai akun anggota Macie lagi.

Jika organisasi Anda menggunakan Macie dalam beberapa kali Wilayah AWS, pastikan juga bahwa Anda mengubah akun administrator Macie yang didelegasikan di setiap Wilayah tempat organisasi Anda menggunakan Macie—akun administrator Macie yang didelegasikan harus sama di semua Wilayah tersebut. Jika Anda mengelola beberapa organisasi AWS Organizations, perhatikan juga bahwa akun dapat menjadi akun administrator Macie yang didelegasikan hanya untuk satu organisasi pada satu waktu. Untuk mempelajari tentang persyaratan tambahan, lihat [Pertimbangan dan rekomendasi untuk menggunakan Amazon Macie dengan AWS Organizations](#).

Untuk menunjuk akun administrator Macie yang berbeda untuk organisasi Anda

Untuk menetapkan akun administrator Macie yang berbeda untuk organisasi Anda, Anda dapat menggunakan konsol Amazon Macie atau kombinasi Amazon Macie dan API. AWS Organizations Hanya pengguna akun AWS Organizations manajemen yang dapat mengubah penunjukan untuk organisasi mereka.

## Console

Untuk mengubah penunjukan dengan menggunakan konsol Amazon Macie, ikuti langkah-langkah ini.

Untuk menunjuk akun administrator Macie yang berbeda

1. Masuk ke AWS Management Console menggunakan akun AWS Organizations manajemen Anda.
2. Dengan menggunakan Wilayah AWS pemilih di sudut kanan atas halaman, pilih Wilayah di mana Anda ingin mengubah penunjukan.
3. [Buka konsol Amazon Macie di https://console.aws.amazon.com/macie/](https://console.aws.amazon.com/macie/).
4. Lakukan salah satu hal berikut, tergantung pada apakah Macie diaktifkan untuk akun manajemen Anda di Wilayah saat ini:
  - Jika Macie tidak diaktifkan, pilih Mulai di halaman selamat datang.
  - Jika Macie diaktifkan, pilih Pengaturan di panel navigasi.
5. Di bawah Administrator yang didelegasikan, pilih Hapus. Untuk mengubah penunjukan, Anda harus terlebih dahulu menghapus penunjukan saat ini.
6. Konfirmasikan bahwa Anda ingin menghapus penunjukan saat ini.
7. Di bawah Administrator yang didelegasikan, masukkan ID akun 12 digit untuk ditetapkan sebagai akun administrator Macie baru Akun AWS untuk organisasi.
8. Pilih Delegasikan.

Ulangi langkah sebelumnya di setiap Wilayah tambahan di mana Anda mengintegrasikan Macie. AWS Organizations

## API

Untuk mengubah penunjukan secara terprogram, Anda menggunakan dua operasi Amazon Macie API dan satu operasi API. AWS Organizations Ini karena Anda harus menghapus penunjukan saat ini di Macie dan AWS Organizations sebelum Anda mengirimkan penunjukan baru.

Untuk menghapus penunjukan saat ini:

1. Gunakan [DisableOrganizationAdminAccount](#) pengoperasian API Macie. Untuk `adminAccountId` parameter yang diperlukan, tentukan ID akun 12 digit untuk Akun AWS yang saat ini ditetapkan sebagai akun administrator Macie untuk organisasi.
2. Gunakan [DeregisterDelegatedAdministrator](#) pengoperasian AWS Organizations API. Untuk `AccountId` parameter, tentukan ID akun 12 digit untuk akun yang saat ini ditetapkan sebagai akun administrator Macie untuk organisasi. Nilai ini harus sesuai dengan ID akun yang Anda tentukan dalam permintaan Macie sebelumnya. Untuk `ServicePrincipal` parameter, tentukan prinsipal layanan Macie (`macie.amazonaws.com`).

Setelah Anda menghapus penunjukan saat ini, kirimkan penunjukan baru dengan menggunakan [EnableOrganizationAdminAccount](#) pengoperasian API Macie. Untuk `adminAccountId` parameter yang diperlukan, tentukan ID akun 12 digit Akun AWS untuk ditunjuk sebagai akun administrator Macie baru untuk organisasi.

Untuk mengubah penunjukan dengan menggunakan [AWS CLI](#), jalankan [disable-organization-admin-account](#) perintah Macie API dan [deregister-delegated-administrator](#) perintah API. AWS Organizations Perintah ini menghapus penunjukan saat ini di Macie dan AWS Organizations, masing-masing. Untuk `account-id` parameter `admin-account-id` dan, tentukan ID akun 12 digit Akun AWS untuk dihapus sebagai akun administrator Macie saat ini. Gunakan `region` parameter untuk menentukan Wilayah tempat penghapusan berlaku. Sebagai contoh:

```
C:\> aws macie2 disable-organization-admin-account --region us-east-1 --admin-account-id 111122223333 && aws organizations deregister-delegated-administrator --region us-east-1 --account-id 111122223333 --service-principal macie.amazonaws.com
```

Di mana:

- **us-east-1** adalah Wilayah tempat penghapusan berlaku, Wilayah AS Timur (Virginia N.).
- **111122223333** adalah ID akun untuk menghapus akun sebagai akun administrator Macie.
- `macie.amazonaws.com` adalah kepala layanan Macie.

Setelah Anda menghapus penunjukan saat ini, kirimkan penunjukan baru dengan menjalankan [enable-organization-admin-account](#) perintah Macie API. Untuk `admin-account-id` parameter, tentukan ID akun 12 digit Akun AWS untuk ditunjuk sebagai akun administrator Macie baru untuk

organisasi. Gunakan `region` parameter untuk menentukan Wilayah tempat penunjukan berlaku. Sebagai contoh:

```
C:\> aws macie2 enable-organization-admin-account --region us-east-1 --admin-account-id 444455556666
```

Di mana `us-east-1` adalah Wilayah tempat penunjukan berlaku (Wilayah AS Timur (Virginia N.)) dan `444455556666` adalah ID akun untuk akun yang akan ditetapkan sebagai akun administrator Macie yang baru.

## Menonaktifkan integrasi Amazon Macie dengan AWS Organizations

Setelah AWS Organizations organisasi terintegrasi dengan Amazon Macie, akun AWS Organizations manajemen selanjutnya dapat menonaktifkan integrasi. Sebagai pengguna akun AWS Organizations manajemen, Anda dapat melakukan ini dengan menonaktifkan akses layanan tepercaya untuk Macie di AWS Organizations

Saat Anda menonaktifkan akses layanan tepercaya untuk Macie, hal berikut terjadi:

- Macie kehilangan statusnya sebagai layanan tepercaya di AWS Organizations.
- Akun administrator Macie organisasi kehilangan akses ke semua pengaturan, data, dan sumber daya Macie untuk semua akun anggota Macie secara keseluruhan. Wilayah AWS
- Semua akun anggota Macie menjadi akun Macie mandiri. Jika Macie diaktifkan untuk akun anggota di satu atau beberapa Wilayah, Macie terus diaktifkan untuk akun di Wilayah tersebut. Namun, akun tersebut tidak lagi dikaitkan dengan akun administrator Macie di Wilayah mana pun.

Untuk informasi tambahan tentang hasil menonaktifkan akses layanan tepercaya, lihat [Menggunakan AWS Organizations dengan yang lain Layanan AWS](#) di AWS Organizations Panduan Pengguna.

Untuk menonaktifkan akses layanan tepercaya untuk Macie

Untuk menonaktifkan akses layanan tepercaya, Anda dapat menggunakan AWS Organizations konsol atau AWS Organizations API. Hanya pengguna akun AWS Organizations manajemen yang dapat menonaktifkan akses layanan tepercaya untuk Macie. Untuk detail tentang izin yang Anda perlukan, lihat [Izin yang diperlukan untuk menonaktifkan akses tepercaya](#) di AWS Organizations Panduan Pengguna.

Sebelum Anda menonaktifkan akses layanan tepercaya, secara opsional bekerja dengan administrator Macie yang didelegasikan agar organisasi Anda menanggung atau menonaktifkan Macie untuk akun anggota dan membersihkan sumber daya Macie untuk akun tersebut.

## Console

Untuk menonaktifkan akses layanan tepercaya dengan menggunakan AWS Organizations konsol, ikuti langkah-langkah ini.

### Cara menonaktifkan akses layanan tepercaya

1. Masuk ke AWS Management Console menggunakan akun AWS Organizations manajemen Anda.
2. Buka AWS Organizations konsol di <https://console.aws.amazon.com/organizations/>.
3. Di panel navigasi, pilih Layanan.
4. Di bawah Layanan terintegrasi, pilih Amazon Macie.
5. Pilih Menonaktifkan akses tepercaya.
6. Konfirmasikan bahwa Anda ingin menonaktifkan akses tepercaya.

## API

Untuk menonaktifkan akses layanan tepercaya secara terprogram, gunakan `AWSServiceAccess` operasi [Nonaktifkan](#) API. AWS Organizations Untuk `ServicePrincipal` parameter, tentukan prinsip layanan Macie (`macie.amazonaws.com`).

Untuk menonaktifkan akses layanan tepercaya dengan menggunakan [AWS Command Line Interface\(AWS CLI\)](#), jalankan [disable-aws-service-access](#) perintah AWS Organizations API. Untuk `service-principal` parameter, tentukan prinsip layanan Macie (`macie.amazonaws.com`). Misalnya:

```
C:\> aws organizations disable-aws-service-access --service-principal
macie.amazonaws.com
```

## Mengelola akun Amazon Macie dengan undangan

Anda dapat mengelola beberapa akun Amazon Macie secara terpusat dengan dua cara, dengan [mengintegrasikan Macie dengan AWS Organizations atau dengan](#) menggunakan undangan

keanggotaan. Jika menggunakan undangan keanggotaan, administrator Macie yang ditunjuk dapat mengelola Macie untuk 1.000 akun. Administrator juga dapat mengakses data inventaris Amazon Simple Storage Service (Amazon S3) dan menemukan data sensitif di bucket Simple Storage Service (Amazon S3). Untuk detail tentang tugas yang dapat dilakukan administrator, lihat [Memahami hubungan antara administrator Amazon Macie dan akun anggota](#).

Di organisasi berbasis undangan, Anda mengaitkan akun Macie satu sama lain dengan mengirim dan menerima undangan keanggotaan di Macie. Jika Anda mengirim undangan dan diterima oleh akun lain, Anda menjadi administrator Macie untuk akun lain dan akun lainnya menjadi akun anggota di organisasi Anda. Jika Anda menerima dan menerima undangan, akun Anda menjadi akun anggota dan administrator Macie dapat mengakses pengaturan, data, dan sumber daya Macie tertentu untuk akun Anda.

#### Tip

Jika Anda membuat organisasi berbasis undangan di Macie, Anda selanjutnya dapat [beralih ke](#) penggunaan sebagai gantinya. AWS Organizations Anda juga dapat menggunakan kedua metode secara bersamaan untuk mengelola beberapa akun Macie. Misalnya, jika AWS lingkungan Anda menyertakan akun pengujian, Anda dapat mengecualikan akun dari organisasi AWS Organizations dan mengelolanya secara terpisah berdasarkan undangan.

Topik di bagian ini menjelaskan cara membuat dan berpartisipasi dalam organisasi berbasis undangan, dan bagaimana melakukan berbagai tugas administrasi untuk organisasi.

#### Topik

- [Pertimbangan dan rekomendasi untuk organisasi berbasis undangan di Amazon Macie](#)
- [Membuat dan mengelola organisasi berbasis undangan di Amazon Macie](#)
- [Meninjau akun Amazon Macie untuk organisasi berbasis undangan](#)
- [Menunjuk akun administrator Amazon Macie yang berbeda untuk organisasi berbasis undangan](#)
- [Mengelola keanggotaan Anda dalam organisasi berbasis undangan di Amazon Macie](#)



## Pertimbangan dan rekomendasi untuk organisasi berbasis undangan di Amazon Macie

Sebelum Anda membuat atau mulai mengelola organisasi berbasis undangan di Amazon Macie, pertimbangkan persyaratan dan rekomendasi berikut. Pastikan juga bahwa Anda memahami [hubungan antara administrator Macie dan akun anggota](#).

### Topik

- [Memilih akun administrator Macie](#)
- [Mengirim undangan dan mengelola akun anggota Macie](#)
- [Menanggapi dan mengelola undangan keanggotaan](#)
- [Transisi ke AWS Organizations](#)

### Memilih akun administrator Macie

Saat Anda menentukan akun mana yang harus menjadi akun administrator Macie untuk organisasi, ingatlah hal berikut:

- Sebuah organisasi hanya dapat memiliki satu akun administrator Macie.
- Akun tidak dapat menjadi administrator Macie dan akun anggota secara bersamaan.
- Macie adalah layanan Regional. Ini berarti bahwa hubungan antara akun administrator Macie dan akun anggota bersifat Regional—asosiasi hanya ada di mana Wilayah AWS undangan dikirim dan diterima. Misalnya, jika administrator Macie mengirim undangan di Wilayah AS Timur (Virginia N.) dan undangan tersebut diterima, administrator Macie hanya dapat mengelola akun anggota di Wilayah tersebut.

Untuk mengelola akun Macie secara terpusat dalam beberapa Wilayah AWS, administrator Macie dapat masuk ke setiap Wilayah tempat organisasi saat ini menggunakan atau akan menggunakan Macie dan mengirim undangan ke akun yang sesuai di masing-masing Wilayah tersebut. Untuk daftar Wilayah di mana Macie saat ini tersedia, lihat [titik akhir dan kuota Amazon Macie](#) di.

### Referensi Umum AWS

- Akun anggota hanya dapat dikaitkan dengan satu akun administrator Macie pada satu waktu. Jika organisasi Anda menggunakan Macie di beberapa Wilayah, ini berarti akun administrator Macie harus sama di semua Wilayah tersebut. Namun, akun administrator dan anggota harus mengirim dan menerima undangan secara terpisah di setiap Wilayah.

- Jika administrator Macie ditangguhkan, diisolasi, atau ditutup, semua akun anggota terkait secara otomatis dihapus sebagai akun anggota tetapi Macie terus diaktifkan untuk akun tersebut. Akun AWS

## Mengirim undangan dan mengelola akun anggota Macie

Sebagai administrator Macie untuk organisasi berbasis undangan, ingatlah hal berikut saat Anda mengirim undangan dan mengelola akun di organisasi:

- Jika Anda mengirim undangan, data terkait mungkin ditransfer ke seluruh Wilayah AWS. Hal ini terjadi karena Macie memverifikasi alamat email akun penerima dengan menggunakan layanan verifikasi email yang hanya beroperasi di Wilayah AS Timur (Virginia N.).
- Anda dapat mengirim undangan ke akun aktif apa pun Akun AWS, termasuk akun yang belum mengaktifkan Macie. Namun, untuk menerima atau menolak undangan, akun penerima harus mengaktifkan Macie di Wilayah tempat undangan dikirim.
- Akun administrator Macie dapat dikaitkan dengan tidak lebih dari 1.000 akun di masing-masing Wilayah AWS akun. Ini termasuk akun yang belum menanggapi undangan. Jika akun Anda memenuhi kuota ini, Anda tidak dapat menambahkan atau mengundang akun tambahan hingga Anda menghapus jumlah akun terkait yang diperlukan, menerima jumlah undangan yang ditolak, atau kombinasi keduanya.

Untuk menentukan berapa banyak akun yang saat ini dikaitkan dengan akun Anda, Anda dapat menggunakan halaman Akun di konsol Amazon Macie atau [ListMembers](#) pengoperasian API Amazon Macie. Untuk informasi selengkapnya, lihat [Meninjau akun Amazon Macie untuk organisasi berbasis undangan](#).

- Akun hanya dapat dikaitkan dengan satu akun administrator Macie pada satu waktu. Ini berarti bahwa akun tidak dapat menerima undangan Anda jika sudah dikaitkan dengan akun administrator Macie lain. Akun harus terlebih dahulu memisahkan diri dari akun administrator Macie saat ini.
- Dalam organisasi berbasis undangan, akun anggota dapat memisahkan diri dari akun administrator Macie-nya kapan saja. Jika ini terjadi, Macie terus diaktifkan untuk akun tersebut dan akun tersebut menjadi akun Macie mandiri. Macie tidak memberi tahu Anda jika akun anggota terputus dari akun administrator Anda. Namun, akun terus muncul di inventaris akun Anda dan memiliki status Anggota mengundurkan diri.
- Jika Anda menghapus akun anggota dari organisasi Anda, Macie terus diaktifkan untuk akun tersebut dan akun tersebut menjadi akun Macie mandiri.

## Menanggapi dan mengelola undangan keanggotaan

Sebagai penerima undangan atau anggota organisasi berbasis undangan, ingatlah hal-hal berikut ketika Anda menanggapi dan mengelola undangan yang Anda terima:

- Sebelum Anda menerima undangan, pastikan Anda [memahami hubungan antara administrator Macie dan akun anggota](#).
- Akun Anda hanya dapat dikaitkan dengan satu akun administrator Macie dalam satu waktu. Jika Anda menerima undangan dan kemudian ingin bergabung dengan organisasi lain (melalui undangan atau melalui AWS Organizations), Anda harus terlebih dahulu memisahkan akun Anda dari akun administrator Macie saat ini. Anda kemudian dapat bergabung dengan organisasi lain.
- Untuk menerima atau menolak undangan, Anda harus mengaktifkan Macie di Wilayah AWS mana undangan dikirim. Akun yang mengirim undangan tidak dapat mengaktifkan Macie di Wilayah itu untuk Anda. Menolak undangan adalah opsional. Jika Anda menolak undangan, Anda dapat menonaktifkan Macie secara opsional di Wilayah yang berlaku setelah Anda menolak undangan.
- Jika Anda seorang administrator Macie, Anda tidak dapat menerima undangan untuk menjadi akun anggota—akun tidak dapat menjadi administrator Macie dan akun anggota secara bersamaan. Untuk menjadi akun anggota, Anda harus terlebih dahulu memisahkan akun Anda dari semua akun anggotanya dengan menghapus semua akun anggota dari organisasi Anda saat ini.
- Macie adalah layanan Regional. Jika Anda menerima undangan, hubungan antara akun Anda dan akun administrator Macie bersifat Regional—asosiasi hanya ada di tempat Wilayah AWS undangan dikirim dan diterima.
- Jika Anda menggunakan Macie di beberapa Wilayah, akun administrator Macie untuk akun Anda harus sama di semua Wilayah tersebut. Namun, administrator Macie harus mengirim undangan kepada Anda secara terpisah di setiap Wilayah, dan Anda harus menerima undangan secara terpisah di setiap Wilayah.
- Anda dapat memisahkan akun Anda dari akun administrator Macie kapan saja. Jika Anda melakukan ini, Macie terus diaktifkan untuk akun Anda dan akun Anda menjadi akun Macie mandiri.
- Jika administrator Macie Anda menghapus akun Anda dari organisasi mereka, Macie terus diaktifkan untuk akun Anda dan akun Anda menjadi akun Macie mandiri.

## Transisi ke AWS Organizations

Setelah Anda membuat organisasi berbasis undangan di Macie, Anda dapat beralih menggunakan sebagai gantinya. AWS Organizations Untuk menyederhanakan transisi, kami sarankan Anda

menetapkan akun administrator berbasis undangan yang ada sebagai akun administrator Macie untuk organisasi di AWS Organizations

Jika Anda melakukan ini, semua akun anggota yang saat ini terkait terus menjadi anggota. Jika akun anggota merupakan bagian dari organisasi AWS Organizations, asosiasi akun secara otomatis berubah dari Melalui undangan menjadi Via AWS Organizations di Macie. Jika akun anggota bukan bagian dari organisasi AWS Organizations, asosiasi akun tetap menjadi Undangan. Dalam kedua kasus, akun terus dikaitkan dengan akun administrator Macie sebagai akun anggota.

Kami merekomendasikan pendekatan ini karena akun anggota hanya dapat dikaitkan dengan satu akun administrator Macie pada satu waktu. Jika Anda menetapkan akun lain sebagai akun administrator Macie untuk organisasi di AWS Organizations, administrator yang ditunjuk tidak akan dapat mengelola akun yang sudah dikaitkan dengan akun administrator Macie lain dengan undangan. Setiap akun anggota harus terlebih dahulu memisahkan diri dari akun administrator berbasis undangan saat ini. Hanya dengan begitu administrator Macie untuk AWS Organizations organisasi dapat menambahkan akun anggota ke organisasi mereka dan mulai mengelola Macie untuk akun tersebut.

Setelah Anda mengintegrasikan Macie dengan AWS Organizations dan Anda mengonfigurasi organisasi Anda di Macie, Anda dapat secara opsional menunjuk akun administrator Macie yang berbeda untuk organisasi tersebut. Anda juga dapat terus menggunakan undangan untuk mengaitkan dan mengelola akun anggota yang bukan bagian dari organisasi Anda. AWS Organizations

## Membuat dan mengelola organisasi berbasis undangan di Amazon Macie

Untuk membuat organisasi berbasis undangan di Amazon Macie, Anda mulai dengan menentukan akun mana yang Anda inginkan menjadi akun administrator Macie untuk organisasi tersebut. Anda kemudian menggunakan akun tersebut untuk menambahkan akun anggota—Anda mengirim undangan keanggotaan ke orang lain Akun AWS, mengundang akun untuk bergabung dengan organisasi sebagai akun anggota Macie saat ini. Wilayah AWS Untuk membuat organisasi di beberapa Wilayah, kirim undangan keanggotaan dari setiap Wilayah di mana akun lain saat ini atau akan menggunakan Macie.

Saat akun menerima undangan, akun tersebut menjadi akun anggota Macie yang terkait dengan akun administrator Macie di Wilayah yang berlaku. Akun administrator Macie kemudian dapat mengakses pengaturan, data, dan sumber daya Macie tertentu untuk akun anggota di Wilayah tersebut.

Sebagai administrator Macie untuk organisasi berbasis undangan, Anda dapat meninjau data inventaris Amazon Simple Storage Service (Amazon S3) dan temuan kebijakan untuk akun anggota. Anda juga dapat melakukan penemuan data sensitif otomatis dan menjalankan pekerjaan penemuan data sensitif untuk mendeteksi data sensitif di bucket S3 yang dimiliki akun anggota. Untuk daftar rinci tugas yang dapat Anda lakukan, lihat [Memahami hubungan antara administrator Amazon Macie dan akun anggota](#).

Secara default, Macie memberi Anda visibilitas ke data dan sumber daya yang relevan untuk organisasi Anda secara keseluruhan. Anda juga dapat menelusuri untuk meninjau data dan sumber daya untuk akun individual di organisasi Anda. Misalnya, jika Anda [menggunakan dasbor Ringkasan](#) untuk menilai postur keamanan Amazon S3 organisasi Anda, Anda dapat memfilter data berdasarkan akun. Demikian pula, jika Anda [memantau perkiraan biaya penggunaan](#), Anda dapat mengakses rincian perkiraan biaya untuk akun anggota individu.

Selain tugas yang umum untuk akun administrator dan anggota, Anda dapat secara terpusat melakukan berbagai tugas administratif untuk organisasi Anda. Sebelum Anda melakukan tugas-tugas ini, ada baiknya untuk meninjau [pertimbangan dan rekomendasi](#) untuk mengelola organisasi berbasis undangan di Macie.

## Tugas

- [Menambahkan akun anggota Amazon Macie ke organisasi berbasis undangan](#)
- [Menangguhkan Amazon Macie untuk akun anggota di organisasi berbasis undangan](#)
- [Menghapus akun anggota Amazon Macie dari organisasi berbasis undangan](#)
- [Menghapus asosiasi dengan akun lain](#)

## Menambahkan akun anggota Amazon Macie ke organisasi berbasis undangan

Sebagai administrator Macie untuk organisasi berbasis undangan, Anda menambahkan akun anggota ke organisasi Anda dengan melakukan dua langkah utama:

1. Tambahkan akun ke inventaris akun Anda di Macie. Ini menghubungkan akun dengan akun Anda.
2. Kirim undangan keanggotaan ke akun.

Ketika sebuah akun menerima undangan Anda, akun tersebut menjadi akun anggota di organisasi Anda.

## Langkah 1: Tambahkan akun

Untuk menambahkan satu atau beberapa akun ke inventaris akun, Anda dapat menggunakan konsol Amazon Macie atau Amazon Macie API.

### Console

Dengan konsol Amazon Macie, Anda dapat menambahkan satu akun sekaligus, atau menambahkan beberapa akun secara bersamaan dengan mengunggah file nilai yang dipisahkan koma (CSV). Ikuti langkah-langkah ini untuk menambahkan satu atau beberapa akun dengan menggunakan konsol.

Untuk menambahkan satu akun

1. [Buka konsol Amazon Macie di https://console.aws.amazon.com/macie/](https://console.aws.amazon.com/macie/).
2. Dengan menggunakan Wilayah AWS pemilih di sudut kanan atas halaman, pilih Wilayah tempat Anda ingin menambahkan akun.
3. Di panel navigasi, di bawah Pengaturan, pilih Akun.
4. Pilih Tambah akun.
5. Di bagian Masukkan detail akun, pilih tab Tambah akun. Kemudian, lakukan hal berikut:
  - Untuk ID Akun, masukkan ID akun 12 digit ke Akun AWS untuk menambahkan.
  - Untuk alamat Email, masukkan alamat email Akun AWS untuk ditambahkan.
6. Pilih Tambah, lalu pilih Berikutnya.

Macie menambahkan akun ke inventaris akun Anda. Jenis akun adalah Dengan undangan dan statusnya Dibuat. Ulangi langkah sebelumnya di setiap Wilayah tambahan di mana Anda ingin menambahkan akun.

Untuk menambahkan beberapa akun

1. Dengan menggunakan editor teks, buat file CSV sebagai berikut:
  - a. Tambahkan header berikut sebagai baris pertama file: Account ID, Email
  - b. Untuk setiap akun, buat baris baru yang memiliki ID akun 12 digit Akun AWS untuk ditambahkan dan alamat email untuk akun tersebut. Pisahkan entri dengan koma, misalnya: 111111111111,janedoe@example.com

Alamat email harus sesuai dengan alamat email yang terkait dengan Akun AWS.

- c. Verifikasi bahwa konten file diformat seperti yang ditunjukkan pada contoh berikut, yang berisi header dan informasi yang diperlukan untuk tiga akun:

```
Account ID,Email
111111111111,janedoe@example.com
222222222222,jorgesouza@example.com
333333333333,lijuan@example.com
```

- d. Simpan file pada komputer anda.

2. [Buka konsol Amazon Macie di https://console.aws.amazon.com/macie/](https://console.aws.amazon.com/macie/).
3. Dengan menggunakan Wilayah AWS pemilih di sudut kanan atas halaman, pilih Wilayah tempat Anda ingin menambahkan akun.
4. Di panel navigasi, di bawah Pengaturan, pilih Akun.
5. Pilih Tambah akun.
6. Di bagian Masukkan detail akun, pilih tab Unggah daftar (CSV).
7. Pilih Browse, lalu pilih file CSV yang Anda buat di langkah 1.
8. Pilih Tambahkan akun, lalu pilih Selanjutnya.

Macie menambahkan akun ke inventaris akun Anda. Tipe mereka adalah Dengan undangan dan status mereka Dibuat. Ulangi langkah 3 hingga 8 di setiap Wilayah tambahan tempat Anda ingin menambahkan akun.

## API

Untuk menambahkan satu atau beberapa akun secara terprogram, gunakan [CreateMember](#) pengoperasian Amazon Macie API. Saat Anda mengirimkan permintaan, gunakan parameter yang didukung untuk menentukan 12 digit ID akun dan alamat email Akun AWS untuk ditambahkan masing-masing. Tentukan juga Wilayah tempat permintaan tersebut berlaku. Untuk menambahkan akun di Wilayah tambahan, kirimkan permintaan di setiap Wilayah tambahan.

Untuk menambahkan akun menggunakan [AWS Command Line Interface\(AWS CLI\)](#), jalankan perintah [create-member](#). Gunakan `region` parameter untuk menentukan Wilayah tempat menambahkan akun. Gunakan `account` parameter untuk menentukan ID akun dan alamat email untuk masing-masing Akun AWS untuk ditambahkan. Misalnya:

```
C:\> aws macie2 create-member --region us-east-1 --account="{\"accountId\":  
\"111111111111\", \"email\": \"janedoe@example.com\"}"
```

*Di mana us-east-1 adalah Wilayah untuk menambahkan akun (Wilayah AS Timur (Virginia N.)) dan account parameter menentukan ID akun (111111111111) dan alamat email (janedoe@example.com) untuk akun yang akan ditambahkan.*

Jika permintaan Anda berhasil, Macie menambahkan setiap akun ke inventaris akun Anda dengan status Created dan Anda menerima output yang serupa dengan berikut ini:

```
{  
  "arn": "arn:aws:macie2:us-east-1:123456789012:member/111111111111"  
}
```

Di arn mana Amazon Resource Name (ARN) dari sumber daya yang dibuat untuk asosiasi antara akun Anda dan akun yang Anda tambahkan. Dalam contoh ini, 123456789012 adalah ID akun untuk akun yang membuat asosiasi dan 111111111111 merupakan ID akun untuk akun yang ditambahkan.

## Langkah 2: Kirim undangan keanggotaan ke akun

Setelah menambahkan akun ke inventaris akun, Anda dapat mengundang akun tersebut untuk bergabung dengan organisasi Anda sebagai akun anggota Macie. Untuk melakukan ini, kirim undangan keanggotaan ke akun. Saat Anda mengirim undangan, lencana Akun dan pemberitahuan akan muncul di konsol Amazon Macie untuk akun penerima, jika Macie diaktifkan untuk akun tersebut. Macie juga membuat AWS Health acara untuk akun tersebut.

Bergantung pada apakah Anda menggunakan konsol Amazon Macie atau API untuk mengirim undangan, Macie juga mengirimkan undangan ke alamat email yang Anda tentukan untuk akun penerima saat Anda menambahkan akun. Pesan email menunjukkan bahwa Anda ingin menjadi administrator Macie untuk akun mereka, dan itu termasuk ID akun untuk Anda Akun AWS dan penerimaAkun AWS. Pesan tersebut juga menjelaskan cara mengakses undangan. Anda dapat menambahkan teks khusus ke pesan secara opsional.

Untuk mengirim undangan keanggotaan ke satu atau beberapa akun, Anda dapat menggunakan konsol Amazon Macie atau Amazon Macie API.



## Console

Ikuti langkah-langkah berikut untuk mengirim undangan keanggotaan dengan menggunakan konsol Amazon Macie.

Untuk mengirim undangan keanggotaan

1. [Buka konsol Amazon Macie di https://console.aws.amazon.com/macie/](https://console.aws.amazon.com/macie/).
2. Dengan menggunakan Wilayah AWS pemilih di sudut kanan atas halaman, pilih Wilayah tempat Anda ingin mengirim undangan.
3. Di panel navigasi, di bagian Pengaturan, pilih Akun.
4. Di tabel Akun, pilih kotak centang untuk setiap akun yang ingin Anda kirim undangan.

### Tip

Untuk lebih mudah mengidentifikasi akun yang Anda tambahkan dan belum mengirim undangan, Anda dapat memfilter tabel. Untuk melakukan ini, letakkan kursor Anda di kotak filter di atas tabel, lalu pilih Status. Kemudian pilih Status = Dibuat.

5. Pada menu Tindakan, pilih Undang.
6. (Opsional) Di kotak Pesan, masukkan teks kustom apa pun yang ingin Anda sertakan dalam pesan email yang berisi undangan. Teks dapat berisi sebanyak 80 karakter alfanumerik.
7. Pilih Undang.

Untuk mengirim undangan tambahan Wilayah AWS, ulangi langkah-langkah sebelumnya di setiap Wilayah tambahan.

Setelah Anda mengirim undangan, status akun penerima berubah menjadi verifikasi Email yang sedang berlangsung di inventaris akun Anda. Jika Macie dapat memverifikasi alamat email akun, status akun kemudian berubah menjadi Diundang. Jika Macie tidak dapat memverifikasi alamat, perubahan status akun ke verifikasi Email gagal. Jika ini terjadi, bekerjalah dengan pemilik akun untuk mendapatkan alamat email yang benar. Kemudian [hapus asosiasi antar akun Anda](#), [tambahkan akun](#) lagi, dan kirim undangan lagi.

Saat penerima menerima undangan, status akun penerima berubah menjadi Diaktifkan di inventaris akun Anda. Jika penerima menolak undangan, akun penerima dipisahkan dari akun Anda dan dihapus dari inventaris akun Anda.

## API

Untuk mengirim undangan secara terprogram, gunakan [CreateInvitations](#) pengoperasian Amazon Macie API. Ketika Anda mengirimkan permintaan Anda, gunakan parameter yang didukung untuk menentukan 12 digit ID akun untuk masing-masing Akun AWS untuk mengirim undangan. ID akun harus sesuai dengan ID akun untuk akun di inventaris akun Anda. Jika tidak, muncul kesalahan. Juga tentukan Wilayah untuk mengirim undangan dari. Untuk mengirim undangan dari Wilayah tambahan, kirimkan permintaan di setiap Wilayah tambahan.

Dalam permintaan Anda, Anda juga dapat menentukan apakah akan mengirim undangan sebagai pesan email, dan apakah akan menyertakan teks khusus dalam pesan itu. Jika Anda memilih untuk mengirim pesan email, Macie mengirimkan undangan ke alamat email yang Anda tentukan untuk akun saat Anda menambahkan akun ke inventaris akun Anda. Untuk mengirim undangan sebagai pesan email, hilangkan `disableEmailNotification` parameter atau atur nilai untuk `false` parameter tersebut. (Nilai default adalah `false`.) Untuk menambahkan teks kustom ke pesan, gunakan `message` parameter untuk menentukan teks yang akan ditambahkan. Teks dapat berisi sebanyak 80 karakter alfanumerik.

Untuk mengirim undangan dengan menggunakan, jalankan perintah AWS CLI [create-invitations](#). Gunakan `region` parameter untuk menentukan Wilayah untuk mengirim undangan dari. Gunakan `account-ids` parameter untuk menentukan ID akun untuk masing-masing Akun AWS untuk mengirim undangan ke. Misalnya:

```
C:\> aws macie2 create-invitations --region us-east-1 --account-ids=["111111111111\", \"222222222222\", \"333333333333\"]
```

Di mana *us-east-1* adalah Wilayah untuk mengirim undangan dari (Wilayah AS Timur (Virginia N.)) dan `account-ids` parameter menentukan ID akun untuk tiga akun untuk mengirim undangan. Untuk mengirim undangan sebagai pesan email juga, sertakan juga `no-disable-email-notification` parameter dan secara opsional sertakan `message` parameter untuk menentukan teks khusus yang akan ditambahkan ke pesan.

Setelah Anda mengirim undangan, status setiap akun penerima berubah menjadi `EmailVerificationInProgress`. Jika Macie dapat memverifikasi alamat email akun, status akun kemudian berubah menjadi `Invited`. Jika Macie tidak dapat memverifikasi alamat, status akun akan berubah menjadi `EmailVerificationFailed`. Jika ini terjadi, bekerjalah dengan pemilik akun untuk mendapatkan alamat yang benar. Kemudian [hapus asosiasi antar akun Anda](#), [tambahkan akun](#) lagi, dan kirim undangan lagi.

Ketika penerima menerima undangan, status akun penerima berubah menjadi inventaris akun Anda. `Enabled` Jika penerima menolak undangan, akun penerima dipisahkan dari akun Anda dan dihapus dari inventaris akun Anda.

## Menangguhkan Amazon Macie untuk akun anggota di organisasi berbasis undangan

Sebagai administrator Macie untuk organisasi, Anda dapat menangguhkan Macie secara spesifik Wilayah AWS untuk akun anggota individu di organisasi Anda. Namun, perhatikan bahwa Anda tidak dapat mengaktifkan kembali Macie untuk akun anggota setelah Anda menangguhkannya. Hanya pengguna akun yang selanjutnya dapat mengaktifkan kembali Macie untuk akun tersebut.

Saat Anda menangguhkan Macie untuk akun anggota:

- Macie kehilangan akses ke dan berhenti memberikan metadata tentang data Amazon S3 akun di Wilayah.
- Macie berhenti melakukan semua aktivitas untuk akun di Wilayah. Ini termasuk memantau bucket S3 untuk keamanan dan kontrol akses, melakukan penemuan data sensitif otomatis, dan menjalankan pekerjaan penemuan data sensitif yang saat ini sedang berlangsung.
- Macie membatalkan semua pekerjaan penemuan data sensitif yang dibuat oleh akun di Wilayah. Pekerjaan tidak dapat dilanjutkan atau dimulai kembali setelah dibatalkan.

Jika Anda membuat lowongan untuk menganalisis data yang dimiliki akun anggota, Macie tidak membatalkan lowongan tersebut. Sebaliknya, pekerjaan melewati sumber daya yang dimiliki oleh akun.

Saat akun ditangguhkan, Macie mempertahankan pengenalan sesi Macie, pengaturan, dan sumber daya untuk akun di Wilayah yang berlaku. Misalnya, temuan akun tetap utuh dan tidak terpengaruh hingga 90 hari. Akun tidak dikenakan biaya untuk menggunakan Macie di Wilayah yang berlaku sementara Macie ditangguhkan untuk akun di Wilayah tersebut.

Untuk menangguhkan Macie untuk akun anggota di organisasi berbasis undangan

Untuk menangguhkan Macie untuk akun anggota di organisasi berbasis undangan, Anda dapat menggunakan konsol Amazon Macie atau Amazon Macie API.

### Console

Ikuti langkah-langkah berikut untuk menangguhkan Macie untuk akun anggota dengan menggunakan konsol Amazon Macie.

Untuk menanggihkan Macie untuk akun anggota

1. [Buka konsol Amazon Macie di https://console.aws.amazon.com/macie/](https://console.aws.amazon.com/macie/).
2. Dengan menggunakan Wilayah AWS pemilih di sudut kanan atas halaman, pilih Wilayah tempat Anda ingin menanggihkan Macie untuk akun anggota.
3. Di panel navigasi, di bagian Pengaturan, pilih Akun.
4. Di tabel Akun, pilih kotak centang agar akun ditanggihkan.
5. Pada menu Tindakan, pilih Tangguhkan Macie.
6. Konfirmasikan bahwa Anda ingin menanggihkan Macie untuk akun yang dipilih.

Setelah Anda mengonfirmasi penanggihan, status akun berubah menjadi Dijeda (ditanggihkan) di inventaris akun Anda.

Ulangi langkah sebelumnya di setiap Wilayah tambahan di mana Anda ingin menanggihkan Macie untuk akun tersebut.

## API

Untuk menanggihkan Macie untuk akun anggota secara terprogram, gunakan [UpdateMemberSession](#) pengoperasian Amazon Macie API. Saat Anda mengirimkan permintaan, gunakan `id` parameter untuk menentukan 12 digit ID akun AWS yang ingin Anda tangguhkan Macie. Untuk `status` parameter, tentukan `PAUSED` sebagai status baru untuk akun Macie. Tentukan juga Wilayah tempat permintaan tersebut berlaku. Untuk menanggihkan Macie di Wilayah tambahan, kirimkan permintaan Anda di setiap Wilayah tambahan.

Untuk mengambil ID akun untuk akun anggota, Anda dapat menggunakan [ListMembers](#) pengoperasian Amazon Macie API. Jika Anda melakukan ini, pertimbangkan untuk memfilter hasil dengan memasukkan `onlyAssociated` parameter dalam permintaan Anda. Jika Anda menyetel nilai parameter `init` ke `true`, Macie mengembalikan `members` larik yang memberikan detail hanya tentang akun yang saat ini menjadi akun anggota untuk akun administrator Anda.

Untuk menanggihkan Macie untuk akun anggota dengan menggunakan AWS CLI, jalankan perintah. [update-member-session](#) Gunakan `region` parameter untuk menentukan Wilayah di mana untuk menanggihkan Macie dan menggunakan `id` parameter untuk menentukan ID akun untuk akun untuk menanggihkan Macie untuk. Untuk `status` parameter, tentukan `PAUSED`.

Misalnya:

```
C:\> aws macie2 update-member-session --region us-east-1 --id 123456789012 --status PAUSED
```

Di mana *us-east-1* adalah Wilayah untuk menanggihkan Macie (Wilayah AS Timur (Virginia N.)), *123456789012* adalah ID akun untuk akun untuk menanggihkan Macie, dan merupakan status baru Macie untuk akun tersebut. PAUSED

Jika permintaan Anda berhasil, Macie mengembalikan respons kosong dan status akun yang ditentukan berubah Paused dalam inventaris akun Anda.

## Menghapus akun anggota Amazon Macie dari organisasi berbasis undangan

Sebagai administrator Macie, Anda dapat menghapus akun anggota dari organisasi Anda. Anda melakukan ini dengan memisahkan akun dari akun administrator Macie Anda.

Jika Anda menghapus akun anggota, Macie terus diaktifkan untuk akun tersebut dan akun tersebut terus muncul di inventaris akun Anda. Namun, akun tersebut menjadi akun Macie mandiri. Macie tidak memberi tahu pemilik akun saat Anda menghapus akun. Oleh karena itu, pertimbangkan untuk menghubungi pemilik akun untuk memastikan bahwa mereka mulai mengelola pengaturan dan sumber daya untuk akun mereka.

Ketika Anda menghapus akun anggota, Anda kehilangan akses ke semua pengaturan Macie, sumber daya, dan data untuk akun tersebut. Ini termasuk temuan kebijakan dan metadata untuk bucket S3 yang dimiliki akun. Selain itu, Anda tidak dapat lagi menggunakan Macie untuk menemukan data sensitif di bucket S3 yang dimiliki akun tersebut. Jika Anda telah membuat pekerjaan penemuan data sensitif untuk melakukan ini, pekerjaan akan melewati bucket yang dimiliki akun tersebut.

Setelah Anda menghapus akun anggota, Anda selanjutnya dapat menambahkannya ke organisasi Anda lagi dengan mengirimkan undangan baru ke akun tersebut. Anda juga dapat menghapusnya dari inventaris akun Anda sepenuhnya dengan menghapus asosiasi antar akun Anda.

### Untuk menghapus akun anggota dari organisasi berbasis undangan

Untuk menghapus akun anggota dari organisasi, Anda dapat menggunakan konsol Amazon Macie atau Amazon Macie API.

#### Console

Ikuti langkah-langkah berikut untuk menghapus akun anggota dengan menggunakan konsol Amazon Macie.

Untuk menghapus akun anggota

1. [Buka konsol Amazon Macie di https://console.aws.amazon.com/macie/](https://console.aws.amazon.com/macie/).
2. Dengan menggunakan Wilayah AWS pemilih di sudut kanan atas halaman, pilih Wilayah tempat Anda ingin menghapus akun anggota.
3. Di panel navigasi, di bagian Pengaturan, pilih Akun.
4. Dalam tabel Akun, pilih kotak centang untuk menghapus akun.
5. Pada menu Tindakan, pilih Disassociate account.
6. Konfirmasikan bahwa Anda ingin menghapus akun yang dipilih sebagai akun anggota.

Setelah Anda mengonfirmasi pilihan Anda, status akun berubah menjadi Dihapus (terputus) di inventaris akun Anda.

Ulangi langkah sebelumnya di setiap Wilayah tambahan di mana Anda ingin menghapus akun anggota.

## API

Untuk menghapus akun anggota secara terprogram, gunakan [DisassociateMember](#) pengoperasian Amazon Macie API. Saat Anda mengirimkan permintaan, gunakan `id` parameter untuk menentukan Akun AWS ID 12 digit untuk dihapus oleh akun anggota. Tentukan juga Wilayah tempat permintaan tersebut berlaku. Untuk menghapus akun di Wilayah tambahan, kirimkan permintaan Anda di setiap Wilayah tambahan.

Untuk mengambil ID akun untuk menghapus akun, Anda dapat menggunakan [ListMembers](#) pengoperasian Amazon Macie API. Jika Anda melakukan ini, pertimbangkan untuk memfilter hasil dengan memasukkan `onlyAssociated` parameter dalam permintaan Anda. Jika Anda menetapkan nilai parameter `initrue`, Macie mengembalikan `members` larik yang memberikan detail hanya tentang akun yang saat ini menjadi akun anggota untuk akun Anda.

Untuk menghapus akun anggota dengan menggunakan AWS CLI, jalankan perintah [disassociate-member](#). Gunakan `region` parameter untuk menentukan wilayah tempat menghapus akun. Gunakan `id` parameter untuk menentukan ID akun untuk menghapus akun. Misalnya:

```
C:\> aws macie2 disassociate-member --region us-east-1 --id 123456789012
```

Dimana **us-east-1** adalah Wilayah untuk menghapus akun (Wilayah AS Timur (Virginia N.)) dan **123456789012** adalah ID akun untuk menghapus akun tersebut.

Jika permintaan Anda berhasil, Macie mengembalikan respons kosong dan status akun yang ditentukan berubah Removed dalam inventaris akun Anda.

## Menghapus asosiasi dengan akun lain

Setelah menambahkan akun ke inventaris akun, Anda dapat menghapus hubungan antara akun Anda dan akun lainnya. Anda dapat melakukan ini untuk akun apa pun di inventaris Anda kecuali:

- Akun yang merupakan bagian dari organisasi Anda AWS Organizations. Jenis asosiasi ini dikendalikan melalui AWS Organizations bukan Macie.
- Akun anggota yang menerima undangan keanggotaan Macie untuk bergabung dengan organisasi Anda. Jika ini masalahnya, Anda harus [menghapus akun anggota](#) sebelum Anda dapat menghapus asosiasi.

Saat Anda menghapus asosiasi, Macie menghapus akun dari inventaris akun Anda. Jika Anda kemudian ingin memulihkan asosiasi, Anda harus menambahkan akun lagi seolah-olah itu adalah akun yang sama sekali baru.

Untuk menghapus asosiasi dengan akun lain

Untuk menghapus asosiasi antara akun Anda dan akun lain, Anda dapat menggunakan konsol Amazon Macie atau Amazon Macie API.

### Console

Untuk menggunakan konsol Amazon Macie untuk menghapus asosiasi dengan akun lain, ikuti langkah-langkah ini.

Untuk menghapus asosiasi

1. [Buka konsol Amazon Macie di https://console.aws.amazon.com/macie/](https://console.aws.amazon.com/macie/).
2. Dengan menggunakan Wilayah AWS pemilih di sudut kanan atas halaman, pilih Wilayah tempat Anda ingin menghapus asosiasi.
3. Di panel navigasi, di bagian Pengaturan, pilih Akun.
4. Di tabel Akun, pilih kotak centang untuk akun yang asosiasinya ingin Anda hapus.
5. Pada menu Tindakan, pilih Hapus akun.
6. Konfirmasikan bahwa Anda ingin menghapus asosiasi yang dipilih.

Ulangi langkah sebelumnya di setiap Wilayah tambahan di mana Anda ingin menghapus asosiasi API

Untuk menghapus asosiasi dengan akun lain secara terprogram, gunakan [DeleteMember](#) pengoperasian Amazon Macie API. Saat Anda mengirimkan permintaan Anda, gunakan `id` parameter untuk menentukan ID akun 12 digit Akun AWS untuk menghapus asosiasi dengan. Tentukan juga Wilayah tempat permintaan tersebut berlaku. Untuk menghapus asosiasi di Wilayah tambahan, kirimkan permintaan Anda di setiap Wilayah tambahan.

Untuk mengambil ID akun akun, Anda dapat menggunakan [ListMembers](#) pengoperasian Amazon Macie API. Jika Anda melakukan ini, sertakan `onlyAssociated` parameter dalam permintaan Anda dan atur nilai parameter ke `false`. Jika operasi berhasil, Macie mengembalikan `members` array yang memberikan rincian tentang semua akun yang terkait dengan akun Anda, termasuk akun yang saat ini bukan akun anggota.

Untuk menghapus asosiasi dengan akun lain dengan menggunakan AWS CLI, jalankan perintah [delete-member](#). Gunakan `region` parameter untuk menentukan Wilayah di mana untuk menghapus asosiasi dan `id` parameter untuk menentukan ID akun untuk akun. Misalnya:

```
C:\> aws macie2 delete-member --region us-east-1 --id 123456789012
```

Dimana *us-east-1* adalah Wilayah di mana untuk menghapus asosiasi dengan akun lain (Wilayah AS Timur (Virginia N.)) dan *123456789012* adalah ID akun untuk akun tersebut.

Jika permintaan Anda berhasil, Macie mengembalikan respons kosong dan hubungan antara akun Anda dan akun lainnya dihapus. Akun yang terkait sebelumnya dihapus dari inventaris akun Anda.

## Meninjau akun Amazon Macie untuk organisasi berbasis undangan

Untuk membantu Anda mengelola akun di organisasi Anda, Amazon Macie menyediakan inventaris akun yang terkait dengan akun Macie Anda di setiap Wilayah AWS tempat Anda menggunakan Macie. Dengan menggunakan inventaris ini, Anda dapat memeriksa status akun individual dan meninjau statistik dan detail akun untuk organisasi Anda. Anda juga dapat mengelola status hubungan antara akun Anda dan akun individual.

Untuk meninjau akun untuk organisasi berbasis undangan



Untuk meninjau akun di organisasi, Anda dapat menggunakan konsol Amazon Macie atau Amazon Macie API.

## Console

Ikuti langkah-langkah berikut untuk meninjau akun organisasi Anda menggunakan konsol Amazon Macie.

Untuk meninjau akun organisasi Anda

1. [Buka konsol Amazon Macie di https://console.aws.amazon.com/macie/](https://console.aws.amazon.com/macie/).
2. Dengan menggunakan Wilayah AWS pemilih di sudut kanan atas halaman, pilih Wilayah tempat Anda ingin meninjau akun organisasi.
3. Di panel navigasi, di bagian Pengaturan, pilih Akun.

Halaman Akun membuka dan menampilkan statistik agregat dan tabel akun yang terkait dengan akun Macie Anda saat ini. Wilayah AWS

Di bagian atas halaman Akun, Anda akan menemukan statistik agregat berikut.

### Melalui AWS Organizations

Jika Anda administrator Macie untuk organisasi diAWS Organizations, Active melaporkan jumlah total akun yang terkait dengan akun Anda AWS Organizations dan saat ini merupakan akun anggota Macie di organisasi Anda. Macie diaktifkan untuk akun ini dan Anda adalah administrator akun Macie.

Semua melaporkan jumlah total akun yang terkait dengan akun AndaAWS Organizations, termasuk akun yang saat ini bukan akun anggota Macie.

### Dengan undangan

Aktif melaporkan jumlah total akun yang saat ini merupakan akun anggota Macie di organisasi berbasis undangan Anda. Macie diaktifkan untuk akun ini dan Anda adalah administrator akun Macie karena mereka menerima undangan keanggotaan dari Anda.

Semua melaporkan jumlah total akun yang terkait dengan akun Anda oleh undangan Macie, termasuk akun yang belum menanggapi undangan dari Anda.

## Aktif/Semua

Aktif melaporkan jumlah total akun yang saat ini merupakan akun anggota Macie untuk akun Anda, baik melalui AWS Organizations atau melalui undangan. Macie diaktifkan untuk akun ini dan Anda adalah administrator akun Macie.

Semua melaporkan jumlah total akun yang terkait dengan akun Anda, baik melalui AWS Organizations atau melalui undangan. Ini termasuk akun yang belum menerima undangan keanggotaan Macie dari Anda. Ini juga termasuk akun yang terkait dengan akun Anda melalui AWS Organizations dan saat ini bukan akun anggota Macie.

Dalam tabel, Anda akan menemukan detail tentang setiap akun di Wilayah saat ini. Tabel ini mencakup semua akun yang terkait dengan akun Macie Anda, baik dengan undangan Macie atau melalui AWS Organizations

### ID Akun

ID akun dan alamat email untuk Akun AWS.

### Nama

Nama akun untuk Akun AWS. Nilai ini biasanya N/A untuk akun yang terkait dengan akun Anda melalui undangan.

### Jenis

Bagaimana akun dikaitkan dengan akun Anda, melalui undangan atau melalui AWS Organizations.

### Status

Status hubungan antara akun Anda dan akun. Untuk akun di organisasi berbasis undangan (Type is By Invitation), nilai yang mungkin adalah:

- Akun ditangguhkan — Akun AWS Ditangguhkan.
- Dibuat (Undangan) - Anda menambahkan akun tetapi belum mengirim undangan keanggotaan ke dalamnya.
- Verifikasi email gagal — Anda mencoba mengirim undangan keanggotaan ke akun tetapi alamat email yang ditentukan tidak valid untuk akun tersebut.
- Verifikasi email sedang berlangsung — Anda mengirim undangan keanggotaan ke akun dan Macie sedang memproses permintaan tersebut.

- Diaktifkan — Akun adalah akun anggota. Macie diaktifkan untuk akun dan Anda adalah administrator akun Macie.
- Diundang - Anda mengirim undangan keanggotaan ke akun dan akun belum menanggapi undangan Anda.
- Anggota mengundurkan diri — Akun tersebut sebelumnya merupakan akun anggota. Namun, akun tersebut mengundurkan diri dari organisasi Anda dengan melepaskan diri dari akun Anda.
- Dijeda (ditangguhkan) — Akun tersebut adalah akun anggota tetapi Macie saat ini ditangguhkan untuk akun tersebut.
- Wilayah dinonaktifkan - Wilayah saat ini dinonaktifkan untuk Akun AWS.
- Dihapus (dipisahkan) - Akun sebelumnya adalah akun anggota. Namun, Anda menghapusnya sebagai akun anggota dengan memutuskannya dari akun Anda.

### Tindakan terakhir

Saat Anda atau akun terkait baru-baru ini melakukan tindakan yang memengaruhi hubungan antar akun Anda.

Untuk mengurutkan tabel berdasarkan bidang tertentu, klik judul kolom untuk bidang. Untuk mengubah urutan pengurutan, klik judul kolom lagi. Untuk memfilter tabel, letakkan kursor Anda di kotak filter, lalu tambahkan kondisi filter untuk bidang. Untuk lebih menyempurnakan hasilnya, tambahkan syarat filter untuk bidang tambahan.

### API

Untuk meninjau akun organisasi Anda secara terprogram, gunakan [ListMembers](#) pengoperasian Amazon Macie API dan pastikan untuk menentukan Wilayah tempat permintaan Anda berlaku. Untuk meninjau detail di Wilayah tambahan, kirimkan permintaan Anda di setiap Wilayah tambahan.

Saat Anda mengirimkan permintaan, gunakan `onlyAssociated` parameter untuk menentukan akun mana yang akan disertakan dalam respons. Secara default, Macie mengembalikan rincian tentang hanya akun yang merupakan akun anggota di Wilayah tertentu, baik melalui undangan atau melalui AWS Organizations. Untuk mengambil detail semua akun terkait, termasuk akun yang bukan akun anggota, sertakan `onlyAssociated` parameter dalam permintaan Anda dan tetapkan nilai parameter ke `false`.

Untuk meninjau akun organisasi Anda menggunakan [AWS Command Line Interface \(AWS CLI\)](#), jalankan perintah [list-member](#). Untuk `only-associated` parameter, tentukan apakah akan

menyertakan semua akun terkait atau hanya akun anggota. Untuk menyertakan hanya akun anggota, hilangkan parameter ini atau atur nilai parameter ke `true`. Untuk menyertakan semua akun, tetapkan nilai ini ke `false`. Misalnya:

```
C:\> aws macie2 list-members --region us-east-1 --only-associated false
```

Di mana *us-timur-1* adalah Wilayah tempat permintaan tersebut berlaku, Wilayah AS Timur (Virginia N.).

Jika permintaan Anda berhasil, Macie mengembalikan array. `members` Array berisi `member` objek untuk setiap akun yang memenuhi kriteria yang ditentukan dalam permintaan. Dalam objek itu, `relationshipStatus` bidang menunjukkan status asosiasi saat ini antara akun Anda dan akun lain di Wilayah yang ditentukan. Untuk akun dalam organisasi berbasis undangan, nilai yang mungkin adalah:

- `AccountSuspended`— Akun AWS Ditangguhkan.
- `Created`— Anda menambahkan akun tetapi belum mengirim undangan keanggotaan untuk itu.
- `EmailVerificationFailed`— Anda mencoba mengirim undangan keanggotaan ke akun tetapi alamat email yang ditentukan tidak berlaku untuk akun tersebut.
- `EmailVerificationInProgress`— Anda mengirim undangan keanggotaan ke akun dan Macie sedang memproses permintaan tersebut.
- `Enabled`— Akun tersebut adalah akun anggota. Macie diaktifkan untuk akun dan Anda adalah administrator akun Macie.
- `Invited`— Anda mengirim undangan keanggotaan ke akun dan akun belum menanggapi undangan Anda.
- `Paused`— Akun tersebut adalah akun anggota tetapi Macie saat ini ditangguhkan (dijeda) untuk akun tersebut.
- `RegionDisabled`— Wilayah saat ini dinonaktifkan untuk Akun AWS.
- `Removed`— Akun tersebut sebelumnya merupakan akun anggota. Namun, Anda menghapusnya sebagai akun anggota dengan memutuskannya dari akun Anda.
- `Resigned`— Akun tersebut sebelumnya merupakan akun anggota. Namun, akun tersebut mengundurkan diri dari organisasi Anda dengan melepaskan diri dari akun Anda.

Untuk informasi tentang bidang lain di `member` objek, lihat [Anggota di Referensi](#) API Amazon Macie.

## Menunjuk akun administrator Amazon Macie yang berbeda untuk organisasi berbasis undangan

Setelah membuat dan membuat organisasi berbasis undangan, Anda dapat mengubah akun administrator Amazon Macie untuk organisasi tersebut. Untuk melakukan ini, administrator dan anggota organisasi harus mengambil langkah-langkah berikut:

1. Administrator Macie saat ini secara opsional mengeksport inventaris akun anggota aktif saat ini untuk organisasi. Ini menyederhanakan transisi dengan membantu Anda mengidentifikasi akun anggota yang harus terus menjadi bagian dari organisasi.
2. Administrator Macie saat ini [menghapus semua akun anggota](#) dari organisasi saat ini. Ini memisahkan akun dari akun administrator saat ini tetapi Macie terus diaktifkan untuk akun tersebut.
3. Administrator Macie baru [menambahkan akun anggota sebelumnya](#) ke organisasi baru. Ini mengaitkan akun dengan akun administrator baru.
4. Setiap akun anggota menerima undangan untuk bergabung dengan organisasi baru. Ketika akun menerima undangan, akun tersebut menjadi akun anggota aktif di organisasi baru. Administrator Macie baru kemudian dapat mengakses pengaturan Macie, data, dan sumber daya untuk akun tersebut.

Jika organisasi Anda menggunakan Macie dalam beberapa kali Wilayah AWS, lakukan langkah-langkah sebelumnya di setiap Wilayah tersebut.

Untuk mengeksport inventaris akun anggota aktif saat ini, administrator Macie saat ini dapat menggunakan konsol Amazon Macie atau Amazon Macie API. Dengan konsol, administrator saat ini dapat mengeksport data ke file nilai yang dipisahkan koma (CSV). Administrator baru kemudian dapat menggunakan konsol untuk mengunggah file CSV dan menambahkan semua akun (secara massal) ke organisasi baru.

Untuk mengeksport data akun anggota dengan menggunakan konsol

1. Masuk ke AWS Management Console menggunakan akun administrator Macie saat ini.
2. Dengan menggunakan Wilayah AWS pemilih di sudut kanan atas halaman, pilih Wilayah tempat Anda ingin mengeksport data.
3. [Buka konsol Amazon Macie di https://console.aws.amazon.com/macie/](https://console.aws.amazon.com/macie/).
4. Di panel navigasi, di bagian Pengaturan, pilih Akun.

5. (Opsional) Untuk memfilter tabel Akun dan hanya menampilkan akun yang saat ini merupakan akun anggota Macie aktif di organisasi, gunakan kotak filter di atas tabel untuk menambahkan kondisi filter berikut:
  - Jenis = Undangan
  - Status = Diaktifkan
6. Dalam tabel Akun, pilih kotak centang untuk setiap akun anggota aktif untuk disertakan dalam data yang diekspor.
7. Pilih Ekspor CSV.
8. Tentukan nama dan lokasi untuk file tersebut.

Dengan Amazon Macie API, administrator Macie saat ini dapat mengambil data dalam format JSON. Administrator Macie baru kemudian dapat menggunakan data tersebut untuk menghasilkan daftar ID akun dan alamat email untuk akun untuk ditambahkan dan diundang ke organisasi baru. Untuk mengambil data dalam format JSON, gunakan [ListMembers](#) pengoperasian Amazon Macie API. Jika operasi berhasil, Macie mengembalikan `members` array yang memberikan rincian tentang semua akun yang terkait dengan akun administrator. Jika akun adalah akun anggota Macie yang aktif di organisasi berbasis undangan saat ini, nilai untuk `relationshipStatus` properti akun tersebut adalah `Enabled` dan `invitedAt` properti menentukan tanggal dan waktu.

## Mengelola keanggotaan Anda dalam organisasi berbasis undangan di Amazon Macie

Jika Anda diundang untuk bergabung dengan organisasi di Amazon Macie, Anda dapat menerima atau menolak undangan secara opsional. Di Macie, organisasi adalah sekumpulan akun yang dikelola secara terpusat sebagai sekelompok akun terkait. Sebuah organisasi terdiri dari satu akun administrator Macie yang ditunjuk dan satu atau lebih akun anggota terkait.

Jika Anda menerima undangan, akun Anda menjadi akun anggota di organisasi. Ketika Anda menerima, akun yang mengirim undangan menjadi akun administrator Macie untuk akun Anda—Anda mengaitkan akun Anda dengan akun lain dan Anda mengaktifkan hubungan administrator-anggota antar akun. Akun administrator Macie kemudian dapat mengakses pengaturan, data, dan sumber daya Macie tertentu untuk akun Anda dalam hal yang berlaku Wilayah AWS. Untuk informasi selengkapnya, lihat [Memahami hubungan antara administrator Amazon Macie dan akun anggota](#).

Jika Anda menolak undangan, status dan pengaturan saat ini untuk akun Macie Anda tidak berubah.

## Topik

- [Menanggapi undangan keanggotaan untuk organisasi](#)
- [Berpisah dari akun administrator Amazon Macie](#)

## Menanggapi undangan keanggotaan untuk organisasi

Saat Anda menerima undangan untuk bergabung dengan organisasi, Amazon Macie memberi tahu Anda dengan beberapa cara. Secara default, Macie mengirimkan undangan kepada Anda sebagai pesan email. Macie juga menciptakan AWS Healthcara untuk AndaAkun AWS. Jika Anda sudah menggunakan Macie diWilayah AWSdari mana undangan dikirim, Macie juga menampilkanAkunlencana dan pemberitahuan pada konsol Macie.

Setelah menerima undangan, Anda dapat menerima atau menolak undangan secara opsional. Sebelum Anda merespons, perhatikan hal berikut:

- Anda dapat menjadi anggota hanya satu organisasi dalam satu waktu. Jika Anda menerima beberapa undangan, Anda hanya dapat menerima satu undangan. Atau, jika Anda sudah menjadi anggota organisasi, Anda harus memisahkan akun Anda dari akun administrator Macie saat ini sebelum dapat bergabung dengan organisasi lain.
- Jika Anda menggunakan Macie di beberapa Wilayah, akun Anda harus memiliki akun administrator Macie yang sama di semua Wilayah tersebut. Administrator Macie harus mengirim undangan kepada Anda secara terpisah dari masing-masing Wilayah, dan Anda harus menerima undangan secara terpisah di setiap Wilayah.
- Untuk menerima atau menolak undangan, Anda harus mengaktifkan Macie di Wilayah tempat undangan dikirim. Menolak undangan adalah opsional. Jika Anda mengaktifkan Macie untuk menolak undangan, Anda bisa[menonaktifkan Macie](#)di Wilayah setelah Anda menolak undangan. Ini membantu memastikan bahwa Anda tidak dikenakan biaya yang tidak perlu untuk menggunakan Macie di Wilayah.

Untuk pertimbangan tambahan, lihat[Menanggapi dan mengelola undangan keanggotaan](#).

Untuk menanggapi undangan keanggotaan untuk organisasi

Untuk menanggapi undangan keanggotaan, Anda dapat menggunakan konsol Amazon Macie atau Amazon Macie API.

## Console

Ikuti langkah-langkah berikut untuk menanggapi undangan keanggotaan dengan menggunakan konsol Amazon Macie.

Untuk menanggapi undangan keanggotaan

1. Buka konsol Amazon Macie di <https://console.aws.amazon.com/macie/>.
2. Dengan menggunakan Wilayah AWS pilih di sudut kanan atas halaman, pilih Wilayah di mana Anda menerima undangan.
3. Jika Anda belum mengaktifkan Macie di Wilayah, pilih **Memulai**, lalu pilih **Aktifkan Macie**. Anda harus mengaktifkan Macie sebelum Anda dapat menerima atau menolak undangan.
4. Di panel navigasi, di bagian Pengaturan, pilih Akun.
5. Di bawah Akun Administrator, lakukan salah satu dari berikut ini:
  - Untuk menerima undangan, nyalakan **Menerima**  di sebelah undangan. Kemudian pilih **Terima undangan** atau **Memperbarui**, tergantung pada apakah Anda sebelumnya menerima undangan lain.
  - Untuk menolak undangan, pilih **Tolak undangan** di sebelah undangan, dan kemudian konfirmasi bahwa Anda ingin menolak undangan.

Jika Anda menerima dan ingin menanggapi undangan di Wilayah tambahan, ulangi langkah-langkah sebelumnya di setiap Wilayah tambahan.

## API

Untuk menanggapi undangan secara terprogram, gunakan [AcceptInvitation](#) atau [DeclineInvitations](#) pengoperasian Amazon Macie API, tergantung pada apakah Anda ingin menerima atau menolak undangan. Saat Anda mengirimkan permintaan Anda, pastikan untuk menentukan Wilayah tempat undangan dikirim. Untuk menanggapi undangan di Wilayah tambahan, kirimkan permintaan Anda di setiap Wilayah tambahan.

Dalam sebuah `AcceptInvitation` permintaan, gunakan `administratorAccountId` parameter untuk menentukan ID akun 12 digit untuk Akun AWS yang mengirim undangan. Gunakan `invitationId` parameter untuk menentukan ID unik untuk undangan untuk menerima.

Dalam sebuah `DeclineInvitations` permintaan, gunakan `accountId` parameter untuk menentukan ID akun 12 digit untuk Akun AWS yang mengirim undangan untuk menolak.



Untuk mengambil ID, Anda dapat menggunakan [ListInvitations](#) pengoperasian Amazon Macie API. Jika operasi berhasil, Macie mengembalikan `invitationsarray` yang menyediakan detail tentang undangan yang telah Anda terima, termasuk ID akun untuk akun yang mengirim setiap undangan dan ID unik untuk setiap undangan. Jika nilai untuk `relationshipStatus` milik undangan adalah `Invited`, Anda belum menanggapi undangan belum.

Untuk menanggapi undangan dengan menggunakan [AWS Command Line Interface \(AWS CLI\)](#), jalankan [terima-undangan](#) atau [menurunkan-undangan](#) perintah, tergantung pada apakah Anda ingin menerima atau menolak undangan. Gunakan `region` parameter untuk menentukan Wilayah tempat undangan dikirim. Misalnya:

```
C:\> aws macie2 accept-invitation --region us-east-1 --administrator-account-id 123456789012 --invitation-id d8bdad0e203fd1242e0a4721bexample
```

Dimana `kami-timur-1` adalah Wilayah tempat undangan dikirim dari (Wilayah AS Timur (Virginia Utara)), `123456789012` adalah ID akun untuk akun yang mengirim undangan, dan `d8bdad0e203fd1242e0a4721bexample` adalah ID unik untuk undangan untuk menerima.

Jika permintaan untuk menerima undangan berhasil, Macie mengembalikan respons kosong. Jika permintaan untuk menolak undangan berhasil, Macie mengembalikan yang kosong `unprocessedAccountsarray`.

Setelah Anda menolak undangan, undangan tetap ada sebagai sumber untuk akun Macie Anda. Anda dapat menghapusnya secara opsional dengan menggunakan [DeleteInvitations](#) operasi atau, untuk AWS CLI, yang [menghapus-undangan](#) perintah.

## Berpisah dari akun administrator Amazon Macie

Jika Anda menerima undangan untuk bergabung dengan organisasi di Amazon Macie, Anda selanjutnya dapat mengundurkan diri dari organisasi dengan memisahkan akun Anda dari akun administrator Macie saat ini. Perhatikan bahwa Anda tidak dapat melakukan ini jika akun Anda adalah akun anggota di AWS Organizations organisasi. Untuk mengundurkan diri dari AWS Organizations organisasi, bekerja dengan administrator Macie Anda untuk menghapus akun Anda sebagai akun anggota Macie.

Jika Anda memisahkan akun Anda dari akun administrator Macie, administrator Macie kehilangan akses ke semua pengaturan, data, dan sumber daya untuk akun Macie Anda. Ini termasuk metadata dan temuan kebijakan untuk data Amazon S3 yang Anda miliki. Ini juga berarti bahwa administrator

tidak dapat lagi menganalisis data Amazon S3 Anda dengan melakukan penemuan data sensitif otomatis atau menjalankan pekerjaan penemuan data sensitif.

Ketika Anda memisahkan akun Anda, Macie terus diaktifkan untuk akun Anda di Wilayah yang berlaku. Namun, akun Anda menjadi akun Macie mandiri di Wilayah. Status akun Anda berubah menjadi Anggota mengundurkan diri di inventaris akun administrator.


Untuk memisahkan diri dari akun administrator Macie

Untuk memisahkan akun Anda dari akun administrator Macie saat ini, Anda dapat menggunakan konsol Amazon Macie atau Amazon Macie API.

## Console

Ikuti langkah-langkah ini untuk memisahkan akun Anda dari akun administrator Macie dengan menggunakan konsol Amazon Macie.

Untuk memisahkan diri dari akun administrator

1. Buka konsol Amazon Macie di <https://console.aws.amazon.com/macie/>.
2. Dengan menggunakan Wilayah AWS, pilih di sudut kanan atas halaman, pilih Wilayah di mana Anda ingin memisahkan akun Anda dari akun administratornya.
3. Di panel navigasi, di bagian Pengaturan, pilih Akun.
4. Di bawah Akun Administrator, matikan Menerima  di sebelah undangan, lalu pilih Memperbarui.

Akun terus muncul di Akun halaman. Jika Anda memutuskan untuk bergabung kembali ke organisasi, Anda dapat menggunakan halaman ini untuk menerima undangan asli lagi. Atau, Anda dapat menolak dan menghapus undangan, yang juga menghapus hubungan antara akun Anda dan akun lainnya. Untuk melakukan ini, pilih Tolak undangan.

Jika Anda ingin memisahkan akun Anda dari akun administrator Macie di Wilayah tambahan, ulangi langkah-langkah sebelumnya di setiap Wilayah tambahan.

## API

Untuk memisahkan akun Anda dari akun administrator Macie secara terprogram, gunakan [DisassociateFromAdministratorAccount](#) pengoperasian Amazon Macie API. Saat Anda mengirimkan permintaan, pastikan untuk menentukan Wilayah tempat permintaan tersebut

berlaku. Untuk memisahkan diri dari akun di Wilayah tambahan, kirimkan permintaan Anda di setiap Wilayah tambahan.

Untuk memisahkan akun Anda dari akun administrator Macie dengan menggunakan AWS CLI, jalankan [disassociate-from-administrator-account](#) perintah. Gunakan `region` parameter untuk menentukan Wilayah di mana untuk memisahkan diri dari akun.

Jika permintaan Anda berhasil, Macie mengembalikan respons kosong.

Setelah Anda memutuskan hubungan dari akun, undangan asli tetap ada sebagai sumber untuk akun Macie Anda kecuali Anda menghapusnya. Jika Anda memutuskan untuk bergabung kembali ke organisasi, Anda dapat menggunakan sumber daya ini untuk menerima undangan asli lagi. Atau, Anda dapat menghapus undangan dengan menggunakan [DeleteInvitations](#) operasi atau, untuk AWS CLI, yang [menghapus-undangan](#) perintah. Jika Anda menghapus undangan, Anda juga menghapus hubungan antara akun Anda dan akun lainnya.

# Keamanan di Amazon Macie

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

Keamanan adalah tanggung jawab bersama antara AWS dan Anda. Model [tanggung jawab bersama](#) menjelaskan hal ini sebagai keamanan dari cloud dan keamanan dalam cloud:

- Keamanan cloud —AWS bertanggung jawab untuk melindungi infrastruktur yang berjalan Layanan AWS di dalam AWS Cloud. AWS juga menyediakan layanan yang dapat Anda gunakan dengan aman. Auditor pihak ketiga melakukan pengujian dan verifikasi secara berkala terhadap efektivitas keamanan kami sebagai bagian dari [Program Kepatuhan AWS](#). Untuk mempelajari tentang program kepatuhan yang berlaku untuk Amazon Macie, lihat [AWS Layanan dalam Lingkup oleh Program Kepatuhan AWS](#).
- Keamanan di dalam cloud — Tanggung jawab Anda ditentukan menurut Layanan AWS yang Anda gunakan. Anda juga bertanggung jawab atas faktor lain termasuk sensitivitas data Anda, persyaratan perusahaan Anda, serta hukum dan peraturan yang berlaku.

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

## Topik

- [Perlindungan Data di Amazon Macie](#)
- [Identity and Access Management untuk Amazon Macie](#)
- [Pencatatan dan pemantauan di Amazon Macie](#)
- [Validasi Kepatuhan untuk Amazon Macie](#)
- [Ketahanan di Amazon Macie](#)
- [Keamanan infrastruktur di Amazon Macie](#)
- [Amazon Macie dan titik akhir VPC antarmuka \(\) AWS PrivateLink](#)

# Perlindungan Data di Amazon Macie

[Model tanggung jawab bersama](#) AWS diterapkan untuk perlindungan data di Amazon Macie.

Sebagaimana diuraikan dalam model ini, AWS bertanggung jawab untuk memberikan perlindungan terhadap infrastruktur global yang menjalankan semua AWS Cloud. Anda harus bertanggung jawab untuk memelihara kendali terhadap konten yang di-hosting pada infrastruktur ini. Anda juga bertanggung jawab atas tugas konfigurasi dan manajemen keamanan untuk Layanan AWS yang Anda gunakan. Untuk informasi selengkapnya tentang privasi data, lihat [FAQ Privasi Data](#). Untuk informasi tentang perlindungan data di Eropa, silakan lihat postingan blog [Model Tanggung Jawab Bersama AWS dan GDPR](#) di Blog Keamanan AWS.

Untuk tujuan perlindungan data, sebaiknya Anda melindungi kredensial Akun AWS dan menyiapkan AWS IAM Identity Center atau AWS Identity and Access Management (IAM) untuk pengguna individu. Dengan cara seperti itu, setiap pengguna hanya diberi izin yang diperlukan untuk memenuhi tanggung jawab tugas mereka. Kami juga merekomendasikan agar Anda mengamankan data Anda dengan cara-cara berikut:

- Gunakan autentikasi multi-faktor (MFA) pada setiap akun.
- Gunakan SSL/TLS untuk melakukan komunikasi dengan sumber daya AWS. Kami membutuhkan TLS 1.2 dan merekomendasikan TLS 1.3.
- Siapkan API dan log aktivitas pengguna dengan AWS CloudTrail.
- Gunakan solusi enkripsi AWS, bersama dengan semua kontrol keamanan default dalam Layanan AWS.
- Gunakan layanan keamanan terkelola lanjutan seperti Amazon Macie, yang membantu menemukan dan mengamankan data sensitif yang disimpan di Amazon S3.
- Jika Anda memerlukan modul kriptografi tervalidasi FIPS 140-2 ketika mengakses AWS melalui antarmuka baris perintah atau API, gunakan titik akhir FIPS. Untuk informasi selengkapnya tentang titik akhir FIPS yang tersedia, silakan lihat [Standar Pemrosesan Informasi Federal \(FIPS\) 140-2](#).

Sebaiknya Anda tidak memasukkan informasi rahasia atau sensitif, seperti alamat email pelanggan, ke dalam tanda atau bidang teks bebas seperti bidang Nama. Ini termasuk saat Anda bekerja dengan Macie atau lainnya Layanan AWS menggunakan konsol, APIAWS CLI, atau AWS SDK. Data apa pun yang Anda masukkan ke dalam tanda atau bidang teks bebas yang digunakan untuk nama dapat digunakan untuk log penagihan atau diagnostik. Saat Anda memberikan URL ke server eksternal, kami sangat menyarankan jangan menyertakan informasi kredensial di URL untuk memvalidasi permintaan Anda ke server tersebut.

## Enkripsi at rest

Amazon Macie menyimpan data Anda secara aman saat data at rest menggunakan solusi enkripsi AWS. Macie mengenkripsi data, seperti temuan, menggunakan Kunci yang dikelola AWS from AWS Key Management Service (). AWS KMS

Jika Anda menonaktifkan Macie, Macie akan menghapus semua sumber daya yang disimpan atau dipelihara secara permanen, seperti tugas penemuan data sensitif, pengidentifikasi data kustom, dan temuan-temuan.

## Enkripsi dalam transit

Macie mengenkripsi semua data dalam transit antara. Layanan AWS

Amazon Macie menganalisis data dari Amazon S3 dan mengekspor hasil penemuan data sensitif ke bucket S3. Setelah Macie mendapat informasi yang dibutuhkan dari objek S3, objek tersebut akan dibuang.

Macie mengakses Amazon S3 menggunakan VPC endpoint yang didukung oleh AWS PrivateLink. Oleh karena itu, lalu lintas antara Macie dan Amazon S3 tetap berada di jaringan Amazon dan tidak melewati internet publik. Untuk informasi selengkapnya, lihat [AWS PrivateLink](#).

## Identity and Access Management untuk Amazon Macie

(IAM) AWS Identity and Access Management adalah Layanan AWS yang membantu seorang administrator dalam mengendalikan akses ke sumber daya AWS secara aman. Administrator IAM mengontrol siapa yang dapat diautentikasi (masuk) dan diberi wewenang (memiliki izin) untuk menggunakan sumber daya Macie. IAM adalah sebuah layanan Layanan AWS yang dapat Anda gunakan tanpa dikenakan biaya tambahan.

Topik

- [Audiens](#)
- [Mengautentikasi dengan identitas](#)
- [Mengelola kebijakan menggunakan akses](#)
- [Bagaimana Amazon Macie bekerja dengan AWS Identity and Access Management](#)
- [Contoh kebijakan berbasis identitas untuk Amazon Macie](#)

- [Peran tertaut layanan untuk Amazon Macie](#)
- [Kebijakan terkelola AWS untuk Amazon Macie](#)
- [Pemecahan Amazon Macie dan Kesalahan](#)

## Audiens

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

Pengguna layanan — Jika Anda menggunakan layanan Macie untuk melakukan pekerjaan Anda, maka administrator Anda memberi Anda kredensi dan izin yang Anda butuhkan. Saat Anda menggunakan lebih banyak fitur Macie 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 Macie, lihat [Pemecahan Amazon Macie dan Kesalahan](#).

Administrator layanan - Jika Anda bertanggung jawab atas sumber daya Macie di perusahaan Anda, Anda mungkin memiliki akses penuh ke Macie. Tugas Anda adalah menentukan fitur dan sumber daya Macie 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 dasar IAM. Untuk mempelajari lebih lanjut tentang bagaimana perusahaan Anda dapat menggunakan IAM dengan Macie, lihat. [Bagaimana Amazon Macie bekerja dengan AWS Identity and Access Management](#)

Administrator IAM - Jika Anda seorang administrator IAM, Anda mungkin ingin mempelajari detail tentang cara menulis kebijakan untuk mengelola akses ke Macie. Untuk melihat contoh kebijakan berbasis identitas Macie yang dapat Anda gunakan di IAM, lihat. [Contoh kebijakan berbasis identitas untuk Amazon Macie](#)

## Mengautentikasi dengan identitas

Autentikasi merupakan cara Anda untuk masuk ke AWS dengan menggunakan kredensial identitas Anda. Anda harus terautentikasi (masuk ke AWS) sebagai Pengguna root akun AWS, sebagai pengguna IAM, atau dengan mengambil peran IAM.

Anda dapat masuk ke AWS sebagai identitas terfederasi dengan menggunakan kredensial yang disediakan melalui sumber identitas. AWS IAM Identity Center Untuk pengguna (Pusat Identitas

IAM), otentikasi sign-on tunggal perusahaan Anda, dan kredensial Google atau Facebook Anda merupakan contoh identitas terfederasi. Saat Anda masuk sebagai identitas terfederasi, administrator Anda sebelumnya menyiapkan federasi identitas dengan menggunakan peran IAM. Ketika Anda mengakses AWS dengan menggunakan federasi, Anda secara tidak langsung mengambil suatu peran.

Tergantung pada jenis pengguna Anda, Anda dapat masuk ke AWS Management Console atau portal akses AWS. Untuk informasi selengkapnya tentang masuk ke AWS, silakan lihat [Cara masuk ke Akun AWS Anda](#) di Panduan Pengguna AWS Sign-In.

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 kredensial Anda. Jika Anda tidak menggunakan peralatan AWS, maka Anda harus menandatangani sendiri permintaan tersebut. Untuk informasi selengkapnya tentang penggunaan metode yang disarankan untuk menandatangani permintaan sendiri, silakan lihat [Menandatangani permintaan API AWS](#) di Panduan Pengguna IAM.

Terlepas dari metode autentikasi yang Anda gunakan, Anda mungkin juga diminta untuk menyediakan informasi keamanan tambahan. Sebagai contoh, AWS menyarankan supaya Anda menggunakan autentikasi multi-faktor (MFA) untuk meningkatkan keamanan akun Anda. Untuk mempelajari selengkapnya, silakan lihat [Autentikasi multi-faktor](#) di Panduan Pengguna AWS IAM Identity Center dan [Menggunakan autentikasi multi-faktor \(MFA\) di AWS](#) di Panduan Pengguna IAM.

## Pengguna root Akun AWS

Ketika Anda membuat Akun AWS, Anda memulai dengan satu identitas masuk yang memiliki akses ke semua Layanan AWS dan sumber daya di akun tersebut. Identitas ini disebut pengguna root Akun AWS dan diakses dengan cara masuk ke alamat email dan kata sandi yang Anda gunakan untuk membuat akun. Kami sangat menyarankan Anda tidak menggunakan pengguna root untuk tugas sehari-hari. Lindungi kredensial pengguna root Anda dan gunakan kredensial tersebut untuk melakukan tugas yang hanya dapat dilakukan pengguna root. Untuk daftar lengkap tugas yang mengharuskan Anda masuk sebagai pengguna root, silakan lihat [Tugas yang memerlukan kredensial pengguna root](#) di Panduan Pengguna IAM.

## Identitas terfederasi

Praktik terbaiknya berupa, mewajibkan pengguna manusia, termasuk pengguna yang memerlukan akses administrator, untuk menggunakan federasi dengan penyedia identitas untuk mengakses Layanan AWS dengan menggunakan kredensial temporer.



Identitas terfederasi adalah pengguna dari direktori pengguna perusahaan Anda, penyedia identitas web, dikenal sebagai AWS Directory Service, direktori Pusat Identitas, atau pengguna mana pun yang mengakses Layanan AWS dengan menggunakan kredensial yang disediakan melalui sumber identitas. Ketika identitas terfederasi mengakses Akun AWS, identitas tersebut mengambil peran, dan peran memberikan kredensial temporer.

Untuk pengelolaan akses terpusat, kami sarankan Anda menggunakan AWS IAM Identity Center. Anda dapat membuat pengguna dan grup di Pusat Identitas IAM, atau Anda dapat menghubungkan dan menyinkronkan ke sekumpulan pengguna dan grup di sumber identitas Anda sendiri untuk digunakan di semua Akun AWS Anda dan aplikasi Anda. Untuk informasi tentang Pusat Identitas IAM, silakan lihat [Apakah Pusat Identitas IAM itu?](#) di User Guide AWS IAM Identity Center.

## Pengguna dan Grup IAM

[Pengguna IAM](#) adalah identitas dalam Akun AWS Anda yang memiliki izin khusus untuk satu orang atau aplikasi. Apabila memungkinkan, kami menyarankan untuk mengandalkan pada kredensial temporer alih-alih 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, kami menyarankan Anda memutar kunci akses. Untuk informasi selengkapnya, silakan lihat [Memutar kunci akses secara teratur untuk kasus penggunaan yang memerlukan kredensial jangka panjang](#) di Panduan Pengguna IAM.

[Grup IAM](#) adalah identitas yang menerangkan secara spesifik kumpulan pengguna IAM. Anda tidak dapat masuk sebagai kelompok. Anda dapat menggunakan grup untuk menerangkan secara spesifik izin untuk beberapa pengguna sekaligus. Grup membuat izin lebih mudah dikelola untuk sekelompok besar pengguna. Sebagai contoh, Anda dapat memiliki grup yang diberi nama AdminIAM 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 digunakan oleh siapa pun yang membutuhkannya. Pengguna memiliki kredensial jangka panjang permanen, tetapi peran memberikan kredensial temporer. Untuk mempelajari selengkapnya, silakan lihat [Kapan harus membuat pengguna IAM \(alih-alih peran\)](#) di Panduan Pengguna IAM.

## Peran IAM

[Peran IAM](#) merupakan identitas dalam Akun AWS Anda yang memiliki izin khusus. Peran ini mirip dengan pengguna IAM, tetapi tidak terkait dengan orang tertentu. Anda dapat menggunakan peran IAM untuk sementara dalam AWS Management Console dengan [berganti peran](#). Anda dapat

mengambil peran dengan cara memanggil operasi API AWS CLI atau AWS atau menggunakan URL kustom. Untuk informasi selengkapnya tentang cara menggunakan peran, silakan lihat [menggunakan peran IAM](#) di Panduan Pengguna IAM.

IAM role dengan kredensial temporer berguna dalam situasi berikut:

- Akses pengguna gabungan – Untuk menetapkan izin ke sebuah identitas terfederasi, Anda harus membuat sebuah peran dan menentukan izin untuk peran tersebut. Ketika identitas gabungan terfederasi mengautentikasi, identitas tersebut terhubung dengan peran dan diberikan izin yang ditentukan oleh peran. Untuk informasi tentang peran-peran untuk federasi, silakan lihat [Membuat sebuah peran untuk Penyedia Identitas pihak ketiga](#) di Panduan Pengguna IAM. Jika Anda menggunakan Pusat Identitas IAM, Anda mengonfigurasi serangkaian izin. Untuk mengontrol apa yang dapat diakses identitas Anda setelah identitas tersebut diautentikasi, Pusat Identitas IAM mengkorelasikan izin yang diatur ke peran dalam IAM. Untuk informasi tentang rangkaian izin, silakan lihat [Rangkaian izin](#) di Panduan Pengguna AWS IAM Identity Center.
- Izin pengguna IAM sementara – Pengguna atau peran IAM dapat mengambil peran IAM untuk sementara mengambil izin berbeda untuk tugas tertentu.
- Akses lintas akun – Anda dapat menggunakan peran IAM untuk mengizinkan seseorang (pengguna utama tepercaya) di akun berbeda untuk mengakses sumber daya yang ada di akun Anda. Peran adalah cara utama untuk memberikan akses lintas akun. Namun, pada beberapa Layanan AWS, Anda dapat melampirkan kebijakan secara langsung ke sumber daya (alih-alih menggunakan suatu peran sebagai proksi). Untuk mempelajari perbedaan antara kebijakan peran dan kebijakan berbasis sumber daya untuk akses lintas akun, silakan lihat [Bagaimana peran IAM role berbeda dari kebijakan berbasis sumber daya](#) dalam Panduan Pengguna IAM.
- Akses lintas layanan – Sebagian Layanan AWS menggunakan fitur di Layanan AWS lainnya. Sebagai contoh, ketika Anda melakukan panggilan dalam suatu layanan, lazim pada 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 tertaut layanan.
- Sesi akses maju (FAS) – Ketika Anda menggunakan pengguna IAM atau peran IAM untuk melakukan tindakan-tindakan di AWS, Anda akan dianggap sebagai seorang pengguna utama. Ketika Anda menggunakan beberapa layanan, Anda mungkin melakukan sebuah tindakan yang kemudian dilanjutkan oleh tindakan lain pada layanan yang berbeda. FAS menggunakan izin dari pengguna utama untuk memanggil Layanan AWS, yang dikombinasikan dengan Layanan AWS yang diminta untuk membuat pengajuan ke layanan hilir. Permintaan FAS hanya diajukan ketika sebuah layanan menerima pengajuan yang memerlukan interaksi dengan Layanan AWS

lain atau sumber daya lain untuk diselesaikan. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan ketika mengajukan permintaan FAS, silakan lihat [Meneruskan sesi akses](#).

- Peran layanan – Sebuah peran layanan adalah sebuah [peran IAM](#) yang dijalankan oleh suatu layanan untuk melakukan tindakan atas nama Anda. Administrator IAM dapat membuat, memodifikasi, dan menghapus peran layanan dari dalam IAM. Untuk informasi selengkapnya, silakan lihat [Membuat sebuah peran untuk mendelegasikan izin ke Layanan AWS](#) dalam Panduan pengguna IAM.
- Peran tertaut layanan – Peran tertaut layanan adalah tipe peran layanan yang tertaut dengan Layanan AWS. Layanan tersebut dapat menjalankan peran untuk melakukan sebuah tindakan atas nama Anda. Peran tertaut layanan akan muncul di Akun AWS Anda dan dimiliki oleh layanan tersebut. Administrator IAM dapat melihat, tetapi tidak dapat mengedit izin untuk peran tertaut layanan.
- Aplikasi yang berjalan di Amazon EC2 – Anda dapat menggunakan peran IAM untuk mengelola kredensial temporer untuk aplikasi yang berjalan di instans EC2 dan mengajukan permintaan AWS CLI atau API AWS. Cara ini lebih baik daripada menyimpan kunci akses dalam instans EC2. Untuk menugaskan sebuah peran AWS ke instans EC2 dan membuatnya tersedia untuk semua aplikasinya, Anda dapat membuat sebuah profil instans yang dilampirkan ke instans. Profil instans berisi peran dan memungkinkan program yang berjalan di instans EC2 untuk mendapatkan kredensial sementara. Untuk informasi selengkapnya, silakan lihat [Menggunakan peran IAM untuk memberikan izin ke aplikasi yang berjalan di instans Amazon EC2](#) di Panduan Pengguna IAM.

Untuk mempelajari apakah kita harus menggunakan peran IAM atau pengguna IAM, silakan lihat [Kapan harus membuat peran IAM \(alih-alih pengguna\)](#) di Panduan Pengguna IAM.

## Mengelola kebijakan menggunakan akses

Anda mengendalikan akses di AWS dengan membuat kebijakan dan melampirkannya ke identitas atau sumber daya AWS. Kebijakan adalah objek di AWS yang, ketika terkait dengan identitas atau sumber daya, akan menentukan izinnya. AWS mengevaluasi kebijakan-kebijakan tersebut ketika seorang pengguna utama (pengguna, root user, atau sesi peran) mengajukan permintaan. Izin dalam kebijakan menentukan apakah permintaan diberikan atau ditolak. Sebagian besar kebijakan disimpan di AWS sebagai dokumen JSON. Untuk informasi selengkapnya tentang struktur dan isi dokumen kebijakan JSON, silakan lihat [Gambaran Umum kebijakan JSON](#) di Panduan Pengguna IAM.

Administrator dapat menggunakan kebijakan JSON AWS untuk menentukan secara spesifik siapa yang memiliki akses pada apa. Yaitu, pengguna utama manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan syarat apa.

Secara bawaan, para pengguna dan peran tidak memiliki izin. Untuk mengabulkan izin kepada pengguna untuk melakukan tindakan di sumber daya yang mereka perlukan, administrator IAM dapat membuat kebijakan IAM. Administrator kemudian akan dapat menambahkan kebijakan IAM ke peran, dan para pengguna dapat mengambil peran.

Kebijakan IAM mendefinisikan izin untuk suatu tindakan terlepas dari metode yang Anda gunakan untuk pengoperasiannya. Sebagai contoh, anggap saja Anda memiliki kebijakan yang mengizinkan tindakan `iam:GetRole`. Pengguna dengan kebijakan tersebut dapat memperoleh informasi peran dari AWS Management Console, AWS CLI, atau APIAWS.

## Kebijakan berbasis identitas

Kebijakan berbasis identitas adalah dokumen kebijakan izin JSON yang dapat Anda lampirkan ke sebuah identitas, misalnya pengguna IAM, grup pengguna IAM, atau peran IAM. Kebijakan ini mengontrol apa yang pengguna tindakan dan peran dapat kerjakan, pada sumber daya mana, dan dalam keadaan apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, silakan lihat [Membuat kebijakan IAM](#) dalam Panduan Pengguna IAM.

Kebijakan berbasis identitas dapat dikategorikan lebih lanjut sebagai kebijakan inline atau kebijakan terkelola. Kebijakan inline ditanam secara langsung ke pengguna tunggal, grup, atau peran. Kebijakan terkelola adalah kebijakan yang berdiri sendiri yang dapat Anda lampirkan ke beberapa pengguna, grup, dan peran di Akun AWS Anda. Kebijakan terkelola mencakup kebijakan terkelola AWS dan kebijakan terkelola pelanggan. Untuk mempelajari cara memilih antara kebijakan terkelola atau kebijakan inline, silakan lihat [Memilih antara kebijakan terkelola dan kebijakan inline](#) di Panduan Pengguna IAM.

## Kebijakan berbasis sumber daya

Kebijakan berbasis sumber daya adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contoh kebijakan-kebijakan berbasis sumber daya adalah kebijakan terpercaya 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, kebijakan tersebut menentukan tindakan apa yang dapat dilakukan oleh pengguna utama yang ditentukan di sumber daya tersebut dan dalam kondisi apa.

Anda harus [menentukan pengguna utama](#) dalam kebijakan berbasis sumber daya. Pengguna utama dapat mencakup akun, pengguna, peran, pengguna gabungan, atau Layanan AWS.

Kebijakan berbasis sumber daya merupakan kebijakan inline yang terletak di layanan tersebut. Anda tidak dapat menggunakan kebijakan terkelola AWS 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 serupa dengan kebijakan berbasis sumber daya, meskipun kebijakan-kebijakan tersebut tidak menggunakan format dokumen kebijakan JSON.

Amazon S3, AWS WAF, dan Amazon VPC adalah contoh-contoh layanan yang mendukung ACL. Untuk mempelajari ACL selengkapnya, silakan lihat [Gambaran umum daftar kontrol akses \(ACL\)](#) di Panduan Pengembang Layanan Penyimpanan Ringkas Amazon.

## Tipe-tipe kebijakan lain

AWS mendukung tipe kebijakan tambahan, yang kurang umum. Tipe-tipe kebijakan ini dapat mengatur izin maksimum yang diberikan kepada Anda oleh tipe kebijakan yang lebih umum.

- Batasan izin – Batasan izin adalah fitur lanjutan tempat Anda mengatur izin maksimum yang dapat diberikan oleh kebijakan berbasis identitas kepada entitas IAM (pengguna IAM atau peran IAM). Anda dapat menetapkan batasan izin untuk suatu entitas. Izin yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas milik entitas dan batas izinnya. Kebijakan berbasis sumber daya yang menentukan pengguna atau peran dalam bidang `Principal` tidak dibatasi oleh batasan izin. Penolakan eksplisit dalam salah satu kebijakan ini menindahi izin. Untuk informasi selengkapnya tentang batasan izin, silakan lihat [Batasan izin untuk entitas IAM](#) di Panduan Pengguna IAM.
- Kebijakan kontrol layanan (SCP) – SCP adalah kebijakan JSON yang menentukan izin maksimum untuk sebuah organisasi atau unit organisasi (OU) di AWS Organizations. AWS Organizations adalah layanan untuk mengelompokkan dan secara terpusat mengelola beberapa Akun AWS yang dimiliki bisnis Anda. Jika Anda mengaktifkan semua fitur di suatu organisasi, maka Anda dapat menerapkan kebijakan kontrol layanan (SCP) ke salah satu atau ke semua akun Anda. SCP membatasi izin untuk entitas dalam akun anggota, termasuk setiap Pengguna root akun AWS. Untuk informasi selengkapnya tentang Organisasi dan SCP, silakan lihat [Cara kerja SCP](#) di Panduan Pengguna AWS Organizations.
- Kebijakan sesi – Kebijakan sesi adalah kebijakan lanjutan yang Anda berikan sebagai parameter ketika Anda membuat sesi sementara secara terprogram untuk peran atau pengguna gabungan.

Izin sesi yang dihasilkan adalah perpotongan kebijakan berbasis identitas pengguna atau peran dan kebijakan sesi. Izin juga dapat berasal dari kebijakan berbasis sumber daya. Penolakan eksplisit dalam salah satu kebijakan ini menindahi izin. Untuk informasi selengkapnya, silakan lihat [Kebijakan sesi](#) di Panduan Pengguna IAM.

## Berbagai tipe kebijakan

Ketika beberapa tipe kebijakan berlaku pada suatu permintaan, izin yang dihasilkan lebih rumit untuk dipahami. Untuk mempelajari cara AWS menentukan apakah akan mengizinkan permintaan ketika beberapa tipe kebijakan dilibatkan, silakan lihat [Logika evaluasi kebijakan](#) di Panduan Pengguna IAM.

## Bagaimana Amazon Macie bekerja dengan AWS Identity and Access Management

Sebelum Anda menggunakan AWS Identity and Access Management (IAM) untuk mengelola akses ke Amazon Macie, pelajari fitur IAM mana yang tersedia untuk digunakan dengan Macie.

Fitur IAM yang dapat Anda gunakan dengan Amazon Macie

Fitur IAM	Dukungan Macie
<a href="#">Kebijakan berbasis identitas</a>	Ya
<a href="#">Kebijakan berbasis sumber daya</a>	Tidak
<a href="#">Tindakan kebijakan</a>	Ya
<a href="#">Sumber daya kebijakan</a>	Ya
<a href="#">Kunci kondisi kebijakan</a>	Ya
<a href="#">Daftar kontrol akses (ACL)</a>	Tidak
<a href="#">Kontrol akses berbasis atribut (ABAC) — tag dalam kebijakan</a>	Ya
<a href="#">Kredensial temporer</a>	Ya

Fitur IAM	Dukungan Macie
<a href="#">Sesi akses teruskan (FAS)</a>	Ya
<a href="#">Peran layanan</a>	Tidak
<a href="#">Peran tertaut layanan</a>	Ya

Untuk tampilan tingkat tinggi tentang bagaimana Macie dan lainnya Layanan AWS bekerja dengan sebagian besar fitur IAM, lihat [Layanan AWS yang bekerja dengan IAM di Panduan Pengguna IAM](#).

## Kebijakan berbasis identitas untuk Amazon Macie

Mendukung kebijakan berbasis identitas	Ya
--	----

Kebijakan berbasis identitas adalah dokumen kebijakan izin JSON yang dapat Anda lampirkan ke sebuah identitas, misalnya pengguna IAM, grup pengguna IAM, atau peran IAM. Kebijakan ini mengontrol apa yang pengguna tindakan dan peran dapat kerjakan, pada sumber daya mana, dan dalam keadaan apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, silakan lihat [Membuat kebijakan IAM](#) dalam Panduan Pengguna IAM.

Dengan kebijakan berbasis identitas IAM, Anda dapat menentukan secara spesifik apakah tindakan dan sumber daya diizinkan atau ditolak, serta persyaratan yang menjadi dasar dikabulkan atau ditolaknya tindakan tersebut. Anda tidak dapat menentukan secara spesifik pengguna utama dalam sebuah kebijakan berbasis identitas karena pengguna utama berlaku bagi pengguna atau peran yang melekat kepadanya. Untuk mempelajari semua elemen yang dapat Anda gunakan dalam kebijakan JSON, silakan lihat [Referensi elemen kebijakan JSON IAM](#) dalam Panduan Pengguna IAM.

Macie mendukung kebijakan berbasis identitas. Sebagai contoh, silakan lihat [Contoh kebijakan berbasis identitas untuk Amazon Macie](#).

## Kebijakan berbasis sumber daya dalam Amazon Macie

Mendukung kebijakan berbasis sumber daya	Tidak
--	-------



Kebijakan berbasis sumber daya adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contoh kebijakan-kebijakan berbasis sumber daya adalah kebijakan terpercaya 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, kebijakan tersebut menentukan tindakan apa yang dapat dilakukan oleh pengguna utama yang ditentukan di sumber daya tersebut dan dalam kondisi apa. Anda harus [menentukan pengguna utama](#) dalam kebijakan berbasis sumber daya. Pengguna utama dapat mencakup akun, pengguna, peran, pengguna gabungan, atau Layanan AWS.

Untuk mengaktifkan akses lintas akun, Anda dapat menentukan secara spesifik seluruh akun atau entitas IAM di akun lain sebagai pengguna utama dalam kebijakan berbasis sumber daya. Menambahkan pengguna utama akun silang ke kebijakan berbasis sumber daya hanya setengah dari membangun hubungan kepercayaan. Ketika pengguna utama dan sumber daya berada dalam Akun AWS yang berbeda, Administrator IAM di akun terpercaya juga harus memberikan izin kepada entitas pengguna utama (pengguna atau peran) untuk mengakses sumber daya. Mereka memberikan izin melampirkan kebijakan berbasis identitas kepada entitas. Namun, jika kebijakan berbasis sumber daya memberikan akses kepada pengguna utama dalam akun yang sama, tidak diperlukan kebijakan berbasis identitas tambahan. Untuk informasi selengkapnya, silakan lihat [Bagaimana peran IAM berbeda dari kebijakan berbasis sumber daya](#) di Panduan Pengguna IAM.

Macie tidak mendukung kebijakan berbasis sumber daya. Artinya, Anda tidak dapat melampirkan kebijakan langsung ke sumber daya Macie.

## Tindakan kebijakan untuk Amazon Macie

Mendukung tindakan kebijakan

Ya

Administrator dapat menggunakan kebijakan JSON AWS untuk menentukan secara spesifik siapa yang memiliki akses pada apa. Yaitu, pengguna utama manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan syarat apa.

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



Menyertakan tindakan dalam suatu kebijakan untuk memberikan izin guna melakukan operasi yang terkait.

Tindakan kebijakan untuk Macie menggunakan awalan berikut sebelum tindakan:

```
macie2
```

Misalnya, untuk memberikan izin kepada seseorang untuk mengakses informasi tentang semua pengidentifikasi data terkelola yang disediakan Macie, yang merupakan tindakan yang sesuai dengan `ListManagedDataIdentifiers` pengoperasian API Amazon Macie, sertakan tindakan `macie2:ListManagedDataIdentifiers` dalam kebijakan mereka:

```
"Action": "macie2:ListManagedDataIdentifiers"
```

Untuk menetapkan secara spesifik beberapa tindakan dalam satu pernyataan, pisahkan tindakan-tindakan tersebut dengan koma. Sebagai contoh:

```
"Action": [  
    "macie2:ListManagedDataIdentifiers",  
    "macie2:ListCustomDataIdentifiers"  
]
```

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

```
"Action": "macie2:List*"
```

Namun, sebagai praktik terbaik, Anda harus membuat kebijakan yang mengikuti prinsip hak istimewa paling sedikit. Dengan kata lain, Anda harus membuat kebijakan yang hanya menyertakan izin yang diperlukan untuk melakukan tugas tertentu.

Untuk daftar tindakan Macie, lihat [Tindakan yang ditentukan oleh Amazon Macie](#) di Referensi Otorisasi Layanan. Untuk contoh kebijakan yang menentukan tindakan Macie, lihat [Contoh kebijakan berbasis identitas untuk Amazon Macie](#).

## Sumber daya kebijakan untuk Amazon Macie

Mendukung sumber daya kebijakan Ya

Administrator dapat menggunakan kebijakan JSON AWS untuk menentukan secara spesifik siapa yang memiliki akses pada apa. Yaitu, pengguna utama manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan syarat apa.

Elemen kebijakan JSON `Resource` menentukan objek atau objek-objek yang menjadi target penerapan tindakan. Pernyataan harus menyertakan entah elemen `Resource` atau `NotResource`. Praktik terbaiknya, tentukan sumber daya menggunakan [Amazon Resource Name \(ARN\)](#). Anda dapat melakukan ini untuk tindakan-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 bagi semua sumber daya.

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

Macie mendefinisikan jenis sumber daya berikut:

- Izinkan daftar
- Pengidentifikasi data kustom
- Aturan filter atau penekanan, juga disebut sebagai filter temuan
- Akun anggota
- Pekerjaan penemuan data sensitif, juga disebut sebagai pekerjaan klasifikasi

Anda dapat menentukan jenis sumber daya ini dalam kebijakan dengan menggunakan ARN.

Misalnya, untuk membuat kebijakan untuk pekerjaan penemuan data sensitif yang memiliki ID pekerjaan `3ce05dbb7ec5505def334104bexample`, Anda dapat menggunakan ARN berikut:

```
"Resource": "arn:aws:macie2:*:*:classification-job/3ce05dbb7ec5505def334104bexample" 
```

Atau, untuk menentukan semua pekerjaan penemuan data sensitif untuk akun tertentu, gunakan wildcard (\*):

```
"Resource": "arn:aws:macie2:*:123456789012:classification-job/*"
```

Dimana **123456789012** adalah ID akun untuk yang menciptakan pekerjaan. Akun AWS Namun, sebagai praktik terbaik, Anda harus membuat kebijakan yang mengikuti prinsip hak istimewa paling sedikit. Dengan kata lain, Anda harus membuat kebijakan yang hanya menyertakan izin yang diperlukan untuk melakukan tugas tertentu pada sumber daya tertentu.

Beberapa tindakan Macie dapat diterapkan ke beberapa sumber daya. Misalnya, `macie2:BatchGetCustomDataIdentifiers` tindakan dapat mengambil detail beberapa pengidentifikasi data kustom. Dalam kasus ini, kepala sekolah harus memiliki izin untuk mengakses semua sumber daya yang berlaku untuk tindakan tersebut. Untuk menentukan beberapa sumber daya dalam satu pernyataan, pisahkan ARN dengan koma:

```
"Resource": [  
  "arn:aws:macie2:*:*:custom-data-identifier/12g4aff9-8e22-4f2b-b3fd-3063eexample",  
  "arn:aws:macie2:*:*:custom-data-identifier/2d12c96a-8e78-4ca6-b1dc-8fd65example",  
  "arn:aws:macie2:*:*:custom-data-identifier/4383a69d-4a1e-4a07-8715-208ddexample"  
]
```

Untuk daftar jenis sumber daya Macie dan sintaks ARN untuk masing-masing, [lihat Jenis sumber daya yang ditentukan oleh Amazon Macie di Referensi Otorisasi Layanan](#). Untuk mempelajari tindakan yang dapat Anda tentukan dengan setiap jenis sumber daya, lihat [Tindakan yang ditentukan oleh Amazon Macie](#) di Referensi Otorisasi Layanan. Untuk contoh kebijakan yang menentukan sumber daya, lihat [Contoh kebijakan berbasis identitas untuk Amazon Macie](#).

## Kunci kondisi kebijakan untuk Amazon Macie

Mendukung kunci-kunci persyaratan kebijakan spesifik layanan      Ya

Administrator dapat menggunakan kebijakan JSON AWS untuk menentukan secara spesifik siapa yang memiliki akses pada apa. Yaitu, pengguna utama manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan syarat apa.

Elemen `Condition` (atau blok `Condition`) akan memungkinkan Anda menentukan syarat yang menjadi dasar suatu pernyataan berlaku. Elemen `Condition` bersifat opsional. Anda dapat

membuat ekspresi bersyarat yang menggunakan [operator syarat](#), misalnya sama dengan atau kurang dari, untuk mencocokkan syarat dalam kebijakan dengan nilai-nilai yang diminta.

Jika Anda menentukan beberapa elemen Condition dalam sebuah pernyataan, atau beberapa kunci dalam elemen Condition tunggal, maka AWS akan mengevaluasinya dengan menggunakan operasi AND yang logis. Jika Anda menentukan beberapa nilai untuk satu kunci persyaratan, maka AWS akan mengevaluasi syarat tersebut menggunakan operasi OR yang logis. Semua persyaratan harus dipenuhi sebelum izin pernyataan diberikan.

Anda juga dapat menggunakan variabel placeholder saat menentukan syarat. Sebagai contoh, Anda dapat memberikan izin kepada pengguna IAM untuk mengakses sumber daya hanya jika izin tersebut mempunyai tag yang sesuai dengan nama pengguna IAM mereka. Untuk informasi selengkapnya, silakan lihat [Elemen kebijakan IAM: variabel dan tag](#) di Panduan Pengguna IAM.

AWS mendukung kunci-kunci syarat global dan kunci-kunci syarat spesifik layanan. Untuk melihat semua kunci persyaratan global AWS, silakan lihat [kunci konteks syarat global AWS](#) di Panduan Pengguna IAM.

Untuk daftar kunci kondisi Macie, lihat Kunci kondisi [untuk Amazon](#) Macie di Referensi Otorisasi Layanan. Untuk mempelajari tindakan dan sumber daya yang dapat digunakan untuk menggunakan kunci kondisi, lihat [Tindakan yang ditentukan oleh Amazon Macie](#). Untuk contoh kebijakan yang menggunakan kunci kondisi, lihat [Contoh kebijakan berbasis identitas untuk Amazon Macie](#).

## Daftar kontrol akses (ACL) di Amazon Macie

Mendukung ACL

Tidak

Daftar kontrol akses (ACL) mengendalikan pengguna utama mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACL serupa dengan kebijakan berbasis sumber daya, meskipun kebijakan-kebijakan tersebut tidak menggunakan format dokumen kebijakan JSON.

Amazon Simple Storage Service (Amazon S3) adalah contoh yang mendukung ACL. Layanan AWS Untuk mempelajari selengkapnya, lihat [Ringkasan daftar kontrol akses \(ACL\)](#) di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

Macie tidak mendukung ACL. Artinya, Anda tidak dapat melampirkan ACL ke sumber daya Macie.

## Kontrol akses berbasis atribut (ABAC) dengan Amazon Macie

Mendukung ABAC (tanda dalam kebijakan) Ya

Kontrol akses berbasis atribut (ABAC) adalah strategi otorisasi yang mendefinisikan izin berdasarkan atribut. Di AWS, atribut-atribut ini disebut tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke banyak sumber daya AWS. Pemberian tag ke entitas dan sumber daya adalah langkah pertama dari ABAC. Kemudian rancanglah kebijakan ABAC untuk mengizinkan operasi-operasi ketika tag milik pengguna utama cocok dengan tag yang ada di sumber daya yang ingin diakses.

ABAC sangat berguna di lingkungan yang berkembang dengan cepat dan berguna di situasi dimana pengelolaan kebijakan menjadi rumit.

Untuk mengendalikan akses berdasarkan tag, berikan informasi tentang tag di [elemen syarat](#) dari sebuah kebijakan dengan menggunakan kunci-kunci persyaratan `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`, atau `aws:TagKeys`.

Jika sebuah layanan mendukung ketiga kunci-kunci persyaratan untuk setiap jenis sumber daya, maka nilainya adalah Ya untuk layanan tersebut. Jika suatu layanan mendukung ketiga kunci persyaratan untuk hanya beberapa jenis sumber daya, maka nilainya adalah Parsial.

Untuk informasi selengkapnya tentang ABAC, silakan lihat [Apa itu ABAC?](#) di Panduan Pengguna IAM. Untuk melihat tutorial yang menguraikan langkah-langkah pengaturan ABAC, silakan lihat [Menggunakan kontrol akses berbasis atribut \(ABAC\)](#) di Panduan Pengguna IAM.

Anda dapat melampirkan tag ke sumber daya Macie—daftar izinkan, pengidentifikasi data kustom, aturan filter dan aturan penindasan, akun anggota, dan pekerjaan penemuan data sensitif. Anda juga dapat mengontrol akses ke jenis sumber daya ini dengan memberikan informasi tag dalam `Condition` elemen kebijakan. Untuk informasi tentang menandai sumber daya Macie, lihat [Menandai sumber daya Amazon Macie](#) Untuk contoh kebijakan berbasis identitas yang mengontrol akses ke sumber daya berdasarkan tag, lihat [Contoh kebijakan berbasis identitas untuk Amazon Macie](#)

## Menggunakan kredensial sementara dengan Amazon Macie

Mendukung kredensial temporer Ya

Beberapa Layanan AWS tidak berfungsi saat Anda masuk dengan menggunakan kredensial temporer. Sebagai informasi tambahan, termasuk tentang Layanan AWS mana saja yang berfungsi dengan kredensial temporer, silakan lihat [Layanan AWS yang berfungsi dengan IAM](#) di Panduan Pengguna IAM.

Anda menggunakan kredensial temporer jika Anda masuk ke AWS Management Console dengan menggunakan metode apa pun kecuali nama pengguna dan kata sandi. Sebagai contoh, ketika Anda mengakses AWS dengan menggunakan tautan masuk tunggal (SSO) milik perusahaan Anda, proses itu secara otomatis akan membuat kredensial temporer. Anda juga akan secara otomatis membuat kredensial temporer ketika Anda masuk ke konsol sebagai seorang pengguna dan kemudian beralih peran. Untuk informasi selengkapnya tentang peralihan peran, silakan lihat [Peralihan peran \(konsol\)](#) di Panduan Pengguna IAM.

Anda dapat secara manual membuat kredensial temporer menggunakan AWS CLI atau API AWS. Anda kemudian dapat menggunakan kredensial temporer tersebut untuk mengakses AWS. AWS menyarankan agar Anda secara dinamis membuat kredensial temporer alih-alih menggunakan kunci akses jangka panjang. Untuk informasi selengkapnya, silakan lihat [Kredensial keamanan temporer di IAM](#).

Macie mendukung penggunaan kredensial sementara.

## Teruskan sesi akses untuk Amazon Macie

Mendukung sesi akses maju (FAS)

Ya

Saat Anda menggunakan pengguna IAM atau peran IAM untuk mengerjakan tindakan di AWS, Anda akan dianggap sebagai pengguna utama. Ketika Anda menggunakan beberapa layanan, Anda mungkin melakukan sebuah tindakan yang kemudian dilanjutkan oleh tindakan lain pada layanan yang berbeda. FAS menggunakan izin dari pengguna utama untuk memanggil Layanan AWS, yang dikombinasikan dengan Layanan AWS yang diminta untuk membuat pengajuan ke layanan hilir. Permintaan FAS hanya diajukan ketika sebuah layanan menerima pengajuan yang memerlukan interaksi dengan Layanan AWS lain atau sumber daya lain untuk diselesaikan. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan ketika mengajukan permintaan FAS, silakan lihat [Meneruskan sesi akses](#).

Macie membuat permintaan FAS ke hilir Layanan AWS saat Anda melakukan tugas-tugas berikut:

- Buat atau perbarui pengaturan Macie untuk daftar izin yang disimpan dalam bucket S3.

- Periksa status daftar izinkan yang disimpan dalam bucket S3.
- Ambil sampel data sensitif dari objek S3 yang terpengaruh dengan menggunakan kredensial pengguna IAM.
- Enkripsi sampel data sensitif yang diambil menggunakan kredensial pengguna IAM atau peran IAM.
- Aktifkan Macie untuk berintegrasi dengan AWS Organizations.
- Tentukan akun administrator Macie yang didelegasikan untuk organisasi di AWS Organizations

Untuk tugas lain, Macie menggunakan peran terkait layanan untuk melakukan tindakan atas nama Anda. Untuk detail tentang peran ini, lihat [Peran terkait layanan untuk Amazon Macie](#).

## Peran layanan untuk Amazon Macie

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, memodifikasi, dan menghapus peran layanan dari dalam IAM. Untuk informasi selengkapnya, lihat [Membuat peran untuk mendelegasikan izin ke Layanan AWS](#) dalam Panduan pengguna IAM.

Macie tidak mengasumsikan atau menggunakan peran layanan. Untuk melakukan tindakan atas nama Anda, Macie terutama menggunakan peran terkait layanan. Untuk detail tentang peran ini, lihat [Peran terkait layanan untuk Amazon Macie](#).

## Peran terkait layanan untuk Amazon Macie

Mendukung peran yang terhubung dengan layanan	Ya
---	----

Peran yang terkait layanan adalah jenis peran layanan yang terkait dengan Layanan AWS. Layanan tersebut dapat menjalankan peran untuk melakukan sebuah tindakan atas nama Anda. Peran terkait layanan akan muncul di Akun AWS Anda dan dimiliki oleh layanan tersebut. Administrator IAM dapat melihat, tetapi tidak dapat mengedit izin untuk peran terkait layanan.

Macie menggunakan peran terkait layanan untuk melakukan tindakan atas nama Anda. Untuk detail tentang peran ini, lihat [Peran tertaut layanan untuk Amazon Macie](#).

## Contoh kebijakan berbasis identitas untuk Amazon Macie

Secara default, pengguna dan peran tidak memiliki izin untuk membuat atau memodifikasi sumber daya. 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 mengambil peran.

Untuk mempelajari cara membuat kebijakan berbasis identitas IAM dengan 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 Macie, termasuk format ARN untuk setiap jenis sumber daya, lihat [Tindakan, sumber daya, dan kunci kondisi untuk Amazon Macie](#) di Referensi Otorisasi Layanan.

Saat Anda membuat kebijakan, pastikan untuk menyelesaikan peringatan keamanan, kesalahan, peringatan umum, dan saran dari AWS Identity and Access Management Access Analyzer (IAM Access Analyzer) sebelum Anda menyimpan kebijakan. [IAM Access Analyzer menjalankan pemeriksaan kebijakan untuk memvalidasi kebijakan terhadap tata bahasa kebijakan IAM dan praktik terbaik](#). Pemeriksaan ini menghasilkan temuan dan memberikan rekomendasi yang dapat ditindaklanjuti untuk membantu Anda membuat kebijakan yang fungsional dan sesuai dengan praktik terbaik keamanan. Untuk mempelajari tentang memvalidasi kebijakan dengan menggunakan IAM Access Analyzer, lihat [validasi kebijakan IAM Access Analyzer](#) di Panduan Pengguna IAM. Untuk meninjau daftar peringatan, kesalahan, dan saran yang dapat dikembalikan oleh IAM Access Analyzer, lihat [referensi pemeriksaan kebijakan IAM Access Analyzer](#) di Panduan Pengguna IAM.

### Topik

- [Praktik terbaik kebijakan](#)
- [Menggunakan konsol Amazon Macie](#)
- [Contoh: Perbolehkan pengguna untuk meninjau izin mereka sendiri](#)
- [Contoh: Memungkinkan pengguna untuk membuat pekerjaan penemuan data sensitif](#)
- [Contoh: Perbolehkan pengguna untuk mengelola tugas penemuan data sensitif](#)
- [Contoh: Memungkinkan pengguna untuk meninjau temuan](#)



- [Contoh: Memungkinkan pengguna untuk meninjau pengidentifikasi data kustom berdasarkan tag](#)

## Praktik terbaik kebijakan

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

- Memulai kebijakan AWS terkelola dan beralih ke izin paling sedikit hak istimewa — Untuk mulai memberikan izin kepada pengguna dan beban kerja Anda, gunakan kebijakan AWS terkelola yang memberikan izin untuk banyak kasus penggunaan umum. Mereka tersedia di AndaAkun AWS. Kami menyarankan Anda mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola AWS pelanggan yang spesifik untuk kasus penggunaan Anda. Untuk informasi selengkapnya, lihat [kebijakan AWS terkelola atau kebijakan terkelola untuk fungsi pekerjaan](#) di Panduan Pengguna IAM.
- Terapkan izin hak akses terkecil — Saat Anda menetapkan izin dengan kebijakan IAM, berikan hanya izin yang diperlukan untuk melaksanakan tugas. Anda melakukan ini dengan menentukan tindakan yang dapat diambil pada sumber daya tertentu dalam kondisi tertentu, juga dikenal sebagai izin paling tidak memiliki hak istimewa. Untuk informasi selengkapnya tentang penggunaan IAM untuk menerapkan izin, lihat [Kebijakan dan izin di IAM dalam Panduan Pengguna IAM](#).
- Gunakan ketentuan dalam kebijakan IAM untuk membatasi akses lebih lanjut — Anda dapat menambahkan kondisi pada kebijakan Anda untuk membatasi akses ke tindakan dan sumber daya. Misalnya, Anda dapat menulis ketentuan kebijakan untuk menentukan bahwa semua permintaan harus dikirim menggunakan SSL. Anda juga dapat menggunakan kondisi untuk memberikan akses ke tindakan layanan jika digunakan melalui spesifik Layanan AWS, seperti AWS CloudFormation. Untuk informasi selengkapnya, lihat [Elemen kebijakan IAM JSON: Syarat](#) dalam Panduan Pengguna IAM.
- Gunakan IAM Access Analyzer untuk memvalidasi kebijakan IAM Anda untuk memastikan izin yang aman dan fungsional - IAM Access Analyzer memvalidasi kebijakan baru dan yang sudah ada sehingga kebijakan mematuhi bahasa kebijakan IAM (JSON) dan praktik terbaik IAM. IAM Access Analyzer menyediakan lebih dari 100 pemeriksaan kebijakan dan rekomendasi yang dapat ditindaklanjuti untuk membantu Anda membuat kebijakan yang aman dan fungsional. Untuk informasi selengkapnya, lihat [validasi kebijakan IAM Access Analyzer di Panduan Pengguna IAM](#).
- Memerlukan otentikasi multi-faktor (MFA) — Jika Anda memiliki skenario yang mengharuskan pengguna IAM atau pengguna root di AndaAkun AWS, aktifkan MFA untuk keamanan tambahan. Untuk mewajibkan MFA saat operasi API dipanggil, tambahkan kondisi MFA ke 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](#) dalam Panduan Pengguna IAM.

## Menggunakan konsol Amazon Macie

Untuk mengakses konsol Amazon Macie, Anda harus memiliki rangkaian izin minimum. Izin ini harus mengizinkan Anda untuk membuat daftar dan melihat detail tentang sumber daya Macie di Anda. Akun AWS Jika Anda membuat kebijakan berbasis identitas yang lebih ketat dari izin minimum yang diperlukan, konsol tidak akan berfungsi sebagaimana dimaksudkan untuk entitas (pengguna atau peran) dengan kebijakan tersebut.

Anda tidak perlu meloloskan izin konsol minimum untuk pengguna yang hanya melakukan panggilan ke AWS CLI atau API AWS. Alih-alih, izinkan akses hanya ke tindakan yang sesuai dengan operasi API yang mereka coba lakukan.

Untuk memastikan bahwa pengguna dan peran dapat menggunakan konsol Amazon Macie, buat kebijakan IAM yang memberi mereka akses konsol. Untuk informasi selengkapnya, lihat [Kebijakan dan Izin dalam IAM](#) dalam Panduan Pengguna IAM.

Jika Anda membuat kebijakan yang memungkinkan pengguna atau peran untuk menggunakan konsol Amazon Macie, pastikan kebijakan tersebut mengizinkan `macie2:GetMacieSession` tindakan tersebut. Jika tidak, pengguna atau peran tersebut tidak akan dapat mengakses sumber daya atau data Macie apa pun di konsol.

Pastikan juga bahwa kebijakan tersebut memungkinkan `macie2:List` tindakan yang sesuai untuk sumber daya yang perlu diakses oleh pengguna atau peran tersebut di konsol. Jika tidak, mereka tidak akan dapat menavigasi atau menampilkan detail tentang sumber daya tersebut di konsol. Misalnya, untuk meninjau detail pekerjaan penemuan data sensitif dengan menggunakan konsol, pengguna harus diizinkan untuk melakukan `macie2:DescribeClassificationJob` tindakan untuk pekerjaan dan `macie2:ListClassificationJobs` tindakan tersebut. Jika pengguna tidak diizinkan untuk melakukan `macie2:ListClassificationJobs` tindakan, pengguna tidak akan dapat menampilkan daftar pekerjaan di halaman Pekerjaan konsol, dan oleh karena itu tidak akan dapat memilih pekerjaan untuk menampilkan detailnya. Agar detail menyertakan informasi tentang pengenalan data kustom yang digunakan pekerjaan, pengguna juga harus diizinkan untuk melakukan `macie2:BatchGetCustomDataIdentifiers` tindakan untuk pengidentifikasi data kustom.

## Contoh: Perbolehkan pengguna untuk meninjau izin mereka sendiri

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

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

## Contoh: Memungkinkan pengguna untuk membuat pekerjaan penemuan data sensitif

Contoh ini menunjukkan bagaimana Anda dapat membuat kebijakan yang mengizinkan pengguna membuat tugas penemuan data sensitif.

Dalam contoh, pernyataan pertama memberikan `macie2:CreateClassificationJob` izin kepada pengguna. Izin ini memungkinkan pengguna untuk membuat pekerjaan. Pernyataan itu juga memberikan `macie2:DescribeClassificationJob` izin. Izin ini memungkinkan pengguna untuk mengakses rincian pekerjaan yang ada. Meskipun izin ini tidak diperlukan untuk membuat pekerjaan, akses ke detail ini dapat membantu pengguna membuat pekerjaan yang memiliki pengaturan konfigurasi unik.

Pernyataan kedua dalam contoh memungkinkan pengguna untuk membuat, mengkonfigurasi, dan meninjau pekerjaan dengan menggunakan konsol Amazon Macie. `macie2:ListClassificationJobs` izin memungkinkan pengguna untuk menampilkan pekerjaan yang ada di halaman Pekerjaan konsol. Semua izin lain dalam pernyataan memungkinkan pengguna untuk mengkonfigurasi dan membuat pekerjaan dengan menggunakan Buat halaman pekerjaan di konsol.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CreateAndReviewJobs",
      "Effect": "Allow",
      "Action": [
        "macie2:CreateClassificationJob",
        "macie2:DescribeClassificationJob"
      ],
      "Resource": "arn:aws:macie2:*:*:classification-job/*"
    },
    {
      "Sid": "CreateAndReviewJobsOnConsole",
      "Effect": "Allow",
      "Action": [
        "macie2:ListClassificationJobs",
        "macie2:ListAllowLists",
        "macie2:ListCustomDataIdentifiers",
        "macie2:ListManagedDataIdentifiers",
        "macie2:SearchResources",
        "macie2:DescribeBuckets"
      ]
    }
  ]
}
```

```

        ],
        "Resource": "*"
    }
]
}

```

## Contoh: Perbolehkan pengguna untuk mengelola tugas penemuan data sensitif

Contoh ini menunjukkan bagaimana Anda dapat membuat kebijakan yang mengizinkan pengguna mengakses detail tugas penemuan data sensitif tertentu, tugas yang ID3ce05dbb7ec5505def334104bexample. Contoh ini juga memungkinkan pengguna untuk mengubah status pekerjaan yang diperlukan.

Pernyataan pertama dalam contoh hibah macie2:DescribeClassificationJob dan macie2:UpdateClassificationJob izin kepada pengguna. Izin ini memungkinkan pengguna untuk mengambil rincian pekerjaan dan mengubah status pekerjaan, masing-masing. Pernyataan kedua memberikan macie2:ListClassificationJobs izin kepada pengguna, yang memungkinkan pengguna mengakses pekerjaan dengan menggunakan halaman Pekerjaan di konsol Amazon Macie.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ManageOneJob",
      "Effect": "Allow",
      "Action": [
        "macie2:DescribeClassificationJob",
        "macie2:UpdateClassificationJob"
      ],
      "Resource": "arn:aws:macie2:*:*:classification-
job/3ce05dbb7ec5505def334104bexample"
    },
    {
      "Sid": "ListJobsOnConsole",
      "Effect": "Allow",
      "Action": "macie2:ListClassificationJobs",
      "Resource": "*"
    }
  ]
}

```

Anda juga dapat mengizinkan pengguna mengakses data pencatatan (peristiwa log) yang diterbitkan Macie ke Amazon CloudWatch Logs untuk pekerjaan tersebut. Untuk melakukan ini, Anda dapat menambahkan pernyataan yang memberikan izin untuk melakukan tindakan CloudWatch Log (logs) pada grup log dan streaming untuk pekerjaan tersebut. Misalnya:

```
"Statement": [
  {
    "Sid": "AccessLogGroupForMacieJobs",
    "Effect": "Allow",
    "Action": [
      "logs:DescribeLogGroups",
      "logs:DescribeLogStreams"
    ],
    "Resource": "arn:aws:logs:*:*:log-group:aws/macie/classificationjobs"
  },
  {
    "Sid": "AccessLogEventsForOneMacieJob",
    "Effect": "Allow",
    "Action": "logs:GetLogEvents",
    "Resource": [
      "arn:aws:logs:*:*:log-group:aws/macie/classificationjobs/*",
      "arn:aws:logs:*:*:log-group:aws/macie/classificationjobs:log-stream:3ce05dbb7ec5505def334104bexample"
    ]
  }
]
```

Untuk informasi tentang mengelola akses ke CloudWatch Log, lihat [Ringkasan mengelola izin akses ke sumber daya CloudWatch Log Anda](#) di Panduan Pengguna Amazon CloudWatch Logs.

### Contoh: Memungkinkan pengguna untuk meninjau temuan

Contoh ini menunjukkan bagaimana Anda dapat membuat kebijakan yang mengizinkan pengguna mengakses data temuan.

Dalam contoh ini, izin `macie2:GetFindings` dan `macie2:GetFindingStatistics` izin mengizinkan pengguna untuk mengambil data dengan menggunakan API Amazon Macie atau konsol Amazon Macie. `macie2:ListFindings` izin memungkinkan pengguna untuk mengambil dan meninjau data dengan menggunakan dasbor Ringkasan dan halaman Temuan di konsol Amazon Macie.

```
{
```

```

"Version": "2012-10-17",
"Statement": [
  {
    "Sid": "ReviewFindings",
    "Effect": "Allow",
    "Action": [
      "macie2:GetFindings",
      "macie2:GetFindingStatistics",
      "macie2:ListFindings"
    ],
    "Resource": "*"
  }
]
}

```

Anda juga dapat mengizinkan pengguna untuk membuat dan mengelola aturan filter dan aturan penindasan untuk temuan. Untuk melakukan ini, Anda dapat menyertakan pernyataan yang memberikan izin berikut: `macie2:CreateFindingsFilter`, `macie2:GetFindingsFilter`, `macie2:UpdateFindingsFilter`, dan `macie2>DeleteFindingsFilter`. Untuk memungkinkan pengguna mengelola aturan dengan menggunakan konsol Amazon Macie, sertakan juga `macie2:ListFindingsFilters` izin dalam kebijakan. Misalnya:

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ReviewFindings",
      "Effect": "Allow",
      "Action": [
        "macie2:GetFindings",
        "macie2:GetFindingStatistics",
        "macie2:ListFindings"
      ],
      "Resource": "*"
    },
    {
      "Sid": "ManageRules",
      "Effect": "Allow",
      "Action": [
        "macie2:GetFindingsFilter",
        "macie2:UpdateFindingsFilter",

```

```

        "macie2:CreateFindingsFilter",
        "macie2>DeleteFindingsFilter"
    ],
    "Resource": "arn:aws:macie2:*:*:findings-filter/*"
  },
  {
    "Sid": "ListRulesOnConsole",
    "Effect": "Allow",
    "Action": "macie2:ListFindingsFilters",
    "Resource": "*"
  }
]
}

```

## Contoh: Memungkinkan pengguna untuk meninjau pengidentifikasi data kustom berdasarkan tag

Dalam kebijakan berbasis identitas, Anda dapat menggunakan ketentuan untuk mengontrol akses ke sumber daya Amazon Macie berdasarkan tag. Contoh ini menunjukkan bagaimana Anda dapat membuat kebijakan yang mengizinkan pengguna meninjau pengidentifikasi data khusus dengan menggunakan konsol Amazon Macie atau API Amazon Macie. Namun, izin diberikan hanya jika nilai untuk `Owner` tag adalah nama pengguna pengguna pengguna pengguna dari pengguna.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ReviewCustomDataIdentifiersIfOwner",
      "Effect": "Allow",
      "Action": "macie2:GetCustomDataIdentifier",
      "Resource": "arn:aws:macie2:*:*:custom-data-identifier/*",
      "Condition": {
        "StringEquals": {"aws:ResourceTag/Owner": "${aws:username}"}
      }
    },
    {
      "Sid": "ListCustomDataIdentifiersOnConsoleIfOwner",
      "Effect": "Allow",
      "Action": "macie2:ListCustomDataIdentifiers",
      "Resource": "*",
      "Condition": {
        "StringEquals": {"aws:ResourceTag/Owner": "${aws:username}"}
      }
    }
  ]
}

```



```
    }  
  }  
]  
}
```

Dalam contoh ini, jika pengguna yang memiliki nama pengguna `richard-roe` mencoba meninjau detail pengenalan data kustom, pengidentifikasi data kustom harus diberi tag `Owner=richard-roe` atau `owner=richard-roe`. Jika tidak, akses pengguna ditolak. Kunci tag kondisi `Owner` cocok dengan keduanya `Owner` dan `owner` karena nama kunci kondisi tidak terpengaruh huruf besar/kecil. Untuk informasi selengkapnya, lihat [Elemen kebijakan JSON IAM: Syarat](#) dalam Panduan Pengguna IAM.

## Peran terkait layanan untuk Amazon Macie

Amazon Macie menggunakan peran terkait [layanan AWS Identity and Access Management](#) (IAM) bernama `AWSServiceRoleForAmazonMacie`. Peran terkait layanan ini adalah peran IAM yang ditautkan langsung ke Macie. Ini telah ditentukan oleh Macie dan mencakup semua izin yang diperlukan Macie untuk memanggil sumber daya lain Layanan AWS dan memantau AWS sumber daya atas nama Anda. Macie menggunakan peran terkait layanan ini di semua Wilayah AWS tempat Macie tersedia.

Peran terkait layanan membuat penyiapan Macie lebih mudah karena Anda tidak perlu menambahkan izin yang diperlukan secara manual. Macie mendefinisikan izin dari peran terkait layanan ini, dan kecuali ditentukan lain, hanya Macie yang dapat mengambil peran tersebut. Izin yang ditentukan mencakup kebijakan kepercayaan dan kebijakan izin, dan kebijakan izin tersebut tidak dapat dilampirkan ke entitas IAM lainnya.

Anda harus mengonfigurasi izin untuk mengizinkan entitas IAM (seperti pengguna atau peran) membuat, mengedit, atau menghapus peran terkait layanan. Untuk informasi selengkapnya, lihat [Izin peran terkait layanan](#) dalam Panduan Pengguna IAM. Anda dapat menghapus peran terkait layanan hanya setelah menghapus sumber daya terkait. Ini melindungi sumber daya Anda karena Anda tidak dapat secara tidak sengaja menghapus izin untuk mengakses sumber daya.

Untuk informasi tentang layanan lain yang mendukung peran terkait layanan, lihat layanan [Layanan AWS yang berfungsi dengan IAM](#) dan cari layanan yang memiliki Ya di kolom Peran terkait layanan. Pilih Ya dengan tautan untuk meninjau dokumentasi peran terkait layanan untuk layanan tersebut.

### Topik

- [Izin peran terkait layanan untuk Amazon Macie](#)

- [Membuat peran terkait layanan untuk Amazon Macie](#)
- [Mengedit peran terkait layanan untuk Amazon Macie](#)
- [Menghapus peran terkait layanan untuk Amazon Macie](#)
- [Didukung Wilayah AWS untuk peran terkait layanan Amazon Macie](#)

## Izin peran terkait layanan untuk Amazon Macie

Amazon Macie menggunakan peran terkait layanan bernama `AWSServiceRoleForAmazonMacie`. Peran terkait layanan ini mempercayai `macie.amazonaws.com` layanan untuk mengambil peran tersebut.

Kebijakan izin untuk peran, yang diberi nama `AmazonMacieServiceRolePolicy`, memungkinkan Macie melakukan tugas seperti berikut pada sumber daya yang ditentukan:

- Gunakan tindakan Amazon S3 untuk mengambil informasi tentang bucket dan objek S3.
- Gunakan tindakan Amazon S3 untuk mengambil objek S3.
- Gunakan AWS Organizations tindakan untuk mengambil informasi tentang akun terkait.
- Gunakan tindakan Amazon CloudWatch Logs untuk mencatat peristiwa untuk pekerjaan penemuan data sensitif.

Peran dikonfigurasi dengan kebijakan izin berikut.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iam:ListAccountAliases",
        "organizations:DescribeAccount",
        "organizations:ListAccounts",
        "s3:GetAccountPublicAccessBlock",
        "s3:ListAllMyBuckets",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketPolicy",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
```

```

    "s3:GetBucketTagging",
    "s3:GetBucketVersioning",
    "s3:GetBucketWebsite",
    "s3:GetEncryptionConfiguration",
    "s3:GetLifecycleConfiguration",
    "s3:GetReplicationConfiguration",
    "s3:ListBucket",
    "s3:GetObject",
    "s3:GetObjectAcl",
    "s3:GetObjectTagging"
  ],
  "Resource": "*"
},
{
  "Effect": "Allow",
  "Action": [
    "logs:CreateLogGroup"
  ],
  "Resource": [
    "arn:aws:logs:*:*:log-group:/aws/macie/*"
  ]
},
{
  "Effect": "Allow",
  "Action": [
    "logs:CreateLogStream",
    "logs:PutLogEvents",
    "logs:DescribeLogStreams"
  ],
  "Resource": [
    "arn:aws:logs:*:*:log-group:/aws/macie/*:log-stream:*"
  ]
}
]
}

```

Untuk detail tentang pembaruan AmazonMacieServiceRolePolicy kebijakan, lihat [Amazon Macie memperbarui keAWSkebijakan dikelola](#). Untuk peringatan otomatis tentang perubahan kebijakan ini, berlangganan umpan RSS di halaman riwayat [dokumen Macie](#).

Anda harus mengonfigurasi izin untuk mengizinkan entitas IAM (seperti pengguna atau peran) membuat, mengedit, atau menghapus peran terkait layanan. Untuk informasi selengkapnya, lihat [Izin peran terkait layanan](#) dalam Panduan Pengguna IAM.

## Membuat peran terkait layanan untuk Amazon Macie

Anda tidak perlu membuat peran `AWSServiceRoleForAmazonMacie` terkait layanan untuk Amazon Macie secara manual. Saat Anda mengaktifkan Macie untuk Anda Akun AWS, Macie secara otomatis membuat peran terkait layanan untuk Anda.

Jika Anda menghapus peran terkait layanan Macie dan kemudian perlu membuatnya lagi, Anda dapat menggunakan proses yang sama untuk membuat ulang peran di akun Anda. Saat Anda mengaktifkan Macie lagi, Macie membuat peran terkait layanan lagi untuk Anda.

## Mengedit peran terkait layanan untuk Amazon Macie

Amazon Macie tidak mengizinkan Anda mengedit peran terkait `AWSServiceRoleForAmazonMacie` layanan. Setelah peran terkait layanan dibuat, Anda tidak dapat mengubah nama peran karena berbagai entitas mungkin mereferensikan peran tersebut. Namun, Anda dapat mengedit deskripsi peran ini menggunakan IAM. Untuk informasi selengkapnya, lihat [Mengedit peran terkait layanan](#) dalam Panduan Pengguna IAM.

## Menghapus peran terkait layanan untuk Amazon Macie

Jika Anda tidak perlu lagi menggunakan Amazon Macie, sebaiknya hapus peran terkait `AWSServiceRoleForAmazonMacie` layanan secara manual. Saat Anda menonaktifkan Macie, Macie tidak menghapus peran untuk Anda.

Sebelum Anda menghapus peran, Anda harus menonaktifkan Macie di setiap Wilayah AWS tempat Anda mengaktifkannya. Anda juga harus secara manual membersihkan sumber daya untuk peran tersebut. Untuk menghapus peran, Anda dapat menggunakan konsol IAM, the AWS CLI, atau AWS API. Untuk informasi selengkapnya, lihat [Menghapus peran terkait layanan](#) dalam Panduan Pengguna IAM.

### Note

Jika Macie menggunakan `AWSServiceRoleForAmazonMacie` peran saat Anda mencoba menghapus sumber daya, penghapusan mungkin gagal. Jika itu terjadi, tunggu beberapa menit dan kemudian coba operasi lagi.

Jika Anda menghapus peran `AWSServiceRoleForAmazonMacie` terkait layanan dan perlu membuatnya lagi, Anda dapat membuatnya lagi dengan mengaktifkan Macie untuk akun Anda. Saat Anda mengaktifkan Macie lagi, Macie membuat peran terkait layanan lagi untuk Anda.

## Didukung Wilayah AWS untuk peran terkait layanan Amazon Macie

Amazon Macie mendukung penggunaan peran `AWSServiceRoleForAmazonMacie` terkait layanan di semua Wilayah AWS tempat Macie tersedia. Untuk daftar Wilayah di mana Macie saat ini tersedia, lihat [titik akhir dan kuota Amazon Macie](#) di. Referensi Umum AWS

## Kebijakan terkelola AWS untuk Amazon Macie

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

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

Anda tidak dapat mengubah izin yang ditentukan dalam AWS kebijakan yang dikelola. Jika AWS memperbarui izin yang didefinisikan dalam AWS kebijakan terkelola, pembaruan mempengaruhi semua identitas utama (pengguna, grup, dan peran) yang dilampirkan kebijakan. AWS kemungkinan besar akan memperbarui AWS kebijakan terkelola saat baru Layanan AWS diluncurkan atau operasi API baru tersedia untuk layanan yang ada.

Untuk informasi selengkapnya, lihat [Kebijakan terkelola AWS](#) dalam Panduan Pengguna IAM.

Amazon Macie menyediakan beberapa AWS kebijakan yang dikelola: `AmazonMacieFullAccess` kebijakan, kebijakan `AmazonMacieReadOnlyAccess` kebijakan, dan `AmazonMacieServiceRolePolicy` kebijakan.

### Topik

- [Kebijakan terkelola AWS: AmazonMacieFullAccess](#)
- [Kebijakan terkelola AWS: AmazonMacieReadOnlyAccess](#)
- [Kebijakan terkelola AWS: AmazonMacieServiceRolePolicy](#)
- [Amazon Macie memperbarui ke AWS kebijakan terkelola](#)

## Kebijakan terkelola AWS: AmazonMacieFullAccess

Anda dapat melampirkan `AmazonMacieFullAccess` kebijakan untuk entitas IAM Anda.

Kebijakan ini memberikan izin administratif penuh yang memungkinkan identitas IAM (utama) untuk membuat [Peran terkait layanan Amazon Macie](#) dan melakukan semua membaca dan menulis tindakan untuk Amazon Macie. Izin termasuk fungsi mutasi seperti membuat, memperbarui, dan menghapus. Jika kebijakan ini dilampirkan ke prinsipal, prinsipal dapat membuat, mengambil, dan mengakses semua sumber daya, data, dan pengaturan Macie untuk akun mereka.

Kebijakan ini harus dilampirkan pada prinsipal sebelum prinsipal dapat mengaktifkan Macie untuk akun mereka—prinsipal harus diizinkan untuk membuat peran terkait layanan Macie untuk mengaktifkan Macie untuk akun mereka.

### Rincian izin

Kebijakan ini mencakup izin berikut:

- `macie2`- Memungkinkan prinsipal untuk melakukan semua tindakan baca dan tulis untuk Amazon Macie.
- `iam`- Memungkinkan prinsipal untuk membuat peran terkait layanan. Yang `Resource` elemen menentukan peran layanan-linked untuk Macie. Yang `Condition` elemen menggunakan `iam:AWSServiceName` [kunci kondisi](#) dan yang `StringLike` [Operator kondisi](#) untuk membatasi izin ke peran terkait layanan untuk Macie.
- `pricing`- Memungkinkan prinsipal untuk mengambil data harga untuk mereka Akun AWS dari AWS Billing and Cost Management. Macie menggunakan data ini untuk menghitung dan menampilkan perkiraan biaya ketika prinsipal membuat dan mengkonfigurasi pekerjaan penemuan data sensitif.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "macie2:*"
      ]
    }
  ]
}
```

```

    ],
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": "iam:CreateServiceLinkedRole",
    "Resource": "arn:aws:iam::*:role/aws-service-role/macie.amazonaws.com/
AWSServiceRoleForAmazonMacie",
    "Condition": {
      "StringLike": {
        "iam:AWSServiceName": "macie.amazonaws.com"
      }
    }
  },
  {
    "Effect": "Allow",
    "Action": "pricing:GetProducts",
    "Resource": "*"
  }
]
}

```

## Kebijakan terkelola AWS: AmazonMacieReadOnlyAccess

Anda dapat melampirkan `AmazonMacieReadOnlyAccess` kebijakan untuk entitas IAM Anda.

Kebijakan ini memberikan izin hanya-baca yang memungkinkan identitas IAM (utama) untuk melakukan semua tindakan baca untuk Amazon Macie. Izin tidak termasuk fungsi mutasi seperti membuat, memperbarui, atau menghapus. Jika kebijakan ini dilampirkan ke prinsipal, prinsipal dapat mengambil tetapi tidak mengakses semua sumber daya, data, dan pengaturan Macie untuk akun mereka.

### Rincian izin

Kebijakan ini mencakup izin berikut:

`macie2`- Memungkinkan prinsipal untuk melakukan semua tindakan baca untuk Amazon Macie.

```
{
```

```

"Version": "2012-10-17",
"Statement": [
  {
    "Effect": "Allow",
    "Action": [
      "macie2:Describe*",
      "macie2:Get*",
      "macie2:List*",
      "macie2:BatchGetCustomDataIdentifiers",
      "macie2:SearchResources"
    ],
    "Resource": "*"
  }
]
}

```

## Kebijakan terkelola AWS: AmazonMacieServiceRolePolicy

Anda tidak dapat melampirkan `AmazonMacieServiceRolePolicy` kebijakan untuk entitas IAM Anda. Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan Macie melakukan tindakan atas nama Anda. Untuk informasi selengkapnya, lihat [Peran tertaut layanan untuk Amazon Macie](#).

## Amazon Macie memperbarui keAWSkebijakan terkelola

Tinjau detail tentang pembaruanAWSkebijakan terkelola untuk Amazon Macie sejak layanan ini mulai melacak perubahan ini. Untuk peringatan otomatis tentang perubahan pada halaman ini, berlangganan umpan RSS di [Sejarah dokumen Macie](#) halaman.

Perubahan	Deskripsi	Tanggal
<a href="#">AmazonMacieReadOnlyAccess</a> - Menambahkan kebijakan baru	Macie menambahkan kebijakan baru, <code>AmazonMacieReadOnlyAccess</code> kebijakan. Kebijakan ini memberikan izin hanya-baca yang mungkin	15 Juni 2023



Perubahan	Deskripsi	Tanggal
	kan prinsipal mengambil semua sumber daya, data, dan pengaturan Macie untuk akun mereka.	
<a href="#">AmazonMacieFullAccess-</a> Memperbarui kebijakan yang ada	Di dalamAmazonMacieFullAccess kebijakan, Macie memperbarui Amazon Resource Name (ARN) peran terkait layanan Macie (aws-service-role/macie.amazonaws.com/AWSServiceRoleForAmazonMacie ).	30 Juni 2022

Perubahan	Deskripsi	Tanggal
<p><a href="#">AmazonMacieService RolePolicy</a>- Memperbarui kebijakan yang ada</p>	<p>Macie menghapus tindakan dan sumber daya untuk Amazon Macie Classic dariAmazonMacieService RolePolicy kebijakan. Amazon Macie Classic telah dihentikan dan tidak lagi tersedia.</p> <p>Lebih khusus lagi, Macie menghapus semuaAWS CloudTrailtindakan. Macie juga menghapus semua tindakan Amazon S3 untuk sumber daya berikut:<code>arn:aws:s3:::awsmacie-*,arn:aws:s3:::awsma cietrail-*</code> , dan<code>arn:aws:s3:::*-aws macietrail-*</code> .</p>	20 Mei 2022

Perubahan	Deskripsi	Tanggal
<a href="#">AmazonMacieFullAccess</a> - Memperbarui kebijakan yang ada	<p>Macie menambahkan AWS Billing and Cost Management (pricing) tindakan ke AmazonMacieFullAccess kebijakan. Tindakan ini memungkinkan prinsipal untuk mengambil data harga untuk akun mereka. Macie menggunakan data ini untuk menghitung dan menampilkan perkiraan biaya ketika prinsipal membuat dan mengkonfigurasi pekerjaan penemuan data sensitif.</p> <p>Macie juga menghapus Amazon Macie Classic (macie) tindakan dari AmazonMacieFullAccess kebijakan.</p>	7 Maret 2022
<a href="#">AmazonMacieServiceRolePolicy</a> - Memperbarui kebijakan yang ada	<p>Macie menambahkan AmazonCloudWatchLog tindakan ke AmazonMacieServiceRolePolicy kebijakan. Tindakan ini memungkinkan Macie untuk mempublikasikan peristiwa logCloudWatchLog untuk pekerjaan penemuan data sensitif.</p>	13 April, 2021
Macie mulai melacak perubahan	Macie mulai melacak perubahan untuk kebijakan terkelola AWS.	13 April, 2021

## Pemecahan Amazon Macie dan Kesalahan

Informasi berikut dapat membantu Anda mendiagnosis dan mengatasi masalah umum yang mungkin Anda temui saat bekerja menggunakan Amazon Macie dan AWS Identity and Access Management (IAM).

### Topik

- [Saya tidak diotorisasi untuk melakukan tindakan di Amazon Macie](#)
- [Saya ingin mengizinkan orang di luar saya Akun AWS untuk Amazon Macie saya](#)

### Saya tidak diotorisasi untuk melakukan tindakan di Amazon Macie

Jika Anda menerima kesalahan bahwa Anda tidak terotorisasi untuk melakukan tindakan.

Contoh kesalahan berikut terjadi ketika pengguna `mateojackson` IAM mencoba menggunakan konsol tersebut untuk melihat detail tentang suatu `my-example-widget` sumber daya fiktif, tetapi tidak memiliki izin `macie2:GetWidget`.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
macie2:GetWidget on resource: my-example-widget
```

Dalam hal ini, kebijakan untuk `mateojackson` pengguna harus diperbarui untuk memungkinkan akses ke `my-example-widget` sumber daya dengan menggunakan `macie2:GetWidget` tindakan.

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

### Saya ingin mengizinkan orang di luar saya Akun AWS untuk Amazon Macie 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 pada orang ke sumber daya Anda.

Untuk mempelajari selengkapnya, periksa hal berikut:

- Untuk mempelajari apakah Macie mendukung fitur-fitur ini, lihat [Bagaimana Amazon Macie bekerja dengan AWS Identity and Access Management](#).

- Untuk mempelajari cara memberikan akses ke sumber daya di seluruh Akun AWS yang Anda miliki, lihat [Menyediakan akses ke pengguna IAM di akun Akun AWS lain yang Anda miliki](#) dalam Panduan Pengguna IAM.
- Untuk mempelajari cara memberikan akses ke sumber daya Anda ke Akun AWS pihak ketiga, lihat [Menyediakan akses ke akun Akun AWS yang dimiliki oleh pihak ketiga](#) dalam Panduan Pengguna IAM.
- Untuk mempelajari cara memberikan akses melalui federasi identitas, lihat [Menyediakan akses ke pengguna terautentikasi eksternal \(gabungan identitas\)](#) dalam Panduan Pengguna IAM .
- Untuk mempelajari perbedaan antara penggunaan peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat [Perbedaan IAM role dan kebijakan berbasis sumber daya](#) di Panduan Pengguna IAM.

## Pencatatan dan pemantauan di Amazon Macie

Amazon Macie terintegrasi dengan AWS CloudTrail, layanan yang menyediakan catatan tindakan yang diambil dalam Macie oleh pengguna, peran, atau peran, atau tindakan Layanan AWS. Hal ini mencakup tindakan dari konsol Amazon Macie dan panggilan program untuk operasi Amazon Macie API. Dengan menggunakan informasi yang dikumpulkan oleh CloudTrail, Anda dapat menentukan permintaan yang dibuat untuk Macie. Untuk setiap permintaan, Anda dapat mengidentifikasi waktu permintaan itu dibuat, tempat alamat IP itu dibuat, siapa yang membuat permintaan, dan detail tambahan lainnya. Untuk informasi selengkapnya, lihat [Mencatat panggilan API Amazon Macie menggunakan AWS CloudTrail](#).


## Validasi Kepatuhan untuk Amazon Macie

Untuk mempelajari apakah an Layanan AWS berada dalam lingkup program kepatuhan khusus, lihat [Layanan AWS di Scope oleh Program](#) Program Kepatuhan yang Anda minati. Untuk informasi umum, silakan lihat [Program Kepatuhan AWS](#) .

Anda bisa 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, serta hukum dan peraturan yang berlaku. AWS menyediakan sumber daya berikut untuk membantu kepatuhan:

- [Panduan Quick Start Keamanan dan Kepatuhan](#) – Panduan Quick Start Keamanan dan Kepatuhan – Panduan deployment ini membahas pertimbangan arsitektur dan menyediakan langkah-langkah untuk melakukan deployment terhadap lingkungan dasar di AWS yang menjadi fokus keamanan dan kepatuhan.
- [Merancang Keamanan dan Kepatuhan HIPAA di Amazon Web Services](#) – Laporan resmi ini menjelaskan cara perusahaan dapat menggunakan AWS untuk membuat aplikasi yang memenuhi syarat HIPAA.

 Note

Tidak semua Layanan AWS memenuhi syarat HIPAA. Untuk informasi selengkapnya, lihat [Referensi Layanan yang Memenuhi Syarat HIPAA](#).

- [Sumber Daya Kepatuhan AWS](#) – Kumpulan buku kerja dan panduan ini mungkin berlaku untuk industri dan lokasi Anda.
- [Panduan Kepatuhan Pelanggan AWS](#) – Pahami model tanggung jawab bersama melalui lensa kepatuhan. Panduan ini merangkum praktik terbaik untuk mengamankan Layanan AWS dan memetakan panduan kontrol keamanan di banyak kerangka kerja (termasuk National Institute of Standards and Technology (NIST), Dewan Standar Keamanan Industri Kartu Pembayaran (PCI), dan Organisasi Internasional untuk Standardisasi (ISO)).
- [Mengevaluasi Sumber Daya dengan Aturan](#) di Panduan Developer AWS Config – Layanan AWS Config menilai seberapa baik konfigurasi sumber daya Anda dalam mematuhi praktik-praktik internal, pedoman industri, dan regulasi internal.
- [AWS Security Hub](#) – Layanan AWS ini memberikan pandangan komprehensif tentang status keamanan Anda di dalam AWS. Security Hub menggunakan kontrol keamanan untuk sumber daya AWS Anda dan untuk memeriksa kepatuhan terhadap standar industri keamanan dan praktik terbaik. Untuk daftar layanan dan kontrol yang didukung, lihat [Referensi kontrol Security Hub](#).
- [AWS Audit Manager](#) – Layanan AWS ini akan membantu Anda untuk terus-menerus mengaudit penggunaan AWS untuk menyederhanakan bagaimana Anda mengelola risiko dan kepatuhan terhadap regulasi dan standar industri.

## Ketahanan di Amazon Macie

Infrastruktur AWS global dibangun di sekitar Wilayah AWS dan Availability Zone. Wilayah memberikan beberapa Zona Ketersediaan yang terpisah dan terisolasi secara fisik, yang terkoneksi melalui jaringan latensi rendah, throughput tinggi, dan sangat redundan. Dengan Zona Ketersediaan, Anda

dapat merancang serta mengoperasikan aplikasi dan basis data yang secara otomatis melakukan fail over di antara zona tanpa gangguan. Availability Zone memiliki ketersediaan yang lebih baik, toleran terhadap kegagalan, dan dapat diukur skalanya jika dibandingkan dengan satu atau beberapa infrastruktur pusat data tradisional.

Untuk informasi selengkapnya tentang Wilayah AWS dan Availability Zone, lihat [Infrastruktur Global AWS](#).

## Keamanan infrastruktur di Amazon Macie

Sebagai layanan terkelola, Amazon Macie dilindungi oleh keamanan jaringan AWS global. Untuk informasi tentang layanan AWS keamanan dan cara AWS melindungi infrastruktur, lihat [Keamanan AWS Cloud](#). Untuk merancang AWS lingkungan Anda menggunakan praktik terbaik untuk keamanan infrastruktur, lihat [Perlindungan](#) Infrastruktur dalam Kerangka Kerja Pilar Keamanan yang AWS Diarsiteksikan dengan Baik.

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

- Transport Layer Security (TLS). Kami membutuhkan TLS 1.2 dan merekomendasikan TLS 1.3.
- Suite cipher dengan kerahasiaan maju sempurna (PFS) seperti DHE (Ephemeral Diffie-Hellman) atau ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Sebagian besar sistem modern seperti Java 7 dan sistem yang lebih baru mendukung mode ini.

Selain itu, permintaan harus ditandatangani menggunakan access key ID dan secret access key yang terkait dengan principal IAM. Atau Anda bisa menggunakan [AWS Security Token Service](#) (AWS STS) untuk membuat kredensial keamanan sementara guna menandatangani permintaan.

## Amazon Macie dan titik akhir VPC antarmuka () AWS PrivateLink

Jika Anda menggunakan Amazon Virtual Private Cloud (Amazon VPC) untuk meng-host AWS sumber daya Anda, Anda dapat membuat koneksi pribadi antara VPC dan Amazon Macie. Amazon VPC adalah Layanan AWS yang dapat Anda gunakan untuk meluncurkan AWS sumber daya di jaringan virtual yang Anda tentukan. Dengan VPC, Anda memiliki kendali terhadap pengaturan jaringan, seperti rentang alamat IP, subnet, tabel rute, dan gateway jaringan.

Untuk menghubungkan VPC Anda ke Macie, Anda membuat antarmuka VPC endpoint untuk Macie. Titik akhir antarmuka didukung oleh [AWS PrivateLink](#), teknologi yang memungkinkan Anda

mengakses API Amazon Macie secara pribadi tanpa gateway internet, perangkat NAT, koneksi VPN, atau koneksi. AWS Direct Connect Instans di VPC Anda tidak memerlukan alamat IP publik untuk berkomunikasi dengan Amazon Macie API. Lalu lintas antara VPC dan Macie Anda tidak meninggalkan jaringan Amazon.

Setiap titik akhir antarmuka diwakili oleh satu atau lebih [antarmuka jaringan elastis](#) dalam subnet Anda. Untuk informasi selengkapnya, lihat [Mengakses titik akhir VPC antarmuka Layanan AWS menggunakan antarmuka di Panduan](#) Pengguna Amazon VPC.

Topik

- [Pertimbangan untuk titik akhir Amazon Macie VPC](#)
- [Membuat titik akhir VPC antarmuka untuk Amazon Macie](#)

## Pertimbangan untuk titik akhir Amazon Macie VPC

Amazon Macie mendukung titik akhir VPC di semua Wilayah AWS tempat yang tersedia saat ini kecuali Wilayah Asia Pasifik (Osaka) dan Israel (Tel Aviv). Untuk daftar Wilayah di mana Macie saat ini tersedia, lihat [titik akhir dan kuota Amazon Macie](#) di. Referensi Umum AWS Selain itu, Macie mendukung panggilan ke semua tindakan API-nya dari VPC.

Jika Anda membuat titik akhir VPC antarmuka untuk Macie, pertimbangkan untuk melakukan hal yang sama untuk yang lain yang Layanan AWS menyediakan dukungan VPC dan berintegrasi dengan Macie, seperti Amazon dan. EventBridge AWS Security Hub Macie dan layanan tersebut kemudian dapat menggunakan titik akhir VPC untuk integrasi. Misalnya, jika Anda membuat titik akhir VPC untuk Macie dan titik akhir VPC untuk Security Hub, Macie dapat menggunakan titik akhir VPC saat mempublikasikan temuan ke Security Hub dan Security Hub dapat menggunakan titik akhir VPC-nya saat menerima temuan. Untuk informasi tentang layanan yang mendukung titik akhir VPC, lihat [Layanan AWS yang terintegrasi dengan AWS PrivateLink](#) dalam Panduan Pengguna Amazon VPC.

Untuk pertimbangan tambahan, lihat [Mengakses titik akhir VPC antarmuka Layanan AWS menggunakan antarmuka di Panduan](#) Pengguna Amazon VPC.

Perhatikan bahwa kebijakan titik akhir VPC tidak didukung untuk Macie. Secara default, akses penuh ke Macie diizinkan melalui titik akhir. Untuk informasi selengkapnya, lihat [Manajemen identitas dan akses untuk titik akhir VPC dan layanan titik akhir VPC di Panduan Pengguna](#) Amazon VPC.



## Membuat titik akhir VPC antarmuka untuk Amazon Macie

Anda dapat membuat titik akhir VPC antarmuka untuk layanan Amazon Macie dengan menggunakan konsol Amazon VPC atau (). AWS Command Line Interface AWS CLI Untuk informasi selengkapnya, lihat [Membuat titik akhir VPC di Panduan Pengguna Amazon VPC](#).

Saat Anda membuat titik akhir VPC untuk Macie, gunakan nama layanan berikut:

- `com.amazonaws.wilayah.macie2`

Dimana *wilayah* adalah kode Wilayah untuk yang berlaku Wilayah AWS.

Jika Anda mengaktifkan DNS pribadi untuk titik akhir, Anda dapat membuat permintaan API ke Macie menggunakan nama DNS default untuk Wilayah, misalnya, `macie2.us-east-1.amazonaws.com` untuk Wilayah AS Timur (Virginia N.).

Untuk informasi selengkapnya, lihat [Mengakses titik akhir VPC antarmuka Layanan AWS menggunakan antarmuka di Panduan Pengguna Amazon VPC](#).

# Mencatat panggilan API Amazon Macie menggunakan AWS CloudTrail

Amazon Macie terintegrasi dengan AWS CloudTrail, yang merupakan layanan yang menyediakan catatan tindakan yang diambil di Macie oleh pengguna, peran, atau lainnya. Layanan AWS CloudTrail menangkap semua panggilan API untuk Macie sebagai acara. Panggilan yang diambil termasuk panggilan dari konsol Amazon Macie dan panggilan terprogram ke operasi Amazon Macie API.

Jika Anda membuat jejak, Anda dapat mengaktifkan pengiriman CloudTrail acara secara terus menerus ke bucket Amazon Simple Storage Service (Amazon S3), termasuk peristiwa untuk Macie. Jika Anda tidak mengonfigurasi jejak, Anda masih dapat meninjau peristiwa terbaru dengan menggunakan riwayat Acara di AWS CloudTrail konsol. Dengan menggunakan informasi yang dikumpulkan oleh CloudTrail, Anda dapat menentukan permintaan yang dibuat untuk Macie, alamat IP dari mana permintaan itu dibuat, siapa yang membuat permintaan, kapan dibuat, dan detail tambahan.

Untuk mempelajari selengkapnya CloudTrail, lihat [Panduan AWS CloudTrail Pengguna](#).

## Topik

- [Informasi Amazon Macie di AWS CloudTrail](#)
- [Memahami entri file log Amazon Macie](#)

## Informasi Amazon Macie di AWS CloudTrail

AWS CloudTrail diaktifkan untuk Anda Akun AWS saat Anda membuat akun. Ketika aktivitas terjadi di Amazon Macie, aktivitas tersebut direkam dalam suatu CloudTrail peristiwa bersama dengan AWS peristiwa lain dalam riwayat Acara. Anda dapat meninjau, mencari, dan mengunduh acara terbaru di situs Anda Akun AWS. Untuk informasi selengkapnya, lihat [Bekerja dengan riwayat CloudTrail Acara](#) di Panduan AWS CloudTrail Pengguna.

Untuk catatan acara yang sedang berlangsung di Anda Akun AWS, termasuk acara untuk Macie, buat jejak. Jejak memungkinkan CloudTrail untuk mengirimkan file log ke bucket Amazon Simple Storage Service (Amazon S3). Secara default, saat Anda membuat jejak dengan menggunakan AWS CloudTrail konsol, jejak berlaku untuk semua Wilayah AWS. Jejak mencatat peristiwa dari semua

Wilayah di partisi AWS dan mengirimkan file log ke bucket 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 lebih lanjut, lihat topik berikut di Panduan Pengguna AWS CloudTrail:

- [Membuat jejak untuk Akun AWS Anda](#)
- [CloudTrail layanan dan integrasi yang didukung](#)
- [Mengonfigurasi notifikasi Amazon SNS untuk CloudTrail](#)
- [Menerima file CloudTrail log dari beberapa Wilayah](#)
- [Menerima file CloudTrail log dari beberapa akun](#)

Semua tindakan Macie dicatat oleh CloudTrail dan didokumentasikan dalam Referensi API [Amazon Macie](#). Misalnya, panggilan ke `CreateClassificationJob`, `DescribeBuckets`, dan `ListFindings` tindakan menghasilkan entri dalam file CloudTrail log.

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

- Apakah permintaan tersebut dibuat dengan kredensial root atau pengguna AWS Identity and Access Management IAM.
- Apakah permintaan tersebut dibuat dengan kredensial keamanan sementara untuk satu peran atau pengguna gabungan.
- Apakah permintaan tersebut dibuat oleh Layanan AWS lain.

Untuk informasi selengkapnya, lihat [elemen CloudTrail UserIdentity](#) di AWS CloudTrailPanduan Pengguna.

## Memahami entri file log Amazon Macie

Trail adalah konfigurasi yang memungkinkan pengiriman peristiwa sebagai file log ke bucket Amazon Simple Storage Service (Amazon S3) yang Anda tentukan. Peristiwa mewakili permintaan tunggal dari sumber manapun dan mencakup informasi tentang tindakan yang diminta, tanggal dan waktu tindakan, parameter permintaan, dan sebagainya. AWS CloudTrailfile log berisi satu atau lebih entri log untuk acara. 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 peristiwa untuk tindakan Amazon Macie. Untuk detail tentang informasi yang mungkin berisi entri log, lihat [referensi peristiwa CloudTrail log](#) di Panduan AWS CloudTrail Pengguna.

Contoh: Daftar temuan

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan peristiwa untuk tindakan Macie [ListFindings](#). Dalam contoh ini, pengguna AWS Identity and Access Management (IAM) (Mary\_Major) menggunakan konsol Amazon Macie untuk mengambil subset informasi tentang temuan kebijakan saat ini untuk akun mereka.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:user/Mary_Major",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "userName": "Mary_Major",
    "sessionContext": {
      "attributes": {
        "creationdate": "2023-11-14T15:49:57Z",
        "mfaAuthenticated": "false"
      }
    }
  },
  "eventTime": "2023-11-14T16:09:56Z",
  "eventSource": "macie2.amazonaws.com",
  "eventName": "ListFindings",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "198.51.100.1",
  "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/119.0.0.0 Safari/537.36",
  "requestParameters": {
    "sortCriteria": {
      "attributeName": "updatedAt",
      "orderBy": "DESC"
    }
  },
  "findingCriteria": {
    "criterion": {
      "archived": {
        "eq": [
```

```

        "false"
      ]
    },
    "category": {
      "eq": [
        "POLICY"
      ]
    }
  }
},
"maxResults": 25,
"nextToken": ""
},
"responseElements": null,
"requestID": "d58af6be-1115-4a41-91f8-ace03example",
"eventID": "ad97fac5-f7cf-4ff9-9cf2-d0676example",
"readOnly": true,
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "123456789012",
"eventCategory": "Management"
}

```

Contoh: Mengambil sampel data sensitif untuk temuan

Contoh ini menunjukkan entri CloudTrail log yang menunjukkan peristiwa untuk mengambil dan mengungkapkan sampel data sensitif yang dilaporkan Macie dalam sebuah temuan. Dalam contoh ini, pengguna IAM (JohnDoe) menggunakan konsol Amazon Macie untuk mengambil dan mengungkapkan sampel data sensitif. Akun Macie pengguna dikonfigurasi untuk mengambil peran IAM (MacieReveal) untuk mengambil dan mengungkapkan sampel data sensitif.

Peristiwa log berikut menunjukkan detail tentang permintaan pengguna untuk mengambil dan mengungkapkan sampel data sensitif dengan melakukan tindakan Macie [GetSensitiveDataOccurrences](#).

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "UU4MH70YK5ZCOAEXAMPLE:JohnDoe",
    "arn": "arn:aws:sts::111122223333:assumed-role/Admin/JohnDoe",
    "accountId": "111122223333",

```

```

    "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "UU4MH70YK5ZCOAEXAMPLE",
        "arn": "arn:aws:iam::111122223333:role/Admin",
        "accountId": "111122223333",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "creationDate": "2023-12-12T14:40:23Z",
        "mfaAuthenticated": "false"
      }
    }
  },
  "eventTime": "2023-12-12T17:04:47Z",
  "eventSource": "macie2.amazonaws.com",
  "eventName": "GetSensitiveDataOccurrences",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "198.51.100.252",
  "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/119.0.0.0 Safari/537.36",
  "requestParameters": {
    "findingId": "3ad9d8cd61c5c390bede45cd2example"
  },
  "responseElements": null,
  "requestID": "c30cb760-5102-47e7-88d8-ff2e8example",
  "eventID": "baf52d92-f9c3-431a-bfe8-71c81example",
  "readOnly": true,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "111122223333",
  "eventCategory": "Management"
}

```

Peristiwa log berikutnya menunjukkan detail tentang Macie kemudian mengasumsikan peran IAM (MacieReveal) yang ditentukan dengan melakukan tindakan AWS Security Token Service (AWS STS). [AssumeRole](#)

```

{
  "eventVersion": "1.08",
  "userIdentity": {

```

```

    "type": "AWSService",
    "invokedBy": "reveal-samples.macie.amazonaws.com"
  },
  "eventTime": "2023-12-12T17:04:47Z",
  "eventSource": "sts.amazonaws.com",
  "eventName": "AssumeRole",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "reveal-samples.macie.amazonaws.com",
  "userAgent": "reveal-samples.macie.amazonaws.com",
  "requestParameters": {
    "roleArn": "arn:aws:iam::111122223333:role/MacieReveal",
    "roleSessionName": "RevealCrossAccount"
  },
  "responseElements": {
    "credentials": {
      "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
      "sessionToken": "XXYYaz...
EXAMPLE_SESSION_TOKEN
XXyYaZAz",
      "expiration": "Dec 12, 2023, 6:04:47 PM"
    },
    "assumedRoleUser": {
      "assumedRoleId": "AROAX0TKAROCSEXAMPLE:RevealCrossAccount",
      "arn": "arn:aws:sts::111122223333:assumed-role/MacieReveal/
RevealCrossAccount"
    }
  },
  "requestID": "d905cea8-2dcb-44c1-948e-19419example",
  "eventID": "74ee4d0c-932d-3332-87aa-8bcf3example",
  "readOnly": true,
  "resources": [
    {
      "accountId": "111122223333",
      "type": "AWS::IAM::Role",
      "ARN": "arn:aws:iam::111122223333:role/MacieReveal"
    }
  ],
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "111122223333",
  "eventCategory": "Management"
}

```

# Menandai sumber daya Amazon Macie

Tag adalah label opsional yang dapat Anda tentukan dan tetapkan ke AWS sumber daya, termasuk jenis sumber daya Amazon Macie tertentu. Tag dapat membantu Anda mengidentifikasi, mengkategorikan, dan mengelola sumber daya dengan cara yang berbeda, seperti dengan tujuan, pemilik, lingkungan, atau kriteria lainnya. Misalnya, Anda dapat menggunakan tag untuk menerapkan kebijakan, mengalokasikan biaya, membedakan antara versi sumber daya, atau mengidentifikasi sumber daya yang mendukung persyaratan kepatuhan atau alur kerja tertentu.

Anda dapat menetapkan tag ke jenis sumber daya Macie berikut: daftar izinkan, pengidentifikasi data kustom, aturan filter, dan aturan penindasan untuk temuan, serta pekerjaan penemuan data sensitif. Jika Anda adalah administrator Macie untuk organisasi, Anda juga dapat menetapkan tag ke akun anggota di organisasi Anda.

## Topik

- [Dasar-dasar penandaan](#)
- [Menggunakan tag dalam kebijakan IAM](#)
- [Menambahkan tag ke sumber daya Amazon Macie](#)
- [Meninjau tag untuk sumber daya Amazon Macie](#)
- [Mengedit tag untuk sumber daya Amazon Macie](#)
- [Menghapus tag dari sumber daya Amazon Macie](#)

## Dasar-dasar penandaan

Sumber daya dapat memiliki sebanyak 50 tag. Setiap tag terdiri dari kunci tag yang diperlukan dan nilai tag opsional, yang keduanya Anda tentukan. Kunci tag adalah label umum yang bertindak sebagai kategori untuk nilai tag yang lebih spesifik. Nilai tag bertindak sebagai deskriptor untuk kunci tag.


Misalnya, jika Anda membuat pengidentifikasi data kustom dan pekerjaan penemuan data sensitif untuk menganalisis data pada titik berbeda dalam alur kerja (satu set untuk data bertahap dan satu lagi untuk data produksi), Anda dapat menetapkan kunci Stack tag ke sumber daya tersebut. Nilai tag untuk kunci tag ini mungkin Staging untuk pengidentifikasi data kustom dan pekerjaan yang dirancang untuk menganalisis data bertahap, dan Production untuk yang lainnya.



Saat Anda menentukan dan menetapkan tag ke sumber daya, ingatlah hal berikut:

- Setiap sumber daya dapat memiliki maksimum 50 tag.
- Untuk setiap sumber daya, setiap kunci tag harus unik dan hanya dapat memiliki satu nilai tag.
- Kunci dan nilai tag peka huruf besar dan kecil. Sebagai praktik terbaik, kami menyarankan Anda menentukan strategi untuk memanfaatkan tag dan menerapkan strategi tersebut secara konsisten di seluruh sumber daya Anda.
- Kunci tag dapat memiliki maksimum 128 karakter UTF-8. Nilai tag dapat memiliki maksimal 256 karakter UTF-8. Karakter dapat berupa huruf, angka, spasi, atau simbol berikut: `_./= + - @`
- `aws` :Awalan dicadangkan untuk digunakan olehAWS. Anda tidak dapat menggunakannya dalam kunci tag atau nilai apa pun yang Anda tentukan. Selain itu, Anda tidak dapat mengubah atau menghapus kunci tag atau nilai yang menggunakan awalan ini. Tag yang menggunakan awalan ini tidak dihitung terhadap kuota 50 tag per sumber daya.
- Setiap tag yang Anda tetapkan hanya tersedia untuk Anda Akun AWS dan hanya Wilayah AWS di tempat Anda menetapkannya.
- Jika Anda menghapus sumber daya, tag apa pun yang ditetapkan ke sumber daya juga akan dihapus.

Untuk pembatasan, tips, dan praktik terbaik tambahan, lihat [Panduan Pengguna Tagging AWS Resources](#).

 Important

Jangan menyimpan data rahasia atau jenis data sensitif lainnya dalam tag. Tag dapat diakses dari banyak orangLayanan AWS, termasukAWS Billing and Cost Management. Mereka tidak dimaksudkan untuk digunakan untuk data sensitif.

Untuk menambahkan dan mengelola tag untuk sumber daya Macie, Anda dapat menggunakan konsol Amazon Macie, Amazon Macie API, Editor Tag di AWS Resource Groups konsol, atau API AWS Resource Groups Penandaan. Dengan Macie, Anda dapat menambahkan tag ke sumber daya saat membuat sumber daya. Anda juga dapat menambahkan dan mengelola tag untuk sumber daya individu yang ada. Dengan Grup Sumber Daya, Anda dapat menambahkan dan mengelola tag secara massal untuk beberapa sumber daya yang ada yang mencakup beberapaLayanan AWS, termasuk Macie. Untuk informasi selengkapnya, lihat [Panduan Pengguna Tagging AWS Resources](#).

## Menggunakan tag dalam kebijakan IAM

Setelah mulai memberi tag pada sumber daya, Anda dapat menentukan izin tingkat sumber daya berbasis tag dalam AWS Identity and Access Management kebijakan (IAM). Dengan menggunakan tag dengan cara ini, Anda dapat menerapkan kontrol terperinci yang pengguna dan peran dalam izin Anda Akun AWS untuk membuat dan menandai sumber daya, dan pengguna dan peran mana yang memiliki izin untuk menambah, mengedit, dan menghapus tag secara lebih umum. Untuk mengontrol akses berdasarkan tag, Anda dapat menggunakan [kunci kondisi terkait tag](#) di [elemen Kondisi kebijakan IAM](#).

Misalnya, Anda dapat membuat kebijakan yang memungkinkan pengguna memiliki akses penuh ke semua sumber daya Amazon Macie, jika Owner tag untuk sumber daya menentukan nama pengguna mereka:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ModifyResourceIfOwner",
      "Effect": "Allow",
      "Action": "macie2:*",
      "Resource": "*",
      "Condition": {
        "StringEqualsIgnoreCase": {"aws:ResourceTag/Owner": "${aws:username}"}
      }
    }
  ]
}
```

Jika Anda menentukan izin berbasis tag, tingkat sumber daya, izin akan segera berlaku. Ini berarti bahwa sumber daya Anda lebih aman segera setelah dibuat, dan Anda dapat dengan cepat mulai menerapkan penggunaan tag untuk sumber daya baru. Anda juga dapat menggunakan izin tingkat sumber daya untuk mengontrol kunci dan nilai tag mana yang dapat dikaitkan dengan sumber daya baru dan yang sudah ada. Untuk informasi selengkapnya, lihat [Mengontrol akses ke AWS sumber daya menggunakan tag](#) di Panduan Pengguna IAM.

# Menambahkan tag ke sumber daya Amazon Macie

Untuk menambahkan tag ke sumber daya Amazon Macie individual, Anda dapat menggunakan konsol Amazon Macie atau Amazon Macie API. Untuk menambahkan tag ke beberapa sumber daya Macie secara bersamaan, gunakan [Editor Tag](#) di AWS Resource Groups konsol atau operasi penandaan API [AWS Resource Groups Tagging](#).

## Important

Menambahkan tag ke sumber daya dapat memengaruhi akses ke sumber daya. Sebelum menambahkan tag ke sumber daya, tinjau kebijakan AWS Identity and Access Management (IAM) apa pun yang mungkin menggunakan tag untuk mengontrol akses ke sumber daya.

## Console

Saat Anda membuat daftar izinkan, pengidentifikasi data kustom, atau pekerjaan penemuan data sensitif, konsol Amazon Macie menyediakan opsi untuk menambahkan tag ke sumber daya. Ikuti petunjuk di konsol untuk menambahkan tag ke jenis sumber daya ini saat Anda membuat sumber daya. Untuk menambahkan tag ke aturan filter atau penindasan atau akun anggota di organisasi, Anda harus membuat sumber daya sebelum dapat menambahkan tag ke dalamnya.

Untuk menambahkan satu atau beberapa tag ke sumber daya yang ada dengan menggunakan konsol Amazon Macie, ikuti langkah-langkah ini.

### Menambahkan tag ke sumber daya

1. Buka konsol Amazon Macie di <https://console.aws.amazon.com/macie/>.
2. Bergantung pada jenis sumber daya yang ingin Anda tambahkan tag, lakukan salah satu hal berikut:

- Untuk daftar izinkan, pilih Izinkan daftar di panel navigasi.

Kemudian, di tabel, pilih kotak centang untuk daftar. Kemudian pilih Kelola tag pada menu Tindakan.

- Untuk pengenalan data kustom, pilih Pengidentifikasi data khusus di panel navigasi.

Kemudian, di tabel, pilih kotak centang untuk pengidentifikasi data kustom. Kemudian pilih Kelola tag pada menu Tindakan.

- Untuk aturan filter atau penindasan, pilih Temuan di panel navigasi.

Kemudian, dalam daftar Aturan tersimpan, pilih ikon edit



di sebelah aturan. Lalu pilih Kelola tag.

- Untuk akun anggota di organisasi Anda, pilih Akun di panel navigasi.

Kemudian, di tabel, pilih kotak centang untuk akun tersebut. Kemudian pilih Kelola tag pada menu Tindakan.

- Untuk pekerjaan penemuan data sensitif, pilih Pekerjaan di panel navigasi.

Kemudian, di tabel, pilih kotak centang untuk pekerjaan itu. Kemudian pilih Kelola tag pada menu Tindakan.

Jendela Manage tags mencantumkan semua tag yang saat ini ditetapkan ke sumber daya.

3. Di jendela Kelola tag, pilih Edit tag.
4. Pilih Tambahkan tanda.
5. Di kotak Key, masukkan kunci tag untuk tag yang akan ditambahkan ke sumber daya. Kemudian, di kotak Nilai, opsional masukkan nilai tag untuk kunci.

Kunci tag dapat berisi sebanyak 128 karakter. Nilai tag dapat berisi sebanyak 256 karakter. Karakter dapat berupa huruf, angka, spasi, atau simbol berikut: `_.:/= + - @`

6. (Opsional) Untuk menambahkan tag lain ke sumber daya, pilih Tambahkan tag, lalu ulangi langkah sebelumnya. Anda dapat menetapkan sebanyak 50 tag ke sumber daya.
7. Setelah selesai menambahkan tag, pilih Simpan.

## API

Untuk membuat sumber daya dan menambahkan satu atau lebih tag ke dalamnya secara terprogram, gunakan `Create` operasi yang sesuai untuk jenis sumber daya yang ingin Anda buat:

- Izinkan daftar - Gunakan [CreateAllowList](#) operasi atau, jika Anda menggunakan AWS Command Line Interface (AWS CLI), jalankan [create-allow-list](#) perintah.
- Pengenal data kustom - Gunakan [CreateCustomDataIdentifier](#) operasi atau, jika Anda menggunakan AWS CLI, jalankan [create-custom-data-identifier](#) perintah.

- Aturan filter atau penindasan - Gunakan [CreateFindingsFilter](#) operasi atau, jika Anda menggunakan AWS CLI, jalankan [create-findings-filter](#) perintah.
- Akun anggota - Gunakan [CreateMember](#) operasi atau, jika Anda menggunakan AWS CLI, jalankan perintah [create-member](#).
- Pekerjaan penemuan data sensitif - Gunakan [CreateClassificationJob](#) operasi atau, jika Anda menggunakan AWS CLI, jalankan [create-classification-job](#) perintah.

Dalam permintaan Anda, gunakan `tags` parameter untuk menentukan kunci tag (`key`) dan nilai tag opsional (`value`) untuk setiap tag yang akan ditambahkan ke sumber daya. `tagsParameter` menentukan string-to-string peta kunci tag dan nilai tag yang terkait.

Untuk menambahkan satu atau beberapa tag ke sumber daya yang ada, gunakan [TagResource](#) pengoperasian Amazon Macie API atau, jika Anda menggunakan AWS CLI, jalankan perintah [tag-resource](#). Dalam permintaan Anda, tentukan Amazon Resource Name (ARN) sumber daya yang ingin Anda tambahkan tag. Gunakan `tags` parameter untuk menentukan kunci tag (`key`) dan nilai tag opsional (`value`) untuk setiap tag yang akan ditambahkan ke sumber daya. Seperti halnya `Create` operasi dan perintah, `tags` parameter menentukan string-to-string peta kunci tag dan nilai tag yang terkait.

Misalnya, AWS CLI perintah berikut menambahkan kunci Stack tag dengan nilai Production tag ke pekerjaan yang ditentukan. Contoh ini diformat untuk Microsoft Windows dan menggunakan karakter kelanjutan garis sisipan (^) untuk meningkatkan keterbacaan.

```
C:\> aws macie2 tag-resource ^
--resource-arn arn:aws:macie2:us-east-1:123456789012:classification-
job/3ce05dbb7ec5505def334104bexample ^
--tags={"Stack":"Production"}
```

Dengan:

- `resource-arn` menentukan ARN pekerjaan untuk menambahkan tag ke.
- `Stack` adalah kunci tag tag untuk ditambahkan ke pekerjaan.
- `Production` adalah nilai tag untuk kunci tag tertentu (`Stack`).

Pada contoh berikut, perintah menambahkan beberapa tag ke pekerjaan:

```
C:\> aws macie2 tag-resource ^
```

```
--resource-arn arn:aws:macie2:us-east-1:123456789012:classification-  
job/3ce05dbb7ec5505def334104bexample ^  
--tags={\"Stack\":\"Production\",\"CostCenter\":\"12345\",\"Owner\":\"jane-doe\"}
```

Untuk setiap tag di tags peta, diperlukan value argumen key dan argumen. Namun, nilai untuk value argumen dapat berupa string kosong. Jika Anda tidak ingin mengaitkan nilai tag dengan kunci tag, jangan tentukan nilai untuk value argumen. Misalnya, AWS CLI perintah berikut menambahkan kunci Owner tag tanpa nilai tag terkait:

```
C:\> aws macie2 tag-resource ^  
--resource-arn arn:aws:macie2:us-east-1:123456789012:classification-  
job/3ce05dbb7ec5505def334104bexample ^  
--tags={\"Owner\":\"\"}
```

Jika operasi penandaan berhasil, Macie mengembalikan respons HTTP 204 kosong. Jika tidak, Macie mengembalikan HTTP 4 xx atau respon 500 yang menunjukkan mengapa operasi gagal.

## Meninjau tag untuk sumber daya Amazon Macie

Anda dapat meninjau tag (baik kunci tag dan nilai tag) untuk sumber daya Amazon Macie dengan menggunakan konsol Amazon Macie atau Amazon Macie API. Jika Anda lebih suka melakukan ini untuk beberapa sumber daya Macie secara bersamaan, Anda dapat menggunakan [Editor Tag](#) di AWS Resource Groups konsol atau operasi penandaan API [AWS Resource Groups Tagging](#).

### Console

Ikuti langkah-langkah berikut untuk meninjau tag sumber daya dengan menggunakan konsol Amazon Macie.

Untuk meninjau tag untuk sumber daya

1. Buka konsol Amazon Macie di <https://console.aws.amazon.com/macie/>.
2. Bergantung pada jenis sumber daya yang tagnya ingin Anda tinjau, lakukan salah satu hal berikut:
  - Untuk daftar izinkan, pilih Izinkan daftar di panel navigasi.

Kemudian, di tabel, pilih kotak centang untuk daftar. Kemudian pilih Kelola tag pada menu Tindakan.

- Untuk pengenalan data kustom, pilih Pengidentifikasi data khusus di panel navigasi.

Kemudian, di tabel, pilih kotak centang untuk pengidentifikasi data kustom. Kemudian pilih Kelola tag pada menu Tindakan.

- Untuk aturan filter atau penindasan, pilih Temuan di panel navigasi.

Kemudian, dalam daftar Aturan tersimpan, pilih ikon edit



di sebelah aturan. Lalu pilih Kelola tag.

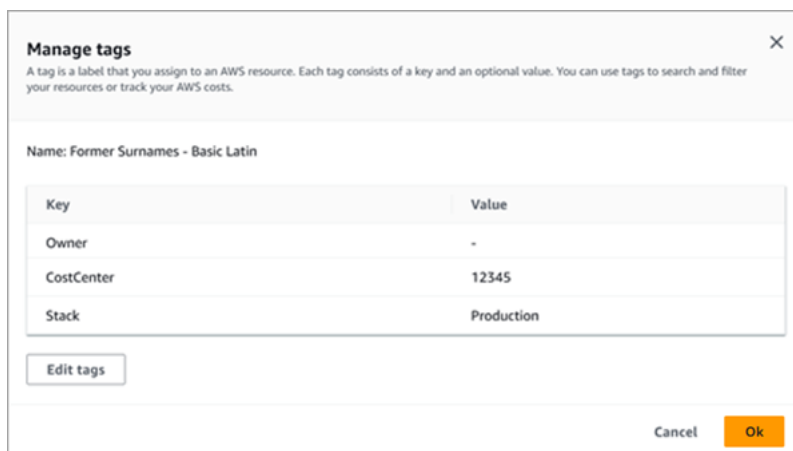
- Untuk akun anggota di organisasi Anda, pilih Akun di panel navigasi.

Kemudian, di tabel, pilih kotak centang untuk akun tersebut. Kemudian pilih Kelola tag pada menu Tindakan.

- Untuk pekerjaan penemuan data sensitif, pilih Pekerjaan di panel navigasi.

Kemudian, di tabel, pilih kotak centang untuk pekerjaan itu. Kemudian pilih Kelola tag pada menu Tindakan.

Jendela Manage tags mencantumkan semua tag yang saat ini ditetapkan ke sumber daya. Misalnya, gambar berikut menunjukkan tag yang ditetapkan ke pengenalan data kustom.



Dalam contoh ini, tiga tag ditetapkan ke pengenalan data kustom: kunci tag Pemilik tanpa nilai tag terkait; kunci CostCentertag dengan 12345 sebagai nilai tag terkait; dan, kunci tag Stack dengan Production sebagai nilai tag terkait.

3. Setelah selesai meninjau tag, pilih Batal untuk menutup jendela.

## API

Untuk mengambil dan meninjau tag sumber daya yang ada secara terprogram, Anda dapat menggunakan yang sesuai `Get` atau `Describe` operasi untuk jenis sumber daya yang ingin Anda tinjau tag. Misalnya, jika Anda menggunakan [GetCustomDataIdentifier](#) operasi atau Anda menjalankan `get-custom-data-identifier` perintah dari AWS Command Line Interface (AWS CLI), respons mencakup tags objek. Objek mencantumkan semua tag (baik kunci tag dan nilai tag) yang saat ini ditugaskan ke sumber daya.

Anda juga dapat menggunakan [ListTagsForResource](#) pengoperasian Amazon Macie API. Dalam permintaan Anda, gunakan `resourceArn` parameter untuk menentukan Amazon Resource Name (ARN) sumber daya. Jika Anda menggunakan AWS CLI, jalankan `list-tags-for-resource` perintah dan gunakan `resource-arn` parameter untuk menentukan ARN sumber daya. Misalnya:

```
C:\> aws macie2 list-tags-for-resource --resource-arn arn:aws:macie2:us-east-1:123456789012:classification-job/3ce05dbb7ec5505def334104bexample
```

Dalam contoh sebelumnya, `arn:aws:macie2:us-east-1:123456789012:classification-job/3ce05dbb7ec5505def334104bexample` adalah ARN dari pekerjaan penemuan data sensitif yang ada.

Jika operasi berhasil, Macie mengembalikan tags objek yang mencantumkan semua tag (baik kunci tag dan nilai tag) yang saat ini ditetapkan ke sumber daya. Misalnya:

```
{
  "tags": {
    "Stack": "Production",
    "CostCenter": "12345",
    "Owner": ""
  }
}
```

Dimana `Stack`, `CostCenter`, dan `Owner` kunci tag yang ditugaskan ke sumber daya. `Production` adalah nilai tag yang terkait dengan kunci `Stack` tag. `12345` adalah nilai tag yang terkait dengan kunci `CostCenter` tag. Kunci `Owner` tag tidak memiliki nilai tag terkait.

Untuk mengambil daftar semua sumber daya Macie yang memiliki tag dan semua tag yang ditetapkan untuk masing-masing sumber daya tersebut, gunakan [GetResources](#) operasi API AWS Resource Groups Tagging. Dalam permintaan Anda, tetapkan nilai untuk



ResourceTypeFilters parameter tersebut macie2. Untuk melakukan ini dengan menggunakan AWS CLI, jalankan perintah [get-resources](#) dan tetapkan nilai untuk resource-type-filters parameter ke. macie2 Misalnya:

```
C:\> aws resourcegroupstaggingapi get-resources --resource-type-filters "macie2"
```

Jika operasi berhasil, Grup Sumber Daya mengembalikan ResourceTagMappingList array yang berisi ARN dari semua sumber daya Macie yang memiliki tag, dan kunci tag dan nilai yang ditetapkan untuk masing-masing sumber daya tersebut.

## Mengedit tag untuk sumber daya Amazon Macie

Untuk mengedit tag (kunci tag atau nilai tag) untuk sumber daya Amazon Macie, Anda dapat menggunakan konsol Amazon Macie atau Amazon Macie API. Untuk melakukan ini untuk beberapa sumber daya Macie secara bersamaan, gunakan [Editor Tag](#) di AWS Resource Groups konsol atau operasi penandaan API [AWS Resource Groups Tagging](#).

### Important

Mengedit tag untuk sumber daya dapat memengaruhi akses ke sumber daya. Sebelum Anda mengedit kunci tag atau nilai sumber daya, tinjau kebijakan AWS Identity and Access Management (IAM) apa pun yang mungkin menggunakan tag untuk mengontrol akses ke sumber daya.

## Console

Ikuti langkah-langkah berikut untuk mengedit tag sumber daya dengan menggunakan konsol Amazon Macie.

Untuk mengedit tag untuk sumber daya

1. Buka konsol Amazon Macie di <https://console.aws.amazon.com/macie/>.
2. Bergantung pada jenis sumber daya yang tagnya ingin Anda edit, lakukan salah satu hal berikut:
  - Untuk daftar izinkan, pilih Izinkan daftar di panel navigasi.

Kemudian, di tabel, pilih kotak centang untuk daftar. Kemudian pilih Kelola tag pada menu Tindakan.

- Untuk pengenalan data kustom, pilih Pengidentifikasi data khusus di panel navigasi.

Kemudian, di tabel, pilih kotak centang untuk pengidentifikasi data kustom. Kemudian pilih Kelola tag pada menu Tindakan.

- Untuk aturan filter atau penindasan, pilih Temuan di panel navigasi.

Kemudian, dalam daftar Aturan tersimpan, pilih ikon edit



di sebelah aturan. Lalu pilih Kelola tag.

- Untuk akun anggota di organisasi Anda, pilih Akun di panel navigasi.

Kemudian, di tabel, pilih kotak centang untuk akun tersebut. Kemudian pilih Kelola tag pada menu Tindakan.

- Untuk pekerjaan penemuan data sensitif, pilih Pekerjaan di panel navigasi.

Kemudian, di tabel, pilih kotak centang untuk pekerjaan itu. Kemudian pilih Kelola tag pada menu Tindakan.

Jendela Manage tags mencantumkan semua tag yang saat ini ditetapkan ke sumber daya.

3. Di jendela Kelola tag, pilih Edit tag.

4. Lakukan langkah-langkah berikut:

- Untuk menambahkan nilai tag ke kunci tag, masukkan nilai di kotak Nilai di samping kunci tag.
- Untuk mengubah kunci tag yang ada, pilih Hapus di samping tag. Kemudian pilih Tambahkan tag. Di kotak Key yang muncul, masukkan kunci tag baru. Secara opsional masukkan nilai tag terkait di kotak Nilai.
- Untuk mengubah nilai tag yang ada, pilih X di kotak Nilai yang berisi nilai. Kemudian masukkan nilai tag baru di Nilai kotak.
- Untuk menghapus nilai tag yang ada, pilih X di kotak Nilai yang berisi nilai.
- Untuk menghapus tag yang ada (baik kunci tag dan nilai tag), pilih Hapus di samping tag.

Sumber daya dapat memiliki sebanyak 50 tag. Kunci tag dapat berisi sebanyak 128 karakter. Nilai tag dapat berisi sebanyak 256 karakter. Karakter dapat berupa huruf, angka, spasi, atau simbol berikut: `_./= + - @`

5. Setelah selesai mengedit tag, pilih Simpan.

## API

Saat mengedit tag untuk sumber daya secara terprogram, Anda akan menimpa tag yang ada dengan nilai baru. Oleh karena itu, cara terbaik untuk mengedit tag tergantung pada apakah Anda ingin mengedit kunci tag, nilai tag, atau keduanya. Untuk mengedit kunci tag, [hapus tag saat ini](#) dan [tambahkan tag baru](#).

Untuk mengedit atau menghapus hanya nilai tag yang terkait dengan kunci tag, tanpa nilai yang ada dengan menggunakan [TagResource](#) pengoperasian Amazon Macie API atau, jika Anda menggunakan AWS Command Line Interface (AWS CLI), jalankan perintah [tag-resource](#). Dalam permintaan Anda, tentukan Amazon Resource Name (ARN) sumber daya yang nilainya tag ingin Anda edit atau hapus.

Untuk mengedit nilai tag untuk kunci tag, gunakan `tags` parameter untuk menentukan kunci tag yang nilai tagnya ingin Anda ubah, dan tentukan nilai tag baru untuk kunci tersebut. Misalnya, perintah berikut mengubah nilai tag dari `Production` ke `Staging` untuk kunci `Stack` tag yang ditetapkan ke tugas penemuan data sensitif yang ditentukan. Contoh ini diformat untuk Microsoft Windows dan menggunakan karakter kelanjutan garis sisipan (^) untuk meningkatkan keterbacaan.

```
C:\> aws macie2 tag-resource ^
--resource-arn arn:aws:macie2:us-east-1:123456789012:classification-
job/3ce05dbb7ec5505def334104bexample ^
--tags={"Stack":"Staging"}
```

Dengan:

- `resource-arn` menentukan ARN pekerjaan.
- `Stack` adalah kunci tag yang terkait dengan nilai tag yang akan diubah.
- `Staging` adalah nilai tag baru untuk kunci tag tertentu (`Stack`).

Untuk menghapus nilai tag dari kunci tag, jangan tentukan nilai `value` argumen dalam `tags` parameter. Misalnya:

```
C:\> aws macie2 tag-resource ^  
--resource-arn arn:aws:macie2:us-east-1:123456789012:classification-  
job/3ce05dbb7ec5505def334104bexample ^  
--tags={"Stack\":"\"\"}
```

Jika operasi berhasil, Macie mengembalikan respons HTTP 204 kosong. Jika tidak, Macie mengembalikan HTTP 4 xx atau respon 500 yang menunjukkan mengapa operasi gagal.

## Menghapus tag dari sumber daya Amazon Macie

Untuk menghapus tag dari sumber daya Amazon Macie, Anda dapat menggunakan konsol Amazon Macie atau Amazon Macie API. Untuk melakukan ini untuk beberapa sumber daya Macie secara bersamaan, gunakan [Editor Tag](#) di AWS Resource Groups konsol atau operasi penandaan API [AWS Resource Groups Tagging](#).

### Important

Menghapus tag dari sumber daya dapat memengaruhi akses ke sumber daya. Sebelum menghapus tag, tinjau kebijakan AWS Identity and Access Management (IAM) apa pun yang mungkin menggunakan tag untuk mengontrol akses ke sumber daya.

## Console

Ikuti langkah-langkah ini untuk menghapus satu atau beberapa tag dari sumber daya dengan menggunakan konsol Amazon Macie.

Untuk menghapus tag dari sumber daya

1. Buka konsol Amazon Macie di <https://console.aws.amazon.com/macie/>.
2. Bergantung pada jenis sumber daya yang ingin Anda hapus tag, lakukan salah satu hal berikut:
  - Untuk daftar izinkan, pilih Izinkan daftar di panel navigasi.

Kemudian, di tabel, pilih kotak centang untuk daftar. Kemudian pilih Kelola tag pada menu Tindakan.

- Untuk pengenalan data kustom, pilih Pengidentifikasi data khusus di panel navigasi.

Kemudian, di tabel, pilih kotak centang untuk pengidentifikasi data kustom. Kemudian pilih Kelola tag pada menu Tindakan.

- Untuk aturan filter atau penindasan, pilih Temuan di panel navigasi.

Kemudian, dalam daftar Aturan tersimpan, pilih ikon edit



di sebelah aturan. Lalu pilih Kelola tag.

- Untuk akun anggota di organisasi Anda, pilih Akun di panel navigasi.

Kemudian, di tabel, pilih kotak centang untuk akun tersebut. Kemudian pilih Kelola tag pada menu Tindakan.

- Untuk pekerjaan penemuan data sensitif, pilih Pekerjaan di panel navigasi.

Kemudian, di tabel, pilih kotak centang untuk pekerjaan itu. Kemudian pilih Kelola tag pada menu Tindakan.

Jendela Manage tags mencantumkan semua tag yang saat ini ditetapkan ke sumber daya.

3. Di jendela Kelola tag, pilih Edit tag.
4. Lakukan langkah-langkah berikut:
  - Untuk menghapus hanya nilai tag untuk tag, pilih X di kotak Nilai yang berisi nilai yang akan dihapus.
  - Untuk menghapus kunci tag dan nilai tag (sebagai pasangan) untuk tag, pilih Hapus di samping tag yang akan dihapus.
5. (Opsional) Untuk menghapus lebih banyak tag dari sumber daya, ulangi langkah sebelumnya untuk setiap tag tambahan untuk dihapus.
6. Setelah selesai menghapus tag, pilih Simpan.

## API

Untuk menghapus satu atau beberapa tag dari sumber daya secara terprogram, gunakan [UntagResource](#) pengoperasian Amazon Macie API. Dalam permintaan Anda, gunakan `resourceArn` parameter untuk menentukan Amazon Resource Name (ARN) sumber daya untuk menghapus tag. Gunakan `tagKeys` parameter untuk menentukan kunci tag tag yang akan dihapus. Untuk menghapus hanya nilai tag tertentu (bukan kunci tag) dari sumber daya, [edit tag](#) alih-alih menghapus tag.

Jika Anda menggunakan AWS Command Line Interface (AWS CLI), jalankan perintah [untag-resource](#) dan gunakan `resource-arn` parameter untuk menentukan ARN sumber daya untuk menghapus tag. Gunakan `tag-keys` parameter untuk menentukan kunci tag tag yang akan dihapus. Misalnya, perintah berikut menghapus Stack tag (baik kunci tag dan nilai tag) dari pekerjaan penemuan data sensitif yang ditentukan:

```
C:\> aws macie2 untag-resource ^  
--resource-arn arn:aws:macie2:us-east-1:123456789012:classification-  
job/3ce05dbb7ec5505def334104bexample ^  
--tag-keys Stack
```

Dimana `resource-arn` menentukan ARN pekerjaan untuk menghapus tag dari, dan **Stack** merupakan kunci tag tag untuk menghapus.

Untuk menghapus beberapa tag dari sumber daya, tambahkan setiap kunci tag tambahan sebagai argumen untuk `tag-keys` parameter. Misalnya:

```
C:\> aws macie2 untag-resource ^  
--resource-arn arn:aws:macie2:us-east-1:123456789012:classification-  
job/3ce05dbb7ec5505def334104bexample ^  
--tag-keys Stack Owner
```

Dimana `resource-arn` menentukan ARN pekerjaan untuk menghapus tag dari, dan **Stack** dan **Owner** kunci tag tag untuk menghapus.

Jika operasi berhasil, Macie mengembalikan respons HTTP 204 kosong. Jika tidak, Macie mengembalikan HTTP 4xx atau respons 500 yang menunjukkan alasan operasi gagal.

# Membuat sumber daya Amazon Macie dengan AWS CloudFormation

Amazon Macie terintegrasi dengan AWS CloudFormation, layanan yang membantu Anda memodelkan dan mengatur AWS sumber daya sehingga Anda dapat lebih cepat dalam membuat dan mengelola sumber daya dan infrastruktur Anda. Anda membuat templat yang menggambarkan AWS sumber daya yang Anda inginkan (seperti pengidentifikasi data kustom), dan memasok AWS CloudFormation persediaan dan mengonfigurasi sumber daya tersebut untuk Anda.

Saat menggunakan AWS CloudFormation, Anda dapat menggunakan kembali templat Anda untuk mengatur sumber daya Macie secara konsisten dan berulang kali. Jelaskan sumber daya Anda satu kali, lalu sediakan sumber daya yang sama berulang kali dalam beberapa Akun AWS dan Wilayah AWS.

## Topik

- [Amazon Macie dan templat AWS CloudFormation](#)
- [Pelajari selengkapnya tentang AWS CloudFormation](#)

## Amazon Macie dan templat AWS CloudFormation

Untuk menyediakan dan mengonfigurasi sumber daya untuk Amazon Macie dan layanan terkait, Anda harus memahami [AWS CloudFormation templat](#). Templat adalah file teks dalam format JSON atau YAKL. Templat ini menjelaskan sumber daya yang ingin Anda sediakan di tumpukan AWS CloudFormation Anda.

Jika Anda tidak terbiasa dengan JSON atau YAKL, Anda dapat menggunakan AWS CloudFormation Designer, yang merupakan alat grafis untuk membuat dan memodifikasi templat. AWS CloudFormation Dengan Designer, Anda dapat membuat diagram sumber daya templat Anda dengan menggunakan drag-and-drop antarmuka, lalu mengedit detailnya menggunakan editor JSON dan YAKL terintegrasi. Untuk informasi selengkapnya, lihat [Apa yang dimaksud dengan AWS CloudFormation Designer?](#) dalam Panduan Pengguna AWS CloudFormation.

Anda dapat membuat AWS CloudFormation template untuk jenis sumber daya Macie berikut:

- Izinkan daftar
- Pengidentifikasi data kustom

- Filter aturan dan aturan penindasan untuk temuan, juga disebut sebagai filter temuan

Untuk informasi selengkapnya, termasuk contoh templat JSON dan YAKL untuk sumber daya ini, lihat Amazon Macie [referensi tipe sumber daya Amazon Macie dalam Panduan Pengguna](#) AWS CloudFormation

## Pelajari selengkapnya tentang AWS CloudFormation

Untuk mempelajari selengkapnya tentang AWS CloudFormation, lihat sumber daya berikut:

- [AWS CloudFormation](#)
- [AWS CloudFormation Panduan Pengguna](#)
- [AWS CloudFormation Referensi API](#)
- [AWS CloudFormation Panduan Pengguna Baris Perintah](#)



# Menangguhkan atau menonaktifkan Amazon Macie

Anda dapat menangguhkan atau menonaktifkan Amazon Macie secara spesifik Wilayah AWS dengan menggunakan konsol Amazon Macie atau Amazon Macie API. Macie kemudian berhenti melakukan semua aktivitas untuk akun Anda di Wilayah tersebut. Anda tidak dikenai biaya karena menggunakan Macie di Wilayah saat ditangguhkan atau dinonaktifkan.

Jika Anda menangguhkan atau menonaktifkan Macie, Anda dapat mengaktifkannya kembali di lain waktu.

## Topik

- [Menangguhkan Amazon Macie](#)
- [Menonaktifkan Amazon Macie](#)

## Menangguhkan Amazon Macie

Jika Anda menangguhkan Amazon Macie, Macie mempertahankan pengenalan sesi, pengaturan, dan sumber daya untuk akun Anda dalam hal yang berlaku Wilayah AWS. Misalnya, temuan Anda yang ada tetap utuh dan dipertahankan hingga 90 hari. Namun, ketika Anda menangguhkan Macie, Macie berhenti melakukan semua aktivitas untuk akun Anda di Wilayah yang berlaku. Ini termasuk memantau data Amazon Simple Storage Service (Amazon S3) Anda, melakukan penemuan data sensitif otomatis, dan menjalankan pekerjaan penemuan data sensitif yang saat ini sedang berlangsung. Macie juga membatalkan semua tugas temuan data sensitif Anda di dalam Wilayah.

Setelah Anda menangguhkan Macie, Anda dapat mengaktifkannya kembali. Anda kemudian mendapatkan kembali akses ke pengaturan dan sumber daya Anda di Wilayah yang berlaku, dan Macie melanjutkan aktivitasnya untuk akun Anda di Wilayah tersebut. Ini termasuk memperbarui inventaris bucket S3 untuk akun Anda dan memantau bucket untuk keamanan dan kontrol akses. Ini tidak termasuk melanjutkan atau memulai ulang pekerjaan penemuan data sensitif Anda. Pekerjaan penemuan data sensitif tidak dapat dilanjutkan atau dimulai ulang setelah dibatalkan.

Topik ini menjelaskan bagaimana cara untuk menangguhkan Macie dengan menggunakan konsol Amazon Macie. Jika Anda lebih suka melakukan ini secara terprogram, Anda dapat menggunakan [UpdateMacieSession](#) pengoperasian Amazon Macie API.

 Note

Jika Anda adalah administrator Macie untuk suatu organisasi, Anda harus menghapus semua akun anggota yang terkait dengan akun Anda sebelum menangguhkan Macie untuk akun Anda. Untuk informasi selengkapnya, lihat [Mengelola beberapa akun](#).


## Untuk menangguhkan Macie

1. Buka konsol Amazon Macie di <https://console.aws.amazon.com/macie/>.
2. Dengan menggunakan pemilih Wilayah AWS di bagian atas kanan pada halaman, pilih Wilayah pada Macie yang ingin Anda tangguhkan.
3. Di panel navigasi, pilih Pengaturan.
4. Pilih Menangguhkan Macie.
5. Saat diminta konfirmasi, masukkan **Suspend**, dan kemudian pilih Menangguhkan.

Untuk menangguhkan Macie di Wilayah tambahan, ulangi langkah-langkah sebelumnya di setiap Wilayah tambahan.

## Menonaktifkan Amazon Macie

Saat Anda menonaktifkan Amazon Macie, Macie berhenti melakukan semua aktivitas untuk akun Anda dalam hal yang berlaku Wilayah AWS. Ini termasuk memantau data Amazon Simple Storage Service (Amazon S3) Anda, melakukan penemuan data sensitif otomatis, dan menjalankan pekerjaan penemuan data sensitif yang saat ini sedang berlangsung. Macie juga menghapus semua pengaturan dan sumber daya yang ada yang disimpan atau dipelihara untuk akun Anda di Wilayah yang berlaku, termasuk temuan Anda dan pekerjaan penemuan data sensitif. Data yang Anda simpan atau dipublikasikan ke yang lain Layanan AWS tetap utuh dan tidak terpengaruh—misalnya, hasil penemuan data sensitif di Amazon S3 dan menemukan peristiwa di Amazon EventBridge.

 Warning

Jika Anda menonaktifkan Macie, Anda juga menghapus semua temuan yang ada secara permanen, pekerjaan penemuan data sensitif, pengidentifikasi data kustom, dan sumber daya lain yang disimpan atau disimpan Macie untuk akun Anda di Wilayah yang berlaku.

Sumber daya ini tidak dapat dipulihkan setelah dihapus. Untuk menjaga sumber daya dan hanya menunda penggunaan Macie Anda, tangguhkan Macie alih-alih menonaktifkannya.

Topik ini menjelaskan cara untuk menonaktifkan Macie dengan menggunakan konsol Amazon Macie. Jika Anda lebih suka melakukan ini secara terprogram, Anda dapat menggunakan [DisableMacie](#) pengoperasian Amazon Macie API.

### Note

Jika akun Anda adalah bagian dari organisasi yang mengelola beberapa akun Macie secara terpusat, Anda harus melakukan hal berikut sebelum menonaktifkan Macie:

- Jika akun Anda adalah akun anggota Macie, bekerjasama dengan administrator Macie Anda untuk menghapus akun Anda sebagai akun anggota.
- Jika akun Anda adalah akun administrator Macie, hapus semua akun anggota yang terkait dengan akun Anda, dan hapus hubungan antara akun Anda dan akun tersebut.

Bagaimana Anda menyelesaikan tugas-tugas sebelumnya tergantung pada apakah akun Macie Anda dikaitkan dengan akun lain melalui AWS Organizations atau dengan undangan. Untuk informasi selengkapnya, lihat [Mengelola beberapa akun](#).

Untuk menonaktifkan Macie

1. Buka konsol Amazon Macie di <https://console.aws.amazon.com/macie/>.
2. Dengan menggunakan pemilih Wilayah AWS di bagian atas kanan pada halaman, pilih Wilayah pada Macie yang ingin Anda nonaktifkan.
3. Di panel navigasi, pilih Pengaturan.
4. Pilih Nonaktifkan Macie.
5. Saat diminta konfirmasi, masukkan **Disable**, dan kemudian pilih Nonaktifkan.

Untuk menonaktifkan Macie di Wilayah tambahan, ulangi langkah-langkah sebelumnya di setiap Wilayah tambahan.

# Kuota Amazon Macie

Akun Akun AWS Anda memiliki kuota default, yang sebelumnya disebut sebagai batasan, untuk setiap layanan Layanan AWS. Kuota ini merupakan jumlah maksimum layanan sumber daya atau operasi untuk akun Anda. Topik ini membuat daftar kuota yang berlaku untuk sumber daya Amazon Macie dan operasi untuk akun Anda. Kecuali sebaliknya dinyatakan lain, setiap kuota berlaku untuk akun Anda di setiap Wilayah AWS.

Beberapa kuota dapat ditingkatkan, sementara yang lain tidak bisa. Untuk meminta peningkatan kuota, gunakan [konsol Service Quotas](#). Untuk mempelajari selengkapnya cara menyampaikan permintaan kenaikan kuota, lihat [Meminta kenaikan kuota](#) dalam Panduan Pengguna Service Quotas. Jika kuota tidak tersedia di konsol Service Quotas, gunakan formulir [peningkatan batas layanan](#) untuk meminta kenaikan kuota. AWS Support Center Console

## Akun

- Akun anggota dengan undangan: 1.000
- Akun anggota melalui AWS Organizations: 10.000

## Temuan

- Aturan filter dan aturan penindasan per akun: 1.000
- Temuan per menjalankan pekerjaan penemuan data sensitif: 100.000 +5% dari temuan yang tersisa setelah ambang batas 100.000 terpenuhi

Kuota ini hanya berlaku untuk konsol Amazon Macie dan Amazon Macie API. Tidak ada kuota untuk jumlah peristiwa penemuan yang diterbitkan Macie ke Amazon EventBridge atau jumlah hasil penemuan data sensitif yang dibuat Macie untuk setiap pekerjaan.

- Lokasi deteksi setiap temuan data sensitif: 15
- Permintaan untuk mengambil dan mengungkapkan sampel data sensitif dari objek Amazon S3: 100 per hari

Kuota ini disetel ulang setiap 24 jam pada pukul 00:00:01 UTC+0.

- Ukuran objek Amazon S3 untuk mengambil dan mengungkapkan sampel data sensitif dari:
  - File wadah objek Apache Avro (.avro): 70 MB
  - Apache Parquet (.parquet) berkas: 100 MB

- Berkas CSV (.csv): 255 MB
- File arsip terkompresi GNU Zip (.gz atau .gzip): 90 MB
- File JSON atau JSON Lines (.json atau .jsonl): 25 MB
- File buku kerja Microsoft Excel (.xlsx): 20 MB
- File teks non-biner (text/plain): 100 MB
- Berkas TSV (.tsv): 75 MB
- File arsip terkompresi ZIP (.zip): 355 MB

Jika temuan berlaku untuk file arsip yang menghasilkan beberapa file.gz untuk [hasil penemuan data sensitif](#) yang sesuai, sampel data sensitif tidak dapat diambil dan diungkapkan dari file arsip.

### Penemuan data sensitif

- Analisis bulanan per akun berdasarkan pekerjaan penemuan data sensitif: 5 TB

Kuota ini hanya berlaku untuk pekerjaan penemuan data sensitif. Untuk menambah kuota hingga 1.000 TB (1 PB), gunakan konsol [Service Quotas](#). Untuk meminta kenaikan lebih dari 1 PB, gunakan [formulir peningkatan batas layanan](#) pada AWS Support Center Console.

- Pengidentifikasi data khusus per akun: 10.000
- Izinkan daftar per akun: 10, 1—5 memungkinkan daftar yang menentukan teks yang telah ditentukan dan 1—5 mengizinkan daftar yang menentukan ekspresi reguler

Kuota tambahan berlaku untuk daftar allow yang menentukan teks yang telah ditetapkan. Daftar tidak dapat berisi lebih dari 100.000 entri dan ukuran penyimpanan daftar tidak boleh melebihi 35 MB.

- Bucket S3 untuk dikecualikan dari penemuan data sensitif otomatis: 1.000

Jika akun Anda adalah akun administrator Macie untuk suatu organisasi, kuota ini berlaku untuk organisasi Anda secara keseluruhan.

- Bucket S3 per pekerjaan penemuan data sensitif: 1.000

Kuota ini tidak berlaku untuk pekerjaan yang menggunakan kriteria bucket runtime untuk menentukan bucket mana yang akan dianalisis. Ini berlaku untuk pekerjaan hanya jika Anda mengonfigurasi pekerjaan untuk menganalisis bucket tertentu yang Anda pilih. Jika akun Anda adalah akun administrator Macie untuk suatu organisasi, Anda dapat memilih sebanyak 1.000 bucket yang mencakup sebanyak 1.000 akun di organisasi Anda.

- Pengidentifikasi data kustom setiap tugas penemuan data sensitif: 30
- Izinkan daftar per pekerjaan penemuan data sensitif: 10, 1—5 mengizinkan daftar yang menentukan teks yang telah ditentukan sebelumnya dan 1—5 mengizinkan daftar yang menentukan ekspresi reguler
- [CreateClassificationJob](#) operasi: 0,1 permintaan per detik
- Waktu untuk menganalisis file individual: 10 jam
- Ukuran file individu untuk menganalisis:
  - File Format Dokumen Portabel Adobe (.pdf): 1.024 MB
  - File kontainer objek Apache Avro (.avro): 8 GB
  - File Apache Parquet (.parquet): 8 GB
  - File pesan email (.eml): 20 GB
  - File arsip terkompresi GNU Zip (.gz atau .gzip): 8 GB
  - File buku kerja Microsoft Excel (.xls atau .xlsx): 512 MB
  - File dokumen Microsoft Word (.doc atau .docx): 512 MB
  - File teks non-biner: 20 GB
  - File arsip TAR (.tar): 20 GB
  - File arsip terkompresi ZIP (.zip): 8 GB

Macie tidak menganalisis data apa pun dalam file, jika file lebih besar dari kuota yang berlaku.

- Ekstraksi dan analisis data dalam file terkompresi atau arsip:
  - Ukuran penyimpanan (terkompresi): 8 GB untuk file arsip terkompresi GNU Zip (.gz atau .gzip) atau file arsip terkompresi ZIP (.zip); 20 GB untuk file arsip TAR (.tar)
  - Kedalaman arsip nest: 10 tingkat
  - File yang diekstrak: 1.000.000
  - Byte yang diekstraksi: 10 GB data tidak terkompresi secara keseluruhan. 3 GB data tidak terkompresi untuk setiap file yang diekstraksi yang menggunakan [jenis file atau format penyimpanan yang didukung](#).

Macie tidak mengekstraksi atau menganalisis data dalam file, jika metadata untuk file terkompresi atau arsip menunjukkan bahwa file berisi lebih dari 10 tingkat nest atau melebihi kuota yang berlaku untuk ukuran penyimpanan atau byte yang diekstrak. Jika Macie mulai mengekstraksi dan menganalisis data dalam file terkompresi atau arsip dan kemudian menentukan bahwa file berisi lebih dari 1.000.000 file atau melebihi kuota untuk bit yang diekstrak, Macie berhenti menganalisis<sup>94</sup>

data dalam file dan menciptakan temuan data sensitif dan hasil penemuan hanya untuk data yang diproses.

- Analisis elemen nest dalam data terstruktur: 256 tingkat setiap file

Kuota ini hanya berlaku untuk file JSON (.json) dan JSON Lines (.jsonl). Jika kedalaman nest dari salah satu tipe file melebihi kuota ini, Macie tidak menganalisis data apa pun dalam file.

- Lokasi deteksi per hasil penemuan data sensitif: 1.000 per tipe deteksi data sensitif
- Deteksi nama lengkap: 1.000 per file, termasuk file arsip

Setelah Macie mendeteksi 1.000 kemunculan nama lengkap pertama dalam sebuah file, Macie berhenti menambah jumlah dan melaporkan data lokasi untuk nama lengkap.

- Deteksi alamat surat: 1.000 per file, termasuk file arsip

Setelah Macie mendeteksi 1.000 kemunculan pertama alamat surat dalam sebuah file, Macie berhenti menambah jumlah dan melaporkan data lokasi untuk alamat surat.

# Riwayat dokumen untuk Panduan Pengguna Amazon Macie

Tabel berikut menjelaskan perubahan penting pada dokumentasi sejak rilis terakhir dari Amazon Macie. Untuk notifikasi tentang pembaruan dokumentasi ini, Anda dapat berlangganan ke umpan RSS.

Pembaruan dokumentasi terbaru: 20 Februari 2024

Perubahan	Deskripsi	Tanggal
<a href="#">Fungsionalitas baru</a>	AWS Security Hub sekarang menyediakan <a href="#">kontrol keamanan</a> yang memeriksa status Macie dan penemuan data sensitif otomatis untuk akun. <a href="#">Jika kontrol ini diaktifkan, Security Hub secara berkala menjalankan pemeriksaan keamanan untuk menentukan apakah Macie diaktifkan untuk Akun AWS (kontrol Macie.1), dan apakah penemuan data sensitif otomatis diaktifkan untuk akun Macie (kontrol Macie.2).</a>	Februari 20, 2024
<a href="#">Fungsionalitas baru</a>	Macie sekarang dapat <a href="#">menganalisis objek Amazon S3</a> yang dienkripsi menggunakan enkripsi sisi server dual-layer dengan (DSSE-KMS). AWS KMS keys Objek ini sekarang memenuhi syarat untuk dianalisis ketika Macie melakukan penemuan data sensitif otomatis atau Anda menjalankan pekerjaan	Januari 17, 2024



penemuan data sensitif. Selain itu, bucket dan objek S3 yang menggunakan enkripsi DSSE-KMS sekarang disertakan dalam [statistik dan metadata](#) yang disediakan Macie tentang data Amazon S3 Anda.

### Fitur baru

Anda sekarang dapat mengonfigurasi Macie untuk mengambil peran AWS Identity and Access Management (IAM) ketika Anda memilih untuk [mengambil dan mengungkapkan sampel data sensitif yang dilaporkan](#) Macie dalam temuan. Sampel dapat membantu Anda memverifikasi sifat data sensitif yang ditemukan Macie, dan menyesuaikan penyelidikan Anda terhadap objek dan bucket Amazon S3 yang terpengaruh.

16 November 2023

Fungsionalitas baru

Macie sekarang menyediakan [pengidentifikasi data terkelola](#) yang dirancang untuk mendeteksi Nomor Rekening Bank Internasional (IBAN) untuk 47 negara dan wilayah tambahan. Anda sekarang dapat menggunakan Macie untuk mendeteksi dan melaporkan kejadian IBAN di lebih dari 50 negara dan wilayah.

1 November 2023

Fungsionalitas baru

Macie sekarang menyediakan [pengidentifikasi data terkelola](#) yang dirancang untuk mendeteksi jenis data sensitif berikut: kunci Google Cloud API, kunci Stripe API, dan nomor Aadhaar, Nomor Akun Permanen (PAN), dan nomor identifikasi SIM untuk India.

25 September 2023

## Kuota baru

Untuk membantu Anda memverifikasi sifat data sensitif yang dilaporkan oleh temuan, kami meningkatkan kuota ukuran untuk [mengambil dan mengungkapkan sampel data sensitif](#) dari objek Amazon S3. Anda sekarang dapat mengambil dan mengungkapkan sampel dari objek S3 yang ukuran penyimpanannya melebihi 10 MB. Untuk daftar kuota baru, lihat Kuota [Amazon Macie](#).

7 September 2023

## Ketersediaan regional

Macie sekarang tersedia di Wilayah Israel (Tel Aviv). Untuk daftar lengkap Wilayah AWS tempat Macie saat ini tersedia, lihat [titik akhir dan kuota Amazon Macie](#) di Referensi Umum AWS

28 Agustus 2023

Fungsionalitas yang diperbarui

Kami menerapkan serangkaian [pengidentifikasi data terkelola default yang baru dan dinamis untuk penemuan data sensitif otomatis](#). Set default mencakup pengidentifikasi data terkelola yang kami rekomendasikan untuk penemuan data sensitif otomatis. Ini dirancang untuk mendeteksi kategori umum dan jenis data sensitif sambil juga mengoptimalkan hasil penemuan data sensitif otomatis Anda.

2 Agustus 2023

Fungsionalitas yang diperbarui

Untuk membantu Anda [menemukan kemunculan data sensitif](#) yang dilaporkan Macie dalam temuan data sensitif dan hasil penemuan data sensitif, kami mengubah batas karakter dari 20 menjadi 240 untuk nama elemen jalur JSON dalam objek. Record Perubahan ini memengaruhi temuan data sensitif baru dan hasil penemuan untuk wadah objek Apache Avro, file Apache Parquet, file JSON, dan file JSON Lines.

Juli 24, 2023

<a href="#">Fungsionalitas yang diperbarui</a>	Jika Anda adalah administrator Macie yang didelegasikan untuk organisasi di AWS Organizations, Anda sekarang dapat <a href="#">mengelola Macie hingga 10.000 akun di</a> organisasi Anda.	Juni 30, 2023
<a href="#">Fitur baru</a>	Anda sekarang dapat <a href="#">membuat dan mengonfigurasi pekerjaan penemuan data sensitif</a> untuk secara otomatis menggunakan kumpulan pengidentifikasi data terkelola yang kami rekomendasikan untuk pekerjaan. <a href="#">Kumpulan pengidentifikasi data terkelola yang direkomendasikan</a> ini dirancang untuk mendeteksi kategori umum dan jenis data sensitif sekaligus mengoptimalkan hasil pekerjaan Anda.	28 Juni 2023
<a href="#">Kebijakan baru</a>	Kami menambahkan <a href="#">kebijakanAWS terkelola</a> baru, AmazonMacieReadOnlyAccess kebijakan. Kebijakan ini memberikan izin hanya-baca yang memungkinkan identitas IAM (prinsipal) untuk mengambil semua sumber daya, data, dan setelan Macie untuk akun mereka.	15 Juni 2023

## Fitur baru

Untuk membantu Anda [menilai dan memantau cakupan penemuan data sensitif otomatis](#) dari data Amazon S3 Anda, konsol Macie sekarang menyertakan halaman cakupan Sumber Daya. Halaman ini menyediakan tampilan terpadu statistik cakupan dan data untuk semua bucket S3 Anda, termasuk rollup masalah analisis (jika ada) yang baru-baru ini terjadi untuk setiap bucket. Jika masalah terjadi, halaman juga menyediakan panduan remediasi.

15 Mei 2023

## Fitur baru

Macie terintegrasi dengan Notifikasi Pengguna AWS, yang merupakan lokasi baru Layanan AWS yang bertindak sebagai lokasi pusat untuk AWS notifikasi Anda di AWS Management Console. Dengan Notifikasi Pengguna, Anda dapat [mengonfigurasi aturan kustom dan saluran pengiriman](#) untuk membuat dan mengirim pemberitahuan tentang EventBridge peristiwa Amazon yang diterbitkan Macie untuk kebijakan dan temuan data sensitif.

5 Mei 2023

## Konten yang diperbarui

Deskripsi [statistik dan metadata](#) yang diperbarui yang disediakan Macie tentang pengaturan enkripsi default untuk bucket S3. Juga memperbarui deskripsi [temuan Policy:IAMUser/S3BucketEncryptionDisabled kebijakan](#). Amazon S3 sekarang secara otomatis menerapkan enkripsi sisi server dengan kunci terkelola Amazon S3 (SSE-S3) sebagai tingkat dasar enkripsi untuk objek yang ditambahkan ke bucket baru dan yang sudah ada. Untuk informasi tentang perubahan ini di Amazon S3, lihat [Menyetel perilaku enkripsi sisi server default untuk bucket S3](#) di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

27 Februari 2023

## Fungsionalitas baru

Macie sekarang dapat menghasilkan jenis [temuan kebijakan](#) tambahan untuk bucket S3: Policy:IAMUser/S3BucketSharedWithCloudFront. Jenis temuan ini menunjukkan bahwa kebijakan bucket diubah untuk memungkinkan bucket dibagikan dengan identitas akses CloudFront asal Amazon (OAI), kontrol akses CloudFront asal (OAC), atau keduanya. Selain itu, bucket yang dibagikan dengan CloudFront OAI atau OAC sekarang dianggap dibagikan secara eksternal dalam statistik dan metadata yang disediakan Macie tentang data Amazon S3 Anda.

Februari 24, 2023



## Fungsionalitas baru

Macie sekarang [mendukung kelas penyimpanan Amazon S3 Glacier Instant Retrieval](#) untuk penemuan data sensitif. Objek S3 yang menggunakan kelas penyimpanan ini sekarang memenuhi syarat untuk dianalisis saat Macie melakukan penemuan data sensitif otomatis atau Anda menjalankan pekerjaan penemuan data sensitif. Mereka juga dianggap sebagai objek yang dapat diklasifikasi dalam statistik dan metadata yang disediakan Macie tentang data Amazon S3 Anda.

21 Desember 2022

## Fitur baru

28 November 2022

Anda sekarang dapat mengonfigurasi Macie untuk [melakukan penemuan data sensitif otomatis](#) untuk akun atau organisasi Anda. Dengan penemuan data sensitif otomatis, Macie terus mengevaluasi data Amazon S3 Anda dan menggunakan teknik pengambilan sampel untuk mengidentifikasi, memilih, dan menganalisis objek yang representatif di bucket S3 Anda, memeriksa objek untuk data sensitif. Anda dapat mengevaluasi hasil analisis dalam statistik, temuan, dan informasi lain yang disediakan Macie tentang data Amazon S3 Anda.

## Fitur baru

Sekarang Anda dapat [membuat dan menggunakan daftar izinkan](#) untuk menentukan pola teks dan teks yang ingin diabaikan Macie saat memeriksa objek Amazon S3 untuk data sensitif. Dengan menggunakan daftar izinkan, Anda dapat menentukan pengecualian data sensitif untuk skenario atau lingkungan tertentu—misalnya, nama perwakilan publik untuk organisasi Anda, nomor telepon tertentu, atau data sampel yang digunakan organisasi Anda untuk pengujian.

30 Agustus 2022

## Fitur baru

Untuk memverifikasi sifat data sensitif yang ditemukan Macie di objek S3, Anda sekarang dapat mengonfigurasi dan menggunakan Macie untuk [mengambil sampel data sensitif](#) yang dilaporkan oleh temuan.

26 Juli 2022

---

<a href="#">Fungsionalitas yang diperbarui</a>	Dalam <a href="#">AmazonMacieFullAccesskebijakan</a> tersebut, kami memperbarui Nama Sumber Daya Amazon (ARN) dari peran terkait layanan Macie ( <code>arn:aws-service-role/macie.amazonaws.com/AWSServiceRoleForAmazonMacie</code> )	30 Juni 2022
<a href="#">Fungsionalitas yang diperbarui</a>	Kami memperbarui <a href="#">AmazonMacieServiceRolePolicykebijakan</a> , yaitu kebijakan yang dilampirkan pada peran terkait layanan Macie ( <code>arn:aws-service-role/macie.amazonaws.com/AWSServiceRoleForAmazonMacie</code> ). Kebijakan tidak lagi menentukan tindakan dan sumber daya untuk Amazon Macie Classic. Amazon Macie Classic telah dihentikan dan tidak lagi tersedia.	Mei 20, 2022
<a href="#">Fungsionalitas baru</a>	Macie sekarang memasukkan <code>OriginType</code> bidang dalam <a href="#">temuan data sensitif yang dipublikasikannya</a> . <a href="#">AWS Security Hub</a> <code>OriginType</code> Bidang menentukan bagaimana Macie menemukan data sensitif yang menghasilkan temuan.	Mei 11, 2022

<a href="#">Konten yang diperbarui</a>	Mengklarifikasi cara kerja kata kunci dan pengaturan jarak pencocokan maksimum untuk <a href="#">pengidentifikasi data khusus</a> .	22 April 2022
<a href="#">Fungsionalitas baru</a>	Macie sekarang menyediakan <a href="#">pengidentifikasi data terkelola</a> yang dirancang untuk mendeteksi header Otorisasi Dasar HTTP, cookie HTTP, dan Token Web JSON.	21 April 2022
<a href="#">Konten baru</a>	Menambahkan deskripsi dan definisi <a href="#">konsep dan istilah</a> kunci untuk Macie.	16 Maret 2022
<a href="#">Fungsionalitas baru</a>	Untuk menghitung dan menampilkan perkiraan biaya saat Anda membuat dan mengonfigurasi pekerjaan penemuan data sensitif, Macie sekarang mengambil data harga untuk Anda Akun AWS . AWS Billing and Cost ManagementUntuk mendukung fungsi ini, kami menambahkan tindakan Billing and Cost Management ke kebijakan <a href="#">AmazonMacieFullAccess</a> .	7 Maret 2022
<a href="#">Fungsionalitas baru</a>	Macie sekarang memasukkan SampLe bidang dalam <a href="#">temuan yang diterbitkannya</a> . AWS Security HubSampLeBidang menentukan apakah temuan adalah <a href="#">temuan sampel</a> .	Februari 24, 2022

---

<a href="#">Konten baru</a>	Menambahkan informasi tentang <a href="#">penggunaan Amazon Virtual Private Cloud</a> untuk membuat koneksi pribadi antara VPC dan Macie Anda.	Januari 19, 2022
<a href="#">Fungsionalitas baru</a>	Sekarang Anda dapat menggunakan konsol Amazon Macie untuk <a href="#">menetapkan dan mengelola tag</a> untuk pengenalan data kustom, aturan filter dan penekanan untuk temuan, pekerjaan penemuan data sensitif, dan, jika Anda administrator Macie untuk organisasi, akun anggota di organisasi Anda. Tag adalah label yang secara opsional Anda tentukan dan tetapkan ke jenis AWS sumber daya tertentu.	12 Januari 2022
<a href="#">Konten baru</a>	Menambahkan informasi tentang <a href="#">penggunaan AWS Identity and Access Management</a> untuk mengelola akses ke Macie.	Desember 20, 2021

## Fitur baru

Saat Anda [membuat pengenalan data kustom](#), Anda sekarang dapat menentukan pengaturan tingkat keparahan untuk temuan data sensitif yang dihasilkannya. Dengan pengaturan ini, Anda dapat menentukan tingkat keparahan yang akan ditetapkan ke temuan berdasarkan jumlah kemunculan teks yang cocok dengan kriteria deteksi pengidentifikasi data kustom.

4 November 2021

## Fungsionalitas baru

Untuk mempelajari tentang berbagai jenis temuan yang disediakan Macie, Anda dapat [menghasilkan temuan sampel](#). Temuan sampel menggunakan data contoh dan nilai placeholder untuk menunjukkan jenis informasi yang mungkin disertakan Macie dalam setiap jenis temuan.

28 Oktober 2021

## Fungsionalitas baru

Macie sekarang memasukkan `OwnerAccountId` bidang dalam [temuan yang diterbitkannya](#). AWS Security HubBidang ini menentukan ID akun untuk pemilik Akun AWS bucket S3 yang terpengaruh.

27 Oktober 2021

## Konten baru

Menambahkan informasi tentang [mengelola beberapa akun Macie secara terpusat](#).

Anda dapat melakukan ini dengan dua cara, dengan mengintegrasikan Macie dengan AWS Organizations atau dengan mengirim undangan keanggotaan dari Macie.

13 Oktober 2021

## Fungsionalitas baru

[Inventaris bucket S3](#) Anda sekarang menunjukkan apakah setelah izin bucket mencegah Macie mengambil informasi tentang bucket atau objek bucket dan mengevaluasi serta memantau keamanan dan privasi data bucket. Selain itu, kami memperbarui referensi AWS KMS keys dan kunci yang dikelola pelanggan untuk mencerminkan terminologi saat ini.

5 Oktober 2021



## Fungsionalitas baru

Macie sekarang menyimpan kebijakan dan temuan data sensitif selama 90 hari, bukan 30 hari. Jika Macie membuat atau memperbarui temuan pada atau setelah 31 Agustus 2021, Anda dapat mengakses temuan tersebut hingga 90 hari dengan menggunakan konsol Macie atau Macie API. Secara pasti Wilayah AWS, Macie mulai mempertahankan temuan selama 90 hari pada awal 27 September 2021.

1 Oktober 2021

## Fitur baru

Saat [membuat pekerjaan penemuan data sensitif](#), Anda sekarang dapat menentukan [pengidentifikasi data terkelola](#) mana yang ingin digunakan pekerjaan saat menganalisis objek S3. Dengan fitur ini, Anda dapat menyesuaikan analisis pekerjaan untuk fokus pada jenis data sensitif tertentu.

September 17, 2021

## Fungsionalitas baru

Temuan data sensitif kini memberikan informasi tambahan untuk membantu Anda [menemukan data sensitif](#) dalam file JSON dan JSON Lines.

6 Juli 2021

---

<a href="#">Fungsionalitas yang diperbarui</a>	Macie sekarang menggunakan jenis <code>AwsS3Bucket</code> sumber daya dalam <a href="#">temuan yang diterbitkan</a> . AWS Security Hub(Macie sebelumnya menetapkan nilai ini ke <code>AWS::S3::Bucket</code> .) <code>AwsS3Bucket</code> adalah nilai tipe sumber daya yang digunakan untuk bucket S3 di AWS Security Finding Format (ASFF).	28 Juni 2021
<a href="#">Fitur baru</a>	Saat <a href="#">membuat pekerjaan penemuan data sensitif</a> , Anda sekarang dapat menentukan <a href="#">kriteria runtime</a> yang menentukan bucket S3 mana yang dianalisis pekerjaan . Dengan fitur ini, cakupan analisis tugas dapat beradaptasi secara dinamis dengan perubahan pada inventaris bucket Anda.	15 Mei 2021

---

<a href="#">Fungsionalitas baru</a>	<a href="#">Inventaris bucket S3</a> Anda dan dasbor Ringkasan kini menyediakan metadata enkripsi dan statistik yang menunjukkan apakah kebijakan bucket memerlukan enkripsi sisi server objek baru. Selain itu, sekarang Anda dapat melakukan penyegaran metadata objek sesuai permintaan untuk masing-masing bucket di inventaris bucket Anda.	30 April 2021
<a href="#">Fitur baru</a>	Anda sekarang dapat <a href="#">menggunakan Amazon CloudWatch Logs untuk memantau dan menganalisis peristiwa</a> yang terjadi saat Anda menjalankan pekerjaan penemuan data sensitif. Untuk mendukung fitur ini, kami menambahkan tindakan CloudWatch Log ke kebijakan AWS terkelola untuk peran terkait <a href="#">layanan</a> Macie.	14 April 2021
<a href="#">Ketersediaan regional</a>	Macie sekarang tersedia di Wilayah AWS Asia Pasifik (Osaka).	5 April 2021
<a href="#">Fitur baru</a>	Sekarang Anda dapat mengonfigurasi Macie untuk <a href="#">menerbitkan temuan data sensitif ke AWS Security Hub</a> .	22 Maret 2021

---

<a href="#">Konten baru</a>	Menambahkan informasi tentang <a href="#">pemantauan dan memprakirakan biaya Macie</a> dan berpartisipasi dalam uji coba gratis.	26 Februari 2021
<a href="#">Konten yang diperbarui</a>	Kami mengganti istilah akun utama dengan istilah akun administrator. Akun administrator digunakan untuk <a href="#">mengelola beberapa akun secara terpusat</a> .	12 Februari 2021
<a href="#">Fungsionalitas baru</a>	Sekarang Anda dapat menyempurnakan cakupan tugas temuan data sensitif dengan <a href="#">menggunakan prefiks objek S3</a> dalam kriteria penyertaan dan pengecualian kustom.	2 Februari 2021
<a href="#">Konten yang diperbarui</a>	Macie sekarang menganut <a href="#">taksonomi tipe temuan</a> dari AWS Security Finding Format (ASFF) ketika menerbitkan temuan kebijakan ke AWS Security Hub	28 Januari 2021
<a href="#">Konten baru</a>	Menambahkan informasi tentang <a href="#">pemantauan data Amazon S3</a> dan menilai keamanan dan privasi data tersebut.	8 Januari 2021

<a href="#">Ketersediaan regional</a>	Macie sekarang tersedia di Wilayah AWS Afrika (Cape Town), Wilayah AWS Eropa (Milan), dan Wilayah Timur AWS Tengah (Bahrain).	21 Desember 2020
<a href="#">Fungsionalitas baru</a>	Jika akun Anda adalah akun administrator Macie, sekarang Anda dapat <a href="#">membuat dan menjalankan tugas temuan data sensitif</a> yang menganalisis data sebanyak 1.000 bucket yang mencakup 1.000 akun di organisasi Anda.	25 November 2020
<a href="#">Fungsionalitas baru</a>	<a href="#">Inventaris bucket S3</a> Anda kini menunjukkan apakah Anda telah mengonfigurasi tugas temuan data sensitif satu kali atau secara berkala untuk menganalisis data dalam bucket. Jika sudah, hal itu juga memberikan detail tentang tugas yang paling baru dijalankan.	23 November 2020
<a href="#">Konten baru</a>	Menambahkan informasi tentang <a href="#">mem-filter temuan</a> .	12 November 2020
<a href="#">Fungsionalitas baru</a>	Temuan data sensitif kini memberikan informasi tambahan untuk membantu Anda <a href="#">menemukan data sensitif</a> dalam kontainer objek Apache Avro, file Apache Parquet, dan buku kerja Microsoft Excel.	9 November 2020

---

<a href="#">Fitur baru</a>	Sekarang Anda dapat menggunakan temuan data sensitif untuk <a href="#">menemukan kejadian individu dari data sensitif</a> dalam objek S3.	22 Oktober 2020
<a href="#">Fitur baru</a>	Sekarang Anda dapat <a href="#">menjeda dan melanjutkan tugas temuan data sensitif</a> .	16 Oktober 2020
<a href="#">Konten baru</a>	Menambahkan detail tentang <a href="#">sistem penilaian kepelikan</a> untuk temuan kebijakan dan temuan data sensitif.	6 Oktober 2020
<a href="#">Fitur baru</a>	Sekarang Anda dapat melihat statistik yang menunjukkan berapa banyak data yang dapat dianalisis Macie dalam bucket S3 individu saat Anda menjalankan tugas temuan data sensitif. Selain itu, Anda dapat <a href="#">melihat perkiraan biaya tugas</a> saat membuat tugas.	3 September 2020
<a href="#">Konten baru</a>	Menambahkan informasi tentang <a href="#">mengonfigurasi, menjalankan, dan mengelola tugas temuan data sensitif</a> .	31 Agustus 2020
<a href="#">Fungsionalitas baru</a>	<a href="#">Pengidentifikasi data terkelola</a> kini dapat mendeteksi beberapa tipe informasi pribadi untuk Brazil.	31 Juli 2020

---

<a href="#">Konten yang diperbarui</a>	Menambahkan informasi tentang sintaks yang didukung untuk ekspresi reguler di <a href="#">pengidentifikasi data kustom</a> .	30 Juli 2020
<a href="#">Konten yang diperbarui</a>	Menambahkan persyaratan kata kunci untuk <a href="#">pengidentifikasi data terkelola</a> , dan meningkatkan <a href="#">Kuota</a> untuk jumlah temuan yang dapat dihasilkan oleh setiap tugas temuan data sensitif.	17 Juli 2020
<a href="#">Konten baru</a>	Menambahkan informasi tentang penggunaan Amazon EventBridge dan AWS Security Hub untuk <a href="#">memantau dan memproses temuan</a> . Ini termasuk skema EventBridge peristiwa untuk temuan dan contoh peristiwa untuk kebijakan dan temuan data sensitif.	22 Juni 2020
<a href="#">Konten baru</a>	Menambahkan informasi tentang <a href="#">menganalisis dan menekan temuan</a> .	17 Juni 2020
<a href="#">Konten baru</a>	Menambahkan petunjuk untuk mengonfigurasi Macie ke <a href="#">menyimpan hasil temuan detail dalam bucket S3</a> .	2 Juni 2020

[Konten baru](#)

Menambahkan informasi tentang [tipe data sensitif](#) yang dapat dideteksi oleh Macie, dan [persyaratan enkripsi](#) untuk mendeteksi data sensitif di objek Amazon S3.

28 Mei 2020

[Ketersediaan umum](#)

Ini adalah rilis publik awal dari Panduan Pengguna Amazon Macie.

13 Mei, 2020



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