aws

Panduan Pengguna

Amazon Inspector

Amazon Inspector: Panduan Pengguna

Table of Contents

Apa itu Amazon Inspector?

Amazon Inspector adalah layanan manajemen kerentanan yang secara terus-menerus memindai AWS beban kerja Anda untuk kerentanan perangkat lunak dan eksposur jaringan yang tidak diinginkan. Amazon Inspector secara otomatis menemukan dan memindai menjalankan instans Amazon EC2, gambar kontainer di Amazon Elastic Container Registry (Amazon ECR), dan AWS Lambda fungsi untuk kerentanan perangkat lunak yang diketahui dan eksposur jaringan yang tidak diinginkan.

Amazon Inspector membuat temuan saat menemukan kerentanan perangkat lunak atau masalah konfigurasi jaringan. Temuan menggambarkan kerentanan, mengidentifikasi sumber daya yang terpengaruh, menilai tingkat keparahan kerentanan, dan memberikan panduan perbaikan. Anda dapat menganalisis temuan menggunakan konsol Amazon Inspector, atau melihat dan memproses temuan Anda melalui yang lain. Layanan AWS Untuk informasi selengkapnya, lihat Memahami temuan di Amazon Inspector.

Topik

Fitur Amazon Inspector

Kelola beberapa akun Amazon Inspector secara terpusat

Jika AWS lingkungan Anda memiliki beberapa akun, Anda dapat mengelola lingkungan secara terpusat melalui akun tunggal dengan menggunakan AWS Organizations. Dengan menggunakan pendekatan ini, Anda dapat menetapkan akun sebagai akun administrator yang didelegasikan untuk Amazon Inspector.

Amazon Inspector dapat diaktifkan untuk seluruh organisasi Anda dengan satu klik. Selain itu, Anda dapat mengotomatiskan pengaktifan layanan untuk anggota future setiap kali mereka bergabung dengan organisasi Anda. Akun administrator yang didelegasikan Amazon Inspector dapat mengelola data temuan dan pengaturan tertentu untuk anggota organisasi. Ini termasuk melihat rincian temuan agregat untuk semua akun anggota, mengaktifkan atau menonaktifkan pemindaian untuk akun anggota, dan meninjau sumber daya yang dipindai dalam organisasi. AWS

Terus memindai lingkungan Anda untuk kerentanan dan eksposur jaringan

Dengan Amazon Inspector, Anda tidak perlu menjadwalkan atau mengonfigurasi pemindaian penilaian secara manual. Amazon Inspector secara otomatis menemukan dan mulai memindai sumber daya Anda yang memenuhi syarat. Amazon Inspector terus menilai lingkungan Anda di seluruh siklus hidup sumber daya Anda dengan memindai ulang sumber daya secara otomatis sebagai respons terhadap perubahan yang dapat menimbulkan kerentanan baru, seperti: menginstal paket baru dalam instans EC2, memasang tambalan, dan saat kerentanan dan eksposur umum baru (CVE) yang memengaruhi sumber daya dipublikasikan. Tidak seperti perangkat lunak pemindaian keamanan tradisional, Amazon Inspector memiliki dampak minimal pada kinerja armada Anda.

Ketika kerentanan atau jalur jaringan terbuka diidentifikasi, Amazon Inspector menghasilkan temuan yang dapat Anda selidiki. Temuan ini mencakup detail komprehensif tentang kerentanan, sumber daya yang terpengaruh, dan rekomendasi remediasi. Jika Anda memperbaiki temuan dengan tepat, Amazon Inspector secara otomatis mendeteksi remediasi dan menutup temuan tersebut.

Menilai kerentanan secara akurat dengan skor Risiko Amazon Inspector

Karena Amazon Inspector mengumpulkan informasi tentang lingkungan Anda melalui pemindaian, Amazon Inspector memberikan skor tingkat keparahan yang secara khusus disesuaikan dengan lingkungan Anda. Amazon Inspector memeriksa metrik keamanan yang menyusun skor dasar National Vulnerability Database (NVD) untuk kerentanan dan menyesuaikannya sesuai dengan lingkungan komputasi Anda. Misalnya, layanan dapat menurunkan skor Amazon Inspector dari temuan untuk instans Amazon EC2 jika kerentanan dapat dieksploitasi melalui jaringan tetapi tidak ada jalur jaringan terbuka ke internet yang tersedia dari instans. Skor ini dalam format CVSS dan merupakan modifikasi dari skor Common Vulnerability Scoring System (CVSS) dasar yang disediakan oleh NVD.

Identifikasi temuan berdampak tinggi dengan dasbor Amazon Inspector

Dasbor Amazon Inspector menawarkan tampilan temuan tingkat tinggi dari seluruh lingkungan Anda. Dari dasbor, Anda dapat mengakses detail terperinci dari temuan. Dasbor berisi informasi yang disederhanakan tentang cakupan pemindaian di lingkungan Anda, temuan Anda yang paling penting, dan sumber daya mana yang paling banyak ditemukan. Panel remediasi berbasis risiko di dasbor Amazon Inspector menyajikan temuan yang memengaruhi jumlah instans dan gambar terbesar. Panel ini memudahkan untuk mengidentifikasi temuan dengan dampak terbesar pada lingkungan Anda, meninjau detail pencarian, dan meninjau solusi yang disarankan.

Mengelola temuan Anda menggunakan tampilan yang dapat disesuaikan

Selain dasbor, konsol Amazon Inspector menawarkan tampilan Temuan. Halaman ini mencantumkan semua temuan untuk lingkungan Anda dan memberikan detail temuan individual. Anda dapat melihat

temuan yang dikelompokkan berdasarkan kategori atau jenis kerentanan. Di setiap tampilan, Anda dapat menyesuaikan hasil lebih lanjut menggunakan filter. Anda juga dapat menggunakan filter untuk membuat aturan penindasan yang menyembunyikan temuan yang tidak diinginkan dari tampilan Anda.

Anda dapat menggunakan filter dan aturan penindasan untuk menghasilkan laporan temuan yang menampilkan semua temuan atau pilihan temuan yang disesuaikan. Laporan dapat dibuat dalam format CSV atau JSON.

Memantau dan memproses temuan dengan layanan dan sistem lainnya

Untuk mendukung integrasi dengan layanan dan sistem lainnya, Amazon Inspector menerbitkan temuan ke Amazon EventBridge sebagai kejadian temuan. EventBridgeadalah layanan bus peristiwa nirserver yang dapat merutekan data temuan ke target seperti AWS Lambda fungsi dan topik Amazon Simple Notification Service (Amazon SNS). Dengan EventBridge demikian, Anda dapat memantau dan memproses temuan secara langsung sebagai bagian dari alur kerja keamanan dan kepatuhan yang ada.

Jika Anda telah mengaktifkan AWS Security Hub, maka Amazon Inspector juga akan mempublikasikan temuan ke 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.

Mengakses Amazon Inspector

Amazon Inspector tersedia di sebagianWilayah AWS. Untuk daftar Wilayah tempat Amazon Inspector saat ini tersedia, lihat Kuota dan titik akhir Amazon Web Services General Reference. Untuk mempelajari selengkapnyaWilayah AWS, lihat Mengelola Wilayah AWS di Referensi Umum Amazon Web Services. Di setiap Wilayah, Anda dapat bekerja dengan Amazon Inspector dengan cara-cara berikut.

AWSKonsol Manajemen

AWS Management Console adalah antarmuka berbasis peramban yang dapat Anda gunakan untuk membuat dan mengelola sumber daya AWS. Sebagai bagian dari konsol tersebut, konsol Amazon Inspector menyediakan akses ke akun dan sumber daya Amazon Inspector Anda. Anda dapat melakukan tugas-tugas Amazon Inspector dari konsol Amazon Inspector.

AWSalat baris perintah perintah baris perintah baris perintah

Dengan alat baris AWS perintah, Anda dapat mengeluarkan perintah di baris perintah sistem Anda untuk melakukan tugas Amazon Inspector. 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 menggunakanAWS CLI, lihat Panduan Pengguna AWS Command Line Interface. Untuk informasi tentang menginstal dan menggunakan Tools forPowerShell, lihat Panduan AWS Tools for PowerShell Pengguna.

AWSSDK

AWSmenyediakan SDK yang terdiri atas pustaka dan kode sampel untuk berbagai bahasa dan platform pemrograman, termasuk Java, Go, Python, C++, dan .NET. SDK menyediakan akses terprogram yang nyaman ke Amazon Inspector 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 Inspector

Amazon Inspector REST API memberi Anda akses terprogram dan komprehensif ke akun dan sumber daya Amazon Inspector Anda. Dengan API ini, Anda dapat mengirim permintaan HTTPS langsung ke Amazon Inspector. 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.

Memulai dengan Amazon Inspector

Tutorial ini memberikan pengenalan langsung ke Amazon Inspector.

Langkah 1 mencakup mengaktifkan pemindaian Amazon Inspector untuk akun mandiri atau sebagai administrator yang didelegasikan Amazon Inspector di lingkungan multi-akun. AWS Organizations

Langkah 2 mencakup pemahaman temuan Amazon Inspector di konsol.

> **Note**
>
> Dalam tutorial ini, Anda menyelesaikan tugas di saat ini Wilayah AWS. Untuk menyiapkan Amazon Inspector di Wilayah lain, Anda harus menyelesaikan langkah-langkah ini di masing-masing Wilayah tersebut.

Topik

Sebelum Anda memulai

Amazon Inspector adalah layanan manajemen kerentanan yang terus-menerus memindai instans Amazon EC2 Anda, gambar wadah Amazon ECR, dan fungsi untuk kerentanan perangkat lunak AWS Lambda dan eksposur jaringan yang tidak diinginkan.

Perhatikan hal berikut sebelum Anda mengaktifkan Amazon Inspector:

- Amazon Inspector adalah layanan Regional, dan data disimpan di Wilayah AWS tempat Anda menggunakan layanan. Setiap prosedur konfigurasi yang Anda selesaikan dalam tutorial ini harus diulang di setiap prosedur Wilayah AWS yang ingin Anda pantau dengan Amazon Inspector.
- Amazon Inspector memberi Anda fleksibilitas untuk mengaktifkan instans Amazon EC2, image container Amazon ECR, dan pemindaian fungsi. AWS Lambda Anda dapat mengelola jenis pemindaian dari halaman manajemen akun di konsol Amazon Inspector atau menggunakan Amazon Inspector API.

- Amazon Inspector dapat memberikan data Common Vulnerabilities and Exposures (CVE) untuk instans EC2 Anda hanya jika agen Amazon EC2 Systems Manager (SSM) diinstal dan diaktifkan. Agen ini sudah diinstal sebelumnya pada banyak instans EC2, tetapi Anda mungkin perlu mengaktifkannya secara manual. Terlepas dari status agen SSM, semua instans EC2 Anda dipindai untuk masalah paparan jaringan. Untuk informasi selengkapnya tentang mengonfigurasi pemindaian untuk Amazon EC2, lihat. Memindai instans Amazon EC2 Amazon ECR dan pemindaian AWS Lambda fungsi tidak memerlukan penggunaan agen.
- Identitas pengguna IAM dengan izin administrator Akun AWS dapat mengaktifkan Amazon Inspector. Untuk tujuan perlindungan data, kami menyarankan Anda untuk melindungi kredensyal Anda dan mengatur pengguna individu dengan AWS IAM Identity Center atau AWS Identity and Access Management (IAM). Dengan begitu, setiap pengguna hanya diberikan izin yang diperlukan untuk mengelola Amazon Inspector. Untuk informasi tentang izin yang diperlukan untuk mengaktifkan Amazon Inspector, lihat. AWS kebijakan terkelola: AmazonInspector2FullAccess
- Saat Anda mengaktifkan Amazon Inspector untuk pertama kalinya di Wilayah mana pun, Amazon Inspector akan membuat peran terkait layanan secara global untuk akun Anda yang dipanggil. `AWSServiceRoleForAmazonInspector2` Peran ini mencakup izin dan kebijakan kepercayaan yang memungkinkan Amazon Inspector mengumpulkan detail paket perangkat lunak dan menganalisis konfigurasi VPC Amazon untuk menghasilkan temuan kerentanan. Untuk informasi selengkapnya, lihat Menggunakan peran tertaut layanan untuk Amazon Inspector. Untuk informasi selengkapnya tentang peran terkait layanan, lihat Menggunakan peran terkait layanan.

Langkah 1: Aktifkan Amazon Inspector

Langkah pertama untuk menggunakan Amazon Inspector adalah mengaktifkannya untuk Anda. Akun AWS Setelah Anda mengaktifkan jenis pemindaian Amazon Inspector, Amazon Inspector segera mulai menemukan dan memindai semua sumber daya yang memenuhi syarat.

Jika Anda ingin mengelola Amazon Inspector untuk beberapa akun dalam organisasi Anda melalui akun administrator terpusat, Anda harus menetapkan administrator yang didelegasikan untuk Amazon Inspector. Pilih salah satu opsi berikut untuk mempelajari cara mengaktifkan Amazon Inspector untuk lingkungan Anda.

Standalone account environment

1. Buka konsol Amazon Inspector di https://console.aws.amazon.com/inspector/v2/home.
2. Pilih Memulai.

3. Pilih Aktifkan Amazon Inspector.

Saat Anda mengaktifkan Amazon Inspector di akun mandiri, semua jenis pemindaian diaktifkan secara default. Anda dapat mengelola jenis pemindaian yang diaktifkan dari halaman manajemen akun dalam konsol Amazon Inspector atau dengan menggunakan Amazon Inspector API. Setelah Amazon Inspector diaktifkan, Amazon Inspector secara otomatis menemukan dan mulai memindai semua sumber daya yang memenuhi syarat. Tinjau informasi jenis pemindaian berikut untuk memahami sumber daya mana yang memenuhi syarat secara default:

Pemindaian Amazon EC2

Untuk menyediakan data Common Vulnerabilities and Exposures (CVE) untuk instans EC2 Anda, Amazon Inspector mengharuskan agen AWS Systems Manager (SSM) diinstal dan diaktifkan. Agen ini sudah diinstal sebelumnya pada banyak instans EC2, tetapi Anda mungkin perlu mengaktifkannya secara manual. Terlepas dari status agen SSM, semua instans EC2 Anda akan dipindai untuk masalah paparan jaringan. Untuk informasi selengkapnya tentang mengonfigurasi pemindaian untuk Amazon EC2, lihat. Memindai instans Amazon EC2 dengan Amazon Inspector

Pemindaian ECR Amazon

Saat Anda mengaktifkan pemindaian Amazon ECR, Amazon Inspector mengonversi semua repositori kontainer di registri pribadi Anda yang dikonfigurasi untuk pemindaian Dasar default yang disediakan oleh Amazon ECR menjadi Pemindaian yang disempurnakan dengan pemindaian berkelanjutan. Anda juga dapat secara opsional mengonfigurasi pengaturan ini untuk memindai on-push saja atau untuk memindai repositori tertentu melalui aturan inklusi. Semua gambar yang didorong dalam 30 hari terakhir dijadwalkan untuk pemindaian Seumur Hidup, pengaturan pemindaian Amazon ECR ini dapat diubah kapan saja. Untuk informasi selengkapnya tentang mengonfigurasi pemindaian untuk Amazon ECR, lihat. Memindai gambar wadah Amazon ECR dengan Amazon Inspector

AWS Lambda pemindaian fungsi

Saat Anda mengaktifkan pemindaian AWS Lambda fungsi, Amazon Inspector menemukan fungsi Lambda di akun Anda dan segera mulai memindai mereka untuk kerentanan. Amazon Inspector memindai fungsi dan lapisan Lambda baru saat digunakan, dan memindainya kembali saat diperbarui atau saat Common Vulnerabilities and Exposures (CVE) baru diterbitkan. Amazon Inspector menawarkan dua tingkat pemindaian fungsi Lambda yang berbeda. Secara default saat Anda pertama kali mengaktifkan Amazon Inspector, pemindaian

standar Lambda diaktifkan, yang memindai dependensi paket dalam fungsi Anda. Anda juga dapat mengaktifkan pemindaian kode Lambda untuk memindai kode pengembang di fungsi Anda untuk kerentanan kode. Untuk informasi selengkapnya tentang mengonfigurasi pemindaian fungsi Lambda, lihat. AWS Lambda Fungsi pemindaian dengan Amazon Inspector

Multi-account environment

> **Important**
>
> Untuk menyelesaikan langkah-langkah ini, Anda harus berada di organisasi yang sama dengan semua akun yang ingin Anda kelola dan memiliki akses ke akun AWS Organizations manajemen untuk mendelegasikan administrator untuk Amazon Inspector dalam organisasi Anda. Izin tambahan mungkin diperlukan untuk mendelegasikan administrator. Untuk informasi selengkapnya, lihat Izin yang diperlukan untuk menetapkan administrator yang didelegasikan.
>
> > **Note**
> >
> > Untuk mengaktifkan Amazon Inspector secara terprogram untuk beberapa akun di beberapa Wilayah, Anda dapat menggunakan skrip shell yang dikembangkan oleh Amazon Inspector. Untuk informasi lebih lanjut tentang penggunaan skrip ini, lihat inspector2- enablement-with-cli on. GitHub

Mendelegasikan administrator untuk Amazon Inspector

1. Masuk ke akun AWS Organizations manajemen.
2. Buka konsol Amazon Inspector di https://console.aws.amazon.com/inspector/v2/home.
3. Dalam panel Administrator yang didelegasikan, masukkan ID dua belas digit Akun AWS yang ingin Anda tetapkan sebagai administrator delegasi Amazon Inspector untuk organisasi. Kemudian pilih Delegasi. Kemudian, di jendela konfirmasi, pilih Delegasi lagi.

> **Note**
>
> Amazon Inspector diaktifkan untuk akun Anda saat Anda mendelegasikan administrator.

Menambahkan akun anggota

Sebagai administrator yang didelegasikan, Anda dapat mengaktifkan pemindaian untuk setiap anggota yang terkait dengan akun manajemen Organisasi. Alur kerja ini mengaktifkan semua jenis pemindaian untuk semua akun anggota. Namun, anggota juga dapat mengaktifkan Amazon Inspector untuk akun mereka sendiri, atau pemindaian untuk layanan dapat diaktifkan secara selektif oleh administrator yang didelegasikan. Untuk informasi selengkapnya, lihat Mengelola beberapa akun.

1. Masuk ke akun administrator yang didelegasikan.
2. Buka konsol Amazon Inspector di https://console.aws.amazon.com/inspector/v2/home.
3. Di panel navigasi, pilih Manajemen Akun. Tabel Akun menampilkan semua akun anggota yang terkait dengan akun manajemen Organisasi.
4. Dari halaman Manajemen Akun, Anda dapat memilih Aktifkan pemindaian untuk semua akun dari spanduk atas untuk mengaktifkan instans EC2, gambar wadah ECR, dan, pemindaian AWS Lambda fungsi untuk semua akun di organisasi Anda. Atau, Anda dapat memilih akun yang ingin Anda tambahkan sebagai anggota dengan memilihnya di tabel Akun. Kemudian dari menu Aktifkan, pilih Semua pemindaian.
5. (Opsional) Aktifkan fitur Aktifkan Inspector secara otomatis untuk akun anggota baru dan pilih jenis pemindaian yang akan disertakan untuk mengaktifkan pemindaian tersebut untuk akun anggota baru yang ditambahkan ke organisasi Anda.

Amazon Inspector saat ini menawarkan pemindaian untuk instans EC2, image container ECR, dan fungsi. AWS Lambda Setelah Anda mengaktifkan Amazon Inspector, Amazon Inspector secara otomatis mulai menemukan dan memindai semua sumber daya yang memenuhi syarat. Tinjau informasi jenis pemindaian berikut untuk memahami sumber daya mana yang memenuhi syarat secara default:

Pemindaian Amazon EC2

Untuk menyediakan data kerentanan CVE untuk instans EC2 Anda, Amazon Inspector mengharuskan agen AWS Systems Manager (SSM) diinstal dan diaktifkan. Agen ini sudah diinstal sebelumnya pada banyak instans EC2, tetapi Anda mungkin perlu mengaktifkannya secara manual. Terlepas dari status agen SSM, semua instans EC2 Anda akan dipindai untuk masalah paparan jaringan. Untuk informasi selengkapnya tentang mengonfigurasi pemindaian untuk Amazon EC2, lihat. Memindai instans Amazon EC2 dengan Amazon Inspector

Pemindaian ECR Amazon

Saat Anda mengaktifkan pemindaian Amazon ECR, Amazon Inspector mengonversi semua repositori kontainer di registri pribadi Anda yang dikonfigurasi untuk pemindaian Dasar default yang disediakan oleh Amazon ECR menjadi Pemindaian yang disempurnakan dengan pemindaian berkelanjutan. Anda juga dapat secara opsional mengonfigurasi pengaturan ini untuk memindai on-push saja atau untuk memindai repositori tertentu melalui aturan inklusi. Semua gambar yang didorong dalam 30 hari terakhir dijadwalkan untuk pemindaian Seumur Hidup. Pengaturan pemindaian ECR Amazon ini dapat diubah oleh administrator yang didelegasikan kapan saja. Untuk informasi selengkapnya tentang mengonfigurasi pemindaian untuk Amazon ECR, lihat. Memindai gambar wadah Amazon ECR dengan Amazon Inspector

AWS Lambda pemindaian fungsi

Saat Anda mengaktifkan pemindaian AWS Lambda fungsi, Amazon Inspector menemukan fungsi Lambda di akun Anda dan segera mulai memindai mereka untuk kerentanan. Amazon Inspector memindai fungsi dan lapisan Lambda baru saat digunakan, dan memindainya kembali saat diperbarui atau saat Common Vulnerabilities and Exposures (CVE) baru diterbitkan. Untuk informasi selengkapnya tentang mengonfigurasi pemindaian fungsi Lambda, lihat. AWS Lambda Fungsi pemindaian dengan Amazon Inspector

Langkah 2: Lihat temuan Amazon Inspector

Anda dapat melihat temuan untuk lingkungan Anda di konsol Amazon Inspector atau melalui API. Semua temuan juga didorong ke Amazon EventBridge dan AWS Security Hub (jika diaktifkan). Selain itu, temuan gambar kontainer didorong ke Amazon ECR.

Konsol Amazon Inspector menawarkan beberapa format tampilan berbeda untuk temuan Anda. Dasbor Amazon Inspector memberi Anda ikhtisar risiko tingkat tinggi terhadap lingkungan Anda, sementara tabel Temuan memungkinkan Anda melihat detail temuan tertentu.

Pada langkah ini, Anda menjelajahi detail temuan menggunakan tabel Temuan dan dasbor Temuan. Untuk informasi tentang dasbor Amazon Inspector, lihat. Memahami dasbor

Untuk melihat detail temuan untuk lingkungan Anda di konsol Amazon Inspector:

1. Buka konsol Amazon Inspector di https://console.aws.amazon.com/inspector/v2/home.

2. Dari panel navigasi, pilih Dasbor. Anda dapat memilih salah satu tautan di dasbor untuk menavigasi ke halaman di konsol Amazon Inspector dengan detail lebih lanjut tentang item tersebut.
3. Dari panel navigasi, pilih Temuan.
4. Secara default Anda akan melihat tab Semua temuan, yang menampilkan semua instans EC2, gambar wadah ECR, temuan AWS Lambda fungsi untuk lingkungan Anda.
5. Dalam daftar Temuan, pilih nama temuan di kolom Judul untuk membuka panel detail untuk temuan tersebut. Semua temuan memiliki tab Menemukan detail. Anda dapat berinteraksi dengan tab Menemukan detail dengan cara berikut:

   - Untuk detail selengkapnya tentang kerentanan, ikuti tautan di bagian Detail kerentanan untuk membuka dokumentasi kerentanan ini.
   - Untuk menyelidiki sumber daya Anda lebih lanjut, ikuti tautan ID Sumber Daya di bagian Sumber yang terpengaruh untuk membuka konsol layanan untuk sumber daya yang terpengaruh.

   Temuan tipe kerentanan paket juga memiliki tab Inspector Score and vulnerability intelligence yang menjelaskan bagaimana skor Amazon Inspector dihitung untuk temuan tersebut dan memberikan informasi tentang Common Vulnerability and Exploits (CVE) yang terkait dengan temuan tersebut. Untuk detail selengkapnya tentang menemukan jenis, lihatMenemukan tipe di Amazon Inspector.

Memahami dasbor Amazon Inspector

Dasbor Amazon Inspector menyediakan snapshot statistik yang digabungkan untuk AWS sumber daya Anda di Wilayah saat ini. AWS Statistik ini mencakup metrik utama untuk cakupan sumber daya dan kerentanan aktif. Dasbor juga menampilkan grup data temuan agregat untuk akun Anda, seperti instans Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic Container Registry (Amazon ECR), dan AWS Lambda fungsi dengan temuan paling penting. Untuk melakukan analisis yang lebih dalam, Anda dapat melihat data pendukung untuk item dasbor.

Jika akun Anda adalah akun administrator yang didelegasikan oleh Amazon Inspector untuk sebuah organisasi, dasbor mencakup cakupan akun, statistik dan temuan gabungan untuk semua akun di organisasi Anda, termasuk akun Anda sendiri.

Menampilkan dasbor

Dasbor menunjukkan ikhtisar cakupan lingkungan dan temuan kritis Anda.

Untuk menampilkan dasbor:

1. Buka konsol Amazon Inspector https://console.aws.amazon.com/inspector/v2/home.
2. Di panel navigasi, pilih Dasbor.
3. Anda dapat berinteraksi dengan dasbor dengan cara-cara berikut:

    - Dasbor disegarkan secara otomatis setiap lima menit. Namun, Anda dapat me-refresh data secara manual dengan memilih ikon segarkan di sudut kanan atas halaman.
    - Untuk melihat data pendukung untuk item di dasbor, pilih item.
    - Jika Anda mengelola beberapa akun melalui AWS organisasi sebagai administrator yang didelegasikan oleh Amazon Inspector, dasbor akan menampilkan statistik gabungan untuk akun anggota Anda. Untuk mem-filter dasbor dan menampilkan data hanya untuk akun tertentu, masukkan ID akun di kotak Akun.

Memahami komponen dasbor dan menafsirkan data

Setiap bagian dasbor Amazon Inspector memberikan wawasan metrik kunci atau temuan aktif yang dapat membantu Anda memahami postur kerentanan sumber daya Anda di saat ini. AWS Wilayah AWS

Cakupan lingkungan

Bagian cakupan Lingkungan menyediakan statistik tentang sumber daya yang dipindai oleh Amazon Inspector. Di bagian ini, Anda dapat melihat jumlah dan persentase instans Amazon EC2, gambar Amazon ECR, dan AWS Lambda fungsi yang dipindai oleh Amazon Inspector. Jika Anda mengelola beberapa akun melalui AWS Organizations administrator yang didelegasikan oleh Amazon Inspector, Anda juga akan melihat jumlah total akun organisasi, nomor dengan Amazon Inspector diaktifkan, dan persentase cakupan yang dihasilkan untuk organisasi. Anda juga dapat menggunakan bagian ini untuk menentukan sumber daya mana yang tidak tercakup oleh Amazon Inspector. Sumber daya ini mungkin mengandung kerentanan yang dapat dieksploitasi untuk membahayakan organisasi Anda. Untuk rincian lebih lanjut, lihat Menilai cakupan Amazon Inspector dari lingkungan Anda AWS.

Memilih grup cakupan akan membawa Anda ke halaman Manajemen akun untuk pengelompokan yang Anda pilih. Halaman manajemen akun menunjukkan kepada Anda detail tentang akun mana, instans Amazon EC2, dan repositori Amazon ECR yang dicakup oleh Amazon Inspector.

Kelompok cakupan berikut ini tersedia:

- Akun
- Instans
- Repositori kontainer
- Gambar kontainer
- Lambda

Temuan kritis

Bagian Temuan Kritis menyediakan jumlah kerentanan kritis di lingkungan Anda dan jumlah total semua temuan di lingkungan Anda. Pada bagian ini, jumlah ditampilkan per sumber daya dan jenis penilaian. Untuk informasi selengkapnya tentang temuan kritis dan cara Amazon Inspector menentukan kekritisan, lihat. Memahami temuan di Amazon Inspector

Memilih grup temuan kritis akan membawa Anda ke halaman Semua temuan dan secara otomatis menerapkan filter untuk menampilkan semua temuan penting yang cocok dengan pengelompokan yang Anda pilih.

Kelompok temuan kritis berikut tersedia:

- Temuan gambar kontainer ECR
- Temuan Amazon EC2

- Temuan jangkauan jaringan
- AWS Lambdatemuan fungsi

Remediasi berbasis risiko

Bagian remediasi berbasis risiko menunjukkan lima paket perangkat lunak teratas dengan kerentanan kritis yang memengaruhi sebagian besar sumber daya di lingkungan Anda. Memperbaiki paket-paket ini dapat secara signifikan mengurangi jumlah risiko kritis terhadap lingkungan Anda. Pilih nama paket perangkat lunak untuk melihat detail kerentanan terkait dan sumber daya yang terpengaruh.

Akun dengan temuan paling kritis

Bagian Akun dengan temuan paling kritis menunjukkan lima AWS akun teratas di lingkungan Anda dengan temuan paling penting, dan jumlah total temuan untuk akun tersebut. Bagian ini hanya dapat dilihat dari akun administrator yang didelegasikan saat Amazon Inspector dikonfigurasi untuk pemindaian multi-akun. AWS Organizations Tampilan ini membantu administrator yang didelegasikan memahami akun mana yang paling berisiko dalam organisasi.

Pilih ID Akun untuk melihat informasi lebih lanjut tentang akun anggota yang terpengaruh.

Repositori Amazon ECR dengan temuan paling kritis

Repositori Elastic Container Registry (ECR) dengan bagian temuan paling penting menunjukkan lima repositori Amazon ECR teratas di lingkungan Anda dengan temuan gambar kontainer paling penting. Tampilan menunjukkan nama repositori, pengenal AWS akun, tanggal pembuatan repositori, jumlah kerentanan kritis, dan jumlah kerentanan total. Pandangan ini membantu Anda mengidentifikasi repositori mana yang paling berisiko.

Pilih Nama repositori untuk melihat informasi lebih lanjut tentang repositori yang terpengaruh.

Gambar kontainer dengan temuan paling kritis

Gambar Container dengan temuan paling kritis menunjukkan lima gambar kontainer teratas di lingkungan Anda dengan temuan paling penting. Tampilan menampilkan data tag gambar, nama repositori, intisari gambar, pengenal AWS akun, jumlah kerentanan kritis, dan jumlah kerentanan total. Pandangan ini membantu pemilik aplikasi mengidentifikasi gambar kontainer mana yang mungkin perlu dibangun kembali dan diluncurkan kembali.

Pilih Gambar kontainer untuk melihat informasi selengkapnya tentang image kontainer yang terpengaruh.

Instans dengan temuan paling kritis

Bagian Instans dengan temuan paling kritis menunjukkan lima instans Amazon EC2 teratas dengan temuan paling penting. Tampilan menampilkan pengenal instans, pengenal AWS akun, pengidentifikasi Amazon Machine Image (AMI), jumlah kerentanan kritis, dan jumlah total kerentanan. Tampilan ini membantu pemilik infrastruktur mengidentifikasi instans mana yang mungkin memerlukan penambalan.

Pilih ID Instans untuk melihat informasi selengkapnya tentang instans Amazon EC2 yang terpengaruh.

Amazon Machine Images (AMI) dengan temuan paling kritis

Amazon Machine Images (AMI) dengan bagian temuan paling kritis menunjukkan lima AMI teratas di lingkungan Anda dengan temuan paling penting. Tampilan menunjukkan pengenal AMI, pengenal AWS akun, jumlah instans EC2 yang terpengaruh yang berjalan di lingkungan, tanggal pembuatan AMI, platform sistem operasi AMI, jumlah kerentanan kritis, dan jumlah kerentanan total. Pandangan ini membantu pemilik infrastruktur mengidentifikasi AMI mana yang mungkin memerlukan pembangunan kembali.

Pilih Instans yang terkena dampak untuk melihat informasi selengkapnya tentang instans yang diluncurkan dari AMI yang terpengaruh.

AWS Lambdafungsi dengan temuan paling kritis

Bagian AWS Lambdafungsi dengan temuan paling kritis menunjukkan lima fungsi Lambda teratas di lingkungan Anda dengan temuan paling penting. Tampilan menunjukkan nama fungsi Lambda, pengenal AWS akun, lingkungan waktu proses, jumlah kerentanan kritis, jumlah kerentanan tinggi, dan jumlah kerentanan total. Pandangan ini membantu pemilik infrastruktur mengidentifikasi fungsi Lambda mana yang mungkin memerlukan perbaikan.

Pilih Nama fungsi untuk melihat informasi lebih lanjut tentang AWS Lambda fungsi yang terpengaruh.

Memahami temuan di Amazon Inspector

Temuan adalah laporan terperinci tentang kerentanan yang memengaruhi salah satu AWS sumber daya Anda. Temuan dinamai berdasarkan kerentanan yang terdeteksi dan memberikan peringkat keparahan, informasi tentang sumber daya yang terpengaruh, dan detail yang menjelaskan cara memulihkan kerentanan yang dilaporkan.

Amazon Inspector menghasilkan temuan setiap kali mendeteksi kerentanan dalam instans Amazon EC2, image container di repositori Amazon ECR, atau fungsi. AWS Lambda Amazon Inspector terus memindai lingkungan komputasi Anda dan menyimpan semua temuan aktif Anda sampai Anda memperbaikinya.

Saat Anda memulihkan temuan, temuan ditutup secara otomatis, dan Amazon Inspector menghapus temuan setelah 7 hari. Saat Anda menghapus sumber daya, Amazon Inspector menghapus temuan apa pun yang terkait dengan sumber daya setelah 30 hari.

Jika Anda menonaktifkan Amazon Inspector, temuan akan dihapus setelah 24 jam. Jika AWS menangguhkan akun Anda, temuan akan dihapus setelah 90 hari.

Temuan dikategorikan dalam salah satu negara berikut:

Aktif

Amazon Inspector mengidentifikasi temuan yang belum diperbaiki sebagai Aktif.

Ditekan

Amazon Inspector mengidentifikasi temuan yang tunduk pada satu atau lebih aturan penindasan sebagai Suppressed. Anda dapat menemukan temuan yang ditekan dalam daftar temuan yang ditekan. Untuk informasi selengkapnya, lihat Menekan temuan Amazon Inspector dengan aturan penindasan.

Ditutup

Setelah Anda memulihkan kerentanan, Amazon Inspector secara otomatis mendeteksi ini dan mengubah status temuan menjadi Closed. Temuan tertutup dihapus setelah 7 hari.

Topik

- Amazon Inspector menemukan detail
- Skor Amazon Inspector dan kecerdasan kerentanan
- Tingkat keparahan untuk temuan Amazon Inspector

Menemukan tipe di Amazon Inspector

Amazon Inspector menghasilkan temuan untuk instans Amazon Elastic Compute Cloud (Amazon EC2), gambar kontainer di repositori Amazon Elastic Container Registry (Amazon ECR), dan fungsi. AWS Lambda Amazon Inspector dapat menghasilkan jenis temuan berikut.

Kerentanan Package

Temuan kerentanan Package mengidentifikasi paket perangkat lunak di AWS lingkungan Anda yang terkena Common Vulnerabilities and Exposures (CVE). Penyerang dapat mengeksploitasi kerentanan yang belum ditambal ini untuk membahayakan kerahasiaan, integritas, atau ketersediaan data, atau untuk mengakses sistem lain. Sistem CVE adalah metode referensi untuk kerentanan dan eksposur keamanan informasi yang diketahui publik. Untuk informasi lebih lanjut, lihat https://www.cve.org/.

Deteksi CVE untuk Linux ditambahkan ke Amazon Inspector dalam waktu 24 jam setelah rilis oleh penasihat keamanan vendor. Deteksi CVE untuk Windows ditambahkan ke Amazon Inspector dalam waktu 48 jam setelah dirilis oleh Microsoft. Anda dapat menggunakan Pencarian basis data kerentanan Amazon Inspector untuk melihat apakah deteksi CVE didukung.

Amazon Inspector dapat menghasilkan temuan kerentanan paket untuk instans EC2, image container ECR, dan fungsi Lambda. Temuan kerentanan paket memiliki detail tambahan yang unik untuk jenis temuan ini, ini adalah skor Inspector dan intelijen kerentanan.

Kerentanan kode

Temuan kerentanan kode mengidentifikasi baris dalam kode Anda yang dapat dieksploitasi oleh penyerang. Kerentanan kode termasuk kekurangan injeksi, kebocoran data, kriptografi lemah, atau enkripsi yang hilang dalam kode Anda.

Amazon Inspector mengevaluasi kode aplikasi fungsi Lambda Anda menggunakan penalaran otomatis dan pembelajaran mesin yang menganalisis kode aplikasi Anda untuk kepatuhan keamanan secara keseluruhan. Ini mengidentifikasi pelanggaran kebijakan dan kerentanan berdasarkan detektor internal yang dikembangkan bekerja sama dengan Amazon. CodeGuru Untuk daftar kemungkinan deteksi, lihat Perpustakaan CodeGuru Detektor.

> **Important**
>
> Pemindaian kode Amazon Inspector menangkap cuplikan kode untuk menyoroti kerentanan yang terdeteksi. Cuplikan ini dapat menunjukkan kredensyal hardcode atau materi sensitif lainnya dalam teks biasa.

Amazon Inspector dapat menghasilkan temuan kerentanan Kode untuk fungsi Lambda jika Anda telah mengaktifkannya. Pemindaian kode Amazon Inspector Lambda

Cuplikan kode yang terdeteksi sehubungan dengan kerentanan kode disimpan oleh layanan. CodeGuru Secara default kunci AWS milik yang dikendalikan oleh CodeGuru digunakan untuk mengenkripsi kode Anda, namun, Anda dapat menggunakan kunci yang dikelola pelanggan Anda sendiri untuk enkripsi melalui Amazon Inspector API. Untuk informasi selengkapnya, lihat Enkripsi saat istirahat untuk kode dalam temuan Anda.

Jangkauan jaringan

Temuan jangkauan jaringan menunjukkan bahwa ada jalur jaringan terbuka ke instans Amazon EC2 di lingkungan Anda. Temuan ini muncul ketika port TCP dan UDP Anda dapat dijangkau dari tepi VPC, seperti gateway internet (termasuk contoh di belakang Application Load Balancers atau Classic Load Balancers), koneksi peering VPC, atau VPN melalui gateway virtual. Temuan ini menyoroti konfigurasi jaringan yang mungkin terlalu permisif, seperti grup keamanan yang salah kelola, Daftar Kontrol Akses, atau gateway internet, atau yang memungkinkan akses yang berpotensi berbahaya.

Amazon Inspector hanya menghasilkan temuan jangkauan jaringan untuk instans Amazon EC2. Amazon Inspector melakukan pemindaian untuk temuan jangkauan jaringan setiap 24 jam.

Amazon Inspector mengevaluasi konfigurasi berikut saat memindai jalur jaringan:

- Instans Amazon EC2
- AWS Lambdafungsi
- Penyeimbang Beban Aplikasi
- Connect Langsung
- Penyeimbang Beban Elastis
- Antarmuka Jaringan Elastis
- Gerbang Internet
- Daftar Kontrol Akses Jaringan

- Tabel Rute
- Grup Keamanan
- Subnet
- Awan Pribadi Virtual
- Gateway Pribadi Virtual
- Titik akhir VPC
- Titik akhir gerbang VPC
- Koneksi peering VPC
- Koneksi VPN

Menemukan dan melihat temuan Amazon Inspector

Prosedur di bagian ini menjelaskan cara menemukan dan melihat temuan di Amazon Inspector melalui konsol Amazon Inspector dan API. Menemukan detail bervariasi menurut jenis pencarian, jenis kerentanan, dan sumber daya yang terpengaruh. Untuk informasi selengkapnya, lihat Amazon Inspector menemukan detail.

Console

Untuk melihat temuan di konsol

1. Buka konsol Amazon Inspector di https://console.aws.amazon.com/inspector/v2/home.
2. Dari panel navigasi, pilih Temuan. Anda diarahkan ke layar Temuan di mana Anda dapat melihat semua temuan Anda. Dalam tabel Temuan, Anda dapat memilih temuan dengan memilih nama temuan di bawah kolom Judul.
3. (Opsional) Anda juga dapat melihat temuan yang dikelompokkan berdasarkan kategori. Dari panel navigasi, pilih Temuan, lalu pilih salah satu kategori berikut:
   - Dengan kerentanan
   - Dengan contoh

   > **Note**
   >
   > Temuan yang dikelompokkan berdasarkan contoh tidak menyertakan informasi tentang ketersediaan jaringan.

- Dengan gambar kontainer
- Dengan repositori kontainer
- Dengan fungsi Lambda

API

Jalankan operasi ListFindingsAPI. Dalam permintaan, Anda dapat menentukan `filterCriteria`untuk mengembalikan temuan tertentu.

Amazon Inspector menemukan detail

Di konsol Amazon Inspector, Anda dapat melihat detail untuk setiap temuan. Detail temuan bervariasi berdasarkan tipe temuan.

Untuk melihat detail untuk temuan

1. Buka konsol Amazon Inspector di https://console.aws.amazon.com/inspector/v2/home
2. Pilih Wilayah untuk melihat temuan di.
3. Di panel navigasi, pilih Temuan untuk menampilkan daftar temuan
4. (Opsional) Gunakan bilah filter untuk memilih temuan tertentu. Untuk informasi selengkapnya, lihat Memfilter temuan Amazon Inspector.
5. Pilih temuan untuk melihat panel detailnya.

Panel Finding details berisi fitur identifikasi dasar dari temuan tersebut. Ini termasuk judul temuan serta deskripsi dasar tentang kerentanan yang diidentifikasi, saran remediasi, dan skor keparahan. Untuk informasi tentang penilaian, lihatTingkat keparahan untuk temuan Amazon Inspector.

Detail yang tersedia untuk temuan bervariasi tergantung pada jenis temuan dan Sumber Daya yang terpengaruh.

Semua temuan berisi nomor Akun AWS ID tempat temuan diidentifikasi, tingkat keparahan, Jenis temuan, tanggal penemuan dibuat, dan bagian yang terpengaruh Sumber Daya dengan detail tentang sumber daya itu.

Jenis temuan menentukan informasi intelijen remediasi dan kerentanan yang tersedia untuk temuan tersebut. Tergantung pada jenis temuan, detail temuan yang berbeda tersedia.

Package Vulnerability

Temuan kerentanan paket tersedia untuk instans EC2, gambar kontainer ECR, dan fungsi Lambda. Lihat Kerentanan Package untuk info lebih lanjut.

Temuan kerentanan Package juga termasukSkor Amazon Inspector dan kecerdasan kerentanan.

Jenis temuan ini memiliki detail sebagai berikut:

- Perbaiki tersedia - Menunjukkan jika kerentanan diperbaiki dalam versi yang lebih baru dari paket yang terpengaruh. Memiliki salah satu nilai berikut:
  - `YES`, yang berarti semua paket yang terpengaruh memiliki versi tetap.
  - `NO`, yang berarti tidak ada paket yang terpengaruh memiliki versi tetap.
  - `PARTIAL`, yang berarti satu atau lebih (tetapi tidak semua) paket yang terpengaruh memiliki versi tetap.
- Eksploitasi tersedia - Menunjukkan kerentanan memiliki eksploitasi yang diketahui.
  - `YES`, yang berarti kerentanan yang ditemukan di lingkungan Anda memiliki eksploitasi yang diketahui. Amazon Inspector tidak memiliki visibilitas ke dalam penggunaan eksploitasi di lingkungan.
  - `NO`, yang berarti kerentanan ini tidak memiliki eksploitasi yang diketahui.
- Paket yang terpengaruh - Daftar setiap paket yang diidentifikasi rentan dalam temuan, dan detail setiap paket:
- Filepath — ID volume EBS dan nomor partisi yang terkait dengan temuan. Bidang ini hadir dalam temuan untuk instans EC2 yang dipindai menggunakan. Pemindaian tanpa agen
- Versi terinstal/ Versi tetap - Nomor versi paket yang saat ini diinstal yang kerentanan terdeteksi. Bandingkan nomor versi yang diinstal dengan nilai setelah garis miring (/). Nilai kedua adalah nomor versi paket yang memperbaiki kerentanan yang terdeteksi seperti yang disediakan oleh Common Vulnerabilities and Exposures (CVE) atau saran yang terkait dengan temuan tersebut. Jika kerentanan telah diperbaiki dalam beberapa versi, bidang ini mencantumkan versi terbaru yang menyertakan perbaikan. Jika perbaikan tidak tersedia, nilai ini`None available`.

  > **Note**
  >
  > Jika temuan terdeteksi sebelum Amazon Inspector mulai memasukkan bidang ini dalam temuan, nilai untuk bidang ini kosong. Namun, perbaikan mungkin tersedia.

- Package manager — Manajer paket yang digunakan untuk mengkonfigurasi paket ini.

- Remediasi — Jika perbaikan tersedia melalui paket atau pustaka pemrograman yang diperbarui, bagian ini menyertakan perintah yang dapat Anda jalankan untuk melakukan pembaruan. Anda dapat menyalin perintah yang disediakan dan menjalankannya di lingkungan Anda.

  > **Note**
  >
  > Perintah remediasi disediakan dari umpan data vendor dan dapat bervariasi tergantung pada konfigurasi sistem Anda. Tinjau referensi penemuan atau dokumentasi sistem operasi untuk panduan yang lebih spesifik.

- Detail kerentanan - menyediakan tautan ke sumber pilihan Amazon Inspector untuk CVE yang diidentifikasi dalam temuan, seperti National Vulnerability Database (NVD), REDHAT, atau vendor OS lainnya. Selain itu, Anda akan menemukan skor keparahan untuk temuan tersebut. Untuk informasi lebih lanjut tentang penilaian tingkat keparahan seperti, lihatTingkat keparahan untuk temuan Amazon Inspector. Skor berikut disertakan, termasuk vektor penilaian untuk masing-masing:
  - Skor EPSS
  - Skor Inspector
  - CVSS 3.1 dari Amazon CVE
  - CVSS 3.1 dari NVD
  - CVSS 2.0 dari NVD (jika berlaku, untuk CVE lama)
- Kerentanan terkait - Menentukan kerentanan lain yang terkait dengan temuan. Biasanya ini adalah CVE lain yang memengaruhi versi paket yang sama, atau CVE lain dalam grup yang sama dengan CVE temuan, sebagaimana ditentukan oleh vendor.

Kerentanan kode

Temuan kerentanan kode hanya tersedia untuk fungsi Lambda. Lihat Kerentanan kode untuk info lebih lanjut. Jenis temuan ini memiliki detail sebagai berikut:

- Perbaiki tersedia - Untuk kerentanan kode nilai ini selaluYES.
- Nama detektor — Nama CodeGuru detektor yang digunakan untuk mendeteksi kerentanan kode. Untuk daftar kemungkinan deteksi, lihat Perpustakaan CodeGuru Detektor.
- Tag detektor — CodeGuru Tag yang terkait dengan detektor, CodeGuru menggunakan tag untuk mengkategorikan deteksi.

- CWE yang relevan — ID dari Common Weakness Enumeration (CWE) yang terkait dengan kerentanan kode.
- Jalur file — Lokasi file kerentanan kode.
- Lokasi kerentanan — Untuk kerentanan kode pemindaian kode Lambda, bidang ini menunjukkan baris kode yang tepat di mana Amazon Inspector menemukan kerentanan.
- Remediasi yang disarankan — Ini menunjukkan bagaimana kode dapat diedit untuk memulihkan temuan.

Jangkauan jaringan

Temuan jangkauan jaringan hanya tersedia untuk instans EC2. Lihat Jangkauan jaringan untuk info lebih lanjut. Jenis temuan ini memiliki detail sebagai berikut:

- Rentang port terbuka — Rentang port yang melaluinya instans EC2 dapat diakses.
- Jalur jaringan terbuka - Menunjukkan jalur akses terbuka ke instans EC2. Pilih item di jalur untuk informasi lebih lanjut.
- Remediasi — Merekomendasikan metode untuk menutup jalur jaringan terbuka.

Skor Amazon Inspector dan kecerdasan kerentanan

Di konsol Amazon Inspector, ketika Anda memilih temuan, Anda dapat melihat skor Inspector dan tab intelijen kerentanan yang menunjukkan detail penilaian untuk temuan kerentanan paket, serta detail intelijen kerentanan. Rincian ini hanya tersedia untuk Kerentanan Package temuan.

Skor Amazon Inspector

Skor Amazon Inspector adalah skor kontekstual yang dibuat Amazon Inspector untuk setiap temuan instans EC2. Skor Amazon Inspector ditentukan dengan mengkorelasikan informasi skor CVSS v3.1 dasar dengan informasi yang dikumpulkan dari lingkungan komputasi Anda selama pemindaian, seperti hasil jangkauan jaringan dan data eksploitabilitas. Misalnya, skor Amazon Inspector dari sebuah temuan mungkin lebih rendah dari skor dasar jika kerentanan dapat dieksploitasi melalui jaringan tetapi Amazon Inspector menentukan bahwa tidak ada jalur jaringan terbuka ke instance rentan yang tersedia dari internet.

Skor dasar untuk temuan adalah skor dasar CVSS v3.1 yang disediakan oleh vendor. Skor basis vendor RHEL, Debian, atau Amazon didukung, untuk vendor lain, atau kasus di mana vendor belum memberikan skor Amazon Inspector menggunakan skor dasar dari National Vulnerability Database (NVD). Amazon Inspector menggunakan Kalkulator Common Vulnerability Scoring System Versi 3.1

untuk menghitung skor. Anda dapat melihat sumber skor dasar temuan individu dalam detail temuan di bawah detail kerentanan, sebagai sumber Kerentanan (atau packageVulnerabilityDetails.source dalam temuan JSON)

> **Note**
>
> Skor Amazon Inspector tidak tersedia untuk instance Linux yang menjalankan Ubuntu. Ini karena Ubuntu mendefinisikan tingkat keparahan kerentanannya sendiri yang mungkin berbeda dari tingkat keparahan CVE terkait.

Rincian skor Amazon Inspector

Saat Anda membuka halaman detail temuan, Anda dapat memilih Inspector score and vulnerability intelligence Tab. Panel ini menunjukkan perbedaan antara skor dasar dan skor Inspector. Bagian ini menjelaskan bagaimana Amazon Inspector menetapkan peringkat keparahan berdasarkan kombinasi skor Amazon Inspector dan skor vendor untuk paket perangkat lunak. Jika skor berbeda panel ini menunjukkan penjelasan mengapa.

Di bagian metrik skor CVSS Anda dapat melihat tabel dengan perbandingan antara metrik skor dasar CVSS dan skor Inspector. Metrik yang dibandingkan adalah metrik dasar yang ditentukan dalam dokumen spesifikasi CVSS yang dikelola oleh. first.org Berikut ini adalah ringkasan metrik dasar:

Serangan Vektor

Konteks dimana kerentanan dapat dieksploitasi. Untuk temuan Amazon Inspector, ini bisa berupa Jaringan, Jaringan Berdekatan, atau Lokal.

Kompleksitas Serangan

Ini menggambarkan tingkat kesulitan yang akan dihadapi penyerang saat mengeksploitasi kerentanan. Skor rendah berarti bahwa penyerang harus memenuhi sedikit atau tidak ada kondisi tambahan untuk mengeksploitasi kerentanan. Skor tinggi berarti bahwa penyerang akan perlu menginvestasikan sejumlah besar upaya untuk melakukan serangan yang sukses dengan kerentanan ini.

Hak Istimewa Diperlukan

Ini menggambarkan tingkat hak istimewa yang dibutuhkan penyerang untuk mengeksploitasi kerentanan.

Interaksi Pengguna

Metrik ini menyatakan jika serangan yang berhasil menggunakan kerentanan ini membutuhkan pengguna manusia, selain penyerang.

Lingkup

Ini menyatakan apakah kerentanan dalam satu komponen yang rentan berdampak pada sumber daya dalam komponen di luar lingkup keamanan komponen yang rentan. Jika nilai ini Tidak berubah, sumber daya yang terpengaruh dan sumber daya yang terkena dampak adalah sama. Jika nilai ini diubah maka komponen yang rentan dapat dieksploitasi untuk mempengaruhi sumber daya yang dikelola oleh otoritas keamanan yang berbeda.

Kerahasiaan

Ini mengukur tingkat dampak terhadap kerahasiaan data dalam sumber daya ketika kerentanan dieksploitasi. Ini berkisar dari None, di mana tidak ada kerahasiaan yang hilang, ke High di mana semua informasi dalam sumber daya diungkapkan atau informasi rahasia seperti kata sandi atau kunci enkripsi dapat diungkapkan.

Integritas

Ini mengukur tingkat dampak terhadap integritas data dalam sumber daya yang terkena dampak jika kerentanan dieksploitasi. Integritas berisiko ketika penyerang memodifikasi file dalam sumber daya yang terkena dampak. Skor berkisar dari None, di mana eksploitasi tidak memungkinkan penyerang untuk memodifikasi informasi apa pun, ke Tinggi, di mana jika dieksploitasi, kerentanan akan memungkinkan penyerang untuk memodifikasi salah satu atau semua file, atau file yang dapat dimodifikasi memiliki konsekuensi serius.

Ketersediaan

Ini mengukur tingkat dampak terhadap ketersediaan sumber daya yang terkena dampak ketika kerentanan dieksploitasi. Skor berkisar dari None, ketika kerentanan tidak memengaruhi ketersediaan sama sekali, hingga Tinggi, di mana jika dieksploitasi, penyerang dapat sepenuhnya menolak ketersediaan sumber daya, atau menyebabkan layanan menjadi tidak tersedia.

Kecerdasan Kerentanan

Bagian ini merangkum intelijen yang tersedia tentang CVE dari Amazon serta sumber intelijen keamanan standar industri seperti Recorded Future, dan Cybersecurity and Infrastructure Security Agency (CISA).

> **Note**
>
> Intel dari CISA, Amazon, atau Recorded Future tidak akan tersedia untuk semua CVE.

Anda dapat melihat detail intelijen kerentanan di konsol atau dengan menggunakan BatchGetFindingDetailsAPI. Rincian berikut tersedia di konsol:

ATT&CK

Bagian ini menunjukkan taktik, teknik, dan prosedur MITRE (TTP) yang terkait dengan CVE. TTP terkait ditampilkan, jika ada lebih dari dua TTP yang berlaku, Anda dapat memilih tautan untuk melihat daftar lengkap. Memilih taktik atau teknik membuka informasi tentangnya di situs web MITRE.

CISA

Bagian ini mencakup tanggal yang relevan yang terkait dengan kerentanan. Tanggal Cybersecurity and Infrastructure Security Agency (CISA) menambahkan kerentanan ke Katalog Kerentanan Tereksploitasi yang Diketahui, berdasarkan bukti eksploitasi aktif, dan tanggal jatuh tempo CISA mengharapkan sistem untuk ditambal. Informasi ini bersumber dari CISA.

Malware yang dikenal

Bagian ini mencantumkan kit dan alat eksploitasi yang dikenal yang mengeksploitasi kerentanan ini.

Bukti

Bagian ini merangkum peristiwa keamanan paling penting yang melibatkan kerentanan ini. Jika lebih dari 3 acara memiliki tingkat kekritisan yang sama, tiga peristiwa terbaru ditampilkan.

Terakhir kali dilaporkan

Bagian ini menunjukkan tanggal eksploitasi publik terakhir yang diketahui untuk kerentanan ini.

Tingkat keparahan untuk temuan Amazon Inspector

Ketika Amazon Inspector menghasilkan temuan kerentanan, Amazon Inspector secara otomatis memberikan tingkat keparahan pada temuan tersebut. Kepelikan temuan mencerminkan karakteristik utama dari temuan dan oleh karena itu dapat membantu Anda menilai dan memprioritaskan temuan

Anda. Tingkat kepelikan temuan tidak menyiratkan atau menunjukkan kekritisan atau kepentingan yang mungkin dimiliki sumber daya yang terpengaruh untuk organisasi Anda.

Peringkat keparahan temuan didorong oleh skor numerik yang sesuai dengan salah satu tingkat keparahan berikut: informasi, rendah, sedang, tinggi, atau kritis.

Metode dimana Amazon Inspector menentukan tingkat keparahannya berbeda berdasarkan jenis temuan. Lihat bagian berikut tentang mempelajari lebih lanjut tentang cara Amazon Inspector menentukan peringkat keparahan untuk setiap jenis temuan.

Tingkat keparahan kerentanan paket perangkat lunak

Amazon Inspector menggunakan skor NVD/CVSS sebagai dasar penilaian keparahan untuk kerentanan paket perangkat lunak. Skor NVD/CVSS adalah skor keparahan kerentanan yang diterbitkan oleh NVD dan ditentukan oleh CVSS. Skor NVD/CVSS adalah komposisi metrik keamanan, seperti kompleksitas serangan, kematangan kode eksploitasi, dan hak istimewa yang diperlukan. Amazon Inspector menghasilkan skor numerik dari 1 hingga 10 yang mencerminkan tingkat keparahan kerentanan. Amazon Inspector mengkategorikan ini sebagai skor dasar karena mencerminkan tingkat keparahan kerentanan menurut karakteristik intrinsiknya, yang konstan dari waktu ke waktu. Skor ini juga mengasumsikan dampak kasus terburuk yang wajar di berbagai lingkungan yang diterapkan. Standar CVSS v3 memetakan skor CVSS ke peringkat keparahan berikut.

Skor	Peringkat
0	Informational
0.1–3.9	Low
4.0–6.9	Medium
7.0–8.9	High
9.0–10.0	Critical

Temuan Package vulnerability juga dapat memiliki tingkat keparahan Untriaged. Ini berarti bahwa vendor belum menetapkan skor kerentanan untuk kerentanan yang terdeteksi. Dalam hal ini, kami merekomendasikan menggunakan URL referensi untuk temuan untuk meneliti kerentanan tersebut dan merespons sesuai dengan itu.

Temuan kerentanan Package mencakup skor berikut dan vektor penilaian terkait sebagai bagian dari detail temuan mereka:

- Skor EPSS
- Skor Inspector
- CVSS 3.1 dari Amazon CVE
- CVSS 3.1 dari NVD
- CVSS 2.0 dari NVD (jika berlaku)

Tingkat keparahan kerentanan kode

Untuk temuan kerentanan kode Amazon Inspector menggunakan tingkat keparahan yang ditentukan oleh detektor CodeGuru Amazon yang menghasilkan temuan. Setiap detektor diberi tingkat keparahan menggunakan sistem penilaian CVSS v3. Untuk penjelasan tentang CodeGuru kegunaan keparahan, lihat definisi Keparahan dalam CodeGuru panduan ini. Untuk daftar detektor berdasarkan tingkat keparahan, pilih dari bahasa pemrograman yang didukung di bawah ini:

- Detektor Python berdasarkan tingkat keparahan
- Detektor Java berdasarkan tingkat keparahan

Tingkat keparahan jangkauan jaringan

Amazon Inspector menentukan tingkat keparahan kerentanan jangkauan jaringan berdasarkan layanan, port, dan protokol yang diekspos dan berdasarkan jenis jalur terbuka. Tabel berikut mendefinisikan peringkat keparahan ini. Nilai di kolom Peringkat jalur terbuka mewakili jalur terbuka dari gateway virtual, VPC peered, dan jaringan. AWS Direct Connect Semua layanan, port, dan protokol lain yang terpapar memiliki peringkat tingkat keparahan informasi.

Layanan	Port TCP	Port UDP	Peringkat jalur internet	Peringkat jalur terbuka
DHCP	67, 68, 546, 547	67, 68, 546, 547	Medium	Informational
Elasticsearch	9300, 9200	NA	Medium	Informational
FTP	21	21	High	Medium

Global catalog LDAP	3268	NA	Medium	Informational
Global catalog LDAP over TLS	3269	NA	Medium	Informational
HTTP	80	80	Low	Informational
HTTPS	443	443	Low	Informational
Kerberos	88, 464, 543, 544, 749, 751	88, 464, 749, 750, 751, 752	Medium	Informational
LDAP	389	389	Medium	Informational
LDAP over TLS	636	NA	Medium	Informational
MongoDB	27017, 27018, 27019, 28017	NA	Medium	Informational
MySQL	3306	NA	Medium	Informational
NetBIOS	137, 139	137, 138	Medium	Informational
NFS	111, 2049, 4045, 1110	111, 2049, 4045, 1110	Medium	Informational
Oracle	1521, 1630	NA	Medium	Informational
PostgreSQL	5432	NA	Medium	Informational
Print services	515	NA	High	Medium
RDP	3389	3389	Medium	Low
RPC	111, 135, 530	111, 135, 530	Medium	Informational
SMB	445	445	Medium	Informational
SSH	22	22	Medium	Low
SQL Server	1433	1434	Medium	Informational

Syslog	601	514	Medium	Informational
Telnet	23	23	High	Medium
WINS	1512, 42	1512, 42	Medium	Informational

Mengelola temuan di Amazon Inspector

Amazon Inspector menawarkan beberapa cara untuk mengurutkan, mengelompokkan, dan mengelola temuan Anda. Fitur-fitur ini membantu Anda menyesuaikan temuan dengan lingkungan Anda, mengumpulkan temuan berdasarkan pandangan yang berbeda, dan fokus pada kerentanan terhadap lingkungan spesifik Anda. AWS

Temuan muncul dalam berbagai pandangan berdasarkan keadaannya: aktif, ditekan, atau tertutup. Secara default, setiap tampilan hanya menampilkan temuan aktif. Temuan aktif mewakili masalah keamanan potensial yang terdeteksi oleh Amazon Inspector yang menunjukkan kerentanan atau potensi ancaman. Temuan yang ditekan adalah temuan aktif yang telah Anda kecualikan menggunakan aturan penekanan. Amazon Inspector secara otomatis menetapkan status temuan untuk ditutup ketika mendeteksi bahwa temuan tersebut diperbaiki. Anda tidak menutup temuan secara manual.

Anda juga dapat melihat temuan di AWS Security Hub, layanan yang memberikan pandangan komprehensif tentang keadaan keamanan Anda di seluruh AWS lingkungan Anda. Untuk informasi selengkapnya, lihat Integrasi Amazon Inspector dengan AWS Security Hub. Temuan gambar kontainer juga tersedia di konsol Amazon ECR, dan Anda dapat melihat temuan untuk semua sumber daya menggunakan AWS Command Line Interface (AWS CLI) atau API.

Topik

Melihat temuan Amazon Inspector

Konsol Amazon Inspector menampilkan temuan dalam tampilan tab berdasarkan pengelompokan terkait. Setiap tampilan mencakup informasi yang dapat membantu Anda menganalisis kerentanan tertentu, mengidentifikasi sumber daya Anda yang paling rentan, dan mengukur dampak keseluruhan kerentanan di lingkungan Anda. Anda dapat menavigasi ke tampilan temuan yang berbeda dengan memilih opsi di bawah panel sisi navigasi Temuan. Anda juga dapat membuat filter di setiap tampilan

untuk fokus pada jenis temuan tertentu. Untuk informasi selengkapnya tentang menggunakan filter, lihatMemfilter temuan Amazon Inspector.

Temuan dapat dikelompokkan berdasarkan parameter berikut:

- Berdasarkan kerentanan — Daftar kerentanan paling kritis yang terdeteksi di lingkungan Anda. Pilih judul kerentanan dari tampilan ini untuk membuka panel detail dengan informasi tambahan.
- Berdasarkan akun — Daftar akun Anda, Amazon Inspector memindai persentase cakupan untuk setiap akun, dan jumlah total temuan tingkat keparahan kritis dan tinggi untuk setiap akun. Pengelompokan ini hanya tersedia untuk administrator yang didelegasikan.
- Misalnya — Daftar instans Amazon EC2 yang paling rentan di lingkungan Anda.
- Berdasarkan gambar kontainer - Daftar gambar kontainer Amazon ECR yang paling rentan di lingkungan Anda.
- Dengan repositori kontainer - Menampilkan repositori dengan kerentanan paling banyak.
- Dengan fungsi Lambda - Menunjukkan fungsi Lambda dengan kerentanan paling banyak.
- Semua temuan - Menampilkan daftar lengkap temuan untuk lingkungan Anda. Ini adalah tampilan default saat Anda menavigasi ke halaman Temuan. Dalam tampilan ini Anda dapat memfilter berdasarkan temuan aktif, ditekan, dan tertutup.

Anda dapat membuat aturan penekanan berdasarkan filter untuk mengecualikan temuan dari pandangan temuan. Untuk informasi selengkapnya, lihat Menekan temuan Amazon Inspector dengan aturan penindasan.

Memfilter temuan Amazon Inspector

Filter temuan memungkinkan Anda untuk melihat hanya temuan yang sesuai dengan kriteria yang Anda tentukan. Temuan yang tidak sesuai dengan kriteria filter dikecualikan dari tampilan Anda. Anda dapat membuat filter pencarian menggunakan konsol Amazon Inspector. Untuk menggunakan filter ini untuk secara otomatis menekan temuan yang ada dan yang akan datang, lihatMenekan temuan Amazon Inspector dengan aturan penindasan.

Membuat filter di konsol Amazon Inspector

Di setiap tampilan temuan, Anda dapat menggunakan fungsionalitas filter untuk menemukan temuan dengan karakteristik tertentu. Filter akan dihapus ketika Anda pindah ke tampilan tab yang berbeda.

Filter terdiri dari kriteria filter, yang terdiri dari atribut filter yang dipasangkan dengan nilai filter. Temuan yang tidak sesuai dengan kriteria filter Anda dikeluarkan dari daftar temuan. Misalnya, untuk melihat semua temuan yang terkait dengan akun administrator Anda, Anda dapat memilih atribut ID AWS akun dan memasangkannya dengan nilai ID AWS akun dua belas digit Anda.

Beberapa kriteria filter berlaku untuk semua temuan, sementara yang lain tersedia untuk jenis sumber daya tertentu atau jenis pencarian saja.

Untuk menerapkan filter ke tampilan temuan

1. Buka konsol Amazon Inspector di https://console.aws.amazon.com/inspector/v2/home.
2. Di panel navigasi, pilih Temuan. Tampilan default menampilkan semua temuan dengan status Aktif.
3. Untuk memfilter temuan berdasarkan kriteria, pilih bilah Tambahkan filter untuk melihat daftar semua kriteria filter yang berlaku untuk tampilan tersebut. Kriteria filter yang berbeda tersedia dalam tampilan yang berbeda.
4. Pilih kriteria yang ingin Anda filter dari daftar.
5. Dari panel input kriteria masukkan nilai filter yang diinginkan untuk menentukan kriteria itu.
6. Pilih Terapkan untuk menerapkan kriteria filter tersebut ke hasil Anda saat ini. Anda dapat terus menambahkan kriteria filter lainnya dengan memilih bilah input filter lagi.
7. (Opsional) Untuk melihat temuan Anda yang ditekan atau ditutup, pilih Aktif di bilah filter, lalu pilih Ditekan atau Ditutup. Pilih Tampilkan semua untuk melihat temuan aktif, ditekan, dan tertutup dalam tampilan yang sama.

Menekan temuan Amazon Inspector dengan aturan penindasan

Gunakan aturan penekanan untuk mengecualikan temuan yang sesuai dengan kriteria. Misalnya, Anda dapat membuat aturan yang menekan semua temuan dengan skor kerentanan rendah, sehingga Anda hanya dapat fokus pada temuan yang paling kritis.

> **Note**
>
> Aturan penekanan hanya digunakan untuk memfilter daftar temuan Anda dan tidak berdampak pada temuan atau mencegah Amazon Inspector menghasilkan temuan.

Jika Amazon Inspector menghasilkan temuan yang cocok dengan aturan penekanan, temuan diatur ke Suppressed. Temuan yang cocok dengan aturan penekanan tidak muncul dalam daftar Anda secara default.

Toko Amazon Inspector menekan temuan sampai mereka diperbaiki. Amazon Inspector mendeteksi findigs yang diperbaiki. Ketika Amazon Inspector mendeteksi temuan yang diperbaiki, ia menetapkan temuan ke Closed dan menyimpannya selama 7 hari.

Temuan yang ditekan dipublikasikan ke AWS Security Hub dan Amazon EventBridge sebagai peristiwa. Anda dapat secara otomatis menekan temuan yang tidak diinginkan di Security Hub dengan mengubah status temuan menggunakan EventBridge aturan. Untuk informasi selengkapnya, lihat Cara membuat aturan penindasan otomatis di. AWS Security Hub

Anda tidak dapat membuat aturan penindasan yang menutup atau memulihkan temuan. Anda hanya dapat membuat aturan penekanan untuk memfilter temuan mana yang muncul dalam daftar Anda. Anda dapat melihat temuan yang ditekan kapan saja di konsol Amazon Inspector.

> **Note**
>
> Akun anggota di organisasi tidak dapat membuat atau mengelola aturan penindasan.

Membuat aturan penindasan

Anda dapat membuat aturan penekanan untuk memfilter daftar temuan yang ditampilkan secara default. Anda dapat membuat aturan penekanan secara terprogram dengan menggunakan CreateFilterAPI dan menentukan `SUPRESS` sebagai nilai untuk. `action`

> **Note**
>
> Hanya akun yang berdiri sendiri dan administrator yang didelegasikan Amazon Inspector yang dapat membuat dan mengelola aturan penindasan. Anggota dalam organisasi tidak akan melihat opsi untuk aturan penindasan di panel navigasi.

Untuk membuat aturan penindasan (konsol)

1. Buka konsol Amazon Inspector di https://console.aws.amazon.com/inspector/v2/home.
2. Di panel navigasi, pilih Aturan penindasan. Kemudian, pilih Buat aturan.

3. Untuk setiap kriteria, lakukan hal berikut:
   - Pilih bilah filter untuk melihat daftar kriteria filter yang dapat Anda tambahkan ke aturan penekanan Anda.
   - Pilih kriteria filter untuk aturan penekanan Anda.
4. Setelah selesai menambahkan kriteria, masukkan nama untuk aturan dan deskripsi opsional.
5. Pilih Simpan aturan. Amazon Inspector segera menerapkan aturan penindasan baru dan menyembunyikan temuan apa pun yang sesuai dengan kriteria.

Melihat temuan yang ditekan

Secara default, Amazon Inspector tidak menampilkan temuan yang ditekan di konsol Amazon Inspector. Namun, Anda dapat melihat temuan yang ditekan oleh aturan tertentu.

Untuk melihat temuan yang ditekan

1. Buka konsol Amazon Inspector di https://console.aws.amazon.com/inspector/v2/home.
2. Di panel navigasi, pilih Aturan penindasan.
3. Dalam daftar aturan penindasan, pilih judul aturan.

Mengubah aturan penekanan

Anda dapat membuat perubahan pada aturan penindasan kapan saja.

Untuk memodifikasi aturan penindasan

1. Buka konsol Amazon Inspector di https://console.aws.amazon.com/inspector/v2/home
2. Di panel navigasi, pilih Aturan penindasan.
3. Pilih judul aturan penekanan yang ingin Anda ubah.
4. Buat perubahan yang diinginkan, lalu pilih Simpan untuk memperbarui aturan.

Menghapus aturan penekanan

Anda dapat menghapus aturan penekanan. Jika Anda menghapus aturan penindasan, Amazon Inspector berhenti menekan kemunculan temuan baru dan yang sudah ada yang memenuhi kriteria aturan dan yang tidak ditekan oleh aturan lain.

Setelah Anda menghapus aturan penekanan, kemunculan temuan baru dan yang sudah ada yang memenuhi kriteria aturan memiliki status Aktif. Ini berarti bahwa mereka muncul secara default di konsol Amazon Inspector. Selain itu, Amazon Inspector menerbitkan temuan ini ke AWS Security Hub dan Amazon EventBridge sebagai acara.

Untuk menghapus aturan penindasan

1. Buka konsol Amazon Inspector di https://console.aws.amazon.com/inspector/v2/home.
2. Di panel navigasi, pilih Aturan penindasan.
3. Pilih kotak centang di sebelah judul aturan penekanan yang ingin Anda hapus.
4. Pilih Hapus, lalu konfirmasikan pilihan Anda untuk menghapus aturan secara permanen.

Mengekspor laporan temuan dari Amazon Inspector

Selain mengirimkan temuan ke Amazon EventBridge danAWS Security Hub, Anda dapat secara opsional mengekspor temuan ke bucket Amazon Simple Storage Service (Amazon S3) sebagai laporan temuan. Laporan temuan adalah file CSV atau JSON yang berisi rincian temuan yang Anda pilih untuk dimasukkan dalam laporan. Ini memberikan gambaran rinci dari temuan Anda pada titik waktu tertentu. Untuk setiap temuan, file tersebut menyertakan detail seperti Amazon Resource Name (ARN) dari sumber daya yang terpengaruh, tanggal dan waktu saat temuan dibuat, ID Common Vulnerabilities and Exposures (CVE) terkait, dan tingkat keparahan temuan, status, dan skor Amazon Inspector dan CVSS.

Saat Anda mengonfigurasi laporan temuan, Anda mulai dengan menentukan temuan mana yang akan disertakan dalam laporan. Secara default, Amazon Inspector menyertakan data untuk semua temuan Anda saat ini Wilayah AWS yang berstatus Aktif. Jika Anda adalah administrator Amazon Inspector yang didelegasikan untuk organisasi, ini termasuk data temuan untuk semua akun anggota di organisasi Anda.

Anda dapat menyesuaikan laporan secara opsional dengan memfilter data. Dengan filter, Anda dapat menyertakan atau mengecualikan data untuk temuan yang memiliki karakteristik tertentu—misalnya, semua temuan Kritis yang dibuat selama rentang waktu tertentu, semua temuan Aktif untuk sumber daya tertentu, atau semua temuan Kritis dari jenis tertentu. Jika Anda administrator Amazon Inspector untuk suatu organisasi, Anda dapat menggunakan filter untuk membuat laporan yang menyertakan temuan untuk spesifik Akun AWS di organisasi Anda—misalnya, semua temuan Kritis akun yang memiliki status Aktif dan perbaikannya tersedia. Anda kemudian dapat membagikan laporan dengan pemilik akun untuk perbaikan.

> **Note**
>
> Saat Anda mengekspor laporan temuan menggunakan CreateFindingsReportAPI, Anda hanya akan melihat temuan Aktif secara default. Untuk melihat Temuan yang Ditutup atau Ditutup, Anda harus menentukan `SUPPRESSED` atau `CLOSED` sebagai nilai untuk kriteria filter FindingStatus.

Saat Anda mengekspor laporan temuan, Amazon Inspector mengenkripsi data dengan kunci AWS Key Management Service (AWS KMS) yang Anda tentukan, dan menambahkan laporan ke bucket S3 yang juga Anda tentukan. Kunci enkripsi harus berupa kunci enkripsi simetris yang dikelola pelanggan, AWS Key Management Service (AWS KMS) yang ada saat iniWilayah AWS. Selain itu, kebijakan utama harus mengizinkan Amazon Inspector untuk menggunakan kunci. Bucket S3 juga harus berada di Region saat ini, dan kebijakan bucket harus mengizinkan Amazon Inspector untuk menambahkan objek ke bucket.

Setelah Amazon Inspector selesai mengenkripsi dan menyimpan laporan, Anda dapat mengunduh laporan dari bucket S3 yang Anda tentukan atau memindahkannya ke lokasi lain. Atau, Anda dapat menyimpan laporan di bucket S3 yang sama dan menggunakan bucket tersebut sebagai repositori untuk laporan temuan yang selanjutnya Anda ekspor.

Topik ini memandu Anda melalui proses penggunaan AWS Management Console untuk mengekspor laporan temuan. Prosesnya terdiri dari memverifikasi bahwa Anda memiliki izin yang Anda butuhkan, mengonfigurasi sumber daya yang Anda butuhkan, dan kemudian mengonfigurasi dan mengekspor laporan.

> **Note**
>
> Anda hanya dapat mengekspor satu laporan temuan dalam satu waktu. Jika ekspor sedang berlangsung, tunggu hingga ekspor selesai sebelum Anda mencoba mengekspor laporan lain.

Tugas

- Langkah 1: Verifikasi izin Anda
- Langkah 2: Konfigurasikan bucket S3
- Langkah 3: Konfigurasikan AWS KMS key

- Langkah 4: Konfigurasikan dan ekspor laporan temuan
- Memecahkan masalah kesalahan ekspor

Setelah Anda mengekspor laporan temuan untuk pertama kalinya, langkah 1-3 dapat bersifat opsional. Ini terutama tergantung pada apakah Anda ingin menggunakan bucket S3 yang sama dan AWS KMS key untuk laporan selanjutnya.

Jika Anda lebih suka mengekspor laporan secara terprogram setelah langkah 1-3, gunakan CreateFindingsReportpengoperasian Amazon Inspector API.

Langkah 1: Verifikasi izin Anda

Sebelum mengekspor laporan temuan dari Amazon Inspector, verifikasi bahwa Anda memiliki izin yang Anda perlukan untuk mengekspor laporan temuan dan mengonfigurasi sumber daya untuk mengenkripsi dan menyimpan laporan. 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 diizinkan untuk dilakukan untuk mengekspor laporan temuan.

Amazon Inspector

Untuk Amazon Inspector, verifikasi bahwa Anda diizinkan untuk melakukan tindakan berikut:

- `inspector2:ListFindings`
- `inspector2:CreateFindingsReport`

Tindakan ini memungkinkan Anda untuk mengambil data temuan untuk akun Anda dan mengekspor data tersebut dalam laporan temuan.

Jika Anda berencana untuk mengekspor laporan besar secara terprogram, Anda mungkin juga memverifikasi bahwa Anda diizinkan untuk melakukan tindakan berikut:`inspector2:GetFindingsReportStatus`, untuk memeriksa status laporan, dan`inspector2:CancelFindingsReport`, untuk membatalkan ekspor yang sedang berlangsung.

AWS KMS

UntukAWS KMS, verifikasi bahwa Anda diizinkan untuk melakukan tindakan berikut:

- `kms:GetKeyPolicy`

- `kms:PutKeyPolicy`

Tindakan ini memungkinkan Anda untuk mengambil dan memperbarui kebijakan kunci untuk AWS KMS key yang Anda inginkan Amazon Inspector gunakan untuk mengenkripsi laporan Anda.

Untuk menggunakan konsol Amazon Inspector untuk mengekspor laporan, 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 laporan Anda.

Jika Anda berencana untuk membuat kunci KMS baru untuk enkripsi laporan Anda, Anda juga harus diizinkan untuk melakukan `kms:CreateKey` tindakan.

Amazon S3

Untuk Amazon S3, verifikasi bahwa Anda diizinkan untuk melakukan tindakan berikut:

- `s3:CreateBucket`
- `s3:DeleteObject`
- `s3:PutBucketAcl`
- `s3:PutBucketPolicy`
- `s3:PutBucketPublicAccessBlock`
- `s3:PutObject`
- `s3:PutObjectAcl`

Tindakan ini memungkinkan Anda membuat dan mengonfigurasi bucket S3 tempat Amazon Inspector menyimpan laporan Anda. Mereka juga memungkinkan Anda untuk menambah dan menghapus objek dari ember.

Jika Anda berencana menggunakan konsol Amazon Inspector untuk mengekspor laporan, pastikan juga bahwa Anda diizinkan untuk melakukan tindakan `s3:ListAllMyBuckets` dan `s3:GetBucketLocation` tindakan. Tindakan ini memungkinkan Anda untuk mengambil dan menampilkan informasi tentang bucket S3 untuk akun Anda. Anda kemudian dapat memilih salah satu ember ini untuk menyimpan laporan.

Jika Anda tidak diizinkan untuk melakukan satu atau beberapa tindakan yang diperlukan, mintalah bantuan AWS administrator Anda sebelum melanjutkan ke langkah berikutnya.

Langkah 2: Konfigurasikan bucket S3

Setelah memverifikasi izin, Anda siap mengonfigurasi bucket S3 tempat Anda ingin menyimpan laporan temuan. Ini bisa berupa bucket yang sudah ada untuk akun Anda sendiri, atau bucket yang sudah ada yang dimiliki oleh orang lain Akun AWS dan Anda diizinkan untuk mengaksesnya. Jika Anda ingin menyimpan laporan Anda di bucket baru, buat bucket sebelum melanjutkan.

Bucket S3 harus Wilayah AWS sama dengan data temuan yang ingin Anda ekspor. Misalnya, jika Anda menggunakan Amazon Inspector di Wilayah AS Timur (Virginia N.) dan Anda ingin mengekspor data temuan untuk Wilayah tersebut, bucket tersebut juga harus berada di Wilayah AS Timur (Virginia N.).

Selain itu, kebijakan bucket harus mengizinkan Amazon Inspector untuk menambahkan objek ke bucket. Topik ini menjelaskan cara memperbarui kebijakan bucket dan memberikan contoh pernyataan untuk ditambahkan ke kebijakan. Untuk informasi mendetail tentang menambahkan dan memperbarui kebijakan bucket, lihat Menggunakan kebijakan bucket di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

Jika Anda ingin menyimpan laporan di bucket S3 yang dimiliki oleh akun lain, bekerjalah dengan pemilik bucket untuk memperbarui kebijakan bucket. Dapatkan juga URI untuk bucket. Anda harus memasukkan URI ini saat mengekspor laporan.

Untuk memperbarui kebijakan bucket

1. Buka konsol Amazon S3 di https://console.aws.amazon.com/s3.
2. Di panel navigasi, pilih Bucket.
3. Pilih bucket S3 tempat Anda ingin menyimpan laporan temuan.
4. Pilih tab Izin.
5. Di bagian Kebijakan bucket, pilih Edit.
6. Salin pernyataan contoh berikut ke clipboard Anda:

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

```
    "Sid": "allow-inspector",
    "Effect": "Allow",
    "Principal": {
     "Service": "inspector2.amazonaws.com"
    },
    "Action": [
     "s3:PutObject",
     "s3:PutObjectAcl",
     "s3:AbortMultipartUpload"
    ],
    "Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*",
    "Condition": {
     "StringEquals": {
      "aws:SourceAccount": "111122223333"
     },
     "ArnLike": {
      "aws:SourceArn": "arn:aws:inspector2:Region:111122223333:report/*"
     }
    }
   }
  ]
}
```

7. Di editor kebijakan Bucket di konsol Amazon S3, tempelkan pernyataan sebelumnya ke dalam kebijakan untuk menambahkannya ke kebijakan.

   Ketika Anda menambahkan pernyataan, pastikan bahwa sintaksnya valid. Kebijakan bucket menggunakan format JSON. Ini berarti Anda perlu menambahkan koma sebelum atau sesudah pernyataan, tergantung di mana Anda menambahkan pernyataan ke kebijakan. Jika Anda menambahkan pernyataan sebagai pernyataan terakhir, tambahkan koma setelah tanda kurung kurung penutup untuk pernyataan sebelumnya. Jika Anda menambahkannya sebagai pernyataan pertama atau di antara dua pernyataan yang ada, tambahkan koma setelah tanda kurung kurung penutup untuk pernyataan tersebut.

8. Perbarui pernyataan dengan nilai yang benar untuk lingkungan Anda, di mana:

   - *DOC-EXAMPLE-BUCKET adalah nama bucket*.
   - *111122223333* adalah ID akun untuk Anda. Akun AWS
   - *Wilayah* adalah Wilayah AWS tempat Anda menggunakan Amazon Inspector dan ingin mengizinkan Amazon Inspector menambahkan laporan ke bucket. Misalnya, `us-east-1` untuk Wilayah AS Timur (Virginia N.).

> **Note**
>
> Jika Anda menggunakan Amazon Inspector secara manual diaktifkanWilayah AWS, tambahkan juga kode Region yang sesuai ke nilai untuk bidang tersebut`Service`. Bidang ini menentukan prinsipal layanan Amazon Inspector.
> Misalnya, jika Anda menggunakan Amazon Inspector in the Middle East (Bahrain) Region, yang memiliki kode Region`me-south-1`, ganti `inspector2.amazonaws.com` dengan `inspector2.me-south-1.amazonaws.com` dalam pernyataan.

Perhatikan bahwa pernyataan contoh mendefinisikan kondisi yang menggunakan dua kunci kondisi global IAM:

- aws: SourceAccount — Kondisi ini memungkinkan Amazon Inspector untuk menambahkan laporan ke bucket hanya untuk akun Anda. Ini mencegah Amazon Inspector menambahkan laporan ke bucket untuk akun lain. Lebih khusus lagi, kondisi menentukan akun mana yang dapat menggunakan bucket untuk sumber daya dan tindakan yang ditentukan oleh `aws:SourceArn` kondisi.

  Untuk menyimpan laporan untuk akun tambahan di bucket, tambahkan ID akun untuk setiap akun tambahan ke kondisi ini. Misalnya:

  ```
  "aws:SourceAccount": [111122223333,444455556666,123456789012]
  ```

- 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 Amazon Inspector menambahkan objek ke bucket saat melakukan tindakan lain untuk akun Anda. Lebih khusus lagi, kondisi ini memungkinkan Amazon Inspector untuk menambahkan objek ke bucket hanya jika objek adalah laporan temuan, dan hanya jika laporan tersebut dibuat oleh akun dan di Wilayah yang ditentukan dalam kondisi.

  Agar Amazon Inspector dapat melakukan tindakan yang ditentukan untuk akun tambahan, tambahkan Amazon Resource Names (ARN) untuk setiap akun tambahan ke kondisi ini. Misalnya:

  ```
  "aws:SourceArn": [
      "arn:aws:inspector2:Region:111122223333:report/*",
  ```

```
    "arn:aws:inspector2:Region:444455556666:report/*",
    "arn:aws:inspector2:Region:123456789012:report/*"
]
```

Akun yang ditentukan oleh `aws:SourceAccount` dan `aws:SourceArn` kondisi harus cocok.

Kedua kondisi tersebut membantu mencegah Amazon Inspector digunakan sebagai wakil yang bingung selama transaksi dengan Amazon S3. Meskipun kami tidak merekomendasikannya, Anda dapat menghapus kondisi ini dari kebijakan bucket.

9. Setelah Anda selesai memperbarui kebijakan bucket, pilih Simpan perubahan.

Langkah 3: Konfigurasikan AWS KMS key

Setelah memverifikasi izin dan mengonfigurasi bucket S3, tentukan yang ingin digunakan Amazon Inspector untuk mengenkripsi laporan temuan AWS KMS key Anda. Kuncinya harus berupa kunci KMS enkripsi simetris yang dikelola pelanggan. Selain itu, kuncinya harus Wilayah AWS sama dengan bucket S3 yang Anda konfigurasikan untuk menyimpan laporan.

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 KMS baru, buat kunci sebelum melanjutkan. Jika Anda ingin menggunakan kunci yang ada yang dimiliki akun lain, dapatkan Amazon Resource Name (ARN) dari kunci tersebut. Anda harus memasukkan ARN ini saat mengekspor laporan dari Amazon Inspector. Untuk informasi tentang membuat dan meninjau pengaturan kunci KMS, lihat Mengelola kunci di Panduan AWS Key Management Service Pengembang.

Setelah Anda menentukan kunci KMS mana yang ingin Anda gunakan, berikan izin kepada Amazon Inspector untuk menggunakan kunci tersebut. Jika tidak, Amazon Inspector tidak akan dapat mengenkripsi dan mengekspor laporan. Untuk memberikan izin kepada Amazon Inspector 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

> **Note**
>
> Prosedur berikut adalah memperbarui kunci yang ada untuk memungkinkan Amazon Inspector menggunakannya. Jika Anda belum memiliki kunci yang ada, lihat panduan https://docs.aws.amazon.com/kms/latest/developerguide/create-keys.html untuk membuatnya.

1. Buka konsol AWS KMS di https://console.aws.amazon.com/kms.
2. Untuk mengubahWilayah AWS, gunakan pemilih Wilayah di sudut kanan atas halaman.
3. Di panel navigasi, pilih Kunci yang dikelola pelanggan.
4. Pilih kunci KMS yang ingin Anda gunakan untuk mengenkripsi laporan. Kuncinya harus berupa kunci enkripsi simetris (SYMMETRIC_DEFAULT).
5. Di tab Kebijakan kunci, pilih Edit. Jika Anda tidak melihat kebijakan kunci dengan tombol Edit, Anda harus terlebih dahulu memilih Beralih ke tampilan kebijakan.
6. Salin pernyataan contoh berikut ke clipboard Anda:

```
{
    "Sid": "Allow Amazon Inspector to use the key",
    "Effect": "Allow",
    "Principal": {
        "Service": "inspector2.amazonaws.com"
    },
    "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey*"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:SourceAccount": "111122223333"
        },
        "ArnLike": {
            "aws:SourceArn": "arn:aws:inspector2:Region:111122223333:report/*"
        }
    }
}
```

7. Di editor kebijakan kunci di AWS KMS konsol, tempelkan pernyataan sebelumnya ke kebijakan kunci untuk menambahkannya ke kebijakan.

   Ketika Anda menambahkan pernyataan, pastikan bahwa sintaksnya valid. Kebijakan kunci menggunakan format JSON. Ini berarti Anda perlu menambahkan koma sebelum atau sesudah pernyataan, tergantung di mana Anda menambahkan pernyataan ke kebijakan. Jika Anda menambahkan pernyataan sebagai pernyataan terakhir, tambahkan koma setelah tanda kurung kurung penutup untuk pernyataan sebelumnya. Jika Anda menambahkannya sebagai pernyataan pertama atau di antara dua pernyataan yang ada, tambahkan koma setelah tanda kurung kurung penutup untuk pernyataan tersebut.

8. Perbarui pernyataan dengan nilai yang benar untuk lingkungan Anda, di mana:

   - *111122223333* adalah ID akun untuk Anda. Akun AWS
   - *Wilayah* adalah Wilayah AWS tempat Anda ingin mengizinkan Amazon Inspector mengenkripsi laporan dengan kuncinya. Misalnya, `us-east-1` untuk Wilayah AS Timur (Virginia N.).

   > **Note**
   >
   > Jika Anda menggunakan Amazon Inspector secara manual diaktifkanWilayah AWS, tambahkan juga kode Region yang sesuai ke nilai untuk bidang tersebut`Service`. Misalnya, jika Anda menggunakan Amazon Inspector di Wilayah Timur Tengah (Bahrain), ganti dengan. `inspector2.amazonaws.com` `inspector2.me-south-1.amazonaws.com`

   Seperti pernyataan contoh untuk kebijakan bucket pada langkah sebelumnya, `Condition` bidang dalam contoh ini menggunakan dua kunci kondisi global IAM:

   - aws: SourceAccount — Kondisi ini memungkinkan Amazon Inspector 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 mengizinkan Amazon Inspector melakukan tindakan yang ditentukan untuk akun tambahan, tambahkan ID akun untuk setiap akun tambahan ke kondisi ini. Misalnya:

```
"aws:SourceAccount": [111122223333,444455556666,123456789012]
```

- aws: SourceArn — Kondisi ini mencegah orang lain Layanan AWS melakukan tindakan yang ditentukan. Ini juga mencegah Amazon Inspector menggunakan kunci saat melakukan tindakan lain untuk akun Anda. Dengan kata lain, ini memungkinkan Amazon Inspector untuk mengenkripsi objek S3 dengan kunci hanya jika objek adalah laporan temuan, dan hanya jika laporan tersebut dibuat oleh akun dan di Wilayah yang ditentukan dalam kondisi.

  Untuk mengizinkan Amazon Inspector melakukan tindakan yang ditentukan untuk akun tambahan, tambahkan ARN untuk setiap akun tambahan ke kondisi ini. Misalnya:

  ```
  "aws:SourceArn": [
      "arn:aws:inspector2:us-east-1:111122223333:report/*",
      "arn:aws:inspector2:us-east-1:444455556666:report/*",
      "arn:aws:inspector2:us-east-1:123456789012:report/*"
  ]
  ```

  Akun yang ditentukan oleh `aws:SourceAccount` dan `aws:SourceArn` kondisi harus cocok.

Kondisi ini membantu mencegah Amazon Inspector digunakan sebagai wakil yang bingung selama transaksi dengan. AWS KMS Meskipun kami tidak merekomendasikannya, Anda dapat menghapus kondisi ini dari pernyataan.

9. Setelah selesai memperbarui kebijakan kunci, pilih Simpan perubahan.

Langkah 4: Konfigurasikan dan ekspor laporan temuan

Setelah memverifikasi izin dan mengonfigurasi sumber daya untuk mengenkripsi dan menyimpan laporan temuan, Anda siap mengonfigurasi dan mengekspor laporan.

Untuk mengonfigurasi dan mengekspor laporan temuan

1. Buka konsol Amazon Inspector di https://console.aws.amazon.com/inspector/v2/home.
2. Di panel navigasi, di bawah Temuan, pilih Semua temuan.
3. (Opsional) Dengan menggunakan bilah filter di atas tabel Temuan, tambahkan kriteria filter yang menentukan temuan mana yang akan disertakan dalam laporan. Saat Anda menambahkan kriteria, Amazon Inspector memperbarui tabel untuk menyertakan hanya temuan yang sesuai dengan kriteria. Tabel menyediakan pratinjau data yang akan berisi laporan Anda.

> **Note**
>
> Kami menyarankan Anda menambahkan kriteria filter. Jika tidak, laporan akan menyertakan data untuk semua temuan Anda saat ini Wilayah AWS yang berstatus Aktif. Jika Anda administrator Amazon Inspector untuk suatu organisasi, ini termasuk data temuan untuk semua akun anggota di organisasi Anda.
> Jika laporan menyertakan data untuk semua atau banyak temuan, perlu waktu lama untuk menghasilkan dan mengekspor laporan, dan Anda hanya dapat mengekspor satu laporan pada satu waktu.

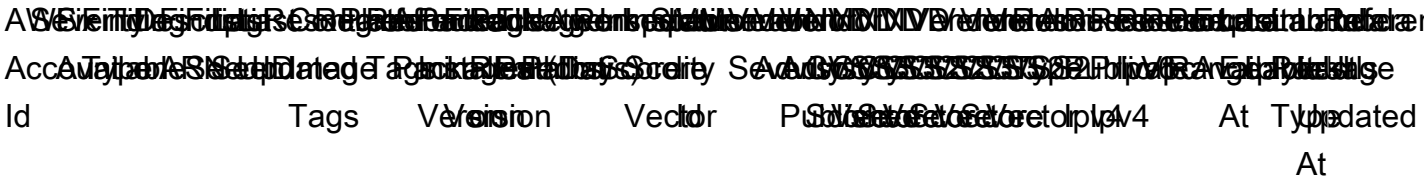
4. Pilih temuan Ekspor.
5. Di bagian Pengaturan ekspor, untuk Ekspor jenis file, tentukan format file untuk laporan:

   - Untuk membuat file JavaScript Object Notation (.json) yang berisi data, pilih JSON.

     Jika Anda memilih opsi JSON, laporan akan menyertakan semua bidang untuk setiap temuan. Untuk daftar kemungkinan bidang JSON, lihat tipe data Finding di referensi Amazon Inspector API.

   - Untuk membuat file nilai dipisahkan koma (.csv) yang berisi data, pilih CSV.

     Jika Anda memilih opsi CSV, laporan hanya akan menyertakan subset bidang untuk setiap temuan, kira-kira 45 bidang yang melaporkan atribut kunci dari temuan. Bidang meliputi: Jenis Penemuan, Judul, Tingkat Keparahan, Status, Deskripsi, Pertama Dilihat, Terakhir Terlihat, Perbaiki Tersedia, ID AWS akun, ID Sumber Daya, Tag Sumber Daya, dan Remediasi. Ini adalah tambahan untuk bidang yang menangkap detail penilaian dan URL referensi untuk setiap temuan. Berikut ini adalah contoh header CSV dalam laporan temuan:

6. Di bawah Lokasi ekspor, untuk URI S3, tentukan bucket S3 tempat Anda ingin menyimpan laporan:

- Untuk menyimpan laporan dalam bucket yang dimiliki akun Anda, pilih Browse S3. Amazon Inspector menampilkan tabel bucket S3 untuk akun Anda. Pilih baris untuk ember yang Anda inginkan, lalu pilih Pilih.

  > **Tip**
  >
  > Untuk juga menentukan awalan jalur Amazon S3 untuk laporan, tambahkan garis miring (/) dan awalan ke nilai di kotak URI S3. Amazon Inspector kemudian menyertakan awalan saat menambahkan laporan ke bucket, dan Amazon S3 menghasilkan jalur yang ditentukan oleh awalan.
  > Misalnya, jika Anda ingin menggunakan Akun AWS ID Anda sebagai awalan dan ID akun Anda adalah 111122223333, tambahkan **`/111122223333`** nilai di kotak URI S3. Awalan mirip dengan jalur direktori dalam bucket S3. Ini memungkinkan Anda untuk mengelompokkan objek serupa bersama-sama dalam ember, seperti Anda mungkin menyimpan file serupa bersama-sama dalam folder pada sistem file. Untuk informasi selengkapnya, lihat Mengatur objek di konsol Amazon S3 menggunakan folder di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

- Untuk menyimpan laporan dalam bucket yang dimiliki akun lain, masukkan URI untuk bucket—misalnya, di mana DOC-EXAMPLE_BUCKET adalah nama bucket. **`s3://DOC-EXAMPLE_BUCKET`** Pemilik ember dapat menemukan informasi ini untuk Anda di properti ember.

7. Untuk kunci KMS, tentukan AWS KMS key yang ingin Anda gunakan untuk mengenkripsi laporan:

   - Untuk menggunakan kunci dari akun Anda sendiri, pilih kunci dari daftar. Daftar ini menampilkan kunci KMS enkripsi simetris yang dikelola pelanggan untuk akun Anda.
   - Untuk menggunakan kunci yang dimiliki akun lain, masukkan Nama Sumber Daya Amazon (ARN) dari kunci tersebut. Pemilik kunci dapat menemukan informasi ini untuk Anda di properti kunci. Untuk informasi selengkapnya, lihat Menemukan ID kunci dan kunci ARN di Panduan AWS Key Management Service Pengembang.

8. Pilih Ekspor.

Amazon Inspector membuat laporan temuan, mengenkripsinya dengan kunci KMS yang Anda tentukan, dan menambahkannya ke bucket S3 yang Anda tentukan. Bergantung pada jumlah temuan yang Anda pilih untuk dimasukkan dalam laporan, proses ini dapat memakan waktu beberapa menit

atau jam. Ketika ekspor selesai, Amazon Inspector menampilkan pesan yang menunjukkan bahwa laporan temuan Anda berhasil diekspor. Secara opsional pilih Lihat laporan dalam pesan untuk menavigasi ke laporan di Amazon S3.

Perhatikan bahwa Anda hanya dapat mengekspor satu laporan dalam satu kali. Jika ekspor sedang berlangsung, tunggu hingga ekspor selesai sebelum Anda mencoba mengekspor laporan lain.

Memecahkan masalah kesalahan ekspor

Jika terjadi kesalahan saat Anda mencoba mengekspor laporan temuan, Amazon Inspector menampilkan pesan yang menjelaskan kesalahan tersebut. Anda dapat menggunakan informasi dalam topik ini sebagai panduan untuk mengidentifikasi kemungkinan penyebab dan solusi untuk kesalahan tersebut.

Misalnya, verifikasi bahwa bucket S3 ada di bucket saat ini Wilayah AWS dan kebijakan bucket memungkinkan Amazon Inspector untuk menambahkan objek ke bucket. Juga verifikasi bahwa AWS KMS key diaktifkan di Wilayah saat ini, dan pastikan bahwa kebijakan kunci memungkinkan Amazon Inspector untuk menggunakan kunci.

Setelah Anda mengatasi kesalahan, coba ekspor laporan lagi.

Tidak dapat memiliki beberapa laporan kesalahan

Jika Anda mencoba membuat laporan tetapi Amazon Inspector sudah membuat laporan, Anda akan menerima kesalahan yang menyatakan Alasan: Tidak dapat memiliki beberapa laporan yang sedang berlangsung. Kesalahan ini terjadi karena Amazon Inspector hanya dapat menghasilkan satu laporan untuk akun pada satu waktu.

Untuk mengatasi kesalahan, Anda dapat menunggu laporan lain selesai atau membatalkannya sebelum meminta laporan baru.

Anda dapat memeriksa status laporan dengan menggunakan GetFindingsReportStatusoperasi, operasi ini mengembalikan ID laporan dari setiap laporan yang sedang dibuat.

Jika perlu, Anda dapat menggunakan ID laporan yang diberikan oleh `GetFindingsReportStatus` operasi untuk membatalkan ekspor yang sedang berlangsung dengan menggunakan CancelFindingsReportoperasi.

Membuat respons kustom untuk temuan Amazon Inspector dengan Amazon EventBridge

Amazon Inspector membuat acara untuk Amazon EventBridge untuk temuan yang baru dibuat, temuan agregat baru, dan perubahan dalam keadaan temuan. Apa pun selain perubahan pada `updatedAt` dan `lastObservedAt` bidang akan menerbitkan acara baru. Ini berarti peristiwa baru untuk temuan dihasilkan ketika Anda mengambil tindakan seperti memulai ulang sumber daya atau mengubah tag yang terkait dengan sumber daya. Namun, ID temuan di `id` lapangan tetap sama. Peristiwa dipancarkan atas dasar upaya terbaik.

> **Note**
>
> Jika akun Anda adalah administrator yang didelegasikan Amazon Inspector, EventBridge publikasikan peristiwa ke akun Anda selain akun anggota asalnya.

Saat menggunakan EventBridge peristiwa dengan Amazon Inspector, Anda dapat mengotomatisasi tugas untuk membantu mengatasi masalah keamanan yang diungkapkan oleh temuan Amazon Inspector.

Amazon Inspector mengeluarkan peristiwa ke bus peristiwa default di Wilayah yang sama. Ini berarti Anda harus mengonfigurasi aturan peristiwa untuk setiap Wilayah tempat Anda menjalankan Amazon Inspector untuk melihat peristiwa untuk Wilayah tersebut.

Untuk menerima notifikasi tentang temuan Amazon Inspector berdasarkan EventBridge peristiwa, Anda harus membuat EventBridge aturan dan target untuk Amazon Inspector. Aturan ini memungkinkan EventBridge pengiriman notifikasi untuk temuan yang dibuat Amazon Inspector ke target yang ditentukan dalam aturan. Untuk informasi selengkapnya, lihat EventBridgeaturan Amazon di Panduan EventBridge Pengguna Amazon.

Skema peristiwa

Berikut ini adalah contoh format peristiwa Amazon Inspector untuk peristiwa temuan EC2. Misalnya skema jenis temuan lain dan jenis acara, lihatEventBridge skema.

```
{
    "version": "0",
    "id": "66a7a279-5f92-971c-6d3e-c92da0950992",
```

```
    "detail-type": "Inspector2 Finding",
    "source": "aws.inspector2",
    "account": "111122223333",
    "time": "2023-01-19T22:46:15Z",
    "region": "us-east-1",
    "resources": ["i-0c2a343f1948d5205"],
    "detail": {
        "awsAccountId": "111122223333",
        "description": "\n It was discovered that the sound subsystem in the Linux
 kernel contained a\n race condition in some situations. A local attacker could use
 this to cause\n a denial of service (system crash).",
        "exploitAvailable": "YES",
        "exploitabilityDetails": {
            "lastKnownExploitAt": "Oct 24, 2022, 11:08:59 PM"
        },
        "findingArn": "arn:aws:inspector2:us-east-1:111122223333:finding/FINDING_ID",
        "firstObservedAt": "Jan 19, 2023, 10:46:15 PM",
        "fixAvailable": "YES",
        "lastObservedAt": "Jan 19, 2023, 10:46:15 PM",
        "packageVulnerabilityDetails": {
            "cvss": [{
                "baseScore": 4.7,
                "scoringVector": "CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H",
                "source": "NVD",
                "version": "3.1"
            }],
            "referenceUrls": ["https://lore.kernel.org/all/
CAFcO6XN7JDM4xSXGhtusQfS2mSBcx50VJKwQpCq=WeLt57aaZA@mail.gmail.com/", "https://
ubuntu.com/security/notices/USN-5792-1", "https://ubuntu.com/security/notices/
USN-5791-2", "https://ubuntu.com/security/notices/USN-5791-1", "https://ubuntu.com/
security/notices/USN-5793-2", "https://git.kernel.org/pub/scm/linux/kernel/git/
torvalds/linux.git/commit/?id=8423f0b6d513b259fdab9c9bf4aaa6188d054c2d", "https://
ubuntu.com/security/notices/USN-5793-1", "https://ubuntu.com/security/notices/
USN-5792-2", "https://ubuntu.com/security/notices/USN-5791-3", "https://ubuntu.com/
security/notices/USN-5793-4", "https://ubuntu.com/security/notices/USN-5793-3",
 "https://git.kernel.org/linus/8423f0b6d513b259fdab9c9bf4aaa6188d054c2d(6.0-rc5)",
 "https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-3303"],
            "relatedVulnerabilities": [],
            "source": "UBUNTU_CVE",
            "sourceUrl": "https://people.canonical.com/~ubuntu-security/cve/2022/
CVE-2022-3303.html",
            "vendorCreatedAt": "Sep 27, 2022, 11:15:00 PM",
            "vendorSeverity": "medium",
            "vulnerabilityId": "CVE-2022-3303",
```

```
            "vulnerablePackages": [{
                "arch": "X86_64",
                "epoch": 0,
                "fixedInVersion": "0:5.15.0.1027.31~20.04.16",
                "name": "linux-image-aws",
                "packageManager": "OS",
                "remediation": "apt update && apt install --only-upgrade linux-image-
aws",
                "version": "5.15.0.1026.30~20.04.16"
            }]
        },
        "remediation": {
            "recommendation": {
                "text": "None Provided"
            }
        },
        "resources": [{
            "details": {
                "awsEc2Instance": {
                    "iamInstanceProfileArn": "arn:aws:iam::111122223333:instance-
profile/AmazonSSMRoleForInstancesQuickSetup",
                    "imageId": "ami-0b7ff1a8d69f1bb35",
                    "ipV4Addresses": ["172.31.85.212", "44.203.45.27"],
                    "ipV6Addresses": [],
                    "launchedAt": "Jan 19, 2023, 7:53:14 PM",
                    "platform": "UBUNTU_20_04",
                    "subnetId": "subnet-8213f2a3",
                    "type": "t2.micro",
                    "vpcId": "vpc-ab6650d1"
                }
            },
            "id": "i-0c2a343f1948d5205",
            "partition": "aws",
            "region": "us-east-1",
            "type": "AWS_EC2_INSTANCE"
        }],
        "severity": "MEDIUM",
        "status": "ACTIVE",
        "title": "CVE-2022-3303 - linux-image-aws",
        "type": "PACKAGE_VULNERABILITY",
        "updatedAt": "Jan 19, 2023, 10:46:15 PM"
    }
}
```

Membuat EventBridge aturan untuk memberi tahu Anda tentang temuan Amazon Inspector

Untuk meningkatkan visibilitas temuan Amazon Inspector, Anda dapat menggunakannya EventBridge untuk mengatur peringatan temuan secara otomatis yang dikirim ke pusat pesan. Topik ini menjelaskan cara mengirim peringatan untuk temuan `CRITICAL` dan `HIGH` tingkat keparahan ke email, Slack, atau Amazon Chime. Anda akan mempelajari cara mengatur topik Amazon Simple Notification Service, kemudian menghubungkannya ke aturan EventBridge peristiwa.

Langkah 1. Mengatur topik Amazon SNS dan titik akhir

Untuk mengatur peringatan secara otomatis, Anda harus terlebih dahulu mengatur topik di Amazon Simple Notification Service dan menambahkan titik akhir. Untuk informasi lebih lanjut, lihat panduan SNS.

Prosedur ini menetapkan tujuan pengiriman data temuan Amazon Inspector. Topik SNS dapat ditambahkan ke aturan EventBridge peristiwa selama atau setelah pembuatan aturan peristiwa.

Email setup

Membuat topik SNS

1. Masuk ke konsol Amazon SNS di https://console.aws.amazon.com/sns/v3/home.
2. Dari panel navigasi, pilih Topik, lalu pilih Buat Topik.
3. Di bagian Buat topik, pilih Standar. Selanjutnya, masukkan nama topik, seperti**`Inspector_to_Email`**. Detail lainnya bersifat opsional.
4. Pilih Buat Topik. Templat ini membuka panel baru dengan detail untuk topik baru Anda.
5. Di bagian Langganan, pilih Buat Langganan.
6. a. Dari menu Protokol, pilih Email.
   b. Untuk bidang Titik Akhir, masukkan alamat email untuk menerima notifikasi.

> **Note**
>
> Anda akan diminta untuk mengonfirmasi langganan Anda melalui klien email Anda setelah membuat langganan.

c. Pilih Buat langganan.

7. Cari pesan langganan di kotak masuk Anda dan pilih Konfirmasi Langganan.

Slack setup

Membuat topik SNS

1. Masuk ke konsol Amazon SNS di https://console.aws.amazon.com/sns/v3/home.
2. Dari panel navigasi, pilih Topik, lalu pilih Buat Topik.
3. Di bagian Buat topik, pilih Standar. Selanjutnya, masukkan nama topik, seperti**`Inspector_to_Slack`**. Detail lainnya bersifat opsional. Pilih Buat topik untuk menyelesaikan pembuatan endpoint.

Mengonfigurasi klien AWS Chatbot

1. Arahkan ke AWS Chatbot konsol dihttps://console.aws.amazon.com/chatbot/.
2. Dari panel Configurated clients, pilih Configure new client.
3. Pilih Slack, lalu pilih Konfigurasi untuk mengonfirmasi.

> **Note**
>
> Saat memilih Slack, Anda harus mengonfirmasi izin AWS Chatbot untuk agar dapat mengakses saluran Anda dengan memilih izinkan.

4. Pilih Konfigurasi saluran baru untuk membuka panel detail konfigurasi.

   a. Masukkan nama untuk saluran.

   b. Untuk saluran Slack, pilih saluran yang ingin Anda gunakan.

   c. Di Slack, salin ID saluran dari saluran pribadi dengan mengeklik kanan pada nama saluran dan memilih Salin Tautan.

   d. PadaAWS Management Console, di AWS Chatbot jendela, tempelkan ID saluran yang Anda salin dari Slack ke bidang ID saluran Pribadi.

   e. Pada bagian Izin, pilih untuk membuat IAM role menggunakan templat jika Anda belum memiliki peran.

f. Untuk Templat kebijakan, pilih Izin pemberitahuan. Berikut adalah templat kebijakan IAM untuk AWS Chatbot. Kebijakan ini menyediakan izin baca dan daftar yang diperlukan untuk CloudWatch alarm, peristiwa, dan log, serta untuk topik Amazon SNS.

g. Untuk kebijakan pagar pembatas Saluran, pilih AmazonInspector 2. ReadOnlyAccess

h. Pilih Wilayah tempat Anda membuat topik SNS sebelumnya, lalu pilih topik Amazon SNS yang Anda buat untuk mengirim notifikasi ke saluran Slack.

5. Pilih Konfigurasi.

Amazon Chime setup

Membuat topik SNS

1. Masuk ke konsol Amazon SNS di https://console.aws.amazon.com/sns/v3/home.
2. Pilih Topik dari panel navigasi, lalu pilih Buat Topik.
3. Di bagian Buat topik, pilih Standar. Selanjutnya, masukkan nama topik, seperti**`Inspector_to_Chime`**. Detail lainnya bersifat opsional. Pilih Buat topik untuk diselesaikan.

Mengonfigurasi klien AWS Chatbot

1. Arahkan ke AWS Chatbot konsol dihttps://console.aws.amazon.com/chatbot/.
2. Dari panel Klien yang dikonfigurasi, pilih Konfigurasikan klien baru.
3. Pilih Berpadu, lalu pilih Konfigurasi untuk mengonfirmasi.
4. Dari panel Detail konfigurasi, masukkan nama untuk saluran.
5. Di Amazon Chime, buka ruang obrolan yang diinginkan.

   a. Pilih ikon roda gigi di sudut kanan atas dan pilih Kelola webhook dan bot.

   b. Pilih Salin URL untuk menyalin URL webhook ke clipboard Anda.

6. PadaAWS Management Console, di AWS Chatbot jendela, tempel URL yang Anda salin ke bidang URL Webhook.
7. Pada bagian Izin, pilih untuk membuat IAM role menggunakan templat jika Anda belum memiliki peran.

8. Untuk Templat kebijakan, pilih Izin pemberitahuan. Berikut adalah templat kebijakan IAM untuk AWS Chatbot. Templat ini menyediakan izin baca dan daftar yang diperlukan untuk CloudWatch alarm, peristiwa, dan log, serta untuk topik Amazon SNS.
9. Pilih Wilayah tempat Anda membuat topik SNS sebelumnya, lalu pilih topik Amazon SNS yang Anda buat untuk mengirim notifikasi ke ruang Amazon Chime.
10. Pilih Konfigurasi.

Langkah 2. Membuat EventBridge aturan untuk temuan Amazon Inspector

1. Buka konsol Amazon EventBridge di https://console.aws.amazon.com/events/.
2. Pilih Aturan dari panel navigasi, lalu pilih Buat aturan.
3. Masukkan nama dan deskripsi opsional untuk aturan Anda.
4. Pilih Aturan dengan pola peristiwa dan kemudian Berikutnya.
5. Di panel Event Pattern, pilih Custom patterns (JSON editor).
6. Tempelkan JSON berikut ke editor.

```
{
  "source": ["aws.inspector2"],
  "detail-type": ["Inspector2 Finding"],
  "detail": {
    "severity": ["HIGH", "CRITICAL"],
    "status": ["ACTIVE"]
  }
}
```

> **Note**
>
> Pola ini mengirimkan notifikasi untuk setiap temuan aktif `CRITICAL` atau `HIGH` tingkat keparahan yang terdeteksi oleh Amazon Inspector.

Pilih Berikutnya ketika Anda selesai memasukkan pola acara.

7. Pada halaman Pilih target, pilih Layanan AWS. Kemudian, untuk Pilih jenis target, pilih topik SNS.
8. Untuk Topik, pilih nama topik SNS yang Anda buat di langkah 1. Kemudian pilih Selanjutnya.

9. Tambahkan tag opsional jika diperlukan dan pilih Berikutnya.
10. Tinjau aturan Anda, lalu pilih Buat aturan.

EventBridgeuntuk lingkungan multiakun Amazon Inspector

Jika Anda administrator didelegasikan Amazon Inspector, EventBridge aturan akan muncul di akun Anda berdasarkan temuan yang berlaku dari akun anggota Anda. Jika Anda menyiapkan pemberitahuan temuan melalui EventBridge akun administrator Anda, seperti yang dijelaskan di bagian sebelumnya, Anda akan menerima pemberitahuan tentang beberapa akun. Dengan kata lain, Anda akan diberi tahu tentang temuan dan peristiwa yang dihasilkan oleh akun anggota Anda selain yang dihasilkan oleh akun Anda sendiri.

Anda dapat menggunakan detail JSON `accountId` dari temuan ini untuk mengidentifikasi akun anggota tempat temuan Amazon Inspector berasal.

Mengekspor SBOM dengan Amazon Inspector

Anda dapat menggunakan konsol Amazon Inspector atau API untuk menghasilkan Software Bill of Materials (SBOM) untuk sumber daya Anda. SBOM adalah inventaris bersarang dari semua komponen perangkat lunak open source dan pihak ketiga dari basis kode Anda. Amazon Inspector menyediakan SBOM untuk sumber daya individual di lingkungan Anda. SBOM yang diekspor dari Amazon Inspector dapat membantu Anda mendapatkan visibilitas informasi tentang pasokan perangkat lunak Anda, seperti paket yang paling umum digunakan, dan kerentanan terkait di seluruh organisasi Anda.

Anda dapat mengekspor SBOM untuk semua sumber daya yang didukung yang sedang dipantau secara aktif oleh Amazon Inspector. Anda dapat meninjau status sumber daya Anda denganMenilai cakupan Amazon Inspector dari lingkungan Anda AWS.

> **Note**
>
> Amazon Inspector tidak mendukung ekspor SBOM untuk instans Windows EC2.

Format Amazon Inspector

Amazon Inspector mendukung ekspor SBOM dalam format yang kompatibel dengan CycloneDX 1.4 dan SPDX 2.3. Amazon Inspector mengekspor SBOM sebagai file `JSON` ke bucket Amazon S3 yang Anda pilih.

> **Note**
>
> Ekspor format SPDX dari Amazon Inspector kompatibel dengan sistem yang menggunakan SPDX 2.3, namun tidak mengandung bidang Creative Commons Zero (CC0). Ini karena menyertakan bidang ini akan memungkinkan pengguna untuk mendistribusikan ulang atau mengedit materi.

Contoh format CycloneDX 1.4 SBOM dari Amazon Inspector

```
                    {
  "bomFormat": "CycloneDX",
```

```
  "specVersion": "1.4",
  "version": 1,
  "metadata": {
    "timestamp": "2023-06-02T01:17:46Z",
    "component": null,
    "properties": [
      {
        "name": "imageId",
        "value":
 "sha256:c8ee97f7052776ef223080741f61fcdf6a3a9107810ea9649f904aa4269fdac6"
      },
      {
        "name": "architecture",
        "value": "arm64"
      },
      {
        "name": "accountId",
        "value": "111122223333"
      },
      {
        "name": "resourceType",
        "value": "AWS_ECR_CONTAINER_IMAGE"
      }
    ]
  },
  "components": [
    {
      "type": "library",
      "name": "pip",
      "purl": "pkg:pypi/pip@22.0.4?path=usr/local/lib/python3.8/site-packages/
pip-22.0.4.dist-info/METADATA",
      "bom-ref": "98dc550d1e9a0b24161daaa0d535c699"
    },
    {
      "type": "application",
      "name": "libss2",
      "purl": "pkg:dpkg/libss2@1.44.5-1+deb10u3?
arch=ARM64&epoch=0&upstream=libss2-1.44.5-1+deb10u3.src.dpkg",
      "bom-ref": "2f4d199d4ef9e2ae639b4f8d04a813a2"
    },
    {
      "type": "application",
      "name": "liblz4-1",
```

```
      "purl": "pkg:dpkg/liblz4-1@1.8.3-1+deb10u1?
arch=ARM64&epoch=0&upstream=liblz4-1-1.8.3-1+deb10u1.src.dpkg",
      "bom-ref": "9a6be8907ead891b070e60f5a7b7aa9a"
    },
    {
      "type": "application",
      "name": "mawk",
      "purl": "pkg:dpkg/mawk@1.3.3-17+b3?
arch=ARM64&epoch=0&upstream=mawk-1.3.3-17+b3.src.dpkg",
      "bom-ref": "c2015852a729f97fde924e62a16f78a5"
    },
    {
      "type": "application",
      "name": "libgmp10",
      "purl": "pkg:dpkg/libgmp10@6.1.2+dfsg-4+deb10u1?
arch=ARM64&epoch=2&upstream=libgmp10-6.1.2+dfsg-4+deb10u1.src.dpkg",
      "bom-ref": "52907290f5beef00dff8da77901b1085"
    },
    {
      "type": "application",
      "name": "ncurses-bin",
      "purl": "pkg:dpkg/ncurses-bin@6.1+20181013-2+deb10u3?
arch=ARM64&epoch=0&upstream=ncurses-bin-6.1+20181013-2+deb10u3.src.dpkg",
      "bom-ref": "cd20cfb9ebeeadba3809764376f43bce"
    }
  ],
  "vulnerabilities": [
    {
      "id": "CVE-2022-40897",
      "affects": [
        {
          "ref": "a74a4862cc654a2520ec56da0c81cdb3"
        },
        {
          "ref": "0119eb286405d780dc437e7dbf2f9d9d"
        }
      ]
    }
  ]
}
```

Contoh format SPDX 2.3 SBOM dari Amazon Inspector


```
{
 "name": "409870544328/EC2/i-022fba820db137c64/ami-074ea14c08effb2d8",
 "spdxVersion": "SPDX-2.3",
 "creationInfo": {
  "created": "2023-06-02T21:19:22Z",
  "creators": [
   "Organization: 409870544328",
   "Tool: Amazon Inspector SBOM Generator"
  ]
 },
 "documentNamespace": "EC2://i-022fba820db137c64/AMAZON_LINUX_2/null/x86_64",
 "comment": "",
 "packages": [{
   "name": "elfutils-libelf",
   "versionInfo": "0.176-2.amzn2",
   "downloadLocation": "NOASSERTION",
   "sourceInfo": "/var/lib/rpm/Packages",
   "filesAnalyzed": false,
   "externalRefs": [{
    "referenceCategory": "PACKAGE-MANAGER",
    "referenceType": "purl",
    "referenceLocator": "pkg:rpm/elfutils-libelf@0.176-2.amzn2?
arch=X86_64&epoch=0&upstream=elfutils-libelf-0.176-2.amzn2.src.rpm"
   }],
   "SPDXID": "SPDXRef-Package-rpm-elfutils-libelf-ddf56a513c0e76ab2ae3246d9a91c463"
  },
  {
   "name": "libcurl",
   "versionInfo": "7.79.1-1.amzn2.0.1",
   "downloadLocation": "NOASSERTION",
   "sourceInfo": "/var/lib/rpm/Packages",
   "filesAnalyzed": false,
   "externalRefs": [{
     "referenceCategory": "PACKAGE-MANAGER",
     "referenceType": "purl",
     "referenceLocator": "pkg:rpm/libcurl@7.79.1-1.amzn2.0.1?
arch=X86_64&epoch=0&upstream=libcurl-7.79.1-1.amzn2.0.1.src.rpm"
    },
    {
     "referenceCategory": "SECURITY",
```

```
      "referenceType": "vulnerability",
      "referenceLocator": "CVE-2022-32205"
     }
    ],
    "SPDXID": "SPDXRef-Package-rpm-libcurl-710fb33829bc5106559bcd380cddb7d5"
   },
   {
    "name": "hunspell-en-US",
    "versionInfo": "0.20121024-6.amzn2.0.1",
    "downloadLocation": "NOASSERTION",
    "sourceInfo": "/var/lib/rpm/Packages",
    "filesAnalyzed": false,
    "externalRefs": [{
     "referenceCategory": "PACKAGE-MANAGER",
     "referenceType": "purl",
     "referenceLocator": "pkg:rpm/hunspell-en-US@0.20121024-6.amzn2.0.1?
arch=NOARCH&epoch=0&upstream=hunspell-en-US-0.20121024-6.amzn2.0.1.src.rpm"
    }],
    "SPDXID": "SPDXRef-Package-rpm-hunspell-en-US-de19ae0883973d6cea5e7e079d544fe5"
   },
   {
    "name": "grub2-tools-minimal",
    "versionInfo": "2.06-2.amzn2.0.6",
    "downloadLocation": "NOASSERTION",
    "sourceInfo": "/var/lib/rpm/Packages",
    "filesAnalyzed": false,
    "externalRefs": [{
      "referenceCategory": "PACKAGE-MANAGER",
      "referenceType": "purl",
      "referenceLocator": "pkg:rpm/grub2-tools-minimal@2.06-2.amzn2.0.6?
arch=X86_64&epoch=1&upstream=grub2-tools-minimal-2.06-2.amzn2.0.6.src.rpm"
     },
     {
      "referenceCategory": "SECURITY",
      "referenceType": "vulnerability",
      "referenceLocator": "CVE-2021-3981"
     }
    ],
    "SPDXID": "SPDXRef-Package-rpm-grub2-tools-minimal-c56b7ea76e5a28ab8f232ef6d7564636"
   },
   {
    "name": "unixODBC-devel",
    "versionInfo": "2.3.1-14.amzn2",
    "downloadLocation": "NOASSERTION",
```

```
   "sourceInfo": "/var/lib/rpm/Packages",
   "filesAnalyzed": false,
   "externalRefs": [{
    "referenceCategory": "PACKAGE-MANAGER",
    "referenceType": "purl",
    "referenceLocator": "pkg:rpm/unixODBC-devel@2.3.1-14.amzn2?
arch=X86_64&epoch=0&upstream=unixODBC-devel-2.3.1-14.amzn2.src.rpm"
   }],
   "SPDXID": "SPDXRef-Package-rpm-unixODBC-devel-1bb35add92978df021a13fc9f81237d2"
  }
 ],
 "relationships": [{
   "spdxElementId": "SPDXRef-DOCUMENT",
   "relatedSpdxElement": "SPDXRef-Package-rpm-elfutils-libelf-
ddf56a513c0e76ab2ae3246d9a91c463",
   "relationshipType": "DESCRIBES"
  },
  {
   "spdxElementId": "SPDXRef-DOCUMENT",
   "relatedSpdxElement": "SPDXRef-Package-rpm-yajl-8476ce2db98b28cfab2b4484f84f1903",
   "relationshipType": "DESCRIBES"
  },
  {
   "spdxElementId": "SPDXRef-DOCUMENT",
   "relatedSpdxElement": "SPDXRef-Package-rpm-unixODBC-
devel-1bb35add92978df021a13fc9f81237d2",
   "relationshipType": "DESCRIBES"
  }
 ],
 "SPDXID": "SPDXRef-DOCUMENT"
}
```

Filter untuk SBOM

Saat Anda mengekspor SBOM, Anda dapat menyertakan filter untuk membuat laporan untuk subset sumber daya tertentu. Jika Anda tidak menyediakan filter, SBOM untuk semua sumber daya aktif yang didukung akan diekspor. Dan jika Anda adalah administrator yang didelegasikan, ini termasuk sumber daya untuk semua anggota juga. Filter berikut tersedia:

- AccountID — Filter ini dapat digunakan untuk mengekspor SBOM untuk sumber daya apa pun yang terkait dengan ID Akun tertentu.

- Tag instans EC2 - Filter ini dapat digunakan untuk mengekspor SBOM untuk instans EC2 dengan tag tertentu.
- Nama fungsi - Filter ini dapat digunakan untuk mengekspor SBOM untuk fungsi Lambda tertentu.
- Tag gambar - Filter ini dapat digunakan untuk mengekspor SBOM untuk gambar kontainer dengan tag tertentu.
- Tag fungsi Lambda - Filter ini dapat digunakan untuk mengekspor SBOM untuk fungsi Lambda dengan tag tertentu.
- Jenis sumber daya - Filter ini dapat digunakan untuk memfilter jenis sumber daya: EC2/ECR/ Lambda.
- ID Sumber Daya — Filter ini dapat digunakan untuk mengekspor SBOM untuk sumber daya tertentu.
- Nama repositori —Filter ini dapat digunakan untuk menghasilkan SBOM untuk gambar kontainer di repositori tertentu.

Konfigurasikan dan ekspor SBOM

Untuk mengekspor SBOM, Anda harus terlebih dahulu mengonfigurasi bucket Amazon S3 dan kunci AWS KMS yang diizinkan untuk digunakan oleh Amazon Inspector. Anda dapat menggunakan filter untuk mengekspor SBOM untuk himpunan bagian tertentu dari sumber daya Anda. Untuk mengekspor SBOM untuk beberapa akun di AWS Organisasi, ikuti langkah-langkah ini saat masuk sebagai administrator yang didelegasikan Amazon Inspector.

Prasyarat

- Sumber daya yang didukung yang sedang dipantau secara aktif oleh Amazon Inspector.
- Bucket Amazon S3 yang dikonfigurasi dengan kebijakan yang memungkinkan Amazon Inspector menambahkan objek. Untuk informasi tentang mengonfigurasi kebijakan, lihat Mengonfigurasi izin ekspor.
- AWS KMSKunci yang dikonfigurasi dengan kebijakan yang memungkinkan Amazon Inspector digunakan untuk mengenkripsi laporan Anda. Untuk informasi tentang mengonfigurasi kebijakan, lihat Mengonfigurasi AWS KMS kunci untuk ekspor.

> **Note**
>
> Jika sebelumnya Anda telah mengonfigurasi bucket Amazon S3 dan AWS KMS kunci untuk ekspor temuan, Anda dapat menggunakan bucket dan kunci yang sama untuk ekspor SBOM.

Pilih metode akses pilihan Anda untuk mengekspor SBOM.

Console

1. Buka konsol Amazon Inspector di https://console.aws.amazon.com/inspector/v2/home.
2. Menggunakan Wilayah AWS pemilih di sudut kanan atas halaman, pilih Wilayah dengan sumber daya yang ingin Anda ekspor SBOM.
3. Di panel navigasi, pilih Ekspor SBOM.
4. (Opsional) Di halaman Ekspor SBOM, gunakan menu Tambahkan filter untuk memilih subset sumber daya untuk membuat laporan. Jika tidak ada filter yang disediakan, Amazon Inspector akan mengekspor laporan untuk semua sumber daya aktif. Jika Anda adalah administrator yang didelegasikan, ini akan mencakup semua sumber daya aktif di organisasi Anda.
5. Di bawah Pengaturan ekspor pilih format yang Anda inginkan untuk SBOM.
6. Masukkan URI Amazon S3 atau pilih Jelajahi Amazon S3 untuk memilih lokasi Amazon S3 untuk menyimpan SBOM.
7. Masukkan AWS KMSkunci yang dikonfigurasi untuk Amazon Inspector untuk digunakan untuk mengenkripsi laporan Anda.

API

- Untuk mengekspor SBOM untuk sumber daya Anda secara terprogram, gunakan CreateSbomExportpengoperasian Amazon Inspector API.

  Dalam permintaan Anda, gunakan `reportFormat` parameter untuk menentukan format output SBOM, pilih `CYCLONEDX_1_4` atau`SPDX_2_3`. `s3Destination`Parameter diperlukan dan Anda harus menentukan bucket S3 yang dikonfigurasi dengan kebijakan yang memungkinkan Amazon Inspector menulis ke sana. Secara opsional gunakan `resourceFilterCriteria` parameter untuk membatasi ruang lingkup laporan ke sumber daya tertentu.

AWS CLI

- Untuk mengekspor SBOM untuk sumber daya Anda menggunakan AWS Command Line Interface jalankan perintah berikut:

  ```
  aws inspector2 create-sbom-export --report-format
  FORMAT --s3-destination bucketName=DOC-EXAMPLE-
  BUCKET1,keyPrefix=PREFIX,kmsKeyArn=arn:aws:kms:Region:111122223333:key/123
  ```

  Dalam permintaan Anda, ganti *FORMAT* dengan format pilihan Anda, `CYCLONEDX_1_4` atau`SPDX_2_3`. Kemudian ganti *user input placeholders*untuk tujuan s3 dengan nama bucket S3 untuk diekspor, awalan yang akan digunakan untuk output di S3, dan ARN untuk kunci KMS yang Anda gunakan untuk mengenkripsi laporan.

Pencarian basis data kerentanan Amazon Inspector

Anda dapat mencari database kerentanan Amazon Inspector untuk kerentanan dan eksposur (CVE). Amazon Inspector menggunakan informasi dari database kerentanan untuk menghasilkan detail yang terkait dengan ID CVE. Anda dapat mengakses detail ini di halaman detail CVE.

Topik ini menjelaskan cara mencari database vulernability Amazon Inspector menggunakan ID CVE dan menginterpet halaman detail CVE. Untuk informasi tentang temuan, lihatAmazon Inspector menemukan detail.

> **Note**
>
> Amazon Inspector melacak dan menghasilkan temuan untuk kerentanan perangkat lunak lain dalam database. Namun, Amazon Inspector hanya mendukung CVE dengan platform yang tercantum di bagian Platform Deteksi pada halaman detail CVE. Saat ini, pencarian CVE tidak mendukungMicrosoft Windows.

Mencari database kerentanan

Bagian ini menjelaskan cara mencari database kerentanan di konsol dan dengan Amazon Inspector API.

> **Note**
>
> Anda harus mengaktifkan Amazon Inspector di saat ini Wilayah AWS sebelum Anda dapat mencari database kerentanan.

Console

1. Buka konsol Amazon Inspector di https://console.aws.amazon.com/inspector/
2. Dari panel navigasi, pilih Pencarian basis data kerentanan.
3. Di bilah pencarian, masukkan ID CVE, dan pilih Cari.

API

Jalankan Amazon Inspector SearchVulnerabilitiesAPI, dan berikan satu ID CVE seperti `filterCriteria` dalam format berikut:. `CVE-<year>-<ID>`

Memahami detail CVE

Bagian ini menjelaskan cara menginterpet halaman detail CVE.

Rincian CVE

Bagian detail CVE mencakup informasi berikut:

- Deskripsi dan ID CVE
- Keparahan CVE
- Skor Common Vulnerability Scoring System (CVSS) dan Exploit Prediction Scoring System (EPSS)
- Platform deteksi

> **Note**
>
> Jika bidang ini kosong, Amazon Inspector tidak mendukung deteksi untuk ID CVE Anda.

- Pencacahan Kelemahan Umum (CWE)
- Tanggal yang dibuat dan diperbarui oleh vendor

Kecerdasan kerentanan

Bagian intelijen kerentanan menyediakan data intelijen ancaman seperti target eksploitasi dan tanggal eksploitasi publik terakhir yang diketahui.

Ini juga menyediakan data dari Cybersecurity and Infrastructure Security Agency (CISA), yang mencakup tindakan remediasi, tanggal CVE ditambahkan ke katalog Known Exploited Vulnerability, dan tanggal waktu CISA mengharapkan agen federal untuk memulihkan CVE.

Referensi

Bagian referensi menyediakan tautan ke sumber daya untuk informasi lebih lanjut tentang CVE.

Skema EventBridge acara Amazon untuk acara Amazon Inspector

Untuk mendukung integrasi dengan aplikasi, layanan, dan sistem lain, seperti pemantauan atau sistem manajemen acara, Amazon Inspector secara otomatis menerbitkan temuan ke Amazon EventBridge sebagai peristiwa. EventBridgeadalah layanan bus acara tanpa server yang mengirimkan aliran data real-time dari aplikasi dan lainnya Layanan AWS ke target seperti fungsi, topik Layanan Pemberitahuan Sederhana AmazonAWS Lambda, dan aliran Data Kinesis Amazon. Untuk mempelajari lebih lanjut tentang EventBridge dan EventBridge acara, lihat Panduan EventBridge Pengguna Amazon.

Amazon Inspector menerbitkan acara untuk temuan, perubahan cakupan sumber daya, dan pemindaian awal sumber daya individu. Setiap peristiwa adalah objek JSON yang sesuai dengan EventBridge skema untuk acara. AWS Karena data terstruktur sebagai suatu EventBridge peristiwa, Anda dapat lebih mudah memantau, memproses, dan menindaklanjuti temuan serta mendukung peristiwa Amazon Inspector dengan menggunakan aplikasi, layanan, dan alat lain.

Topik

Skema EventBridge dasar Amazon untuk Amazon Inspector

Berikut ini adalah contoh skema dasar untuk EventBridge acara Amazon Inspector. Detail acara berbeda berdasarkan jenis acara.

```
{
    "version": "0",
    "id": "Event ID",
    "detail-type": "Inspector2 *event type*",
    "source": "aws.inspector2",
    "account": "Akun AWS ID (string)",
    "time": "event timestamp (string)",
    "region": "Wilayah AWS (string)",
```

```
    "resources": [
        *IDs or ARNs of the resources involved in the event*
    ],
    "detail": {
        *Details of an Amazon Inspector event type*
    }
}
```

Amazon Inspector menemukan contoh skema acara

Berikut ini adalah contoh skema untuk EventBridge acara untuk temuan Amazon Inspector. Menemukan peristiwa dibuat saat Amazon Inspector mengidentifikasi kerentanan perangkat lunak atau masalah jaringan di salah satu sumber daya Anda. Untuk panduan membuat notifikasi sebagai respons terhadap jenis acara ini, lihatMembuat respons kustom untuk temuan Amazon Inspector dengan Amazon EventBridge.

Bidang berikut mengidentifikasi peristiwa temuan:

- Bidang `detail-type` diatur ke `Inspector2 Finding`.
- `detail`Objek menggambarkan temuan tersebut.

Pilih dari opsi untuk melihat skema pencarian acara untuk sumber daya yang berbeda dan jenis pencarian.

Amazon EC2 package vulnerability finding

```
{
    "version": "0",
    "id": "66a7a279-5f92-971c-6d3e-c92da0950992",
    "detail-type": "Inspector2 Finding",
    "source": "aws.inspector2",
    "account": "111122223333",
    "time": "2023-01-19T22:46:15Z",
    "region": "us-east-1",
    "resources": ["i-0c2a343f1948d5205"],
    "detail": {
        "awsAccountId": "111122223333",
        "description": "\n It was discovered that the sound subsystem in the Linux
 kernel contained a\n race condition in some situations. A local attacker could use
 this to cause\n a denial of service (system crash).",
```

```
        "exploitAvailable": "YES",
        "exploitabilityDetails": {
            "lastKnownExploitAt": "Oct 24, 2022, 11:08:59 PM"
        },
        "findingArn": "arn:aws:inspector2:us-east-1:111122223333:finding/
FINDING_ID",
        "firstObservedAt": "Jan 19, 2023, 10:46:15 PM",
        "fixAvailable": "YES",
        "lastObservedAt": "Jan 19, 2023, 10:46:15 PM",
        "packageVulnerabilityDetails": {
            "cvss": [{
                "baseScore": 4.7,
                "scoringVector": "CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H",
                "source": "NVD",
                "version": "3.1"
            }],
            "referenceUrls": ["https://lore.kernel.org/all/
CAFcO6XN7JDM4xSXGhtusQfS2mSBcx50VJKwQpCq=WeLt57aaZA@mail.gmail.com/", "https://
ubuntu.com/security/notices/USN-5792-1", "https://ubuntu.com/security/notices/
USN-5791-2", "https://ubuntu.com/security/notices/USN-5791-1", "https://ubuntu.com/
security/notices/USN-5793-2", "https://git.kernel.org/pub/scm/linux/kernel/git/
torvalds/linux.git/commit/?id=8423f0b6d513b259fdab9c9bf4aaa6188d054c2d", "https://
ubuntu.com/security/notices/USN-5793-1", "https://ubuntu.com/security/notices/
USN-5792-2", "https://ubuntu.com/security/notices/USN-5791-3", "https://ubuntu.com/
security/notices/USN-5793-4", "https://ubuntu.com/security/notices/USN-5793-3",
 "https://git.kernel.org/linus/8423f0b6d513b259fdab9c9bf4aaa6188d054c2d(6.0-rc5)",
 "https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-3303"],
            "relatedVulnerabilities": [],
            "source": "UBUNTU_CVE",
            "sourceUrl": "https://people.canonical.com/~ubuntu-security/cve/2022/
CVE-2022-3303.html",
            "vendorCreatedAt": "Sep 27, 2022, 11:15:00 PM",
            "vendorSeverity": "medium",
            "vulnerabilityId": "CVE-2022-3303",
            "vulnerablePackages": [{
                "arch": "X86_64",
                "epoch": 0,
                "fixedInVersion": "0:5.15.0.1027.31~20.04.16",
                "name": "linux-image-aws",
                "packageManager": "OS",
                "remediation": "apt update && apt install --only-upgrade linux-
image-aws",
                "version": "5.15.0.1026.30~20.04.16"
            }]
```

```
        },
        "remediation": {
            "recommendation": {
                "text": "None Provided"
            }
        },
        "resources": [{
            "details": {
                "awsEc2Instance": {
                    "iamInstanceProfileArn": "arn:aws:iam::111122223333:instance-
profile/AmazonSSMRoleForInstancesQuickSetup",
                    "imageId": "ami-0b7ff1a8d69f1bb35",
                    "ipV4Addresses": ["172.31.85.212", "44.203.45.27"],
                    "ipV6Addresses": [],
                    "launchedAt": "Jan 19, 2023, 7:53:14 PM",
                    "platform": "UBUNTU_20_04",
                    "subnetId": "subnet-8213f2a3",
                    "type": "t2.micro",
                    "vpcId": "vpc-ab6650d1"
                }
            },
            "id": "i-0c2a343f1948d5205",
            "partition": "aws",
            "region": "us-east-1",
            "type": "AWS_EC2_INSTANCE"
        }],
        "severity": "MEDIUM",
        "status": "ACTIVE",
        "title": "CVE-2022-3303 - linux-image-aws",
        "type": "PACKAGE_VULNERABILITY",
        "updatedAt": "Jan 19, 2023, 10:46:15 PM"
    }
}
```

Amazon EC2 network reachability finding

```
{
    "version": "0",
    "id": "d0384f63-1621-1b75-d014-a5e45628ef3e",
    "detail-type": "Inspector2 Finding",
    "source": "aws.inspector2",
```

```
    "account": "111122223333",
    "time": "2023-01-20T09:17:57Z",
    "region": "us-east-1",
    "resources": ["i-0a96278c2206a8e4b"],
    "detail": {
        "awsAccountId": "111122223333",
        "description": "On the instance i-0a96278c2206a8e4b, the port range
 22-22 is reachable from the InternetGateway igw-72069c09 from an attached ENI
 eni-0976efe678170408f.",
        "findingArn": "arn:aws:inspector2:us-east-1:111122223333:finding/
FINDING_ID",
        "firstObservedAt": "Jan 20, 2023, 9:17:57 AM",
        "lastObservedAt": "Jan 20, 2023, 9:17:57 AM",
        "networkReachabilityDetails": {
            "networkPath": {
                "steps": [{
                    "componentId": "igw-72069c09",
                    "componentType": "AWS::EC2::InternetGateway"
                }, {
                    "componentId": "acl-91d74eec",
                    "componentType": "AWS::EC2::NetworkAcl"
                }, {
                    "componentId": "sg-0aaed0af450bd0165",
                    "componentType": "AWS::EC2::SecurityGroup"
                }, {
                    "componentId": "eni-0976efe678170408f",
                    "componentType": "AWS::EC2::NetworkInterface"
                }, {
                    "componentId": "i-0a96278c2206a8e4b",
                    "componentType": "AWS::EC2::Instance"
                }]
            },
            "openPortRange": {
                "begin": 22,
                "end": 22
            },
            "protocol": "TCP"
        },
        "remediation": {
            "recommendation": {
                "text": "You can restrict access to your instance by modifying the
 Security Groups or ACLs in the network path."
            }
        },
```

```
        "resources": [{
            "details": {
                "awsEc2Instance": {
                    "iamInstanceProfileArn": "arn:aws:iam::111122223333:instance-
profile/AmazonSSMRoleForInstancesQuickSetup",
                    "imageId": "ami-0b5eea76982371e91",
                    "ipV4Addresses": ["3.89.90.19", "172.31.93.57"],
                    "ipV6Addresses": [],
                    "keyName": "example-inspector-test",
                    "launchedAt": "Jan 19, 2023, 7:25:02 PM",
                    "platform": "AMAZON_LINUX_2",
                    "subnetId": "subnet-8213f2a3",
                    "type": "t2.micro",
                    "vpcId": "vpc-ab6650d1"
                }
            },
            "id": "i-0a96278c2206a8e4b",
            "partition": "aws",
            "region": "us-east-1",
            "type": "AWS_EC2_INSTANCE"
        }],
        "severity": "MEDIUM",
        "status": "ACTIVE",
        "title": "Port 22 is reachable from an Internet Gateway",
        "type": "NETWORK_REACHABILITY",
        "updatedAt": "Jan 20, 2023, 9:17:57 AM"
    }
}
```

Amazon ECR package vulnerability finding

```
{
    "version": "0",
    "id": "5b52952e-26df-3a51-6d14-4dbe737e58ec",
    "detail-type": "Inspector2 Finding",
    "source": "aws.inspector2",
    "account": "111122223333",
    "time": "2023-01-19T21:59:00Z",
    "region": "us-east-1",
    "resources": [
```

```
        "arn:aws:ecr:us-east-1:111122223333:repository/inspector2/
sha256:98f0304b3a3b7c12ce641177a99d1f3be56f532473a528fda38d53d519cafb13"
    ],
    "detail": {
        "awsAccountId": "111122223333",
        "description": "libcurl would reuse a previously created connection even
 when a TLS or SSHrelated option had been changed that should have prohibited
 reuse.libcurl keeps previously used connections in a connection pool for
 subsequenttransfers to reuse if one of them matches the setup. However, several TLS
 andSSH settings were left out from the configuration match checks, making themmatch
 too easily.",
        "exploitAvailable": "NO",
        "findingArn": "arn:aws:inspector2:us-east-1:111122223333:finding/
FINDING_ID",
        "firstObservedAt": "Jan 19, 2023, 9:59:00 PM",
        "fixAvailable": "YES",
        "inspectorScore": 7.5,
        "inspectorScoreDetails": {
            "adjustedCvss": {
                "adjustments": [],
                "cvssSource": "NVD",
                "score": 7.5,
                "scoreSource": "NVD",
                "scoringVector": "CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N",
                "version": "3.1"
            }
        },
        "lastObservedAt": "Jan 19, 2023, 9:59:00 PM",
        "packageVulnerabilityDetails": {
            "cvss": [
                {
                    "baseScore": 5,
                    "scoringVector": "AV:N/AC:L/Au:N/C:N/I:P/A:N",
                    "source": "NVD",
                    "version": "2.0"
                },
                {
                    "baseScore": 7.5,
                    "scoringVector": "CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N",
                    "source": "NVD",
                    "version": "3.1"
                }
            ],
            "referenceUrls": [
```

```
                "https://hackerone.com/reports/1555796",
                "https://security.gentoo.org/glsa/202212-01",
                "https://lists.debian.org/debian-lts-announce/2022/08/
msg00017.html",
                "https://www.debian.org/security/2022/dsa-5197"
            ],
            "relatedVulnerabilities": [],
            "source": "NVD",
            "sourceUrl": "https://nvd.nist.gov/vuln/detail/CVE-2022-27782",
            "vendorCreatedAt": "Jun 2, 2022, 2:15:00 PM",
            "vendorSeverity": "HIGH",
            "vendorUpdatedAt": "Jan 5, 2023, 5:51:00 PM",
            "vulnerabilityId": "CVE-2022-27782",
            "vulnerablePackages": [
                {
                    "arch": "X86_64",
                    "epoch": 0,
                    "fixedInVersion": "0:7.61.1-22.el8_6.3",
                    "name": "libcurl",
                    "packageManager": "OS",
                    "release": "22.el8",
                    "remediation": "yum update libcurl",
                    "sourceLayerHash":
 "sha256:38a980f2cc8accf69c23deae6743d42a87eb34a54f02396f3fcfd7c2d06e2c5b",
                    "version": "7.61.1"
                },
                {
                    "arch": "X86_64",
                    "epoch": 0,
                    "fixedInVersion": "0:7.61.1-22.el8_6.3",
                    "name": "curl",
                    "packageManager": "OS",
                    "release": "22.el8",
                    "remediation": "yum update curl",
                    "sourceLayerHash":
 "sha256:38a980f2cc8accf69c23deae6743d42a87eb34a54f02396f3fcfd7c2d06e2c5b",
                    "version": "7.61.1"
                }
            ]
        },
        "remediation": {
            "recommendation": {
                "text": "None Provided"
            }
```

```
        },
        "resources": [
            {
                "details": {
                    "awsEcrContainerImage": {
                        "architecture": "amd64",
                        "imageHash":
 "sha256:98f0304b3a3b7c12ce641177a99d1f3be56f532473a528fda38d53d519cafb13",
                        "imageTags": [
                            "o3"
                        ],
                        "platform": "ORACLE_LINUX_8",
                        "pushedAt": "Jan 19, 2023, 7:38:39 PM",
                        "registry": "111122223333",
                        "repositoryName": "inspector2"
                    }
                },
                "id": "arn:aws:ecr:us-east-1:111122223333:repository/inspector2/
sha256:98f0304b3a3b7c12ce641177a99d1f3be56f532473a528fda38d53d519cafb13",
                "partition": "aws",
                "region": "us-east-1",
                "type": "AWS_ECR_CONTAINER_IMAGE"
            }
        ],
        "severity": "HIGH",
        "status": "ACTIVE",
        "title": "CVE-2022-27782 - libcurl, curl",
        "type": "PACKAGE_VULNERABILITY",
        "updatedAt": "Jan 19, 2023, 9:59:00 PM"
    }
}
```


Lambda package vulnerability finding


```
{
    "version": "0",
    "id": "040bb590-3a12-353f-ecb1-05e54b0fbea7",
    "detail-type": "Inspector2 Finding",
    "source": "aws.inspector2",
    "account": "111122223333",
    "time": "2023-01-19T19:20:25Z",
```

```
    "region": "us-east-1",
    "resources": [
        "arn:aws:lambda:us-east-1:111122223333:function:ExampleFunction:$LATEST"
    ],
    "detail": {
        "awsAccountId": "111122223333",
        "description": "Those using Woodstox to parse XML data may be vulnerable to
 Denial of Service attacks (DOS) if DTD support is enabled. If the parser is running
 on user supplied input, an attacker may supply content that causes the parser to
 crash by stackoverflow. This effect may support a denial of service attack.",
        "exploitAvailable": "NO",
        "findingArn": "arn:aws:inspector2:us-east-1:111122223333:finding/
FINDING_ID",
        "firstObservedAt": "Jan 19, 2023, 7:20:25 PM",
        "fixAvailable": "YES",
        "inspectorScore": 7.5,
        "inspectorScoreDetails": {
            "adjustedCvss": {
                "cvssSource": "NVD",
                "score": 7.5,
                "scoreSource": "NVD",
                "scoringVector": "CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H",
                "version": "3.1"
            }
        },
        "lastObservedAt": "Jan 19, 2023, 7:20:25 PM",
        "packageVulnerabilityDetails": {
            "cvss": [
                {
                    "baseScore": 7.5,
                    "scoringVector": "CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H",
                    "source": "NVD",
                    "version": "3.1"
                }
            ],
            "referenceUrls": [
                "https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=47434"
            ],
            "relatedVulnerabilities": [],
            "source": "NVD",
            "sourceUrl": "https://nvd.nist.gov/vuln/detail/CVE-2022-40152",
            "vendorCreatedAt": "Sep 16, 2022, 10:15:00 AM",
            "vendorSeverity": "HIGH",
            "vendorUpdatedAt": "Nov 25, 2022, 11:15:00 AM",
```

```
            "vulnerabilityId": "CVE-2022-40152",
            "vulnerablePackages": [
                {
                    "epoch": 0,
                    "filePath": "lib/woodstox-core-6.2.7.jar",
                    "fixedInVersion": "6.4.0",
                    "name": "com.fasterxml.woodstox:woodstox-core",
                    "packageManager": "JAR",
                    "remediation": "Update woodstox-core to 6.4.0",
                    "version": "6.2.7"
                }
            ]
        },
        "remediation": {
            "recommendation": {
                "text": "None Provided"
            }
        },
        "resources": [
            {
                "details": {
                    "awsLambdaFunction": {
                        "architectures": [
                            "X86_64"
                        ],
                        "codeSha256": "+EwrOrht2um4fdVCD73gj
+O7HJIAUvUxi8AD0eKHSkc=",
                        "executionRoleArn": "arn:aws:iam::111122223333:role/
ExampleFunction-ExecutionRole",
                        "functionName": "Example-function",
                        "lastModifiedAt": "Nov 7, 2022, 8:29:27 PM",
                        "packageType": "ZIP",
                        "runtime": "JAVA_11",
                        "version": "$LATEST"
                    }
                },
                "id": "arn:aws:lambda:us-
east-1:111122223333:function:ExampleFunction:$LATEST",
                "partition": "aws",
                "region": "us-east-1",
                "tags": {
                    "TargetAlias": "DeploymentStack",
                    "SoftwareType": "Infrastructure"
                },
```

```
                "type": "AWS_LAMBDA_FUNCTION"
            }
        ],
        "severity": "HIGH",
        "status": "ACTIVE",
        "title": "CVE-2022-40152 - com.fasterxml.woodstox:woodstox-core",
        "type": "PACKAGE_VULNERABILITY",
        "updatedAt": "Jan 19, 2023, 7:20:25 PM"
    }
}
```

Lambda code vulnerability finding

```
{
   "version":"0",
   "id":"9df01cb1-df24-bc46-5650-085a4087e7aa",
   "detail-type":"Inspector2 Finding",
   "source":"aws.inspector2",
   "account":"111122223333",
   "time":"2023-12-07T22:14:45Z",
   "region":"us-east-1",
   "resources":[
      "arn:aws:lambda:us-east-1:111122223333:function:code-finding:$LATEST"
   ],
   "detail":{
      "awsAccountId":"111122223333",
      "codeVulnerabilityDetails":{
         "detectorId":"python/lambda-override-reserved@v1.0",
         "detectorName":"Override of reserved variable names in a Lambda function",
         "detectorTags":[
            "availability",
            "aws-python-sdk",
            "aws-lambda",
            "data-integrity",
            "maintainability",
            "security",
            "security-context",
            "python"
         ],
         "filePath":{
            "endLine":6,
```

```
            "fileName":"lambda_function.py",
            "filePath":"lambda_function.py",
            "startLine":6
         },
         "ruleId":"Rule-434311"
      },
      "description":"Overriding environment variables that are reserved by AWS
 Lambda might lead to unexpected behavior or failure of the Lambda function.",
      "findingArn":"arn:aws:inspector2:us-east-1:111122223333:finding/FINDING_ID",
      "firstObservedAt":"Aug 8, 2023, 7:33:58 PM",
      "lastObservedAt":"Dec 7, 2023, 10:14:45 PM",
      "remediation":{
         "recommendation":{
            "text":"Your code attempts to override an environment variable that is
 reserved by the Lambda runtime environment. This can lead to unexpected behavior
 and might break the execution of your Lambda function.\n\n[Learn more](https://
docs.aws.amazon.com/lambda/latest/dg/configuration-envvars.html#configuration-
envvars-runtime)"
         }
      },
      "resources":[
         {
            "details":{
               "awsLambdaFunction":{
                  "architectures":[
                     "X86_64"
                  ],
                  "codeSha256":"2mtfH+CgubesG6NYpb2zEqBja5WN6FfbH4AAYDuF8RE=",
                  "executionRoleArn":"arn:aws:iam::193043430472:role/service-role/
code-finding-role-7jgg3wan",
                  "functionName":"code-finding",
                  "lastModifiedAt":"Dec 7, 2023, 10:12:48 PM",
                  "packageType":"ZIP",
                  "runtime":"PYTHON_3_7",
                  "version":"$LATEST"
               }
            },
            "id":"arn:aws:lambda:us-east-1:193043430472:function:code-finding:
$LATEST",
            "partition":"aws",
            "region":"us-east-1",
            "type":"AWS_LAMBDA_FUNCTION"
         }
      ],
```

```
      "severity":"HIGH",
      "status":"ACTIVE",
      "title":"Overriding environment variables that are reserved by AWS Lambda
 might lead to unexpected behavior.",
      "type":"CODE_VULNERABILITY",
      "updatedAt":"Dec 7, 2023, 10:14:45 PM"
   }
}
```

> **Note**
>
> Nilai detail mengembalikan rincian JSON dari temuan tunggal sebagai objek. Itu tidak mengembalikan seluruh sintaks respons temuan, yang mendukung beberapa temuan dalam array.

Contoh skema acara lengkap pemindaian awal Amazon Inspector

Berikut ini adalah contoh skema EventBridge acara untuk acara Amazon Inspector untuk menyelesaikan pemindaian awal. Acara ini dibuat saat Amazon Inspector menyelesaikan pemindaian awal salah satu sumber daya Anda.

Bidang berikut mengidentifikasi peristiwa lengkap pemindaian awal:

- Bidang `detail-type` diatur ke `Inspector2 Scan`.
- `detail`Objek berisi `finding-severity-counts` objek yang merinci jumlah temuan dalam kategori keparahan yang berlaku, seperti`CRITICAL`,`HIGH`, dan`MEDIUM`.

Pilih dari opsi untuk melihat skema peristiwa pemindaian awal yang berbeda menurut jenis sumber daya.

Amazon EC2 instance initial scan

```
{
    "version": "0",
    "id": "28a46762-6ac8-6cc4-4f55-bc9ab99af928",
    "detail-type": "Inspector2 Scan",
```

```
    "source": "aws.inspector2",
    "account": "111122223333",
    "time": "2023-01-20T22:52:35Z",
    "region": "us-east-1",
    "resources": [
        "i-087d63509b8c97098"
    ],
    "detail": {
        "scan-status": "INITIAL_SCAN_COMPLETE",
        "finding-severity-counts": {
            "CRITICAL": 0,
            "HIGH": 0,
            "MEDIUM": 0,
            "TOTAL": 0
        },
        "instance-id": "i-087d63509b8c97098",
        "version": "1.0"
    }
}
```

Amazon ECR image initial scan

```
{
    "version": "0",
    "id": "fdaa751a-984c-a709-44f9-9a9da9cd3606",
    "detail-type": "Inspector2 Scan",
    "source": "aws.inspector2",
    "account": "111122223333",
    "time": "2023-01-20T23:15:18Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ecr:us-east-1:111122223333:repository/inspector2"
    ],
    "detail": {
        "scan-status": "INITIAL_SCAN_COMPLETE",
        "repository-name": "arn:aws:ecr:us-east-1:111122223333:repository/
inspector2",
        "finding-severity-counts": {
            "CRITICAL": 0,
            "HIGH": 0,
            "MEDIUM": 0,
```

```
            "TOTAL": 0
        },
        "image-digest":
 "sha256:965fbcae990b0467ed5657caceaec165018ef44a4d2d46c7cdea80a9dff0d1ea",
        "image-tags": [
            "ubuntu22"
        ],
        "version": "1.0"
    }
}
```

Lambda function initial scan

```
{
  "version": "0",
  "id": "4f290a7c-361b-c442-03c8-a629f6f20d6c",
  "detail-type": "Inspector2 Scan",
  "source": "aws.inspector2",
  "account": "111122223333",
  "time": "2023-02-23T18:06:03Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:lambda:us-west-2:111122223333:function:lambda-example:$LATEST"
  ],
  "detail": {
    "scan-status": "INITIAL_SCAN_COMPLETE",
    "finding-severity-counts": {
      "CRITICAL": 0,
      "HIGH": 0,
      "MEDIUM": 0,
      "TOTAL": 0
    },
    "version": "1.0"
  }
}
```

Contoh skema acara cakupan Amazon Inspector

Berikut ini adalah contoh skema EventBridge acara untuk acara Amazon Inspector untuk liputan. Acara ini dibuat saat cakupan pemindaian Amazon Inspector untuk sumber daya diubah. Bidang berikut mengidentifikasi peristiwa cakupan:

- Bidang `detail-type` diatur ke `Inspector2 Coverage`.
- `detail`Objek berisi `scanStatus` objek yang menunjukkan status pemindaian baru untuk sumber daya.

```
{
    "version": "0",
    "id": "000adda5-0fbf-913e-bc0e-10f0376412aa",
    "detail-type": "Inspector2 Coverage",
    "source": "aws.inspector2",
    "account": "111122223333",
    "time": "2023-01-20T22:51:39Z",
    "region": "us-east-1",
    "resources": [
        "i-087d63509b8c97098"
    ],
    "detail": {
        "scanStatus": {
            "reason": "UNMANAGED_EC2_INSTANCE",
            "statusCodeValue": "INACTIVE"
        },
        "scanType": "PACKAGE",
        "eventTimestamp": "2023-01-20T22:51:35.665501Z",
        "version": "1.0"
    }
}
```

Mengintegrasikan pemindaian Amazon Inspector ke dalam pipeline CI/CD Anda

Anda dapat mengintegrasikan pemindaian gambar penampung Amazon Inspector langsung ke pipeline CI/CD untuk memindai kerentanan perangkat lunak dan memberikan laporan di akhir build. Laporan kerentanan yang dihasilkan oleh Amazon Inspector memungkinkan Anda untuk menyelidiki dan memulihkan risiko sebelum penerapan.

Integrasi Amazon Inspector CI/CD menggunakan kombinasi Amazon Inspector SBOM Generator dan Amazon Inspector Scan API untuk menghasilkan laporan kerentanan untuk gambar kontainer Anda. Amazon Inspector SBOM Generator membuat tagihan bahan perangkat lunak (SBOM) dari gambar kontainer yang disediakan, kemudian, Amazon Inspector Scan API memindai SBOM itu dan membuat laporan dengan detail tentang kerentanan yang terdeteksi.

Anda dapat mencapai integrasi CI/CD dengan Amazon Inspector melalui plugin Amazon Inspector yang sengaja dibuat untuk solusi CI/CD individual dan tersedia di pasar mereka, atau Anda dapat membuat integrasi pemindaian kustom Anda sendiri.

Topik

Integrasi plugin

Amazon Inspector menyediakan plugin untuk solusi CI/CD yang didukung. Anda dapat menginstal plugin ini dari pasar masing-masing dan kemudian menggunakannya untuk menambahkan Amazon Inspector Scan sebagai langkah pembuatan dalam pipeline Anda. Langkah pembuatan plugin

menjalankan generator Amazon Inspector SBOM pada gambar yang Anda berikan, dan kemudian menjalankan Amazon Inspector Scan API pada SBOM yang dihasilkan.

Berikut ini adalah ikhtisar tentang bagaimana integrasi Amazon Inspector CI/CD bekerja melalui plugin:

1. Anda mengonfigurasi Akun AWS untuk mengizinkan akses ke Amazon Inspector Scan API. Untuk petunjuk, lihat Menyiapkan AWS akun untuk menggunakan integrasi Amazon Inspector CI/CD.
2. Anda menginstal plugin Amazon Inspector dari marketplace.
3. Anda menginstal dan mengkonfigurasi biner Amazon Inspector SBOM Generator. Untuk petunjuk, lihat Amazon Inspector SBOM Generator.
4. Anda menambahkan Amazon Inspector Scan sebagai langkah pembuatan di pipeline CI/CD Anda dan mengonfigurasi pemindaian.
5. Saat Anda menjalankan build, plugin mengambil image container Anda sebagai input dan kemudian menjalankan Amazon Inspector SBOM Generator pada image untuk menghasilkan SBOM yang CycloneDX kompatibel.
6. Dari sana, plugin mengirimkan SBOM yang dihasilkan ke titik akhir Amazon Inspector Scan API yang menilai setiap komponen SBOM untuk kerentanan.
7. Respons API Amazon Inspector Scan diubah menjadi laporan kerentanan dalam format CSV, SBOM JSON, dan HTML. Laporan tersebut berisi rincian tentang kerentanan apa pun yang ditemukan Amazon Inspector.

Solusi CI/CD yang didukung

Amazon Inspector saat ini mendukung solusi CI/CD berikut. Untuk petunjuk lengkap tentang pengaturan integrasi CI/CD menggunakan plugin, pilih plugin untuk solusi CI/CD Anda:

- Plugin Jenkins
- TeamCity plugin

Integrasi kustom

Jika Amazon Inspector tidak menyediakan plugin untuk solusi CI/CD Anda, Anda dapat membuat integrasi CI/CD kustom Anda sendiri menggunakan kombinasi Amazon Inspector SBOM Generator dan Amazon Inspector Scan API. Anda juga dapat menggunakan integrasi khusus untuk

menyempurnakan pemindaian menggunakan opsi yang tersedia melalui Amazon Inspector SBOM Generator.

Berikut ini adalah ikhtisar tentang cara kerja integrasi Amazon Inspector CI/CD kustom:

1. Anda mengonfigurasi Akun AWS untuk mengizinkan akses ke Amazon Inspector Scan API. Untuk petunjuk, lihat Menyiapkan AWS akun untuk menggunakan integrasi Amazon Inspector CI/CD.
2. Anda menginstal dan mengkonfigurasi biner Amazon Inspector SBOM Generator. Untuk petunjuk, lihat Amazon Inspector SBOM Generator.
3. Anda menggunakan Amazon Inspector SBOM Generator untuk menghasilkan SBOM yang CycloneDX kompatibel untuk image container Anda.
4. Anda menggunakan Amazon Inspector Scan API pada SBOM yang dihasilkan untuk menghasilkan laporan kerentanan.

Untuk petunjuk tentang menyiapkan integrasi kustom, lihatMembuat integrasi pipeline CI/CD kustom Anda sendiri dengan Amazon Inspector Scan.

Menyiapkan AWS akun untuk menggunakan integrasi Amazon Inspector CI/CD

Anda harus mendaftar Akun AWS untuk menggunakan integrasi Amazon Inspector CI/CD. Peran IAM Akun AWS harus memiliki yang memberikan akses pipleline Anda ke Amazon Inspector Scan API.

Selesaikan tugas dalam topik berikut untuk mendaftar Akun AWS, membuat pengguna administrator, dan mengonfigurasi peran IAM untuk integrasi CI/CD.

> **Note**
>
> Jika Anda sudah mendaftar untuk Akun AWS, Anda dapat melompat keKonfigurasikan peran IAM untuk integrasi CI/CD.

Topik

- Mendaftar untuk Akun AWS
- Membuat pengguna administratif
- Konfigurasikan peran IAM untuk integrasi CI/CD

Mendaftar untuk Akun AWS

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

Untuk mendaftar untuk Akun AWS

1. Buka https://portal.aws.amazon.com/billing/signup.
2. Ikuti petunjuk secara online.

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

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

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

Membuat pengguna administratif

Setelah Anda mendaftar Akun AWS, amankan Pengguna root akun AWS, aktifkan AWS IAM Identity Center, dan buat pengguna administratif sehingga Anda tidak menggunakan pengguna root untuk tugas sehari-hari.

Amankan Anda Pengguna root akun AWS

1. Masuk ke AWS Management Consolesebagai pemilik akun dengan memilih pengguna Root dan memasukkan alamat Akun AWS email Anda. Di halaman berikutnya, masukkan kata sandi Anda.

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

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

Membuat pengguna administratif

1. Aktifkan Pusat Identitas IAM.

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

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

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

Masuk sebagai pengguna administratif

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

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

Konfigurasikan peran IAM untuk integrasi CI/CD

Untuk mengintegrasikan pemindaian Amazon Inspector ke dalam pipeline CI/CD Anda, Anda perlu membuat kebijakan IAM yang memungkinkan akses ke Amazon Inspector Scan API yang memindai tagihan materi perangkat lunak (SBOM). Kemudian, Anda dapat melampirkan kebijakan tersebut ke peran IAM yang dapat diasumsikan akun Anda untuk menjalankan Amazon Inspector Scan API.

1. Masuk ke AWS Management Console dan buka konsol IAM di https://console.aws.amazon.com/iam/.
2. Di panel navigasi konsol IAM, pilih Kebijakan, lalu pilih Buat Kebijakan.
3. Di Editor Kebijakan pilih JSON dan tempel pernyataan berikut:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
```

```
            "Effect": "Allow",
            "Action": "inspector-scan:ScanSbom",
            "Resource": "*"
        }
    ]
}
```

4. Pilih Berikutnya.
5. Beri kebijakan nama, misalnya`InspectorCICDscan-policy`, dan tambahkan deskripsi opsional, lalu pilih Buat Kebijakan. Kebijakan ini akan dilampirkan pada peran yang akan Anda buat di langkah selanjutnya.
6. Di panel navigasi konsol IAM, pilih Peran dan kemudian pilih Buat Peran Baru.
7. Untuk jenis entitas Tepercaya pilih Kebijakan kepercayaan khusus dan tempel kebijakan berikut:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::{ACCOUNT_ID}:root"
            },
            "Action": "sts:AssumeRole",
            "Condition": {}
        }
    ]
}
```

8. Pilih Berikutnya.
9. Di Tambahkan izin, cari dan pilih kebijakan yang Anda buat sebelumnya, lalu pilih Berikutnya.
10. Beri nama peran, misalnya`InspectorCICDscan-role`, dan tambahkan deskripsi opsional, lalu pilih`Create Role`.

Amazon Inspector SBOM Generator

Amazon Inspector SBOM Generator (Sbomgen) adalah alat biner yang menghasilkan tagihan bahan perangkat lunak (SBOM) untuk gambar kontainer. SBOM adalah inventaris yang dikumpulkan dari perangkat lunak yang diinstal pada suatu sistem.

Sbomgenbekerja dengan memindai file yang diketahui berisi informasi tentang paket yang diinstal. Jika salah satu file ini ditemukan, alat mengekstrak nama paket, versi, dan metadata lainnya. Metadata paket ini kemudian diubah menjadi SBOM. CycloneDX

Sbomgendapat digunakan sebagai alat mandiri untuk menyediakan CycloneDX SBOM sebagai file atau ke STDOUT. Ini juga digunakan sebagai bagian dari integrasi Amazon Inspector CI/CD, yang memindai gambar kontainer secara otomatis sebagai bagian dari pipeline penerapan Anda. Untuk informasi selengkapnya, lihat Mengintegrasikan pemindaian Amazon Inspector ke dalam pipeline CI/CD Anda.

Paket dan format gambar yang didukung

Pada saat ini, Sbomgen dapat mengumpulkan inventaris untuk jenis paket berikut:

- Alpine APK
- Debian / Ubuntu DPKG
- Red Hat RPM
- GoPaket melalui `go.mod` dan `go mod cache`
- Javapaket melalui `pom.properties`
- Node.jspaket melalui `package.json` file di dalamnya `node_modules`
- Paket C # melalui file Nuget (`.deps.json`,,, `csproj` packages.lock.json`Packages.config`)
- PHP melalui `installed.json` dan `composer.lock`
- Pythonpaket melalui`requirements.txt`,`Pipfile.lock`,`poetry.lock`, dan `egg/wheel` file
- Rubypaket melalui`Gemfile.lock`,`.gemspec`, dan permata yang diinstal secara global
- RustPaket melalui `Cargo.lock` dan `Cargo.toml`

Sbomgenmendukung format manifes gambar kontainer berikut untuk gambar:

- Manifes gambar OCI
- Dockermanifes gambar versi 2, skema 2

- Dockermanifes gambar versi 2, skema 1
- Dockermanifes gambar versi 1

> **Important**
>
> Sbomgentidak dapat memindai gambar kontainer jika ukurannya lebih besar dari 5 GB, memiliki lebih dari 60 lapisan, atau lebih dari 2.000 paket yang diinstal.

Menginstal Amazon Inspector SBOM Generator () Sbomgen

Sbomgenhanya tersedia untuk sistem operasi Linux. Jika Anda menggunakannya untuk menganalisis gambar kontainer, Anda harus menginstal layanan kontainer, sepertiDocker, Podman, ataucontainerd.

Untuk kinerja terbaik, kami sarankan menjalankan biner dari sistem dengan spesifikasi perangkat keras minimum ini:

- CPU inti 4x
- 8 GB RAM

Untuk menginstal Sbomgen

1. Unduh file Sbomgen zip dari URL yang benar untuk arsitektur Anda:

   Linux AMD64:

   https://amazon-inspector-sbomgen.s3.amazonaws.com/latest/linux/amd64/inspector-sbomgen.zip

   Linux ARM64:

   https://amazon-inspector-sbomgen.s3.amazonaws.com/latest/linux/arm64/inspector-sbomgen.zip
2. Buka zip unduhan menggunakan perintah berikut:

   ```
   unzip inspector-sbomgen.zip
   ```
3. Periksa file-file berikut di arsip:

- `inspector-sbomgen`— Ini adalah biner yang akan Anda jalankan untuk menghasilkan SBOM.
- `README.txt`- Ini adalah dokumentasi untuk digunakanSbomgen.
- `LICENSE.txt`— File ini berisi lisensi perangkat lunak untukSbomgen.
- `licenses`— Folder ini berisi info lisensi untuk paket pihak ketiga yang digunakan olehSbomgen.
- `checksums.txt`— File ini menyediakan hash Sbomgen biner.
- `sbom.json`— Ini adalah CycloneDX SBOM untuk Sbomgen biner.

4. (Opsional) Verifikasi keaslian dan integritas biner menggunakan perintah berikut:

   ```
   sha256sum < inspector-sbomgen
   ```

   - Bandingkan hasilnya dengan isi `checksums.txt` file.

5. Berikan izin yang dapat dieksekusi ke biner menggunakan perintah berikut:

   ```
   chmod +x inspector-sbomgen
   ```

6. Verifikasi bahwa Sbomgen berhasil diinstal menggunakan perintah berikut:

   ```
   ./inspector-sbomgen --version
   ```

   Anda akan melihat output yang mirip dengan yang berikut ini:

   ```
   Version: 1.X.X
   ```

Menggunakan Sbomgen

Anda dapat menggunakan Sbomgen untuk menghasilkan SBOM untuk gambar kontainer.

Anda juga dapat menyesuaikan hasil pembuatan SBOM melalui opsi seperti; tidak termasuk file tertentu, atau menentukan paket mana yang dipindai alat. Untuk contoh kasus penggunaan ini, dan banyak lagi, jalankan perintah berikut:

```
./inspector-sbomgen list-examples
```

Untuk menghasilkan SBOM untuk gambar kontainer dan menampilkan hasilnya ke file

Untuk contoh ini, ganti *`image:tag`*dengan ID gambar Anda, dan *`output_path.json`*dengan jalur untuk menyimpan output ke:

```
./inspector-sbomgen container --image image:tag -o output_path.json
```

Mengautentikasi ke Pendaftar Pribadi dengan Sbomgen

Anda dapat membuat SBOM dari kontainer Anda yang dihosting di registri pribadi dengan memberikan kredensional otentikasi registri pribadi Anda. Anda dapat memberikan kredensi Anda dalam berbagai cara; melalui kredenal cache, melalui metode interaktif, atau melalui metode non-interaktif di mana kredensialnya disediakan sebagai variabel lingkungan sebelum dijalankan. Sbomgen

Mengautentikasi menggunakan kredensi cache (disarankan)

1. Sbomgenakan mencoba menggunakan kredensi cache jika tersedia di agen Anda. Untuk metode ini, pertama otentikasi ke registri kontainer Anda. Misalnya, jika Anda menggunakanDocker, Anda dapat mengautentikasi ke registri Anda menggunakan Docker `login` perintah:

   ```
   docker login
   ```

2. Kemudian, setelah berhasil mengautentikasi ke registri pribadi Anda, Anda dapat menggunakan Sbomgen pada gambar kontainer di registri itu. Untuk menggunakan contoh berikut, ganti *image:tag*dengan nama gambar yang akan dipindai:

   ```
   ./inspector-sbomgen container --image image:tag
   ```

Autentikasi menggunakan metode interaktif

- Untuk metode ini, Anda memberikan nama pengguna Anda sebagai parameter dan Sbomgen akan meminta Anda untuk entri kata sandi yang aman bila diperlukan. Untuk menggunakan contoh berikut, ganti *image:tag*dengan nama gambar yang akan dipindai, dan *your_username*dengan nama pengguna yang memiliki akses ke gambar itu:

  ```
  ./inspector-sbomgen container --image image:tag --username
  your_username
  ```

Autentikasi menggunakan metode non-interaktif

- Untuk menggunakan metode ini, Anda harus menyimpan kata sandi atau token registri Anda dalam file.txt yang hanya dapat dibaca oleh pengguna saat ini. File teks harus hanya berisi

kata sandi atau token Anda pada satu baris. Untuk menggunakan contoh berikut, ganti *your_username* dengan nama pengguna Anda, ganti *password.txt* dengan file yang berisi kata sandi atau token Anda, dan ganti *image:tag* dengan nama gambar untuk dipindai:

```
INSPECTOR_SBOMGEN_USERNAME=your_username\
INSPECTOR_SBOMGEN_PASSWORD=`cat password.txt` \
./inspector-sbomgen container --image image:tag
```

Contoh output dari Sbomgen

Berikut ini adalah contoh SBOM untuk gambar kontainer yang diinventarisasi menggunakan. Sbomgen

Gambar kontainer SBOM


```
{
  "bomFormat": "CycloneDX",
  "specVersion": "1.5",
  "serialNumber": "urn:uuid:828875ef-8c32-4777-b688-0af96f3cf619",
  "version": 1,
  "metadata": {
    "timestamp": "2023-11-17T21:36:38Z",
    "tools": [
      {
        "vendor": "Amazon Web Services, Inc. (AWS)",
        "name": "Amazon Inspector SBOM Generator",
        "version": "1.0.0",
        "hashes": [
          {
            "alg": "SHA-256",
            "content":
 "10ab669cfc99774786301a745165b5957c92ed9562d19972fbf344d4393b5eb1"
          }
        ]
      }
    ],
    "component": {
      "bom-ref": "comp-1",
      "type": "container",
      "name": "fedora:latest",
      "properties": [
```

```
        {
          "name": "amazon:inspector:sbom_generator:image_id",
          "value":
 "sha256:c81c8ae4dda7dedc0711daefe4076d33a88a69a28c398688090c1141eff17e50"
        },
        {
          "name": "amazon:inspector:sbom_generator:layer_diff_id",
          "value":
 "sha256:eddd0d48c295dc168d0710f70364581bd84b1dda6bb386c4a4de0b61de2f2119"
        }
      ]
    }
  },
  "components": [
    {
      "bom-ref": "comp-2",
      "type": "library",
      "name": "dnf",
      "version": "4.18.0",
      "purl": "pkg:pypi/dnf@4.18.0",
      "properties": [
        {
          "name": "amazon:inspector:sbom_generator:source_file_scanner",
          "value": "python-pkg"
        },
        {
          "name": "amazon:inspector:sbom_generator:source_package_collector",
          "value": "python-pkg"
        },
        {
          "name": "amazon:inspector:sbom_generator:source_path",
          "value": "/usr/lib/python3.12/site-packages/dnf-4.18.0.dist-info/METADATA"
        },
        {
          "name": "amazon:inspector:sbom_generator:is_duplicate_package",
          "value": "true"
        },
        {
          "name": "amazon:inspector:sbom_generator:duplicate_purl",
          "value": "pkg:rpm/fedora/python3-dnf@4.18.0-2.fc39?
arch=noarch&distro=39&epoch=0"
        }
      ]
    },
```

```
    {
      "bom-ref": "comp-3",
      "type": "library",
      "name": "libcomps",
      "version": "0.1.20",
      "purl": "pkg:pypi/libcomps@0.1.20",
      "properties": [
        {
          "name": "amazon:inspector:sbom_generator:source_file_scanner",
          "value": "python-pkg"
        },
        {
          "name": "amazon:inspector:sbom_generator:source_package_collector",
          "value": "python-pkg"
        },
        {
          "name": "amazon:inspector:sbom_generator:source_path",
          "value": "/usr/lib64/python3.12/site-packages/libcomps-0.1.20-py3.12.egg-
info/PKG-INFO"
        },
        {
          "name": "amazon:inspector:sbom_generator:is_duplicate_package",
          "value": "true"
        },
        {
          "name": "amazon:inspector:sbom_generator:duplicate_purl",
          "value": "pkg:rpm/fedora/python3-libcomps@0.1.20-1.fc39?
arch=x86_64&distro=39&epoch=0"
        }
      ]
    }
  ]
}
```

Membuat integrasi pipeline CI/CD kustom Anda sendiri dengan Amazon Inspector Scan

Sebaiknya gunakan plugin Amazon Inspector CI/CD jika tersedia di pasar CI/CD Anda. Untuk daftar plugin yang tersedia, lihatSolusi CI/CD yang didukung.

Jika Amazon Inspector tidak menyediakan plugin untuk solusi CI/CD Anda, Anda dapat membuat integrasi CI/CD kustom Anda sendiri menggunakan kombinasi Amazon Inspector SBOM Generator

dan Amazon Inspector Scan API. Anda juga dapat menggunakan integrasi khusus untuk menyempurnakan pemindaian melalui opsi yang tersedia di Amazon Inspector SBOM Generator.

Untuk mengatur integrasi kustom Anda sendiri

1. Konfigurasikan Akun AWS untuk mengizinkan akses ke Amazon Inspector Scan API. Untuk petunjuk, lihat Menyiapkan AWS akun untuk menggunakan integrasi Amazon Inspector CI/CD.
2. Instal dan konfigurasikan biner Amazon Inspector SBOM Generator. Untuk petunjuk, lihat Menginstal Amazon Inspector SBOM Generator () Sbomgen.
3. Gunakan generator SBOM untuk membuat file SBOM untuk gambar kontainer yang ingin Anda pindai. Untuk menggunakan contoh berikut, ganti *image:id*dengan nama gambar yang akan dipindai, dan *sbom_path.json*dengan lokasi untuk menyimpan output SBOM ke:

   ```
   ./inspector-sbomgen container –image image:id -o sbom_path.json
   ```
4. Panggil `inspector-scan` API untuk memindai SBOM yang dihasilkan dan memberikan laporan kerentanan. Untuk menggunakan contoh berikut, ganti *sbom_path.json* dengan filepath ke file SBOM kompatibel CycloneDX yang valid. Kemudian ganti *ENDPOINT dengan titik* akhir API untuk tempat Wilayah AWS Anda saat ini diautentikasi, dan ganti *REGION dengan Region* yang sesuai. Lihat Titik akhir untuk Amazon Inspector Scan API daftar lengkap Wilayah dan titik akhir.

   ```
   aws inspector-scan scan-sbom --sbom file://sbom_path.json --endpoint "ENDPOINT" --region REGION
   ```

Format keluaran API

Amazon Inspector Scan API dapat menampilkan laporan kerentanan dalam format CycloneDX 1.5 atau Amazon Inspector menemukan JSON. Default dapat diubah menggunakan `--output-format` bendera.

Contoh output format CycloneDX 1,5

```
{
  "status": "SBOM parsed successfully, 1 vulnerabilities found",
  "sbom": {
    "bomFormat": "CycloneDX",
    "specVersion": "1.5",
    "serialNumber": "urn:uuid:0077b45b-ff1e-4dbb-8950-ded11d8242b1",
    "metadata": {
```

```
      "properties": [
        {
          "name": "amazon:inspector:sbom_scanner:critical_vulnerabilities",
          "value": "1"
        },
        {
          "name": "amazon:inspector:sbom_scanner:high_vulnerabilities",
          "value": "0"
        },
        {
          "name": "amazon:inspector:sbom_scanner:medium_vulnerabilities",
          "value": "0"
        },
        {
          "name": "amazon:inspector:sbom_scanner:low_vulnerabilities",
          "value": "0"
        }
      ],
      "tools": [
        {
          "name": "CycloneDX SBOM API",
          "vendor": "Amazon Inspector",
          "version": "empty:083c9b00:083c9b00:083c9b00"
        }
      ],
      "timestamp": "2023-06-28T14:15:53.760Z"
    },
    "components": [
      {
        "bom-ref": "comp-1",
        "type": "library",
        "name": "log4j-core",
        "purl": "pkg:maven/org.apache.logging.log4j/log4j-core@2.12.1",
        "properties": [
          {
            "name": "amazon:inspector:sbom_scanner:path",
            "value": "/home/dev/foo.jar"
          }
        ]
      }
    ],
    "vulnerabilities": [
      {
        "bom-ref": "vuln-1",
```

```
        "id": "CVE-2021-44228",
        "source": {
          "name": "NVD",
          "url": "https://nvd.nist.gov/vuln/detail/CVE-2021-44228"
        },
        "references": [
          {
            "id": "SNYK-JAVA-ORGAPACHELOGGINGLOG4J-2314720",
            "source": {
              "name": "SNYK",
              "url": "https://security.snyk.io/vuln/SNYK-JAVA-
ORGAPACHELOGGINGLOG4J-2314720"
            }
          },
          {
            "id": "GHSA-jfh8-c2jp-5v3q",
            "source": {
              "name": "GITHUB",
              "url": "https://github.com/advisories/GHSA-jfh8-c2jp-5v3q"
            }
          }
        ],
        "ratings": [
          {
            "source": {
              "name": "NVD",
              "url": "https://www.first.org/cvss/v3-1/"
            },
            "score": 10.0,
            "severity": "critical",
            "method": "CVSSv31",
            "vector": "AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H"
          },
          {
            "source": {
              "name": "NVD",
              "url": "https://www.first.org/cvss/v2/"
            },
            "score": 9.3,
            "severity": "critical",
            "method": "CVSSv2",
            "vector": "AC:M/Au:N/C:C/I:C/A:C"
          },
          {
```

```
            "source": {
              "name": "EPSS",
              "url": "https://www.first.org/epss/"
            },
            "score": 0.97565,
            "severity": "none",
            "method": "other",
            "vector": "model:v2023.03.01,date:2023-06-27T00:00:00+0000"
          },
          {
            "source": {
              "name": "SNYK",
              "url": "https://security.snyk.io/vuln/SNYK-JAVA-
ORGAPACHELOGGINGLOG4J-2314720"
            },
            "score": 10.0,
            "severity": "critical",
            "method": "CVSSv31",
            "vector": "AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:H"
          },
          {
            "source": {
              "name": "GITHUB",
              "url": "https://github.com/advisories/GHSA-jfh8-c2jp-5v3q"
            },
            "score": 10.0,
            "severity": "critical",
            "method": "CVSSv31",
            "vector": "AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H"
          }
        ],
        "cwes": [
          400,
          20,
          502
        ],
        "description": "Apache Log4j2 2.0-beta9 through 2.15.0 (excluding security
 releases 2.12.2, 2.12.3, and 2.3.1) JNDI features used in configuration, log messages,
 and parameters do not protect against attacker controlled LDAP and other JNDI related
 endpoints. An attacker who can control log messages or log message parameters can
 execute arbitrary code loaded from LDAP servers when message lookup substitution is
 enabled. From log4j 2.15.0, this behavior has been disabled by default. From version
 2.16.0 (along with 2.12.2, 2.12.3, and 2.3.1), this functionality has been completely
```

```
 removed. Note that this vulnerability is specific to log4j-core and does not affect
 log4net, log4cxx, or other Apache Logging Services projects.",
        "advisories": [
          {
            "url": "https://www.intel.com/content/www/us/en/security-center/advisory/
intel-sa-00646.html"
          },
          {
            "url": "https://support.apple.com/kb/HT213189"
          },
          {
            "url": "https://msrc-blog.microsoft.com/2021/12/11/microsofts-response-to-
cve-2021-44228-apache-log4j2/"
          },
          {
            "url": "https://logging.apache.org/log4j/2.x/security.html"
          },
          {
            "url": "https://www.debian.org/security/2021/dsa-5020"
          },
          {
            "url": "https://cert-portal.siemens.com/productcert/pdf/ssa-479842.pdf"
          },
          {
            "url": "https://www.oracle.com/security-alerts/alert-cve-2021-44228.html"
          },
          {
            "url": "https://www.oracle.com/security-alerts/cpujan2022.html"
          },
          {
            "url": "https://cert-portal.siemens.com/productcert/pdf/ssa-714170.pdf"
          },
          {
            "url": "https://lists.fedoraproject.org/archives/list/package-
announce@lists.fedoraproject.org/message/M5CSVUNV4HWZZXGOKNSK6L7RPM7BOKIB/"
          },
          {
            "url": "https://cert-portal.siemens.com/productcert/pdf/ssa-397453.pdf"
          },
          {
            "url": "https://cert-portal.siemens.com/productcert/pdf/ssa-661247.pdf"
          },
          {
```

```
            "url": "https://lists.fedoraproject.org/archives/list/package-
announce@lists.fedoraproject.org/message/VU57UJDCFIASIO35GC55JMKSRXJMCDFM/"
          },
          {
            "url": "https://www.oracle.com/security-alerts/cpuapr2022.html"
          },
          {
            "url": "https://twitter.com/kurtseifried/status/1469345530182455296"
          },
          {
            "url": "https://tools.cisco.com/security/center/content/
CiscoSecurityAdvisory/cisco-sa-apache-log4j-qRuKNEbd"
          },
          {
            "url": "https://lists.debian.org/debian-lts-announce/2021/12/msg00007.html"
          },
          {
            "url": "https://www.kb.cert.org/vuls/id/930724"
          }
        ],
        "created": "2021-12-10T10:15:00Z",
        "updated": "2023-04-03T20:15:00Z",
        "affects": [
          {
            "ref": "comp-1"
          }
        ],
        "properties": [
          {
            "name": "amazon:inspector:sbom_scanner:exploit_available",
            "value": "true"
          },
          {
            "name": "amazon:inspector:sbom_scanner:exploit_last_seen_in_public",
            "value": "2023-03-06T00:00:00Z"
          },
          {
            "name": "amazon:inspector:sbom_scanner:cisa_kev_date_added",
            "value": "2021-12-10T00:00:00Z"
          },
          {
            "name": "amazon:inspector:sbom_scanner:cisa_kev_date_due",
            "value": "2021-12-24T00:00:00Z"
          },
```

```
          {
            "name": "amazon:inspector:sbom_scanner:fixed_version:comp-1",
            "value": "2.15.0"
          }
        ]
      }
    ]
  }
}
```

Contoh output format Inspector

```
                        {
  "status": "SBOM parsed successfully, 1 vulnerability found",
  "inspector": {
    "messages": [
      {
        "name": "foo",
        "purl": "pkg:maven/foo@1.0.0", // Will not exist in output if missing in sbom
        "info": "Component skipped: no rules found."
      }
    ],
    "vulnerability_count": {
      "critical": 1,
      "high": 0,
      "medium": 0,
      "low": 0
    },
    "vulnerabilities": [
      {
        "id": "CVE-2021-44228",
        "severity": "critical",
        "source": "https://nvd.nist.gov/vuln/detail/CVE-2021-44228",
        "related": [
          "SNYK-JAVA-ORGAPACHELOGGINGLOG4J-2314720",
          "GHSA-jfh8-c2jp-5v3q"
        ],
        "description": "Apache Log4j2 2.0-beta9 through 2.15.0 (excluding security
releases 2.12.2, 2.12.3, and 2.3.1) JNDI features used in configuration, log messages,
and parameters do not protect against attacker controlled LDAP and other JNDI related
endpoints. An attacker who can control log messages or log message parameters can
execute arbitrary code loaded from LDAP servers when message lookup substitution is
```

```
 enabled. From log4j 2.15.0, this behavior has been disabled by default. From version
 2.16.0 (along with 2.12.2, 2.12.3, and 2.3.1), this functionality has been completely
 removed. Note that this vulnerability is specific to log4j-core and does not affect
 log4net, log4cxx, or other Apache Logging Services projects.",
        "references": [
          "https://www.intel.com/content/www/us/en/security-center/advisory/intel-
sa-00646.html",
          "https://support.apple.com/kb/HT213189",
          "https://msrc-blog.microsoft.com/2021/12/11/microsofts-response-to-
cve-2021-44228-apache-log4j2/",
          "https://logging.apache.org/log4j/2.x/security.html",
          "https://www.debian.org/security/2021/dsa-5020",
          "https://cert-portal.siemens.com/productcert/pdf/ssa-479842.pdf",
          "https://www.oracle.com/security-alerts/alert-cve-2021-44228.html",
          "https://www.oracle.com/security-alerts/cpujan2022.html",
          "https://cert-portal.siemens.com/productcert/pdf/ssa-714170.pdf",
          "https://lists.fedoraproject.org/archives/list/package-
announce@lists.fedoraproject.org/message/M5CSVUNV4HWZZXGOKNSK6L7RPM7BOKIB/",
          "https://cert-portal.siemens.com/productcert/pdf/ssa-397453.pdf",
          "https://cert-portal.siemens.com/productcert/pdf/ssa-661247.pdf",
          "https://lists.fedoraproject.org/archives/list/package-
announce@lists.fedoraproject.org/message/VU57UJDCFIASIO35GC55JMKSRXJMCDFM/",
          "https://www.oracle.com/security-alerts/cpuapr2022.html",
          "https://twitter.com/kurtseifried/status/1469345530182455296",
          "https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-
sa-apache-log4j-qRuKNEbd",
          "https://lists.debian.org/debian-lts-announce/2021/12/msg00007.html",
          "https://www.kb.cert.org/vuls/id/930724"
        ],
        "created": "2021-12-10T10:15:00Z",
        "updated": "2023-04-03T20:15:00Z",
        "properties": {
          "cisa_kev_date_added": "2021-12-10T00:00:00Z",
          "cisa_kev_date_due": "2021-12-24T00:00:00Z",
          "cwes": [
            400,
            20,
            502
          ],
          "cvss": [
            {
              "source": "NVD",
              "severity": "critical",
              "cvss3_base_score": 10.0,
```

```
              "cvss3_base_vector": "AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H",
              "cvss2_base_score": 9.3,
              "cvss2_base_vector": "AC:M/Au:N/C:C/I:C/A:C"
            },
            {
              "source": "SNYK",
              "severity": "critical",
              "cvss3_base_score": 10.0,
              "cvss3_base_vector": "AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:H"
            },
            {
              "source": "GITHUB",
              "severity": "critical",
              "cvss3_base_score": 10.0,
              "cvss3_base_vector": "AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H"
            }
          ],
          "epss": 0.97565,
          "exploit_available": true,
          "exploit_last_seen_in_public": "2023-03-06T00:00:00Z"
        },
        "affects": [
          {
            "installed_version": "pkg:maven/org.apache.logging.log4j/log4j-
core@2.12.1",
            "fixed_version": "2.15.0",
            "path": "/home/dev/foo.jar"
          }
        ]
      }
    ]
  }
}
```


Menggunakan plugin Amazon Inspector Jenkins

JenkinsPlugin ini memanfaatkan biner Amazon Inspector SBOM Generator dan Amazon Inspector Scan API untuk menghasilkan laporan terperinci di akhir build, sehingga Anda dapat menyelidiki dan memulihkan risiko sebelum penerapan.

Amazon Inspector adalah layanan manajemen kerentanan yang memindai gambar kontainer untuk sistem operasi dan kerentanan paket bahasa pemrograman berdasarkan CVE.

Menggunakan Jenkins plugin Amazon Inspector, Anda dapat menambahkan pemindaian kerentanan Amazon Inspector ke pipeline Anda. Jenkins

> **Note**
>
> Pemindaian kerentanan Amazon Inspector dapat dikonfigurasi untuk lulus atau gagal eksekusi pipeline berdasarkan jumlah dan tingkat keparahan kerentanan yang terdeteksi.

Anda dapat melihat versi terbaru dari Jenkins plugin di Jenkins pasar di https://plugins.jenkins.io/amazon-inspector-image-scanner/.

Langkah-langkah berikut menjelaskan cara mengatur plugin Amazon Inspector Jenkins.

> **Important**
>
> Sebelum menyelesaikan langkah-langkah berikut, Anda harus memutakhirkan Jenkins ke versi 2.387.3 atau lebih tinggi agar plugin dapat berjalan.

Langkah 1. Menyiapkan sebuah Akun AWS

Konfigurasikan Akun AWS dengan peran IAM yang memungkinkan akses ke Amazon Inspector Scan API. Untuk petunjuk, lihat Menyiapkan AWS akun untuk menggunakan integrasi Amazon Inspector CI/CD.

Langkah 2. Instal Plugin Amazon Inspector Jenkins

Prosedur berikut menjelaskan cara menginstal plugin Amazon Inspector Jenkins dari dasbor. Jenkins

1. Dari dasbor Jenkins, pilih Kelola Jenkins, lalu pilih Kelola Plugin.
2. Pilih Tersedia.
3. Dari tab Tersedia, cari Amazon Inspector Scan, lalu instal plugin.

(Opsional) Langkah 3. Tambahkan kredensi docker ke Jenkins

> **Note**
>
> Hanya tambahkan kredensi docker jika image docker ada di repositori pribadi. Jika tidak, lewati langkah ini.

Prosedur berikut menjelaskan cara menambahkan kredensyal docker dari dasbor. Jenkins Jenkins

1. Dari dasbor Jenkins, pilih Manage Jenkins, Credentials, dan kemudian System.
2. Pilih Kredensial global, lalu Tambahkan kredensial.
3. Untuk Jenis, pilih Nama pengguna dengan kata sandi.
4. Untuk Lingkup, pilih Global (Jenkins, node, item, semua item anak, dll).
5. Masukkan detail Anda, lalu pilih OK.

(Opsional) Langkah 4. Tambahkan AWS kredensial

> **Note**
>
> Hanya tambahkan AWS kredensi jika Anda ingin mengautentikasi berdasarkan pengguna IAM. Jika tidak, lewati langkah ini.

Prosedur berikut menjelaskan cara menambahkan AWS kredensyal dari dasbor. Jenkins

1. Dari dasbor Jenkins, pilih Manage Jenkins, Credentials, dan kemudian System.
2. Pilih Kredensial global, lalu Tambahkan kredensial.
3. Untuk Jenis, pilih AWS Credentials.
4. Masukkan detail Anda, termasuk ID Kunci Akses dan Kunci Akses Rahasia, lalu pilih OK.

Langkah 5. Tambahkan dukungan CSS dalam Jenkins skrip

Prosedur berikut menjelaskan cara menambahkan dukungan CSS dalam Jenkikns skrip.

1. Mulai ulang Jenkins.
2. Dari Dashboard, pilih Manage Jenkins, Nodes, Built-in Node, dan kemudian Script Console.
3. Di kotak teks, tambahkan barisSystem.setProperty("hudson.model.DirectoryBrowserSupport.CSP", ""), lalu pilih Jalankan.

Langkah 6. Tambahkan Amazon Inspector Scan ke build Anda

Anda dapat menambahkan Amazon Inspector Scan ke build dengan menambahkan langkah build dalam project Anda atau dengan menggunakan pipeline Jenkins deklaratif.

Amazon Inspector Scan ke build Anda dengan menambahkan langkah build dalam proyek Anda

1. Pada halaman konfigurasi, gulir ke bawah ke Build Steps, dan pilih Add build step. Kemudian pilih Amazon Inspector Scan.
2. Pilih antara dua metode instalasi inspector-sbomgen: Otomatis atau Manual.

    a. (Opsi 1) Pilih Otomatis untuk mengunduh versi terbaru dari inspector-sbomgen. Jika Anda memilih metode ini, pastikan untuk memilih arsitektur CPU yang cocok dengan sistem yang mengeksekusi plugin.

    b. (Opsi 2) Pilih Manual jika Anda ingin mengatur biner Amazon Inspector SBOM Generator untuk pemindaian. Jika Anda memilih metode ini, pastikan untuk memberikan jalur lengkap ke versi inspector-sbomgen yang diunduh sebelumnya.

    Untuk informasi selengkapnya, lihat Menginstal Amazon Inspector SBOM Generator (Sbomgen) di Amazon Inspector SBOM Generator.

3. Selesaikan yang berikut ini untuk menyelesaikan konfigurasi langkah pembuatan Amazon Inspector Scan:

    a. Masukkan Id Gambar Anda. Gambar dapat berupa lokal, jarak jauh, atau diarsipkan. Nama gambar harus mengikuti konvensi Docker penamaan. Jika menganalisis gambar yang diekspor, berikan jalur ke file tar yang diharapkan. Lihat contoh jalur Id Gambar berikut:

        i. Untuk kontainer lokal atau jarak jauh: NAME[:TAG|@DIGEST]

        ii. Untuk file tar: /path/to/image.tar

b. Pilih Wilayah AWSuntuk mengirim permintaan pemindaian melalui.

c. (Opsional) Untuk kredensi Docker, pilih nama pengguna Anda. Docker Lakukan ini hanya jika gambar kontainer Anda ada di repositori pribadi.

d. (Opsional) Anda dapat memberikan metode AWS otentikasi yang didukung berikut ini:

   i. (Opsional) Untuk peran IAM, berikan peran ARN (arn:aws:iam: ::role/). *AccountNumberRoleName*

   ii. (Opsional) Untuk kredensyal AWS, pilih Id untuk diautentikasi berdasarkan pengguna IAM.

   iii. (Opsional) Untuk nama AWS profil, berikan nama profil untuk diautentikasi menggunakan nama profil.

e. (Opsional) Tentukan ambang kerentanan per tingkat keparahan. Jika jumlah yang Anda tentukan terlampaui selama pemindaian, pembuatan gambar akan gagal. Jika nilainya semuanya`0`, build akan berhasil, terlepas dari apakah ada kerentanan yang ditemukan.

4. Pilih Simpan.

Tambahkan Amazon Inspector Scan ke build Anda menggunakan pipeline deklaratif Jenkins

Anda dapat menambahkan Amazon Inspector Scan ke build menggunakan pipeline deklaratif Jenkins secara otomatis atau manual.

Untuk mengunduh pipa deklaratif SBOMgen secara otomatis

- Untuk menambahkan Amazon Inspector Scan ke build, gunakan sintaks contoh berikut. Berdasarkan arsitektur OS pilihan Anda dari unduhan Amazon Inspector SBOM Generator, ganti *SBOMGEN_SOURCE* dengan LinuxAMD64 atau LinuxArm64. Ganti *IMAGE_PATH* dengan jalur ke gambar Anda (seperti *alpine:latest*), IAM_ROLE *dengan* ARN dari peran IAM yang Anda konfigurasikan pada langkah 1, dan *ID dengan ID* kredensyal Anda jika Anda menggunakan repositori pribadi. Docker Anda dapat mengaktifkan ambang kerentanan secara opsional dan menentukan nilai untuk setiap tingkat keparahan.

```
pipeline {
   agent any
   stages {
       stage('amazon-inspector-image-scanner') {
```

```
            steps {
                script {
                step([
                $class:
'com.amazon.inspector.jenkins.amazoninspectorbuildstep.AmazonInspectorBuilder',
                sbomgenSource: 'SBOMGEN_SOURCE', // this can be linuxAmd64 or linuxArm64
                archivePath: 'IMAGE_PATH',
                awsRegion: 'REGION',
                iamRole: 'IAM ROLE',
                credentialId: 'Id', // provide empty string if image not in private
repositories
                awsCredentialId: ''AWS ID;',
                awsProfileName: 'Profile Name',
                isThresholdEnabled: false,
                countCritical: 0,
                countHigh: 0,
                countLow: 10,
                countMedium: 5,
               ])
            }
          }
        }
    }
}
```

Untuk mengunduh pipeline deklaratif SBOMgen secara manual

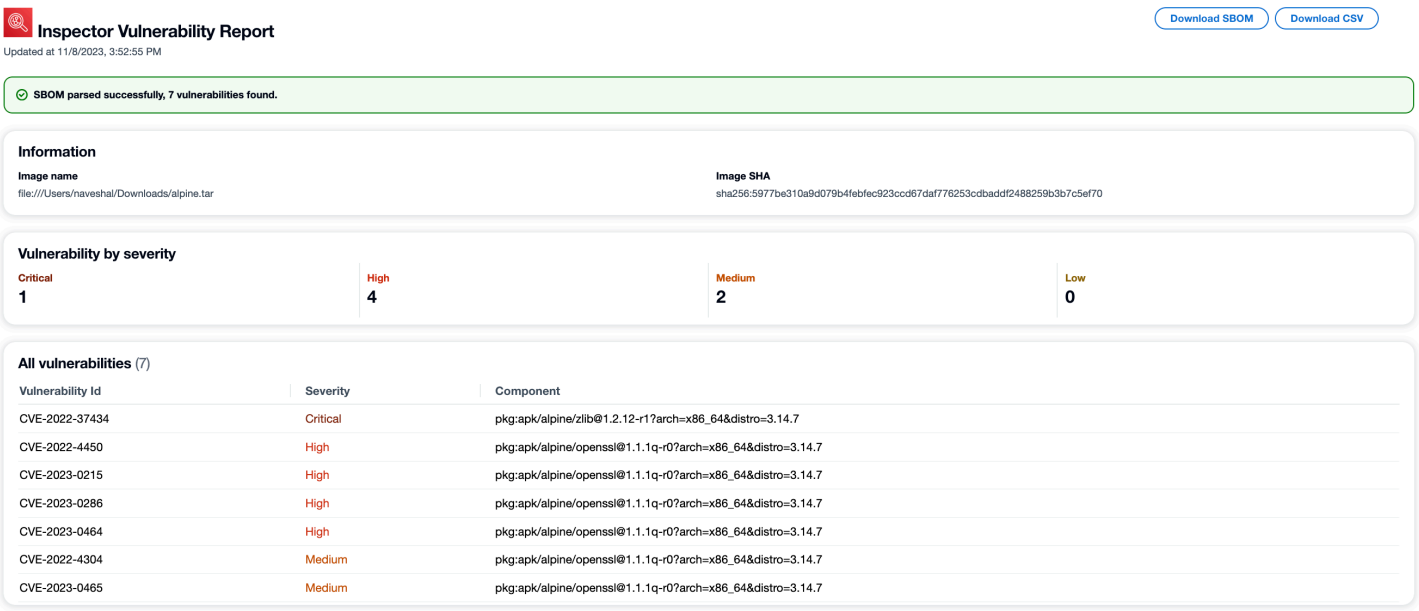
- Untuk menambahkan Amazon Inspector Scan ke build, gunakan sintaks contoh berikut. *Ganti SBOMGEN_PATH dengan jalur ke Amazon Inspector SBOM Generator yang Anda instal di langkah 3, IMAGE_PATH dengan jalur ke gambar Anda (seperti alpine:latest), IAM_ROLE dengan ARN dari peran IAM yang Anda konfigurasi di langkah 1, dan ID dengan ID kredensi Anda jika Anda menggunakan repositori pribadi.* Docker Anda dapat mengaktifkan ambang kerentanan secara opsional dan menentukan nilai untuk setiap tingkat keparahan.

> **Note**
>
> Tempatkan Sbomgen di direktori Jenkins, dan berikan jalur ke direktori Jenkins di plugin (seperti */opt/folder/arm64/inspector-sbomgen*).

```
pipeline {
    agent any
    stages {
        stage('amazon-inspector-image-scanner') {
            steps {
                script {
                step([
                $class:
 'com.amazon.inspector.jenkins.amazoninspectorbuildstep.AmazonInspectorBuilder',
                sbomgenPath: 'SBOMGEN_PATH',
                archivePath: 'IMAGE_PATH',
                awsRegion: 'REGION',
                iamRole: 'IAM ROLE',
                awsCredentialId: ''AWS ID;',
                credentialId: 'Id;', // provide empty string if image not in private
 repositories
                awsProfileName: 'Profile Name',
                isThresholdEnabled: false,
                countCritical: 0,
                countHigh: 0,
                countLow: 10,
                countMedium: 5,
               ])
            }
         }
       }
    }
 }
```

Langkah 7. Lihat laporan kerentanan Amazon Inspector

1. Selesaikan pembangunan baru proyek Anda.
2. Setelah build selesai, pilih format keluaran dari hasil. Jika Anda memilih HTML, Anda memiliki opsi untuk mengunduh laporan versi JSON SBOM atau CSV. Berikut ini menunjukkan contoh laporan HTML:



Memecahkan masalah

Berikut ini adalah kesalahan umum yang dapat Anda temui saat menggunakan plugin Amazon Inspector Scan untuk. Jenkins

Gagal memuat kredensi atau kesalahan pengecualian sts

Kesalahan:

```
InstanceProfileCredentialsProvider(): Failed to load credentials or sts exception.
```

Resulltion

Dapatkan `aws_access_key_id` dan `aws_secret_access_key` untuk AWS akun Anda. Siapkan `aws_access_key_id` dan `aws_secret_access_key` masuk`~/.aws/credentials`.

Kesalahan jalur inspektor-sbomgen

Kesalahan:

```
Exception:com.amazon.inspector.jenkins.amazoninspectorbuildstep.exception.Sbomge
There was an issue running inspector-sbomgen, is /opt/inspector/inspector-sbomgen the correct path?
```

Penyelesaian:

Selesaikan prosedur berikut untuk menyelesaikan masalah.

1. Tempatkan arsitektur OS Inspector-SBOMGEN yang benar di Jenkins direktori Untuk informasi selengkapnya, lihat Amazon Inspector SBOM Generator.
2. Berikan izin yang dapat dieksekusi ke biner menggunakan perintah berikut:. `chmod +x inspector-sbomgen`
3. Berikan jalur Jenkins mesin yang benar di plugin, seperti`/opt/folder/arm64/inspector-sbomgen`.
4. Simpan konfigurasi, dan jalankan Jenkins pekerjaan.

Menggunakan plugin Amazon Inspector TeamCity

TeamCityPlugin Amazon Inspector memberi Anda kemampuan untuk menambahkan pemindaian kerentanan Amazon Inspector ke pipeline Anda. TeamCity Plugin ini memanfaatkan biner Amazon Inspector SBOM Generator dan Amazon Inspector Scan API untuk menghasilkan laporan terperinci di akhir build sehingga Anda dapat menyelidiki dan memulihkan risiko sebelum penerapan. Pemindaian juga dapat dikonfigurasi untuk lulus atau gagal eksekusi pipa berdasarkan jumlah dan tingkat keparahan kerentanan yang terdeteksi.

Amazon Inspector adalah layanan manajemen kerentanan yang ditawarkan oleh AWS yang memindai gambar kontainer untuk sistem operasi dan kerentanan paket bahasa pemrograman berdasarkan CVE. Untuk informasi selengkapnya tentang integrasi CI/CD Amazon Inspector, lihat. Mengintegrasikan pemindaian Amazon Inspector ke dalam pipeline CI/CD Anda

Untuk daftar paket dan format gambar kontainer, plugin Amazon Inspector mendukung lihat,. Paket dan format gambar yang didukung

Anda dapat melihat versi terbaru dari plugin di TeamCity pasar di https://plugins.jetbrains.com/plugin/23236 - amazon-inspector-scanner. Atau, ikuti langkah-langkah di setiap bagian dokumen ini untuk menyiapkan plugin Amazon Inspector TeamCity:

1. Mengatur sebuah Akun AWS.
   - Konfigurasikan Akun AWS dengan peran IAM yang memungkinkan akses ke Amazon Inspector Scan API. Untuk petunjuk, lihat Menyiapkan AWS akun untuk menggunakan integrasi Amazon Inspector CI/CD.
2. Instal plugin Amazon InspectorTeamCity.

a. Dari dasbor Anda, buka Administrasi > Plugin.

b. Cari Amazon Inspector Scan.

c. Instal plugin.

3. Instal Amazon Inspector SBOM Generator.

   - Instal biner Amazon Inspector SBOM Generator di direktori server Teamcity Anda. Untuk petunjuk, lihat Menginstal Amazon Inspector SBOM Generator () Sbomgen.

4. Tambahkan langkah pembuatan Amazon Inspector Scan ke proyek Anda.

   a. Pada halaman konfigurasi, gulir ke bawah ke Build Steps, pilih Add build step, lalu pilih Amazon Inspector Scan.

   b. Konfigurasikan langkah pembuatan Amazon Inspector Scan dengan mengisi detail berikut:

      - Tambahkan nama Langkah.
      - Pilih di antara dua metode instalasi Amazon Inspector SBOM Generator: Otomatis atau Manual.
        - Otomatis mengunduh versi terbaru Amazon Inspector SBOM Generator berdasarkan sistem dan arsitektur CPU Anda.
        - Manual mengharuskan Anda menyediakan jalur lengkap ke versi Amazon Inspector SBOM Generator yang diunduh sebelumnya.

        Untuk informasi lebih lanjut, lihat Menginstal Amazon Inspector SBOM Generator (Sbomgen) di Amazon Inspector SBOM Generator.
      - Masukkan Id Gambar Anda. Gambar Anda dapat berupa lokal, jarak jauh, atau diarsipkan. Nama gambar harus mengikuti konvensi Docker penamaan. Jika menganalisis gambar yang diekspor, berikan jalur ke file tar yang diharapkan. Lihat contoh jalur Id Gambar berikut:
        - Untuk kontainer lokal atau jarak jauh: `NAME[:TAG|@DIGEST]`
        - Untuk file tar: `/path/to/image.tar`
      - Untuk Peran IAM, masukkan ARN untuk peran yang Anda konfigurasikan pada langkah 1.
      - Pilih Wilayah AWSuntuk mengirim permintaan pemindaian melalui.
      - (Opsional) Untuk Otentikasi Docker masukkan Nama Pengguna Docker dan Kata Sandi Docker Anda. Lakukan ini hanya jika gambar kontainer Anda ada di repositori pribadi.

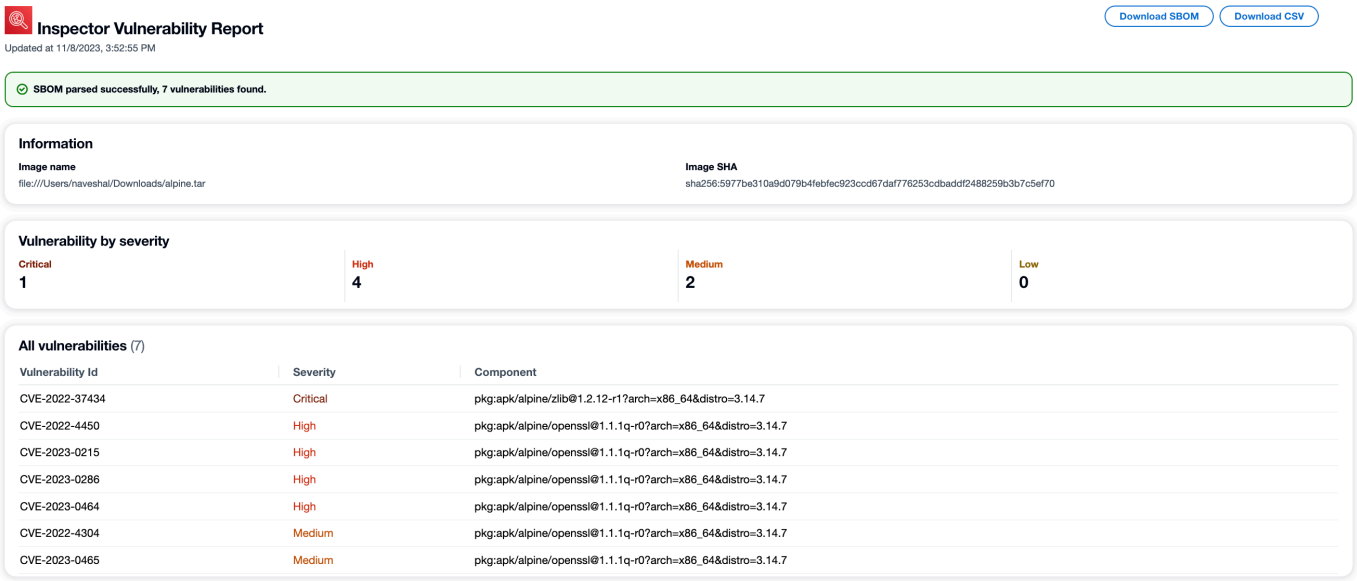
- (Opsional) Untuk AWS Otentikasi, masukkan ID kunci AWS akses dan kunci AWS rahasia Anda. Lakukan ini hanya jika Anda ingin mengautentikasi berdasarkan AWS kredensional.
- (Opsional) Tentukan ambang kerentanan per tingkat keparahan. Jika jumlah yang Anda tentukan terlampaui selama pemindaian, build gambar akan gagal. Jika nilainya semua `0` build akan berhasil terlepas dari jumlah kerentanan yang ditemukan.

c. Pilih Simpan.

5. Lihat laporan kerentanan Amazon Inspector Anda.

a. Selesaikan pembangunan baru proyek Anda.

b. Saat build selesai, pilih format keluaran dari hasil. Saat Anda memilih HTML, Anda memiliki opsi untuk mengunduh laporan versi JSON SBOM atau CSV. Berikut ini adalah contoh dari laporan HTML:



Ruang nama Amazon Inspector CycloneDX

Amazon Inspector telah memesan CycloneDX ruang nama dan nama properti untuk digunakan dengan SBOM yang diproduksi oleh Amazon Inspector SBOM Generator dan Amazon Inspector Scan API. Halaman ini mendokumentasikan semua properti kunci/nilai kustom yang dapat ditambahkan ke komponen di CycloneDX SBOM yang dibuat menggunakan alat Amazon Inspector. Untuk informasi lebih lanjut tentang taksonomi CycloneDX properti, lihat dokumentasi resmi.

`amazon:inspector:sbom_scanner` taksonomi namespace

`amazon:inspector:sbom_scanner` Namespace digunakan oleh Amazon Inspector Scan API. Ini memiliki sifat-sifat berikut:

Properti	Deskripsi
`amazon:inspector:sbom_scanner:critical_vulnerabilities`	Hitungan jumlah total kerentanan keparahan kritis yang ditemukan di SBOM.
`amazon:inspector:sbom_scanner:high_vulnerabilities`	Hitungan jumlah total kerentanan tingkat keparahan tinggi yang ditemukan di SBOM.
`amazon:inspector:sbom_scanner:medium_vulnerabilities`	Hitungan jumlah total kerentanan tingkat keparahan sedang yang ditemukan di SBOM.
`amazon:inspector:sbom_scanner:low_vulnerabilities`	Hitungan jumlah total kerentanan tingkat keparahan rendah yang ditemukan di SBOM.
`amazon:inspector:sbom_scanner:info`	Menyediakan konteks pemindaian untuk komponen tertentu, misalnya: “Komponen dipindai: tidak ada kerentanan yang ditemukan .”
`amazon:inspector:sbom_scanner:warning`	Menyediakan konteks mengapa komponen tertentu tidak dipindai, misalnya: “Komponen dilewati: tidak ada purl yang disediakan.”
`amazon:inspector:sbom_scanner:fixed_version:` *`component_bom_ref`*	Menyediakan versi tetap dari komponen yang ditunjukkan untuk kerentanan yang diberikan.
`amazon:inspector:sbom_scanner:exploit_available`	Menunjukkan apakah eksploitasi tersedia untuk kerentanan yang diberikan.
`amazon:inspector:sbom_scanner:exploit_last_seen_in_public`	Menunjukkan kapan eksploitasi terakhir terlihat di depan umum untuk kerentanan yang diberikan.

Properti	Deskripsi
`amazon:inspector:sbom_scanner:cisa_kev_date_added`	Menunjukkan kapan kerentanan ditambahkan ke katalog CISA Known Exploited Vulnerabilities.
`amazon:inspector:sbom_scanner:cisa_kev_date_due`	Menunjukkan kapan perbaikan kerentanan jatuh tempo sesuai dengan katalog CISA Known Exploited Vulnerabilities.
`amazon:inspector:sbom_scanner:path`	Jalur ke file yang menghasilkan informasi paket subjek.

`amazon:inspector:sbom_generator`taksonomi namespace

`amazon:inspector:sbom_generator`Namespace digunakan oleh Amazon Inspector SBOM Generator. Ini memiliki sifat-sifat berikut:

Properti	Deskripsi
`amazon:inspector:sbom_generator:os_hostname`	Nama host dari sistem yang sedang diinventarisasi.
`amazon:inspector:sbom_generator:kernel_name`	Nama kernel dari sistem yang sedang diinventarisasi.
`amazon:inspector:sbom_generator:kernel_version`	Versi kernel dari sistem yang sedang diinventarisasi.
`amazon:inspector:sbom_generator:cpu_architecture`	Arsitektur CPU dari sistem yang sedang diinventarisasi, seperti x86_64.
`amazon:inspector:sbom_generator:image_id`	Hash dari file konfigurasi gambar kontainer, juga dikenal sebagai ID Gambar.
`amazon:inspector:sbom_generator:layer_diff_id`	Hash dari layer gambar kontainer yang tidak terkompresi.

Properti	Deskripsi
`amazon:inspector:sbom_generator:source_file_scanner`	Pemindai yang menemukan file yang berisi informasi paket, misalnya:`/var/lib/dpkg/status` .
`amazon:inspector:sbom_generator:source_package_collector`	Kolektor yang mengekstrak nama paket dan versi dari file tertentu.
`amazon:inspector:sbom_generator:source_path`	Jalur ke file tempat informasi paket subjek diekstraksi.
`amazon:inspector:sbom_generator:is_duplicate_package`	Menunjukkan bahwa paket subjek ditemukan oleh lebih dari satu pemindai file.
`amazon:inspector:sbom_generator:go_toolchain`	Menunjukkan versi Go compiler atau toolchain yang digunakan untuk menghasilkan Go executable.
`amazon:inspector:sbom_generator:expires_before`	tanggal sebelum sertifikat SSL valid.
`amazon:inspector:sbom_generator:expires_after`	tanggal setelah sertifikat SSL tidak valid.
`amazon:inspector:sbom_generator:is_expired`	nilai Boolean yang menunjukkan jika sertifikat SSL telah kedaluwarsa.

Pemindaian sumber daya otomatis dengan Amazon Inspector

Pemindaian tanpa agen Amazon Inspector untuk Amazon EC2 sedang dalam rilis pratinjau. Penggunaan Anda atas fitur pemindaian Amazon EC2 tanpa agen tunduk pada Bagian 2 dari AWS Ketentuan Layanan (“Beta dan Pratinjau”).

Amazon Inspector menggunakan mesin pemindaian yang dibuat khusus. Mesin ini memantau sumber daya Anda untuk kerentanan perangkat lunak atau jalur jaringan terbuka yang dapat mengakibatkan beban kerja yang terganggu, penggunaan sumber daya yang berbahaya, atau akses tidak sah ke data Anda. Ketika Amazon Inspector mendeteksi kerentanan, itu menciptakan temuan. Temuan mencakup detail yang terkait dengan deteksi untuk membantu Anda memulihkan kerentanan. Anda dapat meninjau temuan di konsol Amazon Inspector dan dengan menggunakan Amazon Inspector API. Untuk informasi selengkapnya, lihat Mengelola temuan di Amazon Inspector.

Saat diaktifkan, Amazon Inspector secara otomatis menemukan semua sumber daya yang memenuhi syarat dan memulai pemindaian berkelanjutan dari sumber daya tersebut. Amazon Inspector memindai kerentanan perangkat lunak dan paparan jaringan yang tidak diinginkan. Amazon Inspector juga menjalankan pemindaian sebagai respons terhadap peristiwa, seperti pemasangan aplikasi atau tambalan baru.

Saat Anda mengaktifkan Amazon Inspector untuk pertama kalinya, akun Anda secara otomatis terdaftar di semua jenis pemindaian. Topik berikut mencakup detail spesifik tentang jenis pemindaian yang disediakan Amazon Inspector. Amazon Inspector mengkategorikan jenis pemindaian berdasarkan jenis sumber daya yang dipengaruhi oleh kerentanan. Topik berikut mencakup sumber daya yang dipindai Amazon Inspector, apa yang memulai pemindaian baru untuk sumber daya tersebut, dan cara mengonfigurasi pemindaian untuk setiap jenis sumber daya.

Topik

- Menonaktifkan jenis pemindaian

Saat Anda mengaktifkan Amazon Inspector untuk pertama kalinya, akun Anda secara otomatis terdaftar dalam jenis pemindaian berikut: Pemindaian Amazon Amazon EC2, Pemindaian Amazon ECR, pemindaian standar Lambda. Pemindaian kode Lambda adalah lapisan opsional pemindaian fungsi Lambda yang dapat Anda aktifkan kapan saja.

Ikhtisar jenis pemindaian Amazon Inspector

Amazon Inspector menawarkan berbagai jenis pemindaian berbeda yang berfokus pada jenis sumber daya tertentu di lingkungan Anda AWS .

Pemindaian Amazon EC2

Saat Anda mengaktifkan pemindaian Amazon EC2, Amazon Inspector akan memindai instans Amazon EC2 Anda untuk mengetahui paket sistem operasi dan kerentanan paket bahasa pemrograman, serta jangkauan jaringan. Amazon Inspector memindai instans EC2 Anda untuk masalah Kerentanan dan Eksposur Umum (CVE) dan eksposur jaringan. Amazon Inspector melakukan pemindaian melalui penggunaan agen SSM yang diinstal pada instans Anda, atau melalui snapshot instans Amazon EBS. Untuk informasi selengkapnya tentang pemindaian Amazon EC2, lihat. Memindai instans Amazon EC2 dengan Amazon Inspector

Pemindaian ECR Amazon

Saat Anda mengaktifkan pemindaian Amazon ECR, Amazon Inspector mengonversi semua repositori kontainer pemindaian Dasar di registri pribadi Anda menjadi Pemindaian yang disempurnakan dengan pemindaian berkelanjutan. Anda juga dapat secara opsional mengonfigurasi pengaturan ini untuk memindai on-push saja atau untuk memindai repositori tertentu melalui aturan inklusi. Semua gambar yang didorong dalam 30 hari terakhir, atau ditarik dalam 90 hari terakhir pada awalnya dipindai. Amazon Inspector terus memantau gambar selama durasi 90 hari secara default, pengaturan ini dapat diubah kapan saja. Untuk informasi selengkapnya tentang pemindaian Amazon ECR, lihat. Memindai gambar wadah Amazon ECR dengan Amazon Inspector

Pemindaian standar Lambda

Saat Anda mengaktifkan pemindaian standar Lambda, Amazon Inspector menemukan fungsi Lambda di akun Anda dan segera mulai memindai mereka untuk kerentanan. Amazon Inspector memindai fungsi dan layer Lambda baru saat di-deploy, dan memindainya kembali saat diperbarui

atau saat Common Vulnerabilities and Exposures (CVE) baru diterbitkan. Untuk informasi selengkapnya tentang pemindaian fungsi Lambda, lihat. AWS Lambda Fungsi pemindaian dengan Amazon Inspector

Pemindaian standar Lambda+pemindaian kode Lambda

Opsi ini dapat menggabungkan pemindaian standar Lambda dengan pemindaian kode Lambda. Saat pemindaian kode Lambda diaktifkan, Amazon Inspector menemukan fungsi dan lapisan Lambda di akun Anda dan memindai kerentanan kode, dependensi paket aplikasi Anda. Pemindaian kode Lambda memindai kode aplikasi khusus di fungsi Lambda Anda untuk kerentanan kode. Kedua jenis pemindaian ini harus diaktifkan bersama. Untuk informasi selengkapnya, lihat Pemindaian kode Amazon Inspector Lambda.

Mengaktifkan jenis pemindaian

Anda dapat mengaktifkan jenis pemindaian Amazon Inspector baru kapan saja. Setelah Anda mengaktifkan jenis pemindaian, Amazon Inspector akan segera mulai memindai sumber daya yang memenuhi syarat untuk jenis pemindaian tersebut. Untuk ikhtisar jenis pemindaian yang tersedia, lihatIkhtisar jenis pemindaian Amazon Inspector. Berikut ini menjelaskan apa yang terjadi ketika Anda pertama kali mengaktifkan setiap jenis pemindaian:

- Pemindaian Amazon EC2 — Saat Anda mengaktifkan pemindaian Amazon Inspector Amazon EC2 untuk akun, Amazon Inspector memindai semua instans yang memenuhi syarat di akun Anda untuk mengetahui kerentanan paket dan masalah jangkauan jaringan. Plugin Amazon Inspector SSM diinstal pada semua host yang dikelola SSM Anda. Windows Untuk informasi selengkapnya, lihat WindowsContoh pemindaian. Selain itu, Amazon Inspector membuat asosiasi SSM berikut di akun Anda:
  - `InspectorDistributor-do-not-delete`
  - `InspectorInventoryCollection-do-not-delete`
  - `InspectorLinuxDistributor-do-not-delete`
  - `InvokeInspectorLinuxSsmPlugin-do-not-delete`
  - `InvokeInspectorSsmPlugin-do-not-delete`.
- Pemindaian Amazon ECR - Saat Anda mengaktifkan pemindaian gambar kontainer Amazon ECR untuk sebuah akun, jenis pemindaian Amazon ECR untuk repositori pribadi di akun tersebut berubah dari Pemindaian Dasar dengan Amazon ECR menjadi Pemindaian yang Ditingkatkan dengan Amazon Inspector. Kemudian semua gambar kontainer Amazon ECR yang memenuhi

syarat didorong dalam 30 hari terakhir, atau ditarik dalam 90 hari terakhir, dipindai untuk kerentanan paket. Selain itu, durasi pemindaian ulang Amazon ECR Anda diatur ke 90 hari untuk tanggal push dan pull image.

- Pemindaian standar Lambda - Saat Anda mengaktifkan pemindaian standar Lambda di akun, semua fungsi Lambda di akun Anda yang dipanggil atau diperbarui dalam 90 hari terakhir dipindai untuk mengetahui kerentanan paket. Selain itu, saluran terkait CloudTrail layanan dibuat di akun Anda.
- Pemindaian standar Lambda+Pemindaian kode Lambda - Jenis pemindaian fungsi Lambda ini diaktifkan bersama. Saat Anda mengaktifkan pemindaian kode Lambda di akun, semua fungsi Lambda di akun Anda yang dipanggil atau diperbarui dalam 90 hari terakhir dipindai untuk mencari kerentanan kode.

Mengaktifkan pemindaian

Jika Anda adalah administrator yang didelegasikan untuk Amazon Inspector di AWS organisasi, Anda dapat mengaktifkan berbagai jenis pemindaian Amazon Inspector untuk beberapa akun di beberapa Wilayah secara otomatis menggunakan skrip shell yang dikembangkan oleh Amazon Inspector inspector2- on. enablement-with-cli GitHub Jika tidak, untuk menyelesaikan prosedur ini untuk lingkungan multi-akun melalui konsol, selesaikan langkah-langkah berikut saat masuk sebagai administrator yang didelegasikan Amazon Inspector.

Console

Untuk mengaktifkan pemindaian

1. Buka konsol Amazon Inspector di https://console.aws.amazon.com/inspector/v2/home.
2. Menggunakan Wilayah AWS pemilih di sudut kanan atas halaman, pilih Wilayah tempat Anda ingin mengaktifkan jenis pemindaian baru.
3. Di panel navigasi, pilih Manajemen akun.
4. Pada halaman Manajemen akun, pilih akun yang ingin Anda aktifkan jenis pemindaian.
5. Pilih Aktifkan dan pilih jenis pemindaian yang ingin Anda aktifkan.
6. (Disarankan) Ulangi langkah-langkah ini di masing-masing Wilayah AWS yang ingin Anda aktifkan jenis pemindaian itu.

API

Jalankan operasi Aktifkan API. Dalam permintaan, berikan ID akun yang Anda aktifkan pemindaian, dan token idempotensi, dan satu atau lebih dari,`EC2`, `ECR`LAMBDA, atau `LAMBDA_CODE` `resourceTypes` untuk mengaktifkan pemindaian jenis itu.

Memindai instans Amazon EC2 dengan Amazon Inspector

Pemindaian tanpa agen Amazon Inspector untuk Amazon EC2 sedang dalam rilis pratinjau. Penggunaan Anda atas fitur pemindaian Amazon EC2 tanpa agen tunduk pada Bagian 2 dari AWS Ketentuan Layanan (“Beta dan Pratinjau”).

Pemindaian Amazon Inspector EC2 mengekstrak metadata dari instans EC2 Anda, kemudian, membandingkan metadata ini dengan aturan yang dikumpulkan dari penasihat keamanan untuk menghasilkan temuan. Amazon Inspector memindai instans untuk kerentanan paket dan masalah jangkauan jaringan. Untuk informasi tentang jenis temuan yang dihasilkan untuk masalah ini, lihatMenemukan tipe di Amazon Inspector.

Amazon Inspector melakukan pemindaian jangkauan jaringan setiap 24 jam sekali, sementara pemindaian kerentanan paket dilakukan pada irama variabel tergantung pada metode pemindaian yang terkait dengan instance.

Metode pemindaian

Package vulnerability scan dapat dilakukan dengan menggunakan metode pemindaian berbasis agen atau agentless. Metode pemindaian ini menentukan bagaimana dan kapan Amazon Inspector mengumpulkan inventaris perangkat lunak dari instans EC2 untuk pemindaian kerentanan paket. Metode berbasis agen bergantung pada agen SSM untuk mengumpulkan inventaris perangkat lunak, sedangkan metode tanpa agen menggunakan snapshot Amazon EBS alih-alih agen.

Metode pemindaian yang digunakan oleh Amazon Inspector bergantung pada setelan mode pemindaian akun Anda, Untuk informasi selengkapnya lihat,. Mengelola mode pemindaian

Untuk mengaktifkan pemindaian Amazon EC2, lihat. Mengaktifkan jenis pemindaian

Pemindaian berbasis agen

Pemindaian berbasis agen dilakukan terus menerus menggunakan agen SSM pada semua instance yang memenuhi syarat. Untuk pemindaian berbasis agen, Amazon Inspector menggunakan asosiasi SSM, dan plugin yang diinstal melalui asosiasi ini, untuk mengumpulkan inventaris perangkat lunak dari instans Anda. Selain pemindaian kerentanan paket untuk paket sistem operasi, pemindaian berbasis agen Amazon Inspector juga dapat mendeteksi kerentanan paket untuk paket bahasa pemrograman aplikasi dalam instance berbasis Linux. Inspeksi mendalam Amazon Inspector untuk instans Amazon EC2 Linux

Proses berikut menjelaskan bagaimana Amazon Inspector menggunakan SSM untuk mengumpulkan inventaris dan melakukan pemindaian berbasis agen:

1. Amazon Inspector membuat asosiasi SSM di akun Anda untuk mengumpulkan inventaris dari instans Anda. Untuk beberapa jenis Instance (Windows, dan Linux), asosiasi ini menginstal plugin pada instance individual untuk mengumpulkan inventaris.
2. Menggunakan SSM, Amazon Inspector mengekstrak inventaris paket dari sebuah instance.
3. Amazon Inspector mengevaluasi inventaris yang diekstraksi dan menghasilkan temuan untuk setiap kerentanan yang terdeteksi.

Contoh yang memenuhi syarat

Amazon Inspector akan menggunakan metode berbasis agen untuk memindai instance jika memenuhi ketentuan berikut:

- Instans memiliki OS yang didukung. Untuk daftar OS yang didukung, lihat kolom dukungan pemindaian berbasis agen. the section called “Sistem operasi yang didukung untuk pemindaian Amazon EC2”
- Instans tidak dikecualikan dari pemindaian oleh tag pengecualian Amazon Inspector EC2.
- Instans ini dikelola SSM. Untuk petunjuk tentang memverifikasi dan mengonfigurasi agen, lihatMengkonfigurasi Agen SSM.

Perilaku pemindaian berbasis agen

Saat menggunakan metode pemindaian berbasis agen, Amazon Inspector memulai pemindaian kerentanan baru instans EC2 dalam situasi berikut:

- Saat Anda meluncurkan instans EC2 baru.
- Ketika Anda menginstal perangkat lunak baru pada instans EC2 yang ada (Linux dan Mac).
- Saat Amazon Inspector menambahkan item common vulnerabilities and exposure (CVE) baru ke database-nya, dan CVE tersebut relevan dengan instans EC2 Anda (Linux dan Mac).

Amazon Inspector memperbarui bidang yang dipindai terakhir untuk instans EC2 saat pemindaian awal selesai. Setelah ini, bidang Last scanned diperbarui saat Amazon Inspector mengevaluasi inventaris SSM (setiap 30 menit secara default), atau saat instance dipindai ulang karena CVE baru yang memengaruhi instance tersebut ditambahkan ke database Amazon Inspector.

Anda dapat memeriksa kapan instans EC2 terakhir dipindai untuk mencari kerentanan dari tab Instans di halaman Manajemen akun, atau dengan menggunakan perintah. ListCoverage

Mengkonfigurasi Agen SSM

Agar Amazon Inspector mendeteksi kerentanan perangkat lunak untuk instans Amazon EC2 menggunakan metode pemindaian berbasis agen, instans harus berupa instans terkelola di Amazon EC2 Systems Manager (SSM). Instans terkelola SSM memiliki Agen SSM yang diinstal dan dijalankan, dan SSM memiliki izin untuk mengelola instance. Jika Anda sudah menggunakan SSM untuk mengelola instans Anda, tidak ada langkah lain yang diperlukan untuk pemindaian berbasis agen.

Agen SSM diinstal secara default pada instans EC2 yang dibuat dari beberapa Amazon Machine Images (AMI). Untuk informasi selengkapnya, lihat Tentang Agen SSM di Panduan AWS Systems Manager Pengguna. Namun, meskipun sudah diinstal, Anda mungkin perlu mengaktifkan Agen SSM secara manual, dan memberikan izin SSM untuk mengelola instans Anda.

Prosedur berikut menjelaskan cara mengonfigurasi instans Amazon EC2 sebagai instans terkelola menggunakan profil instans IAM. Prosedur ini juga menyediakan tautan ke informasi yang lebih rinci di Panduan AWS Systems Manager Pengguna.

AmazonSSMManagedInstanceCoreadalah kebijakan yang disarankan untuk digunakan saat Anda melampirkan profil instance. Kebijakan ini memiliki semua izin yang diperlukan untuk pemindaian Amazon Inspector EC2.

> **Note**
>
> Anda juga dapat mengotomatiskan manajemen SSM dari semua instans EC2 Anda, tanpa menggunakan profil instans IAM menggunakan Konfigurasi Manajemen Host Default SSM. Untuk informasi selengkapnya, lihat Konfigurasi Manajemen Host Default.

Untuk mengonfigurasi SSM untuk instans Amazon EC2

1. Jika belum diinstal oleh vendor sistem operasi Anda, instal Agen SSM. Untuk informasi lebih lanjut, lihat Bekerja dengan SSM Agent.
2. Gunakan AWS CLI untuk memverifikasi bahwa Agen SSM sedang berjalan. Untuk informasi selengkapnya, lihat Memeriksa status SSM Agent dan memulai agen.
3. Berikan izin kepada SSM untuk mengelola instans Anda. Anda dapat memberikan izin dengan membuat profil instans IAM dan melampirkannya ke instans Anda. Sebaiknya gunakan kebijakan ini, karena AmazonSSMManagedInstanceCorekebijakan ini memiliki izin untuk Distributor SSM, Inventaris SSM, dan manajer SSM State, yang dibutuhkan Amazon Inspector untuk pemindaian. Untuk petunjuk cara membuat profil instans dengan izin ini dan melampirkannya sebagai instance, lihat Mengonfigurasi izin instans untuk Systems Manager Systems Manager.
4. (Opsional) Aktifkan pembaruan otomatis untuk Agen SSM. Untuk informasi selengkapnya, lihat Mengotomatiskan pembaruan ke Agen SSM.
5. (Opsional) Konfigurasikan Systems Manager untuk menggunakan titik akhir Amazon Virtual Private Cloud (Amazon VPC). Untuk informasi selengkapnya, lihat Membuat titik akhir VPC Amazon.

> **Important**
>
> Amazon Inspector memerlukan asosiasi Manajer Negara Systems Manager di akun Anda untuk mengumpulkan inventaris aplikasi perangkat lunak. Amazon Inspector secara otomatis membuat asosiasi yang disebut `InspectorInventoryCollection-do-not-delete` jika belum ada.
>
> Amazon Inspector juga memerlukan sinkronisasi data sumber daya dan secara otomatis membuat yang dipanggil `InspectorResourceDataSync-do-not-delete` jika belum ada. Untuk informasi selengkapnya, lihat Mengonfigurasi sinkronisasi data sumber daya untuk Inventaris di Panduan AWS Systems Manager Pengguna. Setiap akun dapat memiliki sejumlah sinkronisasi data sumber daya per Wilayah. Untuk informasi selengkapnya, lihat

Jumlah maksimum sinkronisasi data sumber daya (per Akun AWS per Wilayah) di titik akhir dan kuota SSM. Jika Anda telah mencapai maksimum ini, Anda harus menghapus sinkronisasi data sumber daya, lihat Mengelola sinkronisasi data sumber daya.

Sumber daya SSM dibuat untuk pemindaian

Amazon Inspector memerlukan sejumlah sumber daya SSM di akun Anda untuk menjalankan pemindaian Amazon EC2. Sumber daya berikut dibuat saat Anda pertama kali mengaktifkan pemindaian Amazon Inspector EC2:

> **Note**
>
> Jika salah satu sumber daya SSM ini dihapus saat pemindaian Amazon Inspector Amazon EC2 diaktifkan untuk akun Anda, Amazon Inspector akan mencoba membuatnya kembali pada interval pemindaian berikutnya.

`InspectorInventoryCollection-do-not-delete`

Ini adalah asosiasi Systems Manager State Manager (SSM) yang digunakan Amazon Inspector untuk mengumpulkan inventaris aplikasi perangkat lunak dari instans Amazon EC2 Anda. Jika akun Anda sudah memiliki asosiasi SSM untuk mengumpulkan inventaris`InstanceIds*`, Amazon Inspector akan menggunakannya alih-alih membuatnya sendiri.

`InspectorResourceDataSync-do-not-delete`

Ini adalah sinkronisasi data sumber daya yang digunakan Amazon Inspector untuk mengirim data inventaris yang dikumpulkan dari instans Amazon EC2 Anda ke bucket Amazon S3 yang dimiliki oleh Amazon Inspector. Untuk informasi selengkapnya, lihat Mengonfigurasi sinkronisasi data sumber daya untuk Inventaris di Panduan AWS Systems Manager Pengguna.

`InspectorDistributor-do-not-delete`

Ini adalah asosiasi SSM yang digunakan Amazon Inspector untuk memindai instance Windows. Asosiasi ini menginstal plugin Amazon Inspector SSM pada instans Windows Anda. Jika file plugin dihapus secara tidak sengaja, asosiasi ini akan menginstalnya kembali pada interval asosiasi berikutnya.

`InvokeInspectorSsmPlugin-do-not-delete`

Ini adalah asosiasi SSM yang digunakan Amazon Inspector untuk memindai instance Windows. Asosiasi ini memungkinkan Amazon Inspector untuk memulai pemindaian menggunakan plugin, Anda juga dapat menggunakannya untuk mengatur interval khusus untuk pemindaian instance Windows. Untuk informasi selengkapnya, lihat Mengatur jadwal khusus untuk pemindaian Windows misalnya.

`InspectorLinuxDistributor-do-not-delete`

Ini adalah asosiasi SSM yang digunakan Amazon Inspector untuk inspeksi mendalam Amazon EC2 Linux. Asosiasi ini menginstal plugin Amazon Inspector SSM pada instans Linux Anda.

`InvokeInspectorLinuxSsmPlugin-do-not-delete`

Ini adalah asosiasi SSM yang digunakan Amazon Inspector untuk inspeksi mendalam Amazon EC2 Linux. Asosiasi ini memungkinkan Amazon Inspector untuk memulai pemindaian menggunakan plugin.

> **Note**
>
> Saat Anda menonaktifkan pemindaian Amazon Inspector Amazon EC2 atau inspeksi mendalam, semua sumber daya SSM akan dihapus secara otomatis dari host Linux yang sesuai.

Pemindaian tanpa agen

Amazon Inspector menggunakan metode pemindaian tanpa agen pada instans yang memenuhi syarat saat akun Anda dalam mode pemindaian hibrida (yang mencakup pemindaian berbasis agen dan tanpa agen). Untuk pemindaian tanpa agen, Amazon Inspector menggunakan snapshot EBS untuk mengumpulkan inventaris perangkat lunak dari instans Anda. Instans yang dipindai menggunakan metode tanpa agen dipindai untuk paket sistem operasi, dan kerentanan paket bahasa pemrograman aplikasi.

> **Note**
>
> Saat memindai instance Linux untuk kerentanan paket bahasa pemrograman aplikasi, metode tanpa agen memindai semua jalur yang tersedia, sedangkan pemindaian berbasis agen hanya memindai jalur default dan jalur tambahan yang Anda tentukan sebagai bagian

darinya. Inspeksi mendalam Amazon Inspector untuk instans Amazon EC2 Linux Hal ini dapat mengakibatkan contoh yang sama memiliki temuan yang berbeda tergantung pada apakah itu dipindai menggunakan metode berbasis agen atau metode tanpa agen.

Proses berikut menjelaskan bagaimana Amazon Inspector menggunakan snapshot EBS untuk mengumpulkan inventaris dan melakukan pemindaian tanpa agen:

1. Amazon Inspector membuat snapshot EBS dari semua volume yang dilampirkan ke instance. Saat Amazon Inspector menggunakannya, snapshot disimpan di akun Anda dan ditandai `InspectorScan` sebagai kunci tag, dan ID pemindaian unik sebagai nilai tag.
2. Amazon Inspector mengambil data dari snapshot menggunakan API langsung EBS dan mengevaluasi kerentanannya. Temuan dihasilkan untuk setiap kerentanan yang terdeteksi.
3. Amazon Inspector menghapus snapshot EBS yang dibuatnya di akun Anda.

Contoh yang memenuhi syarat

Amazon Inspector akan menggunakan metode agentless untuk memindai instance jika memenuhi ketentuan berikut:

- Instans memiliki OS yang didukung. Untuk daftar OS yang didukung, lihat kolom dukungan pemindaian berbasis agen. the section called “Sistem operasi yang didukung untuk pemindaian Amazon EC2”
- Instans tidak dikecualikan dari pemindaian oleh tag pengecualian Amazon Inspector EC2.
- Instance memiliki status`Unmanaged EC2 instance`,`Stale inventory`, atau`No inventory`.
- Instans ini didukung EBS dan memiliki salah satu format sistem file berikut:
  - `ext3`
  - `ext4`
  - `xfs`

Perilaku pemindaian tanpa agen

Saat akun Anda dikonfigurasi untuk pemindaian Hybrid, Amazon Inspector melakukan pemindaian tanpa agen pada instans yang memenuhi syarat setiap 24 jam. Amazon Inspector mendeteksi dan memindai instans baru yang memenuhi syarat setiap jam, yang mencakup instans baru tanpa

agen SSM, atau instans yang sudah ada sebelumnya dengan status yang telah berubah menjadi. `SSM_UNMANAGED`

Amazon Inspector memperbarui bidang yang dipindai Terakhir untuk instans Amazon EC2 setiap kali memindai snapshot yang diekstraksi dari instance setelah pemindaian tanpa agen.

Anda dapat memeriksa kapan instans EC2 terakhir dipindai untuk mencari kerentanan dari tab Instans di halaman Manajemen akun, atau dengan menggunakan perintah. ListCoverage

Mengelola mode pemindaian

Mode pemindaian EC2 Anda menentukan metode pemindaian yang akan digunakan Amazon Inspector saat melakukan pemindaian EC2 di akun Anda. Anda dapat melihat mode pemindaian untuk akun Anda dari halaman pengaturan pemindaian EC2 di bawah Pengaturan umum. Akun mandiri atau administrator yang didelegasikan Amazon Inspector dapat mengubah mode pemindaian. Saat Anda menyetel mode pemindaian sebagai administrator yang didelegasikan Amazon Inspector, mode pemindaian disetel untuk semua akun anggota di organisasi Anda. Amazon Inspector memiliki mode pemindaian berikut:

Pemindaian berbasis agen — Dalam mode pemindaian ini, Amazon Inspector akan secara eksklusif menggunakan metode pemindaian berbasis agen saat memindai kerentanan paket. Mode pemindaian ini hanya memindai instans terkelola SSM di akun Anda, tetapi memiliki manfaat menyediakan pemindaian berkelanjutan sebagai respons terhadap CVE baru atau perubahan pada instans. Pemindaian berbasis agen juga menyediakan Inspeksi mendalam Amazon Inspector untuk instans yang memenuhi syarat. Ini adalah mode pemindaian default untuk akun yang baru diaktifkan.

Pemindaian hibrida — Dalam mode pemindaian ini, Amazon Inspector menggunakan kombinasi metode berbasis agen dan tanpa agen untuk memindai kerentanan paket. Untuk instans EC2 yang memenuhi syarat yang memiliki agen SSM diinstal dan dikonfigurasi, Amazon Inspector menggunakan metode berbasis agen. Untuk instans yang memenuhi syarat yang tidak dikelola SSM, Amazon Inspector akan menggunakan metode tanpa agen untuk instans yang didukung EBS yang memenuhi syarat.

Untuk mengubah mode pemindaian

1. Buka konsol Amazon Inspector di https://console.aws.amazon.com/inspector/v2/home.
2. Menggunakan Wilayah AWS pemilih di sudut kanan atas halaman, pilih Wilayah tempat Anda ingin mengubah mode pemindaian EC2 Anda.
3. Dari panel navigasi samping, di bawah Pengaturan umum, pilih pengaturan pemindaian EC2.

4. Di bawah Mode Pindai, pilih Edit.
5. Pilih mode pemindaian dan kemudian pilih Simpan perubahan.

Mengecualikan instance dari pemindaian Amazon Inspector

Anda dapat menandai instance tertentu untuk mengecualikannya dari pemindaian Amazon Inspector. Mengecualikan instance dari pemindaian dapat membantu mencegah peringatan yang tidak dapat ditindaklanjuti. Anda tidak dikenakan biaya untuk instans yang dikecualikan.

Untuk mengecualikan instans EC2 dari pemindaian, beri tag instance tersebut dengan kunci berikut:

- `InspectorEc2Exclusion`

Nilai adalah opsional.

Untuk informasi selengkapnya tentang menambahkan tag, lihat Menandai sumber daya Amazon EC2 Anda.

Selain itu, Anda dapat mengecualikan volume EBS terenkripsi dari pemindaian tanpa agen dengan menandai AWS KMS kunci yang digunakan untuk mengenkripsi volume tersebut dengan tag. `InspectorEc2Exclusion` Untuk informasi selengkapnya, lihat Menandai kunci

Sistem operasi yang didukung

Amazon Inspector memindai instans Mac, Windows, dan Linux EC2 yang didukung untuk kerentanan dalam paket sistem operasi. Untuk instance Linux, Amazon Inspector dapat menghasilkan temuan untuk paket bahasa pemrograman aplikasi yang digunakan. Inspeksi mendalam Amazon Inspector untuk instans Amazon EC2 Linux Untuk instance Mac dan Windows hanya paket sistem operasi yang dipindai.

Untuk informasi tentang sistem operasi yang didukung, termasuk sistem operasi mana yang dapat dipindai tanpa agen SSM, lihat. Sistem operasi yang didukung untuk pemindaian Amazon EC2

Inspeksi mendalam Amazon Inspector untuk instans Amazon EC2 Linux

Amazon Inspector memperluas cakupan pemindaian Amazon EC2 untuk menyertakan inspeksi mendalam. Dengan pemeriksaan mendalam, Amazon Inspector mendeteksi kerentanan paket untuk paket bahasa pemrograman aplikasi dalam instans Amazon EC2 berbasis Linux Anda.

Amazon Inspector memindai jalur default untuk pustaka paket bahasa pemrograman. Anda juga dapat mengonfigurasi jalur khusus selain jalur default. Untuk informasi selengkapnya, lihat Jalur khusus untuk inspeksi mendalam Amazon Inspector.

Amazon Inspector melakukan pemindaian inspeksi mendalam menggunakan data yang dikumpulkan dengan plugin Amazon Inspector SSM. Untuk mengelola plugin dan melakukan inspeksi mendalam untuk Linux, Amazon Inspector secara otomatis membuat asosiasi SSM berikut `InvokeInspectorLinuxSsmPlugin-do-not-delete` di akun Anda. Ini terjadi ketika Amazon Inspector mengaktifkan inspeksi mendalam.

Amazon Inspector mengumpulkan inventaris aplikasi yang diperbarui dari instans untuk pemeriksaan mendalam setiap 6 jam.

Untuk daftar bahasa pemrograman yang didukung Amazon Inspector untuk inspeksi mendalam, lihat. Bahasa pemrograman yang didukung: Inspeksi mendalam Amazon EC2

> **Note**
>
> Inspeksi mendalam tidak didukung untuk instance Windows atau Mac.

Mengaktifkan atau menonaktifkan inspeksi mendalam

> **Note**
>
> Inspeksi mendalam diaktifkan secara otomatis sebagai bagian dari pemindaian Amazon EC2 untuk akun yang mengaktifkan Amazon Inspector setelah 17 April 2023.

Anda dapat memeriksa untuk melihat apakah inspeksi mendalam aktif untuk akun di konsol Amazon Inspector dari kolom pemindaian Amazon EC2 di halaman Manajemen akun. Jika inspeksi mendalam tidak aktif, kolom ini akan mengatakan Diaktifkan (inspeksi mendalam dinonaktifkan). Untuk memeriksa status aktivasi secara terprogram, gunakan API. GetEc2DeepInspectionConfiguration Atau, untuk beberapa akun, gunakan BatchGetMemberEc2DeepInspectionStatusAPI.

Jika Anda mengaktifkan Amazon Inspector sebelum 17 April 2023, Anda dapat mengaktifkan inspeksi mendalam melalui spanduk konsol atau API. UpdateEc2DeepInspectionConfiguration Jika Anda adalah administrator yang didelegasikan untuk organisasi di Amazon Inspector, Anda dapat

menggunakan BatchUpdateMemberEc2DeepInspectionStatusAPI untuk mengaktifkannya untuk diri sendiri dan akun anggota Anda.

Anda dapat menonaktifkan inspeksi mendalam melalui UpdateEc2DeepInspectionConfigurationAPI. Akun anggota di organisasi tidak dapat menonaktifkan inspeksi mendalam. Sebagai gantinya, akun anggota harus dinonaktifkan oleh administrator yang didelegasikan menggunakan API. BatchUpdateMemberEc2DeepInspectionStatus

Tentang plugin Amazon Inspector SSM untuk Linux

Amazon Inspector menggunakan plugin Amazon Inspector SSM untuk melakukan inspeksi mendalam terhadap instans Linux Anda. Plugin Amazon Inspector SSM secara otomatis diinstal pada instance Linux Anda di direktori berikut:. `/opt/aws/inspector/bin` Nama executable adalah. `inspectorssmplugin`

> **Note**
>
> Amazon Inspector menggunakan Systems Manager Distributor untuk menyebarkan plugin di instans Amazon EC2 Anda. Systems Manager Distributor mendukung sistem operasi yang terdaftar sebagai platform dan arsitektur paket yang didukung dalam panduan Systems Manager. Sistem operasi instans Amazon EC2 Anda harus didukung oleh Systems Manager Distributor dan Amazon Inspector untuk Amazon Inspector untuk melakukan pemindaian inspeksi mendalam.

Amazon Inspector membuat direktori file berikut untuk mengelola data yang dikumpulkan untuk pemeriksaan mendalam oleh plugin Amazon Inspector SSM:

- `/opt/aws/inspector/var/input`
- `/opt/aws/inspector/var/output`
  - `packages.txt`Di direktori ini menyimpan jalur lengkap ke paket yang ditemukan oleh inspeksi mendalam. Jika Amazon Inspector mendeteksi paket yang sama beberapa kali pada instance Anda, file ini mencantumkan setiap lokasi paket yang ditemukan.

Amazon Inspector menyimpan log untuk plugin di direktori. `/var/log/amazon/inspector`

Menghapus instalasi plugin Amazon Inspector SSM

Jika `inspectorssmplugin` file dihapus secara tidak sengaja, asosiasi `InspectorLinuxDistributor-do-not-delete` SSM akan mencoba menginstal ulang plugin pada interval pemindaian berikutnya.

Jika Anda menonaktifkan pemindaian Amazon EC2, plugin akan dihapus secara otomatis dari semua host Linux.

Jalur khusus untuk inspeksi mendalam Amazon Inspector

Anda dapat mengonfigurasi jalur kustom untuk Amazon Inspector untuk mencari saat melakukan inspeksi mendalam terhadap instans Amazon EC2 Linux Anda. Saat Anda menambahkan jalur kustom Amazon Inspector memindai paket di direktori itu dan semua sub-direktori di dalamnya.

Semua akun dapat menentukan hingga 5 jalur khusus untuk akun masing-masing. Jika Anda adalah administrator yang didelegasikan untuk organisasi Anda, Anda dapat menentukan 5 jalur tambahan yang akan diterapkan di seluruh organisasi Anda. Jumlah ini mencapai total hingga 10 jalur kustom yang dipindai per akun di organisasi.

Amazon Inspector memindai semua jalur kustom selain jalur default berikut yang dipindai untuk semua akun:

- `/usr/lib`
- `/usr/lib64`
- `/usr/local/lib`
- `/usr/local/lib64`

> **Note**
>
> Jalur khusus harus berupa jalur lokal. Amazon Inspector tidak memindai jalur jaringan yang dipetakan seperti mount Network File System (NFS) atau mount sistem file Amazon S3.

Memformat untuk jalur kustom

Berikut ini adalah contoh format untuk jalur kustom: `/home/usr1/project01`

Jalur kustom Anda tidak boleh lebih dari 256 karakter.

Ada batas paket 5.000 per instance dan batas waktu pengumpulan persediaan paket maksimum 15 menit. Kami menyarankan Anda mencoba memilih jalur khusus untuk membantu Anda menghindari batasan ini.

Tetapkan jalur kustom di konsol

Console

Masuk sebagai administrator yang didelegasikan Amazon Inspector dan ikuti langkah-langkah berikut untuk menambahkan jalur khusus untuk organisasi Anda.

1. Buka konsol Amazon Inspector di https://console.aws.amazon.com/inspector/v2/home.
2. Menggunakan Wilayah AWS pemilih di sudut kanan atas halaman, pilih Wilayah tempat Anda ingin mengaktifkan pemindaian standar Lambda.
3. Dari panel navigasi samping, di bawah Pengaturan umum, pilih pengaturan pemindaian EC2.
4. Di bawah Jalur khusus untuk akun Anda sendiri, pilih Edit untuk menambahkan jalur untuk akun individual Anda. Jika Anda administrator yang didelegasikan, Anda dapat memilih Edit di jalur kustom untuk panel organisasi Anda untuk menambahkan jalur kustom untuk semua akun dalam organisasi.
5. Masukkan jalur kustom Anda di kotak teks.
6. Pilih Simpan untuk menyimpan jalur kustom Anda. Amazon Inspector akan memasukkan jalur ini dalam inspeksi mendalam berikutnya.

API

Jalankan perintah UpdateEc2DeepInspectionConfiguration. Untuk `packagePaths` menentukan array jalur untuk memindai.

Bahasa pemrograman yang didukung

Untuk instance Linux, inspeksi mendalam Amazon Inspector dapat menghasilkan temuan untuk paket bahasa pemrograman aplikasi selain kerentanan dalam paket sistem operasi. Untuk instance Mac dan Windows hanya paket sistem operasi yang dipindai.

Untuk informasi tentang bahasa pemrograman yang didukung, lihatBahasa pemrograman yang didukung untuk inspeksi mendalam Amazon Inspector.

Memindai instans Windows EC2 dengan Amazon Inspector

> **Note**
>
> Pada 31 Agustus 2022, Amazon Inspector memperluas cakupan pemindaian Amazon EC2 untuk menyertakan instans EC2 yang berjalan. Windows

Amazon Inspector secara otomatis menemukan semua Windows instans yang didukung dan menyertakannya dalam pemindaian berkelanjutan tanpa tindakan tambahan apa pun. Untuk informasi tentang instance mana yang didukung, lihatSistem operasi yang didukung untuk pemindaian Amazon EC2.

Tidak seperti pemindaian untuk instance berbasis Linux, Amazon Inspector Windows menjalankan pemindaian secara berkala. WindowsContoh awalnya dipindai pada penemuan dan kemudian dipindai setiap 6 jam. Namun, interval pemindaian 6 jam default dapat disesuaikan. Untuk informasi selengkapnya, lihat Mengatur jadwal khusus untuk pemindaian Windows misalnya. Berikut ini adalah ikhtisar bagaimana Amazon Inspector memindai Windows instance:

1. Saat pemindaian Amazon EC2 diaktifkan, Amazon Inspector membuat asosiasi SSM baru untuk sumber daya Windows `InspectorDistributor-do-not-delete` Anda:,, dan. `InspectorInventoryCollection-do-not-delete` `InvokeInspectorSsmPlugin-do-not-delete`
2. Asosiasi `InspectorDistributor-do-not-delete` SSM menggunakan dokumen `AWS-ConfigureAWSPackage` SSM dan paket Distributor `AmazonInspector2-InspectorSsmPlugin` SSM untuk menginstal plugin Amazon Inspector SSM pada instans Anda. Windows Untuk informasi selengkapnya, lihat Tentang plugin Amazon Inspector SSM untuk Windows.
3. Asosiasi `InvokeInspectorSsmPlugin-do-not-delete` SSM menjalankan plugin Amazon Inspector SSM secara berkala untuk mengumpulkan data instans dan menghasilkan temuan Amazon Inspector. Secara default, intervalnya setiap 6 jam. Namun, Anda dapat menyesuaikan ini dengan menyetel ekspresi cron atau ekspresi tingkat untuk asosiasi menggunakan SSM. Untuk informasi selengkapnya, lihat Referensi: Cron dan ekspresi tingkat untuk Systems Manager di Panduan AWS Systems Manager Pengguna.

> **Note**
>
> Amazon Inspector akan memperbarui file definisi Open Vulnerability and Assessment Language (OVAL) ke bucket S3. `inspector2-oval-prod-`*`REGION`* Bucket S3 ini berisi definisi OVAL yang digunakan dalam pemindaian dan tidak boleh dimodifikasi. Mengubah setelan ini akan mencegah Amazon Inspector memindai CVE baru saat dirilis.

Persyaratan pemindaian Amazon Inspector untuk instans Windows

Untuk memindai Windows instance, Amazon Inspector mengharuskan instans memenuhi kriteria berikut:

- Instans ini adalah instance terkelola SSM. Untuk petunjuk tentang pengaturan instans Anda untuk pemindaian, lihatMengkonfigurasi Agen SSM.
- Sistem operasi instance adalah salah satu sistem Windows operasi yang didukung. Untuk daftar lengkap sistem operasi yang didukung, lihatSistem operasi yang didukung untuk pemindaian Amazon EC2.
- Instans memiliki plugin Amazon Inspector SSM diinstal. Amazon Inspector secara otomatis menginstal plugin Amazon Inspector SSM untuk instans terkelola setelah penemuan. Lihat topik berikutnya untuk detail tentang plugin.

> **Note**
>
> Jika host Anda berjalan di VPC Amazon tanpa akses internet keluar, Windows pemindaian mengharuskan host Anda untuk dapat mengakses titik akhir Amazon S3 Regional. Untuk mempelajari cara mengonfigurasi titik akhir Amazon S3 Amazon VPC, lihat Membuat titik akhir gateway di Panduan Pengguna Amazon Virtual Private Cloud. Jika kebijakan endpoint Amazon VPC membatasi akses ke bucket S3 eksternal, Anda harus secara khusus mengizinkan akses ke bucket yang dikelola oleh Amazon Inspector yang menyimpan definisi OVAL Wilayah AWS yang digunakan untuk mengevaluasi instans Anda. Bucket ini memiliki format sebagai berikut:`inspector2-oval-prod-`*`REGION`*.

Tentang plugin Amazon Inspector SSM untuk Windows

Plugin Amazon Inspector SSM diperlukan untuk Amazon Inspector untuk memindai instans Anda. Windows Plugin Amazon Inspector SSM diinstal secara otomatis pada Windows instance Anda`C:\Program Files\Amazon\Inspector`, dan file biner yang dapat dieksekusi diberi nama. `InspectorSsmPlugin.exe`

Lokasi file berikut dibuat untuk menyimpan data yang dikumpulkan oleh plugin Amazon Inspector SSM:

- `C:\ProgramData\Amazon\Inspector\Input`
- `C:\ProgramData\Amazon\Inspector\Output`
- `C:\ProgramData\Amazon\Inspector\Logs`

> **Note**
>
> Secara default, plugin Amazon Inspector SSM berjalan di bawah prioritas normal.

Menghapus instalasi plugin Amazon Inspector SSM

Jika `InspectorSsmPlugin.exe` file dihapus secara tidak sengaja, asosiasi `InspectorDistributor-do-not-delete` SSM akan menginstal ulang plugin pada interval pemindaian berikutnya. Windows Jika Anda ingin menghapus plugin Amazon Inspector SSM, Anda dapat menggunakan tindakan Uninstall pada dokumen. `AmazonInspector2-ConfigureInspectorSsmPlugin`

Selain itu, plugin Amazon Inspector SSM akan dihapus secara otomatis dari semua Windows host jika Anda menonaktifkan pemindaian Amazon EC2.

> **Note**
>
> Jika Anda menghapus instalan Agen SSM sebelum menonaktifkan Amazon Inspector, plugin Amazon Inspector SSM akan tetap berada Windows di host tetapi tidak akan lagi mengirim data ke plugin Amazon Inspector SSM. Untuk informasi selengkapnya, lihat Menonaktifkan Amazon Inspector.

Mengatur jadwal khusus untuk pemindaian Windows misalnya

Anda dapat menyesuaikan waktu antara pemindaian instans Windows Amazon EC2 dengan menyetel ekspresi cron atau ekspresi laju untuk asosiasi menggunakan SSM. `InvokeInspectorSsmPlugin-do-not-delete` Untuk informasi selengkapnya, lihat Referensi: Cron dan ekspresi nilai untuk Systems Manager di Panduan AWS Systems Manager Pengguna atau gunakan petunjuk berikut.

Pilih dari contoh kode berikut untuk mengubah irama pemindaian untuk Windows instance dari default 6 jam menjadi 12 jam menggunakan ekspresi laju atau ekspresi cron.

Contoh berikut mengharuskan Anda untuk menggunakan AssociationIduntuk asosiasi bernama`InvokeInspectorSsmPlugin-do-not-delete`. Anda dapat mengambil Anda AssociationIddengan menjalankan AWS CLI perintah berikut:

```
$ aws ssm list-associations --association-filter-list
 "key=AssociationName,value=InvokeInspectorSsmPlugin-do-not-delete" --region us-east-1
```

> **Note**
>
> AssociationIdIni Regional, jadi Anda harus terlebih dahulu mengambil ID unik untuk masing-masing Wilayah AWS. Anda kemudian dapat menjalankan perintah untuk mengubah irama pemindaian di setiap Wilayah tempat Anda ingin mengatur jadwal pemindaian khusus untuk Windows instance.

Example rate expression

```
$ aws ssm update-association \
--association-id "YourAssociationId" \
--association-name "InvokeInspectorSsmPlugin-do-not-delete" \
--schedule-expression "rate(12 hours)"
```

Example cron expression

```
$ aws ssm update-association \
--association-id "YourAssociationId" \
--association-name "InvokeInspectorSsmPlugin-do-not-delete" \
--schedule-expression "cron(0 0/12 * * ? *)"
```

Memindai gambar wadah Amazon ECR dengan Amazon Inspector

Amazon Inspector memindai gambar kontainer yang disimpan di Amazon ECR untuk mencari kerentanan perangkat lunak guna menghasilkan temuan Package Vulnerability. Untuk informasi tentang jenis temuan yang dihasilkan untuk masalah ini, lihatMenemukan tipe di Amazon Inspector.

Saat mengaktifkan pemindaian Amazon Inspector untuk Amazon ECR, Anda menetapkan Amazon Inspector sebagai layanan pemindaian pilihan untuk registri pribadi Anda. Ini menggantikan pemindaian dasar default, yang disediakan tanpa biaya oleh Amazon ECR, dengan pemindaian yang Ditingkatkan, yang disediakan dan ditagih melalui Amazon Inspector.

Pemindaian yang disempurnakan yang disediakan oleh Amazon Inspector memberi Anda manfaat pemindaian kerentanan untuk sistem operasi dan paket bahasa pemrograman di tingkat registri. Anda dapat meninjau temuan yang ditemukan menggunakan pemindaian yang disempurnakan pada tingkat gambar, untuk setiap lapisan gambar, di konsol Amazon ECR. Selain itu, Anda dapat meninjau dan bekerja dengan temuan ini di layanan lain yang tidak tersedia untuk temuan pemindaian dasar, termasuk AWS Security Hub dan Amazon EventBridge. Anda dapat melihat temuan yang ditemukan dengan pemindaian di konsol Amazon Inspector di https://console.aws.amazon.com/inspector/v2/home. Untuk informasi tentang bekerja dengan temuan, lihatMengelola temuan di Amazon Inspector.

Untuk petunjuk tentang mengaktifkan pemindaian Amazon ECR lihat. Mengaktifkan jenis pemindaian

Perilaku pemindaian untuk pemindaian Amazon ECR

Saat Anda pertama kali mengaktifkan pemindaian ECR, dan repositori Anda dikonfigurasi untuk pemindaian berkelanjutan, Amazon Inspector mendeteksi semua gambar yang memenuhi syarat yang telah Anda dorong dalam 30 hari, atau ditarik dalam 90 hari terakhir. Kemudian Amazon Inspector memindai gambar yang terdeteksi dan menetapkan status pemindaian mereka. `active` Amazon Inspector terus memantau gambar selama gambar didorong atau ditarik dalam 90 hari terakhir (secara default), atau dalam durasi pemindaian ulang ECR yang Anda konfigurasikan. Untuk informasi selengkapnya, lihat Mengkonfigurasi durasi pemindaian ulang ECR.

Untuk pemindaian berkelanjutan, Amazon Inspector memulai pemindaian kerentanan baru gambar kontainer dalam situasi berikut:

- Setiap kali gambar kontainer baru didorong.

- Setiap kali Amazon Inspector menambahkan item common vulnerabilities and exposure (CVE) baru ke database-nya, dan CVE tersebut relevan dengan image container tersebut (hanya pemindaian berkelanjutan).

Jika Anda mengonfigurasi repositori untuk pemindaian push, gambar hanya dipindai saat Anda mendorongnya.

Anda dapat memeriksa kapan gambar kontainer terakhir diperiksa untuk kerentanan dari tab Gambar kontainer di halaman Manajemen akun, atau dengan menggunakan ListCoverageAPI. Amazon Inspector memperbarui bidang Terakhir dipindai di bidang gambar Amazon ECR sebagai tanggapan atas peristiwa berikut:

- Saat Amazon Inspector menyelesaikan pemindaian awal gambar kontainer.
- Saat Amazon Inspector memindai ulang image container karena item common vulnerabilities and exposure (CVE) baru yang memengaruhi image container tersebut ditambahkan ke database Amazon Inspector.

Sistem operasi dan jenis media yang didukung

Untuk informasi tentang sistem operasi yang didukung, lihatSistem operasi yang didukung untuk pemindaian Amazon ECR.

Pemindaian Amazon Inspector dari repositori Amazon ECR mencakup jenis media yang didukung berikut:

- `"application/vnd.docker.distribution.manifest.v1+json"`
- `"application/vnd.docker.distribution.manifest.v1+prettyjws"`
- `"application/vnd.oci.image.manifest.v1+json"`
- `"application/vnd.docker.distribution.manifest.v2+json"`

> **Note**
>
> Gambar dan `DockerV2ListMediaType` gambar goresan tidak didukung.

Mengkonfigurasi pemindaian yang disempurnakan untuk repositori Amazon ECR

Saat Anda mengaktifkan pemindaian Amazon Inspector untuk gambar penampung Amazon ECR, Anda mengubah pengaturan konfigurasi pemindaian untuk registri pribadi Anda. Jenis pemindaian untuk registri Anda diubah dari pemindaian Dasar ke Pemindaian yang Disempurnakan yang disediakan oleh Amazon Inspector. Untuk informasi selengkapnya, lihat Pemindaian gambar di panduan pengguna Amazon ECR.

Anda dapat mengelola pengaturan untuk pemindaian yang ditingkatkan di tingkat repositori di ECR. Anda dapat memilih pemindaian berkelanjutan atau pemindaian on-push untuk repositori Anda. Pemindaian berkelanjutan mencakup pemindaian on-push dan pemindaian ulang otomatis. Pemindaian on-push hanya memindai ketika Anda awalnya mendorong gambar. Untuk kedua opsi, Anda dapat menyempurnakan cakupan pemindaian melalui filter inklusi. Secara default, ketika Anda pertama kali mengaktifkan pemindaian yang disempurnakan, pengaturan Anda diatur ke Pindai terus menerus semua repositori.

Untuk mengonfigurasi pengaturan pemindaian yang disempurnakan

1. Buka konsol Amazon ECR di https://console.aws.amazon.com/ecr/.
2. Di Wilayah AWS pemilih di sudut kanan atas halaman, pilih Wilayah yang memiliki repositori yang Anda pindai.
3. Di panel navigasi, pilih Registri pribadi, lalu pilih Pemindaian.
4. Di bawah jenis Pindai, pastikan Pemindaian yang ditingkatkan dipilih. Jika tidak, pilih Pemindaian yang ditingkatkan.

   Secara default, opsi Pindai terus menerus semua repositori dipilih yang mengaktifkan cakupan pemindaian Amazon Inspector lengkap untuk semua repositori.
5. Hapus pilihan Pindai semua repositori secara terus menerus untuk memfilter repositori mana yang dipindai terus menerus atau on-push.

Untuk informasi selengkapnya tentang mengonfigurasi pemindaian yang disempurnakan, lihat Menggunakan pemindaian yang disempurnakan di panduan pengguna Amazon ECR.

Mengkonfigurasi durasi pemindaian ulang ECR

Pengaturan durasi pemindaian ulang ECR menentukan berapa lama Amazon Inspector terus memantau gambar kontainer di repositori. Anda dapat mengonfigurasi durasi pemindaian ulang untuk tanggal push gambar dan tanggal tarik gambar. Durasi pemindaian default untuk akun baru, termasuk akun baru yang ditambahkan ke organisasi, adalah 90 hari.

Durasi tanggal push gambar

Durasi tanggal push image menentukan berapa lama Amazon Inspector terus memantau gambar setelah didorong ke repositori setelah tanggal tarik terbaru. Opsi berikut tersedia sebagai durasi pemindaian ulang:

- 14 hari
- 30 hari
- 60 hari
- 90 hari (default)
- 180 hari
- Seumur hidup

Durasi tanggal tarik gambar

Durasi tanggal tarik gambar menentukan berapa lama Amazon Inspector terus memantau gambar setelah tanggal tarik terbaru. Opsi berikut tersedia sebagai durasi pemindaian ulang:

- 14 hari
- 30 hari
- 60 hari
- 90 hari (default)
- 180 hari

Amazon Inspector akan terus memantau dan memindai ulang gambar selama itu didorong atau ditarik dalam tanggal push dan pull yang dikonfigurasi. Jika gambar belum didorong atau ditarik dalam tanggal push dan pull yang dikonfigurasi, Amazon Inspector berhenti memantaunya.

> **Note**
>
> Saat Amazon Inspector berhenti memantau gambar, Amazon Inspector akan menyetel kode status pemindaian gambar `inactive` dan kode alasannya. `expired` Kemudian menjadwalkan semua temuan gambar terkait untuk ditutup.

Atur durasi pemindaian ulang agar sesuai dengan lingkungan Anda. Misalnya, jika Anda sering membuat gambar, pilih durasi pemindaian yang lebih pendek. Demikian pula, jika Anda menggunakan gambar untuk jangka waktu yang lama, pilih durasi pemindaian yang lebih lama.

Saat Anda mengonfigurasi durasi pemindaian ulang dari akun administrator yang didelegasikan, Amazon Inspector menerapkan pengaturan ke semua akun anggota di organisasi.

Untuk mengonfigurasi durasi pemindaian ulang ECR

1. Buka konsol Amazon Inspector di https://console.aws.amazon.com/inspector/v2/home.
2. Dari panel navigasi, pilih Pengaturan umum, lalu pilih Pengaturan pemindaian ECR.
3. Pada pengaturan pemindaian ECR, di bawah durasi pemindaian ulang ECR, pilih durasi tanggal push gambar dan durasi tanggal tarik gambar yang ingin Anda atur.
4. Pilih Simpan. Pengaturan baru Anda diterapkan segera.

> **Note**
>
> Jika Anda meningkatkan durasi tanggal push, Amazon Inspector menerapkan perubahan ke semua gambar yang dipindai secara aktif di repositori yang dikonfigurasi untuk pemindaian berkelanjutan. Namun, gambar yang tidak aktif tetap tidak aktif, bahkan jika Anda mendorongnya dalam durasi baru.

AWS Lambda Fungsi pemindaian dengan Amazon Inspector

Dukungan Amazon Inspector untuk AWS Lambda fungsi menyediakan penilaian kerentanan keamanan otomatis yang berkelanjutan untuk fungsi dan lapisan Lambda. Amazon Inspector menawarkan dua jenis pemindaian untuk Lambda. Jenis pemindaian ini mencari berbagai jenis kerentanan.

Pemindaian standar Amazon Inspector Lambda

Ini adalah jenis pemindaian Lambda default. Pemindaian standar Lambda memindai dependensi aplikasi dalam fungsi Lambda dan lapisannya untuk kerentanan paket. Untuk informasi selengkapnya, lihat Pemindaian standar Lambda.

Pemindaian kode Amazon Inspector Lambda

Jenis pemindaian ini memindai kode aplikasi khusus dalam fungsi dan lapisan Anda untuk kerentanan kode. Anda dapat mengaktifkan pemindaian standar Lambda atau mengaktifkan pemindaian standar Lambda bersama dengan pemindaian kode Lambda. Untuk informasi selengkapnya, lihat Pemindaian kode Amazon Inspector Lambda.

Saat Anda mengaktifkan pemindaian Lambda, Amazon Inspector membuat saluran terkait layanan AWS CloudTrail berikut di akun Anda:

- `cloudtrail:CreateServiceLinkedChannel`
- `cloudtrail:DeleteServiceLinkedChannel`

Amazon Inspector mengelola saluran ini dan menggunakannya untuk memantau CloudTrail acara Anda untuk pemindaian. Untuk informasi selengkapnya tentang saluran terkait layanan, lihat Melihat saluran terkait layanan untuk CloudTrail menggunakan CLI. AWS

> **Note**
>
> Saluran terkait layanan yang dibuat oleh Amazon Inspector memungkinkan Anda CloudTrail melihat peristiwa di akun Anda seolah-olah Anda CloudTrail memiliki jejak, namun, kami menyarankan Anda membuat CloudTrail sendiri untuk mengelola acara untuk akun Anda.

Untuk petunjuk tentang mengaktifkan pemindaian fungsi Lambda, lihat. Mengaktifkan jenis pemindaian

Memindai perilaku untuk pemindaian fungsi Lambda

Setelah aktivasi, Amazon Inspector memindai semua fungsi Lambda yang dipanggil atau diperbarui dalam 90 hari terakhir di akun Anda. Amazon Inspector memulai pemindaian kerentanan fungsi Lambda dalam situasi berikut:

- Segera Amazon Inspector menemukan fungsi Lambda yang ada.
- Saat Anda menerapkan fungsi Lambda baru ke layanan Lambda.
- Saat Anda menerapkan pembaruan ke kode aplikasi atau dependensi fungsi Lambda yang ada atau lapisannya.
- Setiap kali Amazon Inspector menambahkan item common vulnerabilities and exposure (CVE) baru ke database-nya, dan CVE tersebut relevan dengan fungsi Anda.

Amazon Inspector memantau setiap fungsi Lambda sepanjang masa pakainya hingga dihapus atau dikecualikan dari pemindaian.

Anda dapat memeriksa kapan fungsi Lambda terakhir diperiksa kerentanan dari tab fungsi Lambda di halaman Manajemen akun, atau dengan menggunakan API. ListCoverage Amazon Inspector memperbarui bidang Terakhir dipindai di untuk fungsi Lambda sebagai respons terhadap peristiwa berikut:

- Saat Amazon Inspector menyelesaikan pemindaian awal fungsi Lambda.
- Saat fungsi Lambda diperbarui.
- Saat Amazon Inspector memindai ulang fungsi Lambda karena item CVE baru yang memengaruhi fungsi tersebut ditambahkan ke database Amazon Inspector.

Runtime yang didukung dan fungsi yang memenuhi syarat

Amazon Inspector mendukung runtime yang berbeda untuk pemindaian standar Lambda dan pemindaian kode Lambda. Untuk daftar runtime yang didukung untuk setiap jenis pemindaian, lihat Runtime yang didukung: Pemindaian standar Amazon Inspector Lambda danRuntime yang didukung: Pemindaian kode Amazon Inspector Lambda.

Selain memiliki runtime yang didukung, fungsi Lambda harus memenuhi kriteria berikut agar memenuhi syarat untuk pemindaian Amazon Inspector:

- Fungsi telah dipanggil atau diperbarui dalam 90 hari terakhir.
- Fungsinya ditandai`$LATEST`.
- Fungsi ini tidak dikecualikan dari pemindaian oleh tag.

> **Note**
>
> Fungsi Lambda yang belum dipanggil atau dimodifikasi dalam 90 hari terakhir secara otomatis dikecualikan dari pemindaian. Amazon Inspector akan melanjutkan pemindaian fungsi yang dikecualikan secara otomatis jika dipanggil lagi atau jika perubahan dilakukan pada kode fungsi Lambda.

Pemindaian standar Amazon Inspector Lambda

Pemindaian standar Amazon Inspector Lambda mengidentifikasi kerentanan perangkat lunak dalam dependensi paket aplikasi yang Anda tambahkan ke kode fungsi dan lapisan Lambda Anda. Misalnya, jika fungsi Lambda Anda menggunakan versi `python-jwt` paket dengan kerentanan yang diketahui, pemindaian standar Lambda akan menghasilkan temuan untuk fungsi itu.

Jika Amazon Inspector mendeteksi kerentanan dalam dependensi paket aplikasi fungsi Lambda Anda, Amazon Inspector akan menghasilkan temuan tipe Package Vulnerability yang terperinci.

Untuk petunjuk tentang mengaktifkan jenis pemindaian lihatMengaktifkan jenis pemindaian.

> **Note**
>
> Pemindaian standar Lambda tidak memindai ketergantungan AWS SDK yang diinstal secara default di lingkungan runtime Lambda. Amazon Inspector hanya memindai dependensi yang diunggah dengan kode fungsi atau diwarisi dari lapisan.

> **Note**
>
> Menonaktifkan pemindaian standar Amazon Inspector Lambda juga akan menonaktifkan pemindaian kode Amazon Inspector Lambda.

Tidak termasuk fungsi dari pemindaian standar Lambda

Anda dapat menandai fungsi tertentu untuk mengecualikannya dari pemindaian standar Amazon Inspector Lambda. Mengecualikan fungsi dari pemindaian dapat membantu mencegah peringatan yang tidak dapat ditindaklanjuti.

Untuk mengecualikan fungsi Lambda dari pemindaian standar Lambda, beri tag fungsi dengan pasangan nilai kunci berikut:

- Kunci: `InspectorExclusion`
- Nilai: `LambdaStandardScanning`

Untuk mengecualikan fungsi dari pemindaian standar Lambda

1. Buka konsol Lambda di https://console.aws.amazon.com/lambda/.
2. Pilih Fungsi.
3. Dari tabel fungsi, pilih nama fungsi yang ingin Anda kecualikan dari pemindaian standar Amazon Inspector Lambda.
4. Pilih Konfigurasi dan pilih Tag dari menu.
5. Pilih Kelola tag, lalu Tambahkan tag baru.
6. Di bidang Kunci, masukkan`InspectorExclusion`, lalu, di bidang Nilai, masukkan`LambdaStandardScanning`.
7. Pilih Simpan untuk menambahkan tag dan mengecualikan fungsi Anda dari pemindaian standar Amazon Inspector Lambda.

Untuk informasi selengkapnya tentang menambahkan tag di Lambda, lihat Menggunakan tag pada fungsi Lambda.

Pemindaian kode Amazon Inspector Lambda

> **Important**
>
> Pemindaian kode menangkap cuplikan kode dari fungsi Lambda untuk menyoroti kerentanan yang terdeteksi. Cuplikan ini dapat menunjukkan kredensi hardcode atau materi sensitif lainnya dalam teks biasa.

Pemindaian kode Amazon Inspector Lambda memindai kode aplikasi khusus dalam fungsi Lambda untuk kerentanan kode berdasarkan praktik terbaik keamanan. AWS Pemindaian kode Lambda dapat mendeteksi kekurangan injeksi, kebocoran data, kriptografi lemah, atau enkripsi yang hilang dalam kode Anda. Untuk informasi tentang Wilayah yang tersedia, lihatKetersediaan fitur khusus wilayah.

Pemindaian standar Lambda adalah fitur yang mengevaluasi dependensi paket aplikasi yang digunakan dalam fungsi untuk kerentanan dan eksposur umum (CVE). Anda dapat mengaktifkan pemindaian kode Lambda bersama dengan pemindaian standar Lambda.

Amazon Inspector mengevaluasi kode aplikasi fungsi Lambda Anda menggunakan penalaran otomatis dan pembelajaran mesin yang menganalisis kode aplikasi Anda untuk kepatuhan keamanan secara keseluruhan. Ini mengidentifikasi pelanggaran kebijakan dan kerentanan berdasarkan detektor internal yang dikembangkan bekerja sama dengan Amazon. CodeGuru Untuk daftar kemungkinan deteksi, lihat Perpustakaan CodeGuru Detektor.

Jika Amazon Inspector mendeteksi kerentanan dalam kode aplikasi fungsi Lambda Anda, Amazon Inspector menghasilkan temuan tipe Kerentanan Kode yang terperinci. Jenis temuan ini mencakup lokasi pasti masalah dalam kode, cuplikan kode yang menunjukkan masalah, dan perbaikan yang disarankan. Remediasi yang disarankan mencakup blok plug-and-play kode yang dapat Anda gunakan untuk mengganti baris kode Anda yang rentan. Perbaikan kode yang disarankan ini disediakan selain panduan remediasi kode umum untuk temuan itu.

> **Important**
>
> Saran remediasi kode didukung oleh penalaran otomatis dan layanan kecerdasan buatan generatif, dan dengan demikian mungkin tidak berfungsi sebagaimana dimaksud. Anda bertanggung jawab atas saran remediasi kode yang Anda adopsi. Selalu tinjau saran remediasi kode sebelum mengadopsinya. Anda mungkin perlu mengedit saran remediasi kode untuk memastikan bahwa kode Anda berfungsi sebagaimana dimaksud. Silakan lihat Kebijakan AI yang Bertanggung Jawab.

Mengenkripsi kode Anda dalam temuan kerentanan kode

Cuplikan kode yang terdeteksi sehubungan dengan temuan kerentanan kode menggunakan pemindaian kode Lambda disimpan oleh layanan. CodeGuru Secara default kunci AWS milik yang dikendalikan oleh CodeGuru digunakan untuk mengenkripsi kode Anda, namun, Anda dapat menggunakan kunci yang dikelola pelanggan Anda sendiri untuk enkripsi melalui Amazon Inspector API. Untuk informasi lebih lanjut lihat Enkripsi saat istirahat untuk kode dalam temuan Anda

Pemindaian kode Lambda dapat diaktifkan bersama dengan pemindaian standar Lambda. Untuk petunjuk tentang mengaktifkan jenis pemindaian lihatMengaktifkan jenis pemindaian.

Tidak termasuk fungsi dari pemindaian kode Lambda

Anda dapat menandai fungsi tertentu untuk mengecualikannya dari pemindaian kode Amazon Inspector Lambda. Mengecualikan fungsi dari pemindaian dapat membantu mencegah peringatan yang tidak dapat ditindaklanjuti.

Untuk mengecualikan fungsi Lambda dari Amazon Inspector, kode Lambda memindai tag fungsi dengan pasangan kunci-nilai berikut:

- Kunci: `InspectorCodeExclusion`
- Nilai: `LambdaCodeScanning`

Untuk mengecualikan fungsi dari pemindaian kode Lambda

1. Masuk ke konsol Lambda di https://console.aws.amazon.com/lambda/.
2. Pilih Fungsi.
3. Dari tabel fungsi, pilih nama fungsi yang ingin Anda kecualikan dari pemindaian kode Amazon Inspector Lambda.
4. Pilih Konfigurasi dan pilih Tag dari menu.
5. Pilih Kelola tag, lalu Tambahkan tag baru.
6. Di bidang Kunci, masukkan`InspectorCodeExclusion`, lalu, di bidang Nilai, masukkan`LambdaCodeScanning`.
7. Pilih Simpan untuk menambahkan tag dan mengecualikan fungsi Anda dari pemindaian kode Amazon Inspector Lambda.

Untuk informasi selengkapnya tentang menambahkan tag di Lambda, lihat Menggunakan tag pada fungsi Lambda.

Menonaktifkan jenis pemindaian

Anda dapat menonaktifkan jenis pemindaian Amazon Inspector baru kapan saja. Ketika Anda menonaktifkan jenis pemindaian, Anda kehilangan akses ke temuan yang ada yang Anda miliki yang dihasilkan oleh jenis pemindaian tersebut. Jika Anda mengaktifkan kembali jenis pemindaian, sumber daya yang memenuhi syarat dipindai dan Amazon Inspector akan menghasilkan temuan baru. Untuk menyimpan catatan data temuan Anda, Anda dapat mengekspor temuan Anda sebelum

Anda menonaktifkan. Untuk informasi selengkapnya, lihat Mengekspor laporan temuan dari Amazon Inspector.

Ketika Anda menonaktifkan jenis pemindaian, perubahan tertentu dapat terjadi di AWS akun tersebut tergantung pada jenis pemindaian yang dinonaktifkan. Berikut ini adalah perubahan yang akan terjadi ketika Anda menonaktifkan jenis pemindaian ini:

- Pemindaian Amazon EC2 - Saat Anda menonaktifkan pemindaian Amazon Inspector Amazon EC2 untuk akun, asosiasi SSM berikut yang digunakan oleh Amazon Inspector akan dihapus:
  - `InspectorDistributor-do-not-delete`
  - `InspectorInventoryCollection-do-not-delete`
  - `InspectorLinuxDistributor-do-not-delete`
  - `InvokeInspectorLinuxSsmPlugin-do-not-delete`
  - `InvokeInspectorSsmPlugin-do-not-delete`. Selain itu, plugin Amazon Inspector SSM yang diinstal melalui asosiasi ini dihapus dari semua host Anda. Windows Untuk informasi selengkapnya, lihat WindowsContoh pemindaian.
- Pemindaian Amazon ECR - Saat Anda menonaktifkan pemindaian gambar kontainer Amazon ECR untuk akun, jenis pemindaian Amazon ECR untuk akun tersebut berubah dari Pemindaian yang Ditingkatkan dengan Amazon Inspector ke Pemindaian Dasar dengan Amazon ECR.
- Pemindaian standar Lambda - Ketika Anda menonaktifkan pemindaian standar Lambda di akun, itu akan menonaktifkan pemindaian kode Lambda jika pemindaian kode juga aktif. Selain itu, saluran terkait CloudTrail layanan yang dibuat saat pemindaian diaktifkan dihapus.

Menonaktifkan pemindaian

Menonaktifkan semua jenis pemindaian untuk akun menonaktifkan Amazon Inspector untuk akun tersebut di dalamnya. Wilayah AWS Untuk informasi selengkapnya, lihat Menonaktifkan Amazon Inspector.

Untuk menyelesaikan prosedur ini untuk lingkungan multi-akun, ikuti langkah-langkah ini saat masuk sebagai administrator yang didelegasikan Amazon Inspector.

Console

Untuk menonaktifkan pemindaian

1. Buka konsol Amazon Inspector di https://console.aws.amazon.com/inspector/v2/home.

2. Dengan menggunakan Wilayah AWS pemilih di sudut kanan atas halaman, pilih Wilayah tempat Anda ingin menonaktifkan pemindaian.
3. Di panel navigasi, pilih Manajemen akun.
4. Pilih tab Akun untuk menampilkan status pemindaian akun.
5. Pilih kotak centang setiap akun yang ingin Anda nonaktifkan pemindaian.
6. Pilih Tindakan, dan, dari opsi Nonaktifkan, pilih jenis pemindaian yang ingin Anda nonaktifkan.
7. (Disarankan) Ulangi langkah-langkah ini di masing-masing Wilayah AWS yang ingin Anda nonaktifkan jenis pemindaian itu.

API

Jalankan operasi Nonaktifkan API. Dalam permintaan, berikan ID akun yang Anda nonaktifkan pemindaian, dan untuk `resourceTypes` berikan satu atau lebih,, `EC2` `ECR` `LAMBDA`, atau `LAMBDA_CODE` untuk menonaktifkan pemindaian.

Pusat Keamanan Internet (CIS) memindai instans EC2

Saat mengaktifkan pemindaian Amazon Inspector EC2 untuk akun, Anda mengaktifkan Amazon Inspector untuk melakukan atau menjadwalkan pemindaian CIS. Amazon Inspector CIS memindai benchmark sistem operasi instans Amazon EC2 Anda untuk melihat apakah mereka dikonfigurasi sesuai dengan rekomendasi praktik terbaik yang ditetapkan oleh Pusat Keamanan Internet. Program Tolok Ukur Keamanan CIS menyediakan garis dasar konfigurasi standar industri dan praktik terbaik untuk mengonfigurasi sistem dengan aman. Untuk informasi lebih lanjut, lihat Apa itu Tolok Ukur CIS?

Amazon Inspector melakukan pemindaian CIS pada instans Amazon EC2 target berdasarkan tag instans dan jadwal pemindaian yang Anda tentukan dalam konfigurasi pemindaian. Untuk setiap instans yang ditargetkan, Amazon Inspector melakukan serangkaian pemeriksaan pada instance. Setiap pemeriksaan mengevaluasi apakah konfigurasi sistem Anda memenuhi rekomendasi CIS Benchmark tertentu. Setiap cek memiliki ID cek CIS dan judul, yang berkorelasi langsung dengan rekomendasi CIS Benchmark untuk platform itu. Saat pemindaian selesai, Anda dapat melihat hasilnya dan melihat pemeriksaan mana yang diteruskan, gagal, atau dilewati untuk sistem tersebut.

Persyaratan instans EC2 untuk pemindaian Amazon Inspector CIS

Untuk menjalankan pemindaian CIS pada instans Anda, Amazon Inspector mengharuskan instans memenuhi kriteria berikut:

- Sistem operasi instance adalah salah satu sistem operasi yang didukung untuk pemindaian CIS. Untuk daftar lengkap sistem operasi yang didukung, lihatSistem operasi yang didukung: pemindaian CIS.
- Instans ini adalah instans terkelola Amazon EC2 Systems Manager (SSM). Untuk informasi lebih lanjut, lihat Bekerja dengan SSM Agent.
- Instans memiliki plugin Amazon Inspector SSM diinstal. Amazon Inspector secara otomatis menginstal plugin ini untuk instans terkelola SSM.
- Instance memiliki profil instance yang memberikan izin kepada SSM untuk mengelola instance, dan Amazon Inspector untuk menjalankan pemindaian CIS untuk instance tersebut. Untuk memberikan izin ini, lampirkan ManagedCispolicy kebijakan AmazonInspector2FullAccess, AmazonSSM, ManagedInstanceCore dan AmazonInspector2 ke peran IAM dan lampirkan peran tersebut ke instance Anda sebagai profil instance. Untuk petunjuk cara membuat dan melampirkan profil instans, lihat Bekerja dengan peran IAM di Panduan Pengguna Amazon EC2.

> **Note**
>
> Mengaktifkan inspeksi mendalam Amazon Inspector tidak lagi menjadi persyaratan saat menjalankan pemindaian CIS pada sebuah instance. Jika Anda menonaktifkan inspeksi mendalam, Amazon Inspector masih terus menginstal Agen SSM, tetapi plugin tidak akan dipanggil untuk menjalankan inspeksi mendalam lagi. Ini berarti asosiasi berikut akan ada di akun Anda:`InspectorLinuxDistributor-do-not-delete`.

Menjalankan pemindaian CIS

Anda dapat menjalankan pemindaian CIS sekali sesuai permintaan atau sebagai pemindaian berulang yang dijadwalkan. Untuk menjalankan pemindaian, pertama-tama Anda membuat konfigurasi pemindaian.

Saat membuat konfigurasi pemindaian, Anda menentukan pasangan nilai kunci tag yang akan digunakan untuk menargetkan instance. Jika Anda adalah administrator yang didelegasikan Amazon Inspector untuk organisasi, Anda dapat menentukan beberapa akun dalam konfigurasi pemindaian, dan Amazon Inspector akan mencari instance dengan tag yang ditentukan di masing-masing akun tersebut. Anda memilih level CIS Benchmark untuk pemindaian. Untuk setiap benchmark, CIS mendukung profil level 1 dan level 2 yang dirancang untuk memberikan garis dasar untuk berbagai tingkat keamanan yang mungkin diperlukan oleh lingkungan yang berbeda.

- Level 1 — merekomendasikan pengaturan keamanan dasar penting yang dapat dikonfigurasi pada sistem apa pun. Menerapkan pengaturan ini harus menyebabkan sedikit atau tidak ada gangguan layanan. Tujuan dari rekomendasi ini adalah untuk mengurangi jumlah titik masuk ke sistem Anda, mengurangi risiko keamanan siber Anda secara keseluruhan.
- Level 2 — merekomendasikan pengaturan keamanan yang lebih canggih untuk lingkungan dengan keamanan tinggi. Menerapkan pengaturan ini membutuhkan perencanaan dan koordinasi untuk meminimalkan risiko dampak bisnis. Tujuan dari rekomendasi ini adalah untuk membantu Anda mencapai kepatuhan terhadap peraturan.

Level 2 memperluas level 1. Saat Anda memilih Level 2, Amazon Inspector memeriksa semua konfigurasi yang direkomendasikan untuk level 1 dan level 2.

Setelah menentukan parameter untuk pemindaian Anda, Anda dapat memilih apakah akan menjalankannya sebagai pemindaian satu kali, yang berjalan setelah Anda menyelesaikan

konfigurasi, atau pemindaian berulang. Pemindaian berulang dapat berjalan setiap hari, mingguan, atau bulanan, pada waktu pilihan Anda.

> **Tip**
>
> Sebaiknya pilih hari dan waktu yang paling tidak memengaruhi sistem Anda saat pemindaian sedang berjalan.

Untuk membuat konfigurasi pemindaian CIS

1. Buka konsol Amazon Inspector di https://console.aws.amazon.com/inspector/v2/home.
2. Menggunakan Wilayah AWS pemilih di sudut kanan atas halaman, pilih Wilayah AWS tempat Anda ingin menjalankan pemindaian CIS.
3. Dari panel navigasi, di bawah pemindaian On-Demand, pilih pemindaian CIS.
4. Pilih Buat pemindaian baru.
    a. Masukkan nama konfigurasi Pindai.
    b. Untuk sumber daya Target masukkan Kunci dan Nilai yang sesuai dari tag pada instance yang ingin Anda pindai. Anda dapat menentukan total 25 tag untuk disertakan dalam pemindaian, dan untuk setiap tombol, Anda dapat menentukan hingga lima nilai yang berbeda.
    c. Pilih level Tolok Ukur CIS. Anda dapat memilih Level 1 untuk konfigurasi keamanan dasar, atau Level 2 untuk konfigurasi keamanan lanjutan.
5. Untuk akun Target, tentukan akun mana yang akan disertakan dalam pemindaian. Akun mandiri atau anggota dalam organisasi dapat memilih Self untuk membuat konfigurasi pemindaian untuk akun mereka. Administrator yang didelegasikan Amazon Inspector dapat memilih Semua akun untuk menargetkan semua akun dalam organisasi, atau pilih Tentukan akun dan tentukan subset akun anggota yang akan ditargetkan. Administrator yang didelegasikan dapat masuk `SELF` alih-alih ID akun untuk membuat konfigurasi pemindaian untuk akun mereka sendiri. Untuk informasi selengkapnya, lihat Pertimbangan untuk mengelola pemindaian Amazon Inspector CIS dalam suatu organisasi AWS.
6. Pilih Jadwal untuk pemindaian. Pilih antara Satu kali pemindaian, yang akan berjalan segera setelah Anda selesai membuat konfigurasi pemindaian, atau Pemindaian berulang, yang akan berjalan pada waktu yang dijadwalkan yang Anda pilih hingga dihapus.
7. Pilih Buat untuk menyelesaikan pembuatan konfigurasi pemindaian.

Melihat dan mengedit konfigurasi pemindaian CIS

Anda dapat melihat atau mengedit pemindaian yang dijadwalkan sebelumnya kapan saja.

Untuk melihat atau mengedit konfigurasi pemindaian CIS

1. Buka konsol Amazon Inspector di https://console.aws.amazon.com/inspector/v2/home.
2. Menggunakan Wilayah AWS pemilih di sudut kanan atas halaman, pilih Wilayah AWS tempat Anda membuat konfigurasi pemindaian CIS Anda.
3. Dari panel navigasi, di bawah pemindaian On-Demand, pilih pemindaian CIS.
4. Pilih Terjadwal untuk melihat konfigurasi pemindaian terjadwal.
5. Pilih item dari kolom nama konfigurasi Pindai untuk membuka detail konfigurasi pemindaian itu.
6. (Opsional) Pilih Edit untuk mengubah parameter pemindaian ini.

Melihat hasil dari pemindaian CIS Anda

Amazon Inspector membuat tugas pemindaian setiap kali konfigurasi pemindaian berjalan, dan mengumpulkan hasil pemindaian di bawah ID Pemindaian yang unik.

Hasil pemindaian tersedia selama 90 hari setelah pemindaian selesai. Anda dapat melihat hasil pemindaian yang dikumpulkan dengan cek atau dengan sumber daya target.

Hasil pemindaian dikumpulkan berdasarkan cek

Hasil pemindaian dikelompokkan berdasarkan setiap pemeriksaan individu yang dilakukan selama pemindaian. Untuk setiap pemeriksaan, Anda mendapatkan laporan tentang berapa banyak sumber daya yang lulus, gagal, atau dilewati.

Hasil pemindaian dikumpulkan berdasarkan sumber daya

Hasil pemindaian dikelompokkan berdasarkan setiap sumber daya yang ditargetkan oleh konfigurasi pemindaian. Untuk setiap sumber daya, Anda mendapatkan laporan yang memeriksa sumber daya yang diteruskan, gagal, atau dilewati untuk sumber daya tersebut.

Untuk melihat hasil pemindaian

1. Buka konsol Amazon Inspector di https://console.aws.amazon.com/inspector/v2/home.

2. Menggunakan Wilayah AWS pemilih di sudut kanan atas halaman, pilih Wilayah AWS tempat Anda ingin melihat hasil pemindaian.
3. Dari panel navigasi, di bawah pemindaian On-Demand, pilih pemindaian CIS.
4. Pilih ID pemindaian yang ingin Anda lihat hasilnya dari kolom Scan ID.
5. Pilih cara melihat hasil pemindaian Anda:
   - Pilih tab Cek untuk melihat hasil pemindaian yang dikumpulkan berdasarkan cek.
     - Untuk pemeriksaan yang tercantum, pilih nomor dari diteruskan, dilewati, atau gagal di kolom Status sumber daya untuk membuka tampilan sumber daya yang difilter oleh status tersebut dan pemeriksaan tersebut.
   - Pilih tab Sumber daya yang dipindai untuk melihat hasil pemindaian yang dikumpulkan berdasarkan sumber daya.
     - Pilih sumber daya untuk membuka panel detail yang mencantumkan pemeriksaan yang diteruskan, gagal, atau dilewati sumber daya.
6. (Opsional) Gunakan bilah filter di kedua tampilan untuk menyempurnakan hasil Anda.

Anda dapat mengunduh hasil pemindaian CIS menggunakan konsol atau API.

Untuk mengunduh hasil pemindaian

1. Buka konsol Amazon Inspector di https://console.aws.amazon.com/inspector/v2/home.
2. Menggunakan Wilayah AWS pemilih di sudut kanan atas halaman, pilih Wilayah AWS tempat Anda ingin melihat hasil pemindaian.
3. Dari panel navigasi, di bawah pemindaian On-Demand, pilih pemindaian CIS.
4. Pilih ID pemindaian yang ingin Anda lihat hasilnya dari kolom Scan ID.
5. Pilih Unduh. Jika Anda administrator yang didelegasikan, Anda dapat memilih untuk mengunduh hasil untuk akun anggota tertentu.

Pertimbangan untuk mengelola pemindaian Amazon Inspector CIS dalam suatu organisasi AWS

Saat menjalankan pemindaian CIS dalam suatu organisasi, akun anggota dan administrator yang didelegasikan Amazon Inspector berinteraksi dengan konfigurasi pemindaian CIS dan hasil pemindaian dengan cara yang berbeda.

Ketika administrator yang didelegasikan membuat konfigurasi pemindaian CIS untuk semua akun atau daftar ID akun anggota, organisasi memiliki konfigurasi pemindaian tersebut. Akun mana pun administrator yang didelegasikan saat ini dapat mengelola konfigurasi pemindaian yang dimiliki oleh organisasi, bahkan jika akun lain membuatnya. Konfigurasi pemindaian CIS yang dimiliki oleh organisasi akan memiliki ARN yang mencantumkan ID organisasi sebagai pemilik, mengikuti pola:. `arn:aws:inspector2:Region:111122223333:owner/OrganizationId/cis-configuration/scanId` ID akun akan menjadi ID akun manajemen Organisasi.

> **Important**
>
> Anda tidak dapat menambahkan tag ke konfigurasi pemindaian CIS yang dimiliki oleh organisasi.

Ketika administrator yang didelegasikan membuat konfigurasi pemindaian dan menentukan `SELF` sebagai akun target, akun mereka memiliki konfigurasi pemindaian tersebut. Bahkan jika mereka meninggalkan organisasi mereka, mereka masih dapat mengelola konfigurasi pemindaian itu.

> **Note**
>
> Administrator yang didelegasikan tidak dapat mengubah target konfigurasi pemindaian yang menargetkan`SELF`.

Konfigurasi pemindaian yang dibuat oleh akun anggota, akun mandiri, atau administrator yang didelegasikan `SELF` sebagai target, dimiliki oleh akun yang membuatnya. Konfigurasi pemindaian CIS ini memiliki ARN yang mencantumkan akun tersebut sebagai pemilik mengikuti pola:. `arn:aws:inspector2:Region:111122223333:owner/111122223333/cis-configuration/scanId` ID akun akan menjadi akun yang membuat pemindaian.

Akun anggota dalam organisasi dapat membuat konfigurasi pemindaian untuk akun mereka sendiri. Administrator yang didelegasikan dapat melihat konfigurasi pemindaian yang dibuat oleh anggota tetapi tidak dapat mengedit atau menghapusnya. Jika akun anggota meninggalkan organisasi, administrator yang didelegasikan tidak akan lagi dapat melihat konfigurasi pemindaian yang dibuat oleh akun tersebut.

Administrator yang didelegasikan dapat melihat hasil pemindaian akun apa pun di organisasi, termasuk yang dijadwalkan oleh anggota. Akun anggota dapat melihat hasil pemindaian CIS

apa pun untuk sumber daya di akun mereka, termasuk yang dijadwalkan oleh administrator yang didelegasikan.

Amazon Inspector memiliki ember Amazon S3 yang digunakan untuk pemindaian Amazon Inspector CIS

Amazon Inspector memperbarui file definisi Open Vulnerability and Assessment Language (OVAL) yang diperlukan untuk pemindaian CIS. Tabel berikut mencantumkan semua bucket Amazon S3 milik Amazon Inspector Amazon dengan definisi OVAL yang digunakan pemindaian CIS per didukung. Wilayah AWS Ember harus diizinkan terdaftar dalam VPC jika perlu.

> **Note**
>
> Detail untuk masing-masing bucket Amazon S3 milik Amazon Inspector berikut tidak dapat berubah. Namun, daftar tersebut mungkin diperbarui untuk mencerminkan dukungan baru yang baru Wilayah AWS. Anda tidak dapat menggunakan bucket ini untuk operasi Amazon S3 lainnya atau di bucket Amazon S3 Anda sendiri.

Ember CIS	Wilayah AWS
`cis-datasets-prod-arn-5908f6f`	Eropa (Stockholm)
`cis-datasets-prod-bah-8f88801`	Timur Tengah (Bahrain)
`cis-datasets-prod-bjs-0f40506`	Tiongkok (Beijing)
`cis-datasets-prod-bom-435a167`	Asia Pasifik (Mumbai)
`cis-datasets-prod-cdg-f3a9c58`	Eropa (Paris)
`cis-datasets-prod-cgk-09eb12f`	Asia Pasifik (Jakarta)
`cis-datasets-prod-cmh-63030b9`	AS Timur (Ohio)
`cis-datasets-prod-cpt-02c5c6f`	Afrika (Cape Town)
`cis-datasets-prod-dub-984936f`	Eropa (Irlandia)

Ember CIS	Wilayah AWS
cis-datasets-prod-fra-6eb96eb	Eropa (Frankfurt)
cis-datasets-prod-gru-de69f99	Amerika Selatan (Sao Paulo)
cis-datasets-prod-hkg-8e30800	Asia Pasifik (Hong Kong)
cis-datasets-prod-iad-8438411	AS Timur (Virginia Utara)
cis-datasets-prod-icn-f4eff1c	Asia Pasifik (Seoul)
cis-datasets-prod-kix-5743b21	Asia Pasifik (Osaka)
cis-datasets-prod-lhr-8b1fbd0	Eropa (London)
cis-datasets-prod-mxp-7b1bbce	Eropa (Milan)
cis-datasets-prod-nrt-464f684	Asia Pasifik (Tokyo)
cis-datasets-prod-osu-5bead6f	AWS GovCloud (AS-Timur)
cis-datasets-prod-pdt-adadf9c	AWS GovCloud (AS-Barat)
cis-datasets-prod-pdx-acfb052	AS Barat (Oregon)
cis-datasets-prod-sfo-1515ba8	AS Barat (California Utara)
cis-datasets-prod-sin-309725b	Asia Pasifik (Singapura)
cis-datasets-prod-syd-f349107	Asia Pacific (Sydney)
cis-datasets-prod-yul-5e0c95e	Kanada (Pusat)
cis-datasets-prod-zhy-5a8eacb	Tiongkok (Ningxia)
cis-datasets-prod-zrh-67e0e3d	Eropa (Zurich)

Menilai cakupan Amazon Inspector dari lingkungan Anda AWS

Untuk membantu Anda menilai dan menafsirkan cakupan Amazon Inspector tentang lingkungan AWS Anda, halaman Manajemen akun di konsol Amazon Inspector menyediakan statistik dan detail tentang status pemindaian Amazon Inspector untuk akun dan sumber daya Anda. Dengan halaman ini, Anda dapat meninjau statistik gabungan dan data lainnya untuk sumber daya Anda. Anda juga dapat melakukan analisis mendalam tentang cakupan Amazon Inspector untuk sumber daya individu dan menelusuri untuk meninjau temuan untuk sumber daya tertentu. Jika Anda adalah administrator Amazon Inspector yang didelegasikan untuk organisasi, data tersebut mencakup statistik dan detail untuk semua akun di organisasi Anda.

Untuk menilai cakupan Amazon Inspector dari lingkungan Anda AWS

1. Buka konsol Amazon Inspector di https://console.aws.amazon.com/inspector/v2/home.
2. Di panel navigasi, pilih Manajemen akun.
3. Pada halaman Manajemen akun, pilih tab untuk salah satu dari lima tampilan cakupan yang berbeda:

    - Akun, untuk cakupan tingkat akun.
    - Instans, untuk cakupan instans Amazon Elastic Compute Cloud (Amazon EC2).
    - Repositori, untuk cakupan repositori Amazon Elastic Container Registry (Amazon ECR).
    - Gambar, untuk cakupan gambar kontainer Amazon ECR.
    - Lambda, untuk cakupan fungsi Lambda.

Topik di bagian ini menjelaskan informasi yang disediakan setiap tab, termasuk status pemindaian yang dapat dimiliki sumber daya individu.

Topik

Menilai cakupan tingkat akun

Jika akun Anda bukan bagian dari organisasi atau bukan akun administrator Amazon Inspector yang didelegasikan untuk organisasi, tab Akun memberikan informasi tentang akun Anda dan status pemindaian sumber daya untuk akun Anda. Pada tab ini, Anda dapat mengaktifkan atau menonaktifkan pemindaian untuk semua atau hanya jenis sumber daya tertentu untuk akun Anda. Untuk informasi selengkapnya, lihat Pemindaian sumber daya otomatis dengan Amazon Inspector.

Jika akun Anda adalah akun administrator Amazon Inspector yang didelegasikan untuk organisasi, tab Akun menyediakan setelan aktivasi otomatis untuk akun di organisasi Anda, dan mencantumkan semua akun di organisasi Anda. Untuk setiap akun, daftar menunjukkan apakah Amazon Inspector diaktifkan untuk akun dan, jika demikian, jenis pemindaian sumber daya yang diaktifkan untuk akun tersebut. Sebagai administrator yang didelegasikan, Anda dapat menggunakan tab ini untuk mengubah pengaturan aktivasi otomatis untuk organisasi Anda. Anda juga dapat mengaktifkan atau menonaktifkan jenis pemindaian sumber daya tertentu untuk akun anggota individu. Untuk informasi selengkapnya, lihat Mengaktifkan pemindaian Amazon Inspector untuk akun anggota.

Menilai cakupan instans Amazon EC2

Tab Instans menampilkan instans Amazon EC2 di lingkungan Anda. AWS Daftar disusun ke dalam kelompok-kelompok pada tab berikut:

- Semua - Menunjukkan semua contoh di lingkungan Anda. Kolom Status menunjukkan status pemindaian saat ini untuk sebuah instance.
- Scanning - Menunjukkan semua instance yang Amazon Inspector secara aktif memantau dan memindai di lingkungan Anda.
- Tidak memindai - Menunjukkan semua contoh yang Amazon Inspector tidak memantau dan memindai di lingkungan Anda. Kolom Alasan menunjukkan mengapa Amazon Inspector tidak memantau dan memindai instance.

  Instans EC2 dapat muncul di tab Not scanning karena beberapa alasan. Amazon Inspector menggunakan AWS Systems Manager (SSM) dan Agen SSM untuk secara otomatis memantau dan memindai instans EC2 Anda untuk kerentanan. Jika instans tidak menjalankan Agen SSM, tidak memiliki peran AWS Identity and Access Management (IAM) yang mendukung Systems Manager, atau tidak menjalankan sistem operasi atau arsitektur yang didukung, Amazon Inspector tidak dapat memantau dan memindai instance. Untuk informasi selengkapnya, lihat Memindai instans Amazon EC2.

Pada setiap tab, kolom Account menentukan Akun AWS yang memiliki instance.

Tag instans EC2 - Kolom ini menunjukkan tag yang terkait dengan instance dan dapat digunakan untuk menentukan apakah instance Anda telah dikecualikan dari pemindaian oleh tag.

Sistem operasi — Kolom ini menunjukkan kepada Anda jenis sistem operasi, yang dapat berupa`WINDOWS`,`MAC`,`LINUX`, atau`UNKNOWN`.

Dipantau menggunakan - Thiscolumn menunjukkan apakah Amazon Inspector menggunakan metode pemindaian berbasis agen atau tanpa agen pada instance ini.

Terakhir dipindai - Kolom ini menunjukkan kepada Anda kapan Amazon Inspector terakhir memeriksa sumber daya tersebut untuk kerentanan. Frekuensi Amazon Inspector melakukan pemindaian bergantung pada metode pemindaian yang digunakan untuk memindai instance.

Untuk meninjau detail tambahan tentang instans EC2, pilih tautan di kolom instans EC2. Amazon Inspector kemudian menampilkan detail tentang instance dan temuan terkini untuk instance tersebut. Untuk meninjau detail temuan, pilih tautan di kolom Judul. Untuk informasi tentang detail ini, lihatAmazon Inspector menemukan detail.

Memindai nilai status untuk instans Amazon EC2

Untuk instans Amazon Elastic Compute Cloud (Amazon EC2), nilai Status yang mungkin adalah:

- Pemantauan aktif - Amazon Inspector terus memantau dan memindai instance.
- Instans EC2 dihentikan — Amazon Inspector menghentikan pemindaian untuk instance karena instance dalam status berhenti. Setiap temuan yang ada akan bertahan sampai instance dihentikan. Jika instance dimulai ulang, Amazon Inspector akan secara otomatis melanjutkan pemindaian instance.
- Kesalahan internal - Terjadi kesalahan internal saat Amazon Inspector mencoba memindai instance. Amazon Inspector akan secara otomatis mengatasi kesalahan dan melanjutkan pemindaian sesegera mungkin.
- Tidak ada inventaris — Amazon Inspector tidak dapat menemukan inventaris aplikasi perangkat lunak untuk memindai instance. Asosiasi Amazon Inspector untuk instance tersebut mungkin telah dihapus atau mungkin gagal dijalankan.

  Untuk mengatasi masalah ini, gunakan AWS Systems Manager untuk memastikan bahwa `InspectorInventoryCollection-do-not-delete` asosiasi ada dan status asosiasinya

berhasil. Selain itu, gunakan AWS Systems Manager Fleet Manager untuk memverifikasi inventaris aplikasi perangkat lunak untuk instance tersebut.

- Menunggu penonaktifan - Amazon Inspector telah berhenti memindai instance. Instance sedang dinonaktifkan, menunggu penyelesaian tugas pembersihan.
- Pemindaian awal yang tertunda - Amazon Inspector telah mengantri instance untuk pemindaian awal.
- Sumber daya dihentikan - Instance dihentikan. Amazon Inspector saat ini sedang membersihkan temuan dan data cakupan yang ada untuk instance tersebut.
- Inventaris basi — Amazon Inspector tidak dapat mengumpulkan inventaris aplikasi perangkat lunak yang diperbarui yang ditangkap dalam 7 hari terakhir untuk instance tersebut.

  Untuk mengatasi masalah ini, gunakan AWS Systems Manager untuk memastikan bahwa asosiasi Amazon Inspector yang diperlukan ada dan berjalan untuk instans. Selain itu, gunakan AWS Systems Manager Fleet Manager untuk memverifikasi inventaris aplikasi perangkat lunak untuk instance tersebut.
- Instans EC2 yang tidak dikelola — Amazon Inspector tidak memantau atau memindai instans. Instance tidak dikelola olehAWS Systems Manager.

  Untuk mengatasi masalah ini, Anda dapat menggunakan yang AWSSupport-TroubleshootManagedInstance runbookdisediakan oleh AWS Systems Manager Automation. Setelah Anda mengonfigurasi AWS Systems Manager untuk mengelola instans, Amazon Inspector akan secara otomatis mulai memantau dan memindai instans secara otomatis.
- OS yang tidak didukung - Amazon Inspector tidak memantau atau memindai instans. Instans menggunakan sistem operasi atau arsitektur yang tidak didukung Amazon Inspector. Untuk daftar sistem operasi yang didukung Amazon Inspector, lihat. Sistem operasi yang didukung untuk pemindaian Amazon EC2
- Memantau secara aktif dengan kesalahan sebagian — Status ini berarti bahwa pemindaian EC2 aktif, tetapi ada kesalahan yang terkait dengannyaInspeksi mendalam Amazon Inspector untuk instans Amazon EC2 Linux. Kemungkinan kesalahan inspeksi mendalam adalah:
  - Batas pengumpulan paket inspeksi mendalam terlampaui - Instance telah melampaui batas paket 5000 untuk inspeksi mendalam Amazon Inspector. Untuk melanjutkan pemeriksaan mendalam untuk contoh ini, Anda dapat mencoba menyesuaikan jalur kustom yang terkait dengan akun.
  - Batas inventaris ssm harian inspeksi mendalam terlampaui — Agen SSM tidak dapat mengirim inventaris ke Amazon Inspector karena kuota SSM untuk data Inventaris yang dikumpulkan per

instans per hari telah tercapai untuk contoh ini. Untuk informasi selengkapnya, lihat titik akhir dan kuota Amazon EC2 Systems Manager.

- Batas waktu pengumpulan inspeksi mendalam terlampaui - Amazon Inspector gagal mengekstrak inventaris paket karena waktu pengumpulan paket melebihi ambang batas maksimum 15 menit.
- Inspeksi mendalam tidak memiliki inventaris - Plugin Amazon Inspector SSM belum dapat mengumpulkan inventaris paket untuk contoh ini. Ini biasanya merupakan hasil dari pemindaian yang tertunda, namun, jika status ini berlanjut setelah 6 jam, gunakan Amazon EC2 Systems Manager untuk memastikan bahwa asosiasi Amazon Inspector yang diperlukan ada dan berjalan untuk instance.

Untuk detail tentang mengonfigurasi pengaturan pemindaian untuk instans EC2, lihat. Memindai instans Amazon EC2

Menilai cakupan repositori Amazon ECR

Tab Repositori menunjukkan repositori Amazon ECR di lingkungan Anda. AWS Daftar disusun ke dalam kelompok-kelompok pada tab berikut:

- Semua - Menampilkan semua repositori di lingkungan Anda. Kolom Status menunjukkan status pemindaian saat ini untuk repositori.
- Diaktifkan - Menampilkan semua repositori yang Amazon Inspector dikonfigurasi untuk memantau dan memindai di lingkungan Anda. Kolom Status menunjukkan status pemindaian saat ini untuk repositori.
- Tidak diaktifkan - Menampilkan semua repositori yang Amazon Inspector tidak memantau dan memindai di lingkungan Anda. Kolom Alasan menunjukkan mengapa Amazon Inspector tidak memantau dan memindai repositori.

Pada setiap tab, kolom Account menentukan Akun AWS yang memiliki repositori.

Untuk meninjau detail tambahan tentang repositori, pilih nama repositori. Amazon Inspector kemudian menampilkan daftar gambar kontainer di repositori dan detail untuk setiap gambar. Detailnya termasuk tag gambar, intisari gambar, dan status pemindaian. Mereka juga termasuk statistik temuan kunci, seperti jumlah temuan kritis untuk gambar. Untuk menelusuri dan meninjau data pendukung untuk menemukan statistik, pilih tag gambar untuk gambar.

Memindai nilai status untuk repositori Amazon ECR

Untuk repositori Amazon Elastic Container Registry (Amazon ECR), nilai Status yang mungkin adalah:

- Activated (Continuous) - Untuk repositori, Amazon Inspector terus memantau gambar di repositori ini. Pengaturan pemindaian yang disempurnakan untuk repositori diatur ke pemindaian berkelanjutan. Amazon Inspector awalnya memindai gambar baru ketika mereka didorong dan memindai ulang gambar jika CVE baru yang relevan dengan gambar itu diterbitkan. Amazon Inspector akan terus memantau gambar di repositori ini untuk durasi pemindaian ECR yang Anda konfigurasikan.
- Diaktifkan (On push) - Amazon Inspector secara otomatis memindai gambar kontainer individual di repositori saat gambar baru didorong. Pemindaian yang ditingkatkan diaktifkan untuk repositori dan diatur untuk memindai saat push.
- Akses ditolak - Amazon Inspector tidak diizinkan mengakses repositori atau gambar kontainer apa pun di repositori.

  Untuk mengatasi masalah ini, pastikan bahwa kebijakan AWS Identity and Access Management (IAM) untuk repositori memungkinkan Amazon Inspector mengakses repositori.
- Dinonaktifkan (Manual) - Amazon Inspector tidak memantau atau memindai gambar kontainer apa pun di repositori. Pengaturan pemindaian Amazon ECR untuk repositori diatur ke pemindaian manual dasar.

  Untuk mulai memindai gambar di repositori dengan Amazon Inspector, ubah pengaturan pemindaian untuk repositori menjadi pemindaian yang disempurnakan, lalu pilih apakah akan memindai gambar secara terus menerus atau hanya ketika gambar baru didorong.
- Diaktifkan (On push) - Amazon Inspector secara otomatis memindai gambar kontainer individual di repositori saat gambar baru didorong. Pengaturan pemindaian yang disempurnakan untuk repositori diatur untuk memindai saat push.
- Kesalahan internal - Terjadi kesalahan internal saat Amazon Inspector mencoba memindai repositori. Amazon Inspector akan secara otomatis mengatasi kesalahan dan melanjutkan pemindaian sesegera mungkin.

Untuk detail tentang mengkonfigurasi pengaturan pemindaian untuk Memindai gambar wadah Amazon ECR repositori.

Menilai cakupan gambar kontainer Amazon ECR

Tab Gambar menunjukkan gambar kontainer Amazon ECR di AWS lingkungan Anda. Daftar disusun ke dalam kelompok-kelompok pada tab berikut:

- Semua - Menampilkan semua gambar kontainer di lingkungan Anda. Kolom Status menunjukkan status pemindaian saat ini untuk gambar.
- Scanning - Menampilkan semua gambar kontainer yang Amazon Inspector dikonfigurasi untuk memantau dan memindai di lingkungan Anda. Kolom Status menunjukkan status pemindaian saat ini untuk gambar.
- Tidak memindai - Menampilkan semua gambar kontainer yang Amazon Inspector tidak memantau dan memindai di lingkungan Anda. Kolom Alasan menunjukkan mengapa Amazon Inspector tidak memantau dan memindai gambar.

  Gambar kontainer dapat muncul di tab Tidak diaktifkan karena beberapa alasan. Gambar mungkin disimpan dalam repositori yang tidak diaktifkan oleh pemindaian Amazon Inspector, atau aturan pemfilteran Amazon ECR mencegah repositori tersebut dipindai. Atau gambar belum didorong atau ditarik dalam jumlah hari yang Anda konfigurasi untuk durasi pemindaian ulang ECR. Untuk informasi selengkapnya, lihat Mengkonfigurasi durasi pemindaian ulang ECR.

Pada setiap tab, kolom nama Repositori menentukan nama repositori yang menyimpan gambar kontainer. Kolom Akun menentukan Akun AWS yang memiliki repositori. Kolom terakhir yang dipindai menunjukkan kepada Anda kapan Amazon Inspector terakhir memeriksa sumber daya tersebut untuk kerentanan. Ini dapat mencakup pemeriksaan ketika ada pembaruan untuk menemukan metadata, ketika ada pembaruan ke inventaris aplikasi sumber daya, atau ketika pemindaian ulang dilakukan sebagai respons terhadap CVE baru. Untuk informasi selengkapnya, lihat Perilaku pemindaian untuk pemindaian Amazon ECR.

Untuk meninjau detail tambahan tentang gambar kontainer, pilih tautan di kolom gambar kontainer ECR. Amazon Inspector kemudian menampilkan detail tentang gambar dan temuan terkini untuk gambar tersebut. Untuk meninjau detail temuan, pilih tautan di kolom Judul. Untuk informasi tentang detail ini, lihatAmazon Inspector menemukan detail.

Memindai nilai status untuk gambar kontainer Amazon ECR

Untuk image container Amazon Elastic Container Registry, nilai Status yang mungkin adalah:

- Pemantauan aktif (Berkelanjutan) - Amazon Inspector terus memantau dan gambar serta pemindaian baru dilakukan di atasnya setiap kali CVE baru yang relevan diterbitkan. Durasi pemindaian ulang Amazon ECR untuk gambar disegarkan setiap kali gambar didorong atau ditarik. Pemindaian yang disempurnakan diaktifkan untuk repositori yang menyimpan gambar, dan pengaturan pemindaian yang disempurnakan untuk repositori diatur ke pemindaian berkelanjutan.
- Diaktifkan (On push) - Amazon Inspector secara otomatis memindai gambar setiap kali gambar baru didorong. Pemindaian yang disempurnakan diaktifkan untuk repositori yang menyimpan gambar, dan pengaturan pemindaian yang disempurnakan untuk repositori diatur untuk memindai saat push.
- Kesalahan internal - Terjadi kesalahan internal saat Amazon Inspector mencoba memindai gambar kontainer. Amazon Inspector akan secara otomatis mengatasi kesalahan dan melanjutkan pemindaian sesegera mungkin.
- Pemindaian awal yang tertunda - Amazon Inspector telah mengantri gambar untuk pemindaian awal.
- Kelayakan pemindaian kedaluwarsa (Berkelanjutan) - Amazon Inspector menangguhkan pemindaian untuk gambar. Gambar belum diperbarui dalam durasi yang Anda tentukan untuk pemindaian ulang otomatis gambar di repositori. Anda dapat mendorong atau menarik gambar untuk melanjutkan pemindaian.
- Kelayakan pemindaian kedaluwarsa (On push) - Amazon Inspector menangguhkan pemindaian untuk gambar. Gambar belum diperbarui dalam durasi yang Anda tentukan untuk pemindaian ulang otomatis gambar di repositori. Anda dapat mendorong gambar untuk melanjutkan pemindaian.
- Manual frekuensi pemindaian (Manual) - Amazon Inspector tidak memindai gambar wadah Amazon ECR. Pengaturan pemindaian Amazon ECR untuk repositori yang menyimpan gambar diatur ke pemindaian manual dasar. Untuk mulai memindai gambar secara otomatis dengan Amazon Inspector, ubah pengaturan repositori menjadi pemindaian yang disempurnakan, lalu pilih apakah akan memindai gambar secara terus menerus atau hanya ketika gambar baru didorong.
- OS yang tidak didukung - Amazon Inspector tidak memantau atau memindai gambar. Gambar didasarkan pada sistem operasi yang Amazon Inspector tidak mendukung, atau menggunakan jenis media yang Amazon Inspector tidak mendukung.

  Untuk daftar sistem operasi yang didukung Amazon Inspector, lihat. Sistem operasi yang didukung untuk pemindaian Amazon ECR Untuk daftar jenis media yang didukung Amazon Inspector, lihat Jenis media yang didukung.

Untuk detail tentang mengonfigurasi pengaturan pemindaian untuk repositori dan gambar, lihat. Memindai gambar wadah Amazon ECR

Menilai cakupan fungsi AWS Lambda

Tab Lambda menunjukkan fungsi Lambda di lingkungan Anda. AWS Halaman ini dua tabel, satu yang menunjukkan detail cakupan fungsi untuk pemindaian standar Lambda dan satu lagi untuk pemindaian kode Lambda. Anda dapat mengelompokkan fungsi berdasarkan tab berikut:

- Semua - Menampilkan semua fungsi Lambda di lingkungan Anda. Kolom Status menunjukkan status pemindaian saat ini untuk fungsi Lambda.
- Scanning - Menunjukkan fungsi Lambda yang Amazon Inspector dikonfigurasi untuk memindai. Kolom Status menunjukkan status pemindaian saat ini untuk setiap fungsi Lambda.
- Tidak memindai - Menunjukkan fungsi Lambda yang Amazon Inspector tidak dikonfigurasi untuk memindai. Kolom Alasan menunjukkan mengapa Amazon Inspector tidak memantau dan memindai suatu fungsi.

  Fungsi Lambda dapat muncul di tab Tidak memindai karena beberapa alasan. Fungsi Lambda mungkin milik akun yang belum ditambahkan ke Amazon Inspector atau aturan pemfilteran mencegah fungsi ini dipindai. Untuk informasi selengkapnya, lihat AWS Lambda Fungsi pemindaian.

Pada setiap tab, kolom nama Fungsi menentukan nama fungsi Lambda. Kolom Akun menentukan Akun AWS yang memiliki fungsi. Runtime menentukan runtime fungsi. Kolom Status menunjukkan status pemindaian saat ini untuk setiap fungsi Lambda. Tag sumber daya menunjukkan tag yang telah diterapkan ke fungsi. Kolom terakhir yang dipindai menunjukkan kepada Anda kapan Amazon Inspector terakhir memeriksa sumber daya tersebut untuk kerentanan. Ini dapat mencakup pemeriksaan ketika ada pembaruan untuk menemukan metadata, ketika ada pembaruan ke inventaris aplikasi sumber daya, atau ketika pemindaian ulang dilakukan sebagai respons terhadap CVE baru. Untuk informasi selengkapnya, lihat Memindai perilaku untuk pemindaian fungsi Lambda.

Memindai nilai status untuk AWS Lambda fungsi

Untuk fungsi Lambda, nilai Status yang mungkin adalah:

- Pemantauan aktif - Amazon Inspector terus memantau dan memindai fungsi Lambda. Pemindaian berkelanjutan mencakup pemindaian awal fungsi baru saat didorong ke repositori dan pemindaian

ulang fungsi otomatis saat diperbarui atau saat Common Vulnerabilities and Exposures (CVE) baru dirilis.

- Dikecualikan oleh tag - Amazon Inspector tidak memindai fungsi ini karena telah dikecualikan dari pemindaian oleh tag.
- Kelayakan pemindaian kedaluwarsa - Amazon Inspector tidak memantau fungsi ini karena sudah 90 hari atau lebih sejak terakhir dipanggil atau diperbarui.
- Kesalahan internal —Terjadi kesalahan internal saat Amazon Inspector mencoba memindai fungsi. Amazon Inspector akan secara otomatis mengatasi kesalahan dan melanjutkan pemindaian sesegera mungkin.
- Pemindaian awal yang tertunda - Amazon Inspector telah mengantri fungsi untuk pemindaian awal.
- Tidak didukung - Fungsi Lambda memiliki runtime yang tidak didukung.

Mengelola beberapa akun di Amazon Inspector with Organizations

Anda dapat menggunakan Amazon Inspector untuk mengelola beberapa akun yang terkait melalui OrganizationsAWS. Untuk mengelola beberapa akun Amazon Inspector, akun manajemen Organisasi menetapkan akun dalam organisasi sebagai akun administrator yang didelegasikan untuk Amazon Inspector. Administrator yang didelegasikan mengelola Amazon Inspector untuk organisasi dan diberikan izin khusus untuk melakukan tugas atas nama organisasi Anda. Tugas-tugas ini termasuk mengaktifkan atau menonaktifkan pemindaian untuk akun anggota, melihat data temuan agregat dari seluruh organisasi, dan membuat dan mengelola aturan penindasan.

> **Note**
>
> Untuk mengaktifkan Amazon Inspector secara terprogram untuk beberapa akun dalam Wilayah AWS beberapa akun, Anda dapat menggunakan skrip shell yang dikembangkan oleh Amazon Inspector. Untuk informasi lebih lanjut tentang menggunakan skrip ini, lihat inspector2- enablement-with-cli di situs web. GitHub

Topik

Memahami hubungan antara administrator dan akun anggota di Amazon Inspector

Saat Anda menggunakan Amazon Inspector di lingkungan beberapa akun, akun administrator yang didelegasikan Amazon Inspector memiliki akses ke metadata tertentu. Metadata ini mencakup data konfigurasi Amazon EC2 dan Amazon ECR serta hasil pencarian keamanan untuk akun anggota. Akun administrator juga dapat membuat aturan penindasan pencarian yang diterapkan ke akun anggota. Untuk informasi selengkapnya, lihat Menekan temuan Amazon Inspector dengan aturan penindasan.

Tindakan administrator yang didelegasikan

Umumnya, ketika administrator yang didelegasikan menerapkan pengaturan ke akun mereka, pengaturan tersebut diterapkan ke semua akun lain di organisasi. Administrator yang didelegasikan juga dapat melihat dan mengambil informasi untuk akun mereka sendiri dan anggota terkait. Akun administrator yang didelegasikan Amazon Inspector dapat melakukan tindakan berikut:

- Melihat dan mengelola status Amazon Inspector untuk akun terkait, termasuk mengaktifkan dan menonaktifkan Amazon Inspector.
- Aktifkan atau nonaktifkan jenis pemindaian untuk semua akun anggota di organisasi.
- Lihat data temuan gabungan di seluruh organisasi dan temukan detail untuk semua akun anggota dalam organisasi.
- Buat dan kelola aturan penindasan yang berlaku untuk temuan untuk semua akun di organisasi.
- Aktifkan pemindaian Amazon ECR yang disempurnakan untuk semua anggota organisasi.
- Lihat cakupan sumber daya untuk seluruh organisasi.
- Tentukan durasi pemindaian ulang otomatis gambar kontainer ECR untuk semua akun anggota di organisasi. Pengaturan durasi pemindaian administrator yang didelegasikan akan mengesampingkan setelan apa pun yang sebelumnya ditetapkan oleh akun anggota. Semua akun di organisasi berbagi durasi pemindaian ulang otomatis Amazon ECR dari administrator yang didelegasikan. Anda tidak dapat mengatur durasi pemindaian ulang yang berbeda untuk masing-masing akun.
- Tentukan lima jalur khusus untuk inspeksi mendalam Amazon Inspector untuk Amazon EC2 yang akan digunakan di semua akun di organisasi. Ini merupakan tambahan dari lima jalur kustom yang dapat ditetapkan oleh administrator yang didelegasikan untuk akun individu mereka. Untuk informasi selengkapnya tentang mengonfigurasi jalur kustom inspeksi mendalam, lihatJalur khusus untuk inspeksi mendalam Amazon Inspector.
- Aktifkan dan nonaktifkan inspeksi mendalam Amazon Inspector untuk akun anggota.
- Ekspor SBOM untuk akun anggota mana pun di organisasi.
- Setel mode pemindaian Amazon EC2 untuk semua akun anggota di organisasi. Untuk informasi selengkapnya, lihat Mengelola mode pemindaian.
- Buat dan kelola konfigurasi pemindaian CIS untuk semua akun di organisasi, kecuali untuk konfigurasi pemindaian apa pun yang dibuat oleh akun anggota.

> **Note**
>
> Jika akun anggota meninggalkan organisasi, administrator yang didelegasikan tidak akan lagi dapat melihat konfigurasi pemindaian yang dijadwalkan oleh akun tersebut.

- Lihat hasil pemindaian CIS untuk semua akun di organisasi.

Tindakan akun anggota

Akun anggota dapat melihat dan mengambil informasi tentang akun mereka di Amazon Inspector, sementara pengaturan untuk akun mereka dikelola oleh administrator yang didelegasikan. Akun anggota dalam organisasi dapat melakukan tindakan berikut di Amazon Inspector:

- Aktifkan Amazon Inspector untuk akun mereka sendiri.
- Lihat cakupan sumber daya untuk akun mereka sendiri.
- Lihat detail temuan untuk akun mereka sendiri.
- Lihat pengaturan durasi pemindaian ulang otomatis gambar kontainer ECR untuk akun mereka sendiri.
- Tentukan lima jalur kustom untuk inspeksi mendalam Amazon Inspector untuk EC2 yang akan digunakan untuk akun masing-masing. Jalur ini dipindai selain jalur kustom apa pun yang telah ditentukan oleh administrator yang didelegasikan untuk organisasi. Untuk informasi selengkapnya tentang mengonfigurasi jalur inspeksi mendalam, lihatJalur khusus untuk inspeksi mendalam Amazon Inspector.
- Lihat jalur kustom yang ditetapkan oleh administrator yang didelegasikan untuk inspeksi mendalam Amazon Inspector.
- Ekspor SBOM untuk sumber daya apa pun yang terkait dengan akun mereka.
- Lihat mode pemindaian untuk akun mereka.
- Buat dan kelola konfigurasi pemindaian CIS untuk akun mereka.
- Lihat hasil pemindaian CIS untuk sumber daya di akun mereka, termasuk yang dijadwalkan oleh administrator yang didelegasikan.

> **Note**
>
> Setelah aktivasi, Amazon Inspector hanya dapat dinonaktifkan oleh akun administrator yang didelegasikan.

Menunjuk administrator yang didelegasikan untuk Amazon Inspector

Pertimbangan penting untuk administrator yang didelegasikan

Perhatikan faktor-faktor berikut yang menentukan cara administrator yang didelegasikan beroperasi di Amazon Inspector:

Administrator yang didelegasikan dapat mengelola maksimal 5.000 anggota.

- Setiap administrator yang didelegasikan Amazon Inspector memiliki kuota 5.000 akun anggota. Namun, organisasi Anda dapat menyertakan lebih dari 5.000 akun. Jika Anda melebihi 5.000 akun anggota, Anda akan menerima pemberitahuan melalui Dashboard CloudWatch Personal Health Amazon dan email ke akun administrator yang didelegasikan.

Administrator yang didelegasikan adalah Regional.

- Tidak sepertiAWS Organizations, Amazon Inspector adalah layanan Regional. Ini berarti Anda harus menunjuk administrator yang didelegasikan, menambahkan akun anggota, dan mengaktifkan jenis pemindaian di setiap tempat Wilayah AWS Anda ingin menggunakan Amazon Inspector.

Sebuah organisasi hanya dapat memiliki satu administrator yang didelegasikan.

- Anda hanya dapat memiliki satu administrator yang didelegasikan untuk Amazon Inspector untuk sebuah organisasi. Jika Anda telah menetapkan akun sebagai administrator yang didelegasikan di satu Wilayah, akun tersebut harus menjadi administrator yang didelegasikan di semua Wilayah lainnya.

Mengubah administrator yang didelegasikan tidak menonaktifkan Amazon Inspector untuk akun anggota.

- Jika Anda menghapus administrator yang didelegasikan, Amazon Inspector tidak akan dinonaktifkan di akun tersebut, dan pengaturan pemindaian tidak akan terpengaruh.

AWSOrganisasi Anda harus mengaktifkan semua fitur.

> Ini adalah pengaturan default untukAWS Organizations. Jika tidak diaktifkan, lihat Mengaktifkan semua fitur di organisasi Anda.

Izin yang diperlukan untuk menetapkan administrator yang didelegasikan

Anda harus memiliki izin untuk mengaktifkan Amazon Inspector dan menunjuk administrator yang didelegasikan Amazon Inspector.

Tambahkan pernyataan berikut ke akhir kebijakan IAM untuk memberikan izin ini.

```
{
    "Sid": "PermissionsForInspectorAdmin",
    "Effect": "Allow",
    "Action": [
        "inspector2:EnableDelegatedAdminAccount",
        "organizations:EnableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization"
    ],
    "Resource": "*"
}
```

Menunjuk administrator yang didelegasikan untuk organisasi Anda AWS

Prosedur berikut menunjukkan cara menunjuk administrator yang didelegasikan untuk organisasi AndaAWS. Ketika penunjukan ini selesai, Amazon Inspector diaktifkan untuk akun manajemen Organizations dan akun administrator yang didelegasikan yang dipilih.

> **Note**
>
> Hanya akun manajemen Organizations yang dapat menunjuk administrator yang didelegasikan.

Mengaktifkan Amazon Inspector untuk pertama kalinya akan membuat peran terkait layanan (`SLRAWSServiceRoleForAmazonInspector`) untuk akun. Untuk informasi selengkapnya tentang cara Amazon Inspector menggunakan peran terkait layanan, lihat. Menggunakan peran tertaut layanan untuk Amazon Inspector Untuk informasi tentang peran terkait layanan secara umum, lihat Menggunakan peran terkait layanan di Panduan Pengguna IAM.

Untuk menunjuk administrator yang didelegasikan untuk Amazon Inspector

Console

Tentukan administrator yang didelegasikan di konsol

1. Masuk ke AWS Management Console menggunakan akun AWS Organizations manajemen.
2. Buka konsol Amazon Inspector di https://console.aws.amazon.com/inspector/v2/home, lalu gunakan Wilayah AWS pemilih di kanan atas untuk menentukan Wilayah tempat Anda ingin menunjuk administrator.
3. Di panel Administrator yang didelegasikan, masukkan ID akun dua belas digit Akun AWS yang ingin Anda tetapkan sebagai administrator delegasi Amazon Inspector untuk organisasi Anda. Kemudian pilih Administrasi delegasi.
4. (Disarankan) Ulangi langkah sebelumnya untuk masing-masingWilayah AWS.

API

Menunjuk administrator yang didelegasikan menggunakan API

- Jalankan operasi EnableDelegatedAdminAccountAPI menggunakan kredensi akun manajemen Organizations. Akun AWS Anda juga dapat menggunakan AWS Command Line Interface untuk melakukan ini dengan menjalankan perintah CLI berikut:. `aws inspector2 enable-delegated-admin-account --delegated-admin-account-id 11111111111`

> **Note**
>
> Pastikan untuk menentukan ID akun akun yang ingin Anda jadikan administrator delegasi Amazon Inspector.

Setelah Anda menentukan administrator yang didelegasikan, Anda harus menggunakan akun AWS Organizations manajemen hanya untuk mengubah atau menghapus akun administrator yang didelegasikan.

Mengaktifkan pemindaian Amazon Inspector untuk akun anggota

Sebagai administrator yang didelegasikan untuk organisasi Anda, Anda dapat mengaktifkan pemindaian Amazon EC2, pemindaian Amazon ECR, atau keduanya, untuk setiap anggota yang terkait dengan AWS Organizations akun manajemen. Saat Anda mengaktifkan pemindaian untuk akun anggota, akun tersebut akan dikaitkan dengan administrator yang didelegasikan, Amazon Inspector diaktifkan secara otomatis, dan pemindaian jenis yang dipilih segera dimulai. Untuk informasi tentang sumber daya apa yang dapat dipindai dan cara mengonfigurasi pemindaian, lihat. Pemindaian sumber daya otomatis dengan Amazon Inspector

Amazon Inspector menyediakan beberapa opsi untuk mengelola dan mengaktifkan pemindaian untuk akun anggota, termasuk mengizinkan akun anggota mengaktifkan Amazon Inspector. Gunakan salah satu opsi berikut untuk memulai pemindaian akun anggota Anda.

Untuk secara otomatis mengaktifkan pemindaian untuk semua akun anggota

1. Masuk ke akun administrator yang didelegasikan.
2. Buka konsol Amazon Inspector di https://console.aws.amazon.com/inspector/v2/home. Kemudian gunakan Wilayah AWS pemilih di kanan atas untuk menentukan Wilayah tempat Anda ingin mengaktifkan pemindaian untuk semua akun anggota.
3. Di panel navigasi, di bawah Pengaturan, pilih Manajemen akun. Tabel akun menampilkan semua akun anggota yang terkait dengan akun AWS Organizations manajemen.
4. Pilih kotak centang di bagian atas tabel untuk memilih semua akun di halaman ini. Kemudian pilih Aktifkan dan pilih opsi jenis pemindaian pilihan Anda dari menu.

   > **Note**
   >
   > Hanya akun yang saat ini terlihat di halaman yang dipilih. Jika Anda memiliki beberapa halaman akun, Anda harus mengulangi proses ini di setiap halaman. Untuk mengubah jumlah akun yang ditampilkan pada halaman, pilih ikon roda gigi.

5. Aktifkan pengaturan Aktifkan Inspector secara otomatis untuk akun anggota baru, lalu pilih jenis pemindaian untuk mengaktifkan anggota baru yang ditambahkan ke organisasi Anda.

6. (Disarankan) Ulangi langkah-langkah ini di setiap Wilayah tempat Anda ingin memindai akun anggota.

Pengaturan Automatic activate Inspector for new member accounts mengaktifkan Amazon Inspector untuk semua anggota organisasi Anda yang akan datang. Hal ini memungkinkan administrator delegasi Amazon Inspector Anda untuk mengelola setiap anggota baru yang ditambahkan ke organisasi. Ketika jumlah akun anggota mencapai kuota 5.000, pengaturan ini secara otomatis dimatikan. Jika akun dihapus dan jumlah total anggota berkurang menjadi kurang dari 5.000, pengaturan secara otomatis diaktifkan kembali.

Untuk mengaktifkan akun anggota secara selektif

1. Masuk ke akun administrator yang didelegasikan.
2. Buka konsol Amazon Inspector di https://console.aws.amazon.com/inspector/v2/home, lalu gunakan Wilayah AWS pemilih di kanan atas untuk menentukan Wilayah tempat Anda ingin mengaktifkan pemindaian untuk akun anggota tertentu.
3. Di panel navigasi, di bawah Pengaturan, pilih Manajemen akun. Tabel akun menampilkan semua akun anggota yang terkait dengan akun AWS Organizations manajemen.
4. Pada halaman Manajemen akun, pilih kotak centang untuk setiap akun anggota yang ingin Anda aktifkan pemindaian.
5. Pilih Aktifkan.
6. Dari menu Aktifkan, pilih jenis pemindaian yang akan diaktifkan untuk akun yang dipilih. Anda dapat memilih dari opsi pemindaian berikut:
   - Semua pemindaian — untuk mengaktifkan semua jenis pemindaian.
   - Pemindaian EC2 — untuk mengaktifkan pemindaian instans Amazon EC2.
   - Pemindaian kontainer ECR — untuk mengaktifkan pemindaian gambar kontainer ECR.
   - AWS Lambdapemindaian standar — untuk mengaktifkan pemindaian fungsi Lambda.
7. (Disarankan) Ulangi langkah-langkah ini di setiap Wilayah tempat Anda ingin mengaktifkan pemindaian untuk anggota tertentu.

Jika akun AWS Organizations manajemen Anda telah mendelegasikan administrator untuk Amazon Inspector, Anda dapat mengaktifkan akun Anda sendiri sebagai anggota dan melihat detail pemindaian untuk akun Anda sendiri.

Untuk mengaktifkan pemindaian sebagai akun anggota

1. Masuk ke akun Anda.
2. Buka konsol Amazon Inspector di https://console.aws.amazon.com/inspector/v2/home, lalu gunakan Wilayah AWS pemilih di kanan atas untuk menentukan Wilayah tempat Anda ingin mengaktifkan pemindaian.
3. Di panel navigasi, di bawah Pengaturan, pilih Manajemen akun.
4. Pada halaman Manajemen akun, pilih kotak centang untuk akun Anda.
5. Dari menu Aktifkan, pilih jenis pemindaian yang akan diaktifkan. Anda dapat memilih dari opsi pemindaian berikut:
   - Semua pemindaian — untuk mengaktifkan semua jenis pemindaian.
   - Pemindaian EC2 — untuk mengaktifkan pemindaian instans Amazon EC2.
   - Pemindaian kontainer ECR — untuk mengaktifkan pemindaian gambar kontainer ECR.
   - AWS Lambdapemindaian standar — untuk mengaktifkan pemindaian fungsi Lambda.
6. (Disarankan) Ulangi langkah-langkah ini di setiap Wilayah tempat Anda ingin mengaktifkan pemindaian.

Memutuskan akun anggota di Amazon Inspector

Prosedur berikut menunjukkan cara memisahkan akun anggota. Akun anggota yang tidak terkait tetap berada di AWS Organizations organisasi Anda sebagai akun Amazon Inspector mandiri. Administrator yang didelegasikan Amazon Inspector tidak lagi memiliki izin untuk mengaktifkan dan mengelola Amazon Inspector untuk akun ini. Anda dapat menambahkan akun yang tidak terkait sebagai anggota lagi nanti.

> **Note**
>
> Memutuskan hubungan akun tidak menonaktifkan pemindaian Amazon Inspector untuk akun tersebut.

Console

Untuk memisahkan akun anggota menggunakan konsol

1. Masuk ke akun administrator yang didelegasikan.

2. Buka konsol Amazon Inspector di https://console.aws.amazon.com/inspector/v2/home, lalu gunakan Wilayah AWS pemilih di kanan atas untuk menentukan Wilayah tempat Anda ingin memisahkan satu atau beberapa akun anggota.
3. Di panel navigasi, di bawah Pengaturan, pilih Manajemen akun.
4. Pada halaman Manajemen akun, pilih kotak centang untuk setiap akun yang ingin Anda pisahkan.
5. Dari menu Tindakan, pilih Putuskan akun.
6. (Disarankan) Ulangi langkah-langkah ini di setiap Wilayah tempat Anda ingin memisahkan akun.

API

Untuk memisahkan akun anggota menggunakan API

Jalankan operasi DisassociateMember API. Dalam permintaan, berikan ID akun yang Anda putuskan.

Menghapus administrator yang didelegasikan oleh Amazon Inspector

Jika Anda harus menetapkan administrator delegasi Amazon Inspector baru, Anda dapat menghapus administrator delegasi yang sudah ada sebagai akun manajemen. AWS Organizations

Saat Anda menghapus administrator yang didelegasikan, administrator tidak akan menonaktifkan Amazon Inspector di akun tersebut atau di akun anggota organisasi mana pun. Akun dalam organisasi Anda dikonversi ke akun mandiri dan mempertahankan setelan pemindaian yang mereka miliki sebelum dikelola oleh administrator yang didelegasikan.

Untuk menghapus administrator yang didelegasikan

1. Masuk ke AWS Management Console menggunakan akun AWS Organizations manajemen.
2. Buka konsol Amazon Inspector di https://console.aws.amazon.com/inspector/v2/home, lalu gunakan Wilayah AWS pemilih di kanan atas untuk menentukan Wilayah tempat Anda ingin menghapus administrator yang didelegasikan.
3. Di panel navigasi, di bawah Pengaturan, pilih Manajemen akun.
4. Di bagian Administrator yang didelegasikan, pilih Hapus, lalu konfirmasikan tindakan Anda.

5. Ulangi langkah-langkah ini di setiap Wilayah tempat Anda mendaftarkan administrator yang didelegasikan ini.

Saat menambahkan administrator delegasi Amazon Inspector baru, Anda harus mengaitkan anggota organisasi secara manual ke akun administrator baru. Gunakan langkah-langkah berikut untuk mengaitkan anggota organisasi ke akun administrator baru.

Untuk mengasosiasikan anggota dengan administrator yang didelegasikan baru

1. Masuk ke AWS Management Console menggunakan akun administrator yang didelegasikan.
2. Buka konsol Amazon Inspector di https://console.aws.amazon.com/inspector/v2/home, lalu gunakan Wilayah AWS pemilih di kanan atas untuk menentukan Wilayah tempat Anda ingin mengaitkan anggota dengan administrator delegasi baru.
3. Di panel navigasi, di bawah Pengaturan, pilih Manajemen akun.
4. Pilih semua akun yang terdaftar di organisasi Anda dengan menggunakan kotak centang atas.
5. Dari menu Tindakan, pilih Tambah anggota.
6. Ulangi langkah-langkah ini di setiap Wilayah tempat Anda ingin mengaitkan anggota dengan administrator yang didelegasikan baru.

Pemantauan Penggunaan dan Biaya di Amazon Inspector

Anda dapat menggunakan konsol Amazon Inspector dan operasi API untuk memproyeksikan biaya bulanan menggunakan Amazon Inspector di lingkungan Anda. Jika Anda adalah administrator Amazon Inspector untuk lingkungan beberapa akun, Anda dapat melihat total biaya untuk seluruh lingkungan dan metrik biaya untuk setiap akun anggota Anda.

Menggunakan konsol penggunaan

Anda dapat menilai penggunaan dan biaya yang diproyeksikan untuk Amazon Inspector dari konsol.

Untuk mengakses statistik penggunaan

1. Buka konsol Amazon Inspector di https://console.aws.amazon.com/inspector/v2/home.
2. Dengan menggunakan Wilayah AWS pemilih di sudut kanan atas halaman, pilih Wilayah yang ingin Anda pantau biaya.
3. Pada panel navigasi, pilih Penggunaan.

Di tab Berdasarkan akun Anda akan melihat total biaya yang diproyeksikan berdasarkan periode 30 hari yang tercantum dalam penggunaan Akun. Dalam tabel di bawah kolom Biaya yang diproyeksikan, pilih nilai untuk melihat rincian penggunaan berdasarkan jenis pemindaian untuk akun tersebut. Di panel detail ini Anda juga dapat melihat jenis pemindaian mana yang memiliki uji coba gratis yang aktif untuk akun tersebut.

Jika Anda adalah administrator yang didelegasikan untuk organisasi, Anda akan melihat baris dalam tabel untuk setiap akun dalam organisasi Anda. Jika akun di organisasi Anda dipisahkan, konsol menunjukkan biaya yang diproyeksikan sebagai -.

Di tab By scan type Anda dapat melihat rincian penggunaan aktual sejauh ini dalam periode 30 hari saat ini berdasarkan jenis pemindaian. Ini adalah informasi yang digunakan untuk menghitung biaya yang diproyeksikan di tab By account.

Jika Anda adalah administrator yang didelegasikan untuk organisasi, Anda dapat melihat penggunaan untuk setiap akun di organisasi Anda.

Di tab ini, Anda dapat memperluas salah satu panel berikut untuk statistik penggunaan:

Pemindaian Amazon EC2

Konsol penggunaan Amazon Inspector melacak metrik berikut untuk pemindaian berbasis agen dan pemindaian tanpa agen:

- Instances (Rata-rata) — Amazon Inspector menggunakan jam cakupan untuk menghitung jumlah rata-rata sumber daya untuk pemindaian instans EC2. Rata-rata adalah total jam pertanggungan dibagi 720 jam (jumlah jam dalam periode 30 hari).
- Jam cakupan — untuk pemindaian Amazon EC2, ini adalah jumlah total jam dalam 30 hari terakhir yang Amazon Amazon Inspector berikan cakupan aktif untuk setiap instans EC2 di akun. Untuk instans EC2, jam cakupan adalah jam dari saat Amazon Inspector menemukan instans hingga dihentikan atau dihentikan, atau dikecualikan dari pemindaian berdasarkan tag. (saat Anda memulai ulang instance yang dihentikan atau menghapus tag pengecualian, Amazon Inspector melanjutkan cakupan dan jam cakupan untuk instance tersebut akan terus bertambah).

Pemindaian Instans CIS — Jumlah total pemindaian CIS yang dilakukan untuk instance di akun.

Pemindaian ECR Amazon

Pemindaian awal — Jumlah total pemindaian gambar pertama kali di akun dalam 30 hari terakhir.

Rescan — Jumlah total pemindaian ulang untuk gambar di akun dalam 30 hari terakhir. Pemindaian ulang adalah pemindaian apa pun yang dilakukan pada gambar ECR yang sebelumnya dipindai Amazon Inspector. Jika Anda telah mengonfigurasi repositori ECR untuk pemindaian berkelanjutan, pemindaian ulang terjadi secara otomatis saat Amazon Inspector menambahkan Common Vulnerabilities and Exposures (CVE) baru ke database-nya.

Pemindaian Lambda

Konsol penggunaan Amazon Inspector melacak metrik berikut untuk pemindaian standar Lambda dan pemindaian kode Lambda:

- Jumlah fungsi Lambda (Rata-rata) - Amazon Inspector menggunakan jam cakupan untuk menghitung jumlah rata-rata fungsi untuk pemindaian fungsi Lambda. Rata-rata adalah total jam pertanggungan dibagi 720 jam (jumlah jam dalam periode 30 hari).
- Jam cakupan - Untuk pemindaian fungsi Lambda, ini adalah jumlah total jam dalam 30 hari terakhir Amazon Inspector menyediakan cakupan aktif untuk setiap fungsi Lambda dalam sebuah akun. Untuk AWS Lambda fungsi, jam cakupan dihitung dari saat Amazon Inspector menemukan fungsi hingga saat dihapus atau dikecualikan dari pemindaian. Jika fungsi yang dikecualikan disertakan lagi, jam cakupan untuk fungsi tersebut akan terus bertambah.

Memahami bagaimana Amazon Inspector menghitung biaya penggunaan

Biaya yang disediakan oleh Amazon Inspector adalah perkiraan, bukan biaya aktual, sehingga mungkin berbeda dari yang ada di konsol AndaAWS Billing.

Perhatikan hal berikut tentang cara Amazon Inspector menghitung biaya di halaman Penggunaan:

- Biaya penggunaan hanya mencerminkan wilayah saat ini. Harga per jenis pemindaian bervariasi menurut AWS Wilayah, untuk meninjau harga pasti per wilayah, lihat Harga untuk Amazon Inspector
- Semua proyeksi penggunaan dibulatkan ke dolar AS terdekat.
- Diskon tidak termasuk dalam biaya yang diproyeksikan.
- Biaya yang diproyeksikan mewakili total biaya untuk periode penggunaan 30 hari per jenis pemindaian. Jika ada kurang dari 30 hari penggunaan untuk akun, Amazon Inspector memproyeksikan biaya setelah 30 hari seolah-olah ada sumber daya yang saat ini tercakup akan tetap ditanggung selama sisa periode 30 hari.
- Biaya per jenis pemindaian dihitung berdasarkan hal berikut:
  - Pemindaian EC2: biaya mencerminkan jumlah rata-rata instans EC2 yang dicakup oleh Amazon Inspector dalam 30 hari terakhir.
  - Pemindaian kontainer ECR: biaya mencerminkan jumlah pemindaian gambar awal+pemindaian ulang gambar dalam 30 hari terakhir.
  - Pemindaian standar Lambda: biaya mencerminkan jumlah rata-rata fungsi Lambda yang dicakup oleh Amazon Inspector dalam 30 hari terakhir.
  - Pemindaian kode Lambda: biaya mencerminkan jumlah rata-rata fungsi Lambda yang dicakup oleh Amazon Inspector dalam 30 hari terakhir.

Tentang uji coba gratis Amazon Inspector

Saat Anda Mengaktifkan jenis pemindaian Amazon Inspector, Anda secara otomatis terdaftar dalam uji coba gratis 15 hari untuk jenis pemindaian tersebut. Setiap jenis pemindaian memiliki jejak bebas independen, ini termasuk: pemindaian EC2, pemindaian ECR, pemindaian standar Lambda, dan pemindaian kode Lambda.

> **Note**
>
> Uji coba gratis tidak berlaku untuk pemindaian CIS.

Jika Anda menonaktifkan jenis pemindaian selama uji coba gratis, uji coba gratis akan dijeda untuk jenis pemindaian tersebut. Jika Anda mengaktifkan kembali layanan itu, uji coba gratis akan dilanjutkan dan Anda akan mendapatkan sisa hari uji coba gratis itu.

Keamanan di Amazon Inspector

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

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

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

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

Topik

Perlindungan data di Amazon Inspector

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

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

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

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

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

Topik

Enkripsi diam

Amazon Inspector menyimpan data Anda dengan aman saat istirahat menggunakan solusi AWS enkripsi secara default. Amazon Inspector mengenkripsi data, seperti inventaris sumber daya yang dikumpulkan menggunakan AWS Systems Manager, inventaris sumber daya yang diuraikan dari image Amazon ECR, dan menghasilkan temuan keamanan, menggunakan kunci enkripsi yang AWS dimiliki dari AWS Key Management Service ().AWS KMS Anda tidak dapat melihat, mengelola, atau menggunakan kunci yang AWS dimiliki, atau mengaudit penggunaannya. Namun, Anda tidak perlu mengambil tindakan apa pun atau mengubah program apa pun untuk melindungi kunci yang mengenkripsi data Anda.. Untuk informasi selengkapnya, lihat kunci yang AWS dimiliki.

Jika Anda menonaktifkan Amazon Inspector, Amazon Inspector akan menghapus secara permanen semua sumber daya yang disimpan atau dipelihara untuk Anda, seperti inventaris yang dikumpulkan dan temuan keamanan.

Enkripsi saat istirahat untuk kode dalam temuan Anda

Untuk pemindaian kode Amazon Inspector Lambda, Amazon Inspector bermitra dengan CodeGuru untuk memindai kode Anda dari kerentanan. Ketika kerentanan terdeteksi, CodeGuru ekstrak cuplikan kode Anda yang berisi kerentanan dan menyimpan kode tersebut hingga Amazon Inspector meminta akses. Secara default CodeGuru menggunakan kunci yang AWS dimiliki untuk mengenkripsi kode yang diekstrak, namun, Anda dapat mengonfigurasi Amazon Inspector untuk menggunakan kunci AWS KMS terkelola pelanggan Anda sendiri untuk enkripsi.

Alur kerja berikut menjelaskan bagaimana Amazon Inspector menggunakan kunci yang Anda konfigurasikan untuk mengenkripsi kode Anda:

1. Anda menyediakan AWS KMS kunci ke Amazon Inspector menggunakan Amazon UpdateEncryptionKeyInspector API.
2. Amazon Inspector meneruskan informasi tentang kunci Anda AWS KMS . CodeGuru CodeGuru menyimpan informasi untuk penggunaan future.

3. CodeGuru meminta hibah dari kunci AWS KMS yang Anda konfigurasikan di Amazon Inspector.
4. CodeGuru membuat kunci data terenkripsi dari AWS KMS kunci Anda dan menyimpannya. Kunci data ini digunakan untuk mengenkripsi data kode Anda yang disimpan oleh CodeGuru.
5. Setiap kali Amazon Inspector meminta data dari pemindaian kode CodeGuru menggunakan hibah untuk mendekripsi kunci data terenkripsi, kemudian menggunakan kunci tersebut untuk mendekripsi data sehingga dapat diambil.

Ketika Anda menonaktifkan pemindaian kode Lambda CodeGuru menghentikan hibah dan menghapus kunci data terkait.

Izin untuk enkripsi kode dengan kunci yang dikelola pelanggan

Untuk menggunakan enkripsi, Anda harus memiliki kebijakan yang memungkinkan akses ke AWS KMS tindakan, serta pernyataan yang memberikan Amazon Inspector CodeGuru dan izin untuk menggunakan tindakan tersebut melalui kunci kondisi.

Jika Anda mengatur, memperbarui, atau mengatur ulang kunci enkripsi untuk akun Anda, Anda harus menggunakan kebijakan administrator Amazon Inspector, seperti. AWS kebijakan terkelola: AmazonInspector2FullAccess Anda juga perlu memberikan izin berikut kepada pengguna hanya-baca yang perlu mengambil cuplikan kode dari temuan atau data tentang kunci yang dipilih untuk enkripsi.

Untuk KMS, kebijakan harus memungkinkan Anda untuk melakukan tindakan berikut:

- `kms:CreateGrant`
- `kms:Decrypt`
- `kms:DescribeKey`
- `kms:GenerateDataKeyWithoutPlainText`
- `kms:Encrypt`
- `kms:RetireGrant`

Setelah Anda memverifikasi bahwa Anda memiliki AWS KMS izin yang benar dalam kebijakan Anda, Anda harus melampirkan pernyataan yang memungkinkan Amazon Inspector CodeGuru dan menggunakan kunci Anda untuk enkripsi. Lampirkan pernyataan kebijakan berikut:

> **Note**
>
> Ganti Wilayah dengan AWS Wilayah tempat Anda mengaktifkan pemindaian kode Amazon Inspector Lambda.

```
{
            "Sid": "allow CodeGuru Security to request a grant for a AWS KMS key",
          "Effect": "Allow",
          "Action": "kms:CreateGrant",
          "Resource": "*",
          "Condition": {
           "ForAllValues:StringEquals": {
            "kms:GrantOperations": [
             "GenerateDataKey",
             "GenerateDataKeyWithoutPlaintext",
             "Encrypt",
             "Decrypt",
             "RetireGrant",
             "DescribeKey"
            ]
           },
           "StringEquals": {
            "kms:ViaService": [
             "codeguru-security.Region.amazonaws.com"
            ]
           }
          }
         },
         {
          "Sid": "allow Amazon Inspector and CodeGuru Security to use your AWS KMS key",
          "Effect": "Allow",
          "Action": [
           "kms:Encrypt",
           "kms:Decrypt",
           "kms:RetireGrant",
           "kms:DescribeKey",
           "kms:GenerateDataKeyWithoutPlaintext"
          ],
          "Resource": "*",
          "Condition": {
```

```
          "StringEquals": {
           "kms:ViaService": [
            "inspector2.Region.amazonaws.com",
            "codeguru-security.Region.amazonaws.com"
           ]
          }
         }
        }
```

> **Note**
>
> Ketika Anda menambahkan pernyataan, pastikan bahwa sintaksnya valid. Kebijakan menggunakan format JSON. Ini berarti Anda perlu menambahkan koma sebelum atau sesudah pernyataan, tergantung di mana Anda menambahkan pernyataan ke kebijakan. Jika Anda menambahkan pernyataan sebagai pernyataan terakhir, tambahkan koma setelah tanda kurung kurung penutup untuk pernyataan sebelumnya. Jika Anda menambahkannya sebagai pernyataan pertama atau di antara dua pernyataan yang ada, tambahkan koma setelah tanda kurung kurung penutup untuk pernyataan tersebut.

Mengkonfigurasi enkripsi dengan kunci yang dikelola pelanggan

Untuk mengonfigurasi enkripsi akun menggunakan kunci terkelola pelanggan, Anda harus menjadi administrator Amazon Inspector dengan izin yang diuraikan. Izin untuk enkripsi kode dengan kunci yang dikelola pelanggan Selain itu, Anda akan memerlukan AWS KMS kunci di AWS Wilayah yang sama dengan temuan Anda, atau kunci multi-wilayah. Anda dapat menggunakan kunci simetris yang ada di akun Anda atau membuat kunci terkelola pelanggan simetris dengan menggunakan AWS Management Console, atau API. AWS KMS Untuk informasi selengkapnya, lihat Membuat AWS KMS kunci enkripsi simetris di panduan AWS KMS pengguna.

Menggunakan Amazon Inspector API untuk mengonfigurasi enkripsi

Untuk menetapkan kunci enkripsi, UpdateEncryptionKeypengoperasian Amazon Inspector API saat masuk sebagai administrator Amazon Inspector. Dalam permintaan API, gunakan `kmsKeyId` bidang untuk menentukan ARN AWS KMS kunci yang ingin Anda gunakan. Untuk `scanType` masuk `CODE` dan `resourceType` masuk`AWS_LAMBDA_FUNCTION`.

Anda dapat menggunakan UpdateEncryptionKeyAPI untuk memeriksa tampilan AWS KMS kunci mana yang digunakan Amazon Inspector untuk enkripsi.

> **Note**
>
> Jika Anda mencoba menggunakan `GetEncryptionKey` ketika Anda belum menetapkan kunci terkelola pelanggan, operasi mengembalikan `ResourceNotFoundException` kesalahan yang berarti bahwa kunci yang AWS dimiliki sedang digunakan untuk enkripsi.

Jika Anda menghapus atau kunci atau mengubah kebijakannya untuk menolak akses ke Amazon Inspector atau CodeGuru Anda tidak akan dapat mengakses temuan kerentanan kode Anda dan pemindaian kode Lambda akan gagal untuk akun Anda.

Anda dapat menggunakan `ResetEncryptionKey` untuk melanjutkan menggunakan kunci yang AWS dimiliki untuk mengenkripsi kode yang diekstraksi sebagai bagian dari temuan Amazon Inspector Anda.

Enkripsi dalam bergerak

AWS mengenkripsi semua data dalam perjalanan antara sistem AWS internal dan layanan lainnya AWS .

Untuk pengumpulan inventaris, Systems Manager mengumpulkan data telemetri dari instans EC2 milik pelanggan yang dikirim kembali ke saluran yang dilindungi Transport Layer Security (TLS) untuk AWS penilaian. Lihat Perlindungan Data di Systems Manager untuk memahami cara SSM mengenkripsi data saat transit.

Demikian juga, temuan pemindaian fungsi Amazon ECR dan AWS Lambda yang dikirim ke Security Hub dienkripsi menggunakan saluran yang dilindungi TLS.

Identity and Access Management untuk Amazon Inspector

AWS Identity and Access Management (IAM) adalah Layanan AWS yang membantu administrator mengontrol akses ke AWS sumber daya dengan aman. Administrator IAM mengontrol siapa yang dapat terautentikasi (masuk) dan berwenang (memiliki izin) untuk menggunakan sumber daya Amazon Inspector. IAM adalah Layanan AWS yang dapat Anda gunakan tanpa biaya tambahan.

Topik

- Audiens
- Mengautentikasi dengan identitas

- Mengelola akses menggunakan kebijakan
- Cara kerja Amazon Inspector dengan IAM
- Contoh kebijakan berbasis identitas untuk Amazon Inspector
- AWS kebijakan terkelola untuk Amazon Inspector
- Menggunakan peran tertaut layanan untuk Amazon Inspector
- Pemecahan masalah identitas dan akses Amazon Inspector

Audiens

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

Pengguna layanan – Jika Anda menggunakan layanan Amazon Inspector untuk melakukan tugas, administrator Anda akan memberikan kredensial dan izin yang dibutuhkan. Saat Anda menggunakan lebih banyak fitur Amazon Inspector untuk melakukan pekerjaan, Anda mungkin memerlukan izin tambahan. Memahami cara akses dikelola dapat membantu Anda meminta izin yang tepat dari administrator Anda. Jika Anda tidak dapat mengakses fitur di Amazon Inspector, lihat Pemecahan masalah identitas dan akses Amazon Inspector.

Administrator layanan – Jika Anda bertanggung jawab atas sumber daya Amazon Inspector di perusahaan Anda, Anda mungkin memiliki akses penuh ke Amazon Inspector. Tugas Anda adalah menentukan fitur dan sumber daya Amazon Inspector mana yang harus diakses pengguna layanan Anda. Kemudian, Anda harus mengirimkan permintaan kepada administrator IAM Anda untuk mengubah izin pengguna layanan Anda. Tinjau informasi di halaman ini untuk memahami konsep Basic IAM. Untuk mempelajari selengkapnya tentang bagaimana perusahaan Anda dapat menggunakan IAM dengan Amazon Inspector, lihat Cara kerja Amazon Inspector dengan IAM.

Administrator IAM – Jika Anda adalah administrator IAM, Anda mungkin ingin belajar dengan lebih detail tentang cara Anda menulis kebijakan untuk mengelola akses Amazon Inspector. Untuk melihat contoh kebijakan berbasis identitas Amazon Inspector yang dapat Anda gunakan di IAM, lihat Contoh kebijakan berbasis identitas untuk Amazon Inspector.

Mengautentikasi dengan identitas

Otentikasi adalah cara Anda masuk AWS menggunakan kredensyal identitas Anda. Anda harus diautentikasi (masuk ke AWS) sebagai Pengguna root akun AWS, sebagai pengguna IAM, atau dengan mengasumsikan peran IAM.

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

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

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

Apa pun metode autentikasi yang digunakan, Anda mungkin diminta untuk menyediakan informasi keamanan tambahan. Misalnya, AWS merekomendasikan agar Anda menggunakan otentikasi multi-faktor (MFA) untuk meningkatkan keamanan akun Anda. Untuk mempelajari lebih lanjut, lihat Autentikasi multi-faktor dalam Panduan Pengguna AWS IAM Identity Center dan Menggunakan autentikasi multi-faktor (MFA) di AWS dalam Panduan Pengguna IAM.

Akun AWS pengguna root

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

Identitas terfederasi

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

Identitas federasi adalah pengguna dari direktori pengguna perusahaan Anda, penyedia identitas web, direktori Pusat Identitas AWS Directory Service, atau pengguna mana pun yang mengakses Layanan AWS dengan menggunakan kredensyal yang disediakan melalui sumber identitas. Ketika identitas federasi mengakses Akun AWS, mereka mengambil peran, dan peran memberikan kredensi sementara.

Untuk pengelolaan akses terpusat, sebaiknya Anda menggunakan AWS IAM Identity Center. Anda dapat membuat pengguna dan grup di Pusat Identitas IAM, atau Anda dapat menghubungkan dan menyinkronkan ke sekumpulan pengguna dan grup di sumber identitas Anda sendiri untuk digunakan di semua aplikasi Akun AWS dan aplikasi Anda. Untuk informasi tentang Pusat Identitas IAM, lihat Apa yang dimaksud Pusat Identitas IAM? dalam Panduan Pengguna AWS IAM Identity Center .

Pengguna dan grup IAM

Pengguna IAM adalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus untuk satu orang atau aplikasi. Jika memungkinkan, sebaiknya andalkan kredensial temporer, dan bukan membuat pengguna IAM yang memiliki kredensial jangka panjang seperti kata sandi dan kunci akses. Namun, jika Anda memiliki kasus penggunaan khusus yang memerlukan kredensial jangka panjang dengan pengguna IAM, sebaiknya rotasikan kunci akses. Untuk informasi selengkapnya, lihat Merotasi kunci akses secara teratur untuk kasus penggunaan yang memerlukan kredensial jangka panjang dalam Panduan Pengguna IAM.

Grup IAM adalah identitas yang menentukan kumpulan pengguna IAM. Anda tidak dapat masuk sebagai grup. Anda dapat menggunakan grup untuk menentukan izin untuk beberapa pengguna sekaligus. Grup membuat izin lebih mudah dikelola untuk sekelompok besar pengguna. Misalnya, Anda dapat memiliki grup yang bernama IAMAdmins dan memberikan izin kepada grup tersebut untuk mengelola sumber daya IAM.

Pengguna berbeda dari peran. Pengguna secara unik terkait dengan satu orang atau aplikasi, tetapi peran tersebut dimaksudkan untuk dapat diambil oleh siapa pun yang membutuhkannya. Pengguna memiliki kredensial jangka panjang permanen, tetapi peran memberikan kredensial sementara. Untuk mempelajari selengkapnya, silakan lihat Kapan harus membuat pengguna IAM (bukan peran) dalam Panduan Pengguna IAM.

Peran IAM

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

Peran IAM dengan kredensial sementara berguna dalam situasi berikut:

- Akses pengguna gabungan – Untuk menetapkan izin ke sebuah identitas gabungan, Anda dapat membuat peran dan menentukan izin untuk peran tersebut. Saat identitas terfederasi diautentikasi, identitas tersebut dikaitkan dengan peran dan diberikan izin yang ditentukan oleh peran. Untuk informasi tentang peran untuk federasi, lihat Membuat peran untuk Penyedia Identitas pihak ketiga dalam Panduan Pengguna IAM. Jika Anda menggunakan Pusat Identitas IAM, Anda mengonfigurasi sekumpulan izin. Untuk mengontrol apa yang dapat diakses identitas Anda setelah identitas tersebut diautentikasi, Pusat Identitas IAM mengaitkan izin yang ditetapkan ke peran dalam IAM. Untuk informasi tentang rangkaian izin, lihat Rangkaian izin dalam Panduan Pengguna AWS IAM Identity Center .
- Izin pengguna IAM sementara – Pengguna atau peran IAM dapat mengambil peran IAM guna mendapatkan berbagai izin secara sementara untuk tugas tertentu.
- Akses lintas akun – Anda dapat menggunakan peran IAM untuk mengizinkan seseorang (pengguna utama tepercaya) dengan akun berbeda untuk mengakses sumber daya yang ada di akun Anda. Peran adalah cara utama untuk memberikan akses lintas akun. Namun, dengan beberapa Layanan AWS, Anda dapat melampirkan kebijakan secara langsung ke sumber daya (alih-alih menggunakan peran sebagai proxy). Untuk mempelajari perbedaan antara kebijakan peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Bagaimana peran IAM berbeda dari kebijakan berbasis sumber daya dalam Panduan Pengguna IAM.
- Akses lintas layanan — Beberapa Layanan AWS menggunakan fitur lain Layanan AWS. Contoh, ketika Anda melakukan panggilan dalam layanan, umumnya layanan tersebut menjalankan aplikasi di Amazon EC2 atau menyimpan objek di Amazon S3. Suatu layanan mungkin melakukan hal tersebut menggunakan izin pengguna utama panggilan, menggunakan peran layanan, atau peran terkait layanan.
  - Sesi akses teruskan (FAS) — Saat Anda menggunakan pengguna atau peran IAM untuk melakukan tindakan AWS, Anda dianggap sebagai prinsipal. Ketika Anda menggunakan beberapa layanan, Anda mungkin melakukan tindakan yang kemudian memulai tindakan lain

di layanan yang berbeda. FAS menggunakan izin dari pemanggilan utama Layanan AWS, dikombinasikan dengan permintaan Layanan AWS untuk membuat permintaan ke layanan hilir. Permintaan FAS hanya dibuat ketika layanan menerima permintaan yang memerlukan interaksi dengan orang lain Layanan AWS atau sumber daya untuk menyelesaikannya. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan ketika mengajukan permintaan FAS, lihat Meneruskan sesi akses.

- Peran IAM – Peran layanan adalah peran IAM yang diambil layanan untuk melakukan tindakan atas nama Anda. Administrator IAM dapat membuat, memodifikasi, dan menghapus peran layanan dari dalam IAM. Untuk informasi selengkapnya, lihat Membuat peran untuk mendelegasikan izin ke Layanan AWS dalam Panduan pengguna IAM.
- Peran terkait layanan — Peran terkait layanan adalah jenis peran layanan yang ditautkan ke peran layanan. Layanan AWS Layanan tersebut dapat mengambil peran untuk melakukan sebuah tindakan atas nama Anda. Peran terkait layanan muncul di Anda Akun AWS dan dimiliki oleh layanan. Administrator IAM dapat melihat, tetapi tidak dapat mengedit izin untuk peran terkait layanan.

- Aplikasi yang berjalan di Amazon EC2 — Anda dapat menggunakan peran IAM untuk mengelola kredensyal sementara untuk aplikasi yang berjalan pada instans EC2 dan membuat atau permintaan API. AWS CLI AWS Cara ini lebih dianjurkan daripada menyimpan kunci akses dalam instans EC2. Untuk menetapkan AWS peran ke instans EC2 dan membuatnya tersedia untuk semua aplikasinya, Anda membuat profil instance yang dilampirkan ke instance. Profil instans berisi peran dan memungkinkan program yang berjalan di instans EC2 mendapatkan kredensial sementara. Untuk informasi selengkapnya, lihat Menggunakan peran IAM untuk memberikan izin ke aplikasi yang berjalan di instans Amazon EC2 dalam Panduan Pengguna IAM.

Untuk mempelajari apakah kita harus menggunakan peran IAM atau pengguna IAM, lihat Kapan harus membuat peran IAM (bukan pengguna) dalam Panduan Pengguna IAM.

Mengelola akses menggunakan kebijakan

Anda mengontrol akses AWS dengan membuat kebijakan dan melampirkannya ke AWS identitas atau sumber daya. Kebijakan adalah objek AWS yang, ketika dikaitkan dengan identitas atau sumber daya, menentukan izinnya. AWS mengevaluasi kebijakan ini ketika prinsipal (pengguna, pengguna root, atau sesi peran) membuat permintaan. Izin dalam kebijakan menentukan apakah permintaan diizinkan atau ditolak. Sebagian besar kebijakan disimpan AWS sebagai dokumen JSON. Untuk informasi selengkapnya tentang struktur dan isi dokumen kebijakan JSON, lihat Ikhtisar kebijakan JSON dalam Panduan Pengguna IAM.

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

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

Kebijakan IAM mendefinisikan izin untuk suatu tindakan terlepas dari metode yang Anda gunakan untuk operasi. Sebagai contoh, anggap saja Anda memiliki kebijakan yang mengizinkan tindakan `iam:GetRole`. Pengguna dengan kebijakan tersebut bisa mendapatkan informasi peran dari AWS Management Console, API AWS CLI, atau AWS API.

Kebijakan berbasis identitas

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

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

Kebijakan berbasis sumber daya

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

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

Daftar kontrol akses (ACL)

Daftar kontrol akses (ACL) mengendalikan pengguna utama mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACL sama dengan kebijakan berbasis sumber daya, meskipun tidak menggunakan format dokumen kebijakan JSON.

Amazon S3, AWS WAF, dan Amazon VPC adalah contoh layanan yang mendukung ACL. Untuk mempelajari ACL selengkapnya, silakan lihat Gambaran umum daftar kontrol akses (ACL) di Panduan Developer Layanan Penyimpanan Ringkas Amazon.

Tipe kebijakan lain

AWS mendukung jenis kebijakan tambahan yang kurang umum. Tipe-tipe kebijakan ini dapat mengatur izin maksimum yang diberikan kepada Anda berdasarkan tipe kebijakan yang lebih umum.

- Batasan izin – Batasan izin adalah fitur lanjutan di mana Anda menetapkan izin maksimum yang dapat diberikan oleh kebijakan berbasis identitas kepada entitas IAM (pengguna atau peran IAM). Anda dapat menetapkan batasan izin untuk suatu entitas. Izin yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas milik entitas dan batasan izinnya. Kebijakan berbasis sumber daya yang menentukan pengguna atau peran dalam bidang `Principal` tidak dibatasi oleh batasan izin. Penolakan secara eksplisit terhadap salah satu kebijakan ini akan mengesampingkan izin tersebut. Untuk informasi selengkapnya tentang batasan izin, lihat Batasan izin untuk entitas IAM dalam Panduan Pengguna IAM.
- Kebijakan kontrol layanan (SCP) — SCP adalah kebijakan JSON yang menentukan izin maksimum untuk organisasi atau unit organisasi (OU) di. AWS Organizations AWS Organizations adalah layanan untuk mengelompokkan dan mengelola secara terpusat beberapa Akun AWS yang dimiliki bisnis Anda. Jika Anda mengaktifkan semua fitur dalam organisasi, Anda dapat menerapkan kebijakan kontrol layanan (SCP) ke sebagian atau semua akun Anda. SCP membatasi izin untuk entitas di akun anggota, termasuk masing-masing. Pengguna root akun AWS Untuk informasi selengkapnya tentang Organisasi dan SCP, lihat Cara kerja SCP dalam Panduan Pengguna AWS Organizations .
- Kebijakan sesi – Kebijakan sesi adalah kebijakan lanjutan yang Anda teruskan sebagai parameter saat Anda membuat sesi sementara secara terprogram untuk peran atau pengguna gabungan. Izin sesi yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas pengguna atau peran dan kebijakan sesi. Izin juga bisa datang dari kebijakan berbasis sumber daya. Penolakan eksplisit

di salah satu kebijakan ini akan membatalkan izin tersebut. Untuk informasi selengkapnya, lihat Kebijakan sesi dalam Panduan Pengguna IAM.

Berbagai jenis kebijakan

Jika beberapa jenis kebijakan diberlakukan untuk satu permintaan, izin yang dihasilkan lebih rumit untuk dipahami. Untuk mempelajari cara AWS menentukan apakah akan mengizinkan permintaan saat beberapa jenis kebijakan terlibat, lihat Logika evaluasi kebijakan di Panduan Pengguna IAM.

Cara kerja Amazon Inspector dengan IAM

Sebelum Anda menggunakan IAM untuk mengelola akses ke Amazon Inspector, pelajari fitur IAM apa yang tersedia untuk digunakan dengan Amazon Inspector.

Fitur IAM yang dapat Anda gunakan dengan Amazon Inspector

Fitur IAM	Dukungan Amazon Inspector
Kebijakan berbasis identitas	Ya
Kebijakan berbasis sumber daya	Tidak
Tindakan kebijakan	Ya
Sumber daya kebijakan	Ya
kunci-kunci persyaratan kebijakan (spesifik layanan)	Ya
ACL	Tidak
ABAC (tanda dalam kebijakan)	Parsial
Kredensial sementara	Ya
Izin pengguna utama	Ya
Peran layanan	Tidak
Peran terkait layanan	Ya

Untuk mendapatkan tampilan tingkat tinggi tentang cara kerja Amazon Inspector dan Layanan AWS lainnya dengan sebagian besar fitur IAM, Layanan AWS lihat fitur tersebut bekerja dengan IAM di Panduan Pengguna IAM.

Kebijakan berbasis identitas untuk Amazon Inspector

Mendukung kebijakan berbasis identitas	Ya

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

Dengan kebijakan berbasis identitas IAM, Anda dapat menentukan tindakan dan sumber daya yang diizinkan atau ditolak, serta ketentuan terkait jenis tindakan yang diizinkan atau ditolak. Anda tidak dapat menentukan pengguna utama dalam kebijakan berbasis identitas karena kebijakan ini berlaku untuk pengguna atau peran yang dilampiri kebijakan. Untuk mempelajari semua elemen yang dapat digunakan dalam kebijakan JSON, lihat Referensi elemen kebijakan JSON IAM dalam Panduan Pengguna IAM.

Contoh kebijakan berbasis identitas untuk Amazon Inspector

Untuk melihat contoh kebijakan berbasis identitas Amazon Inspector, lihat Contoh kebijakan berbasis identitas untuk Amazon Inspector.

Kebijakan berbasis sumber daya dalam Amazon Inspector

Mendukung kebijakan berbasis sumber daya	Tidak

Kebijakan berbasis sumber daya adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah kebijakan kepercayaan peran IAM dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Untuk sumber daya yang dilampiri kebijakan tersebut, kebijakan ini menentukan jenis tindakan yang

dapat dilakukan oleh pengguna utama tertentu di sumber daya tersebut dan apa ketentuannya. Anda harus menentukan pengguna utama dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau. Layanan AWS

Untuk mengaktifkan akses lintas akun, Anda dapat menentukan seluruh akun atau entitas IAM di akun lain sebagai pengguna utama dalam kebijakan berbasis sumber daya. Menambahkan pengguna utama lintas akun ke kebijakan berbasis sumber daya bagian dari membangun hubungan kepercayaan. Ketika prinsipal dan sumber daya berbeda Akun AWS, administrator IAM di akun tepercaya juga harus memberikan izin entitas utama (pengguna atau peran) untuk mengakses sumber daya. Izin diberikan dengan melampirkan kebijakan berbasis identitas ke entitas tersebut. Namun, jika kebijakan berbasis sumber daya memberikan akses kepada pengguna utama dalam akun yang sama, kebijakan berbasis identitas lainnya tidak diperlukan. Untuk informasi selengkapnya, lihat Perbedaan peran IAM dengan kebijakan berbasis sumber daya di Panduan Pengguna IAM.

Tindakan kebijakan untuk Amazon Inspector

Mendukung tindakan kebijakan	Ya

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Yaitu, pengguna utama mana yang dapat melakukan tindakan pada sumber daya apa, dan dalam kondisi apa.

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

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

Untuk melihat daftar tindakan Amazon Inspector, lihat Tindakan yang ditentukan oleh Amazon Inspector di Referensi Otorisasi Layanan.

Tindakan kebijakan di Amazon Inspector menggunakan awalan berikut sebelum tindakan:

```
inspector2
```

Untuk menetapkan secara spesifik beberapa tindakan dalam satu pernyataan, pisahkan tindakan-tindakan tersebut dengan koma.

```
"Action": [
      "inspector2:action1",
      "inspector2:action2"
         ]
```

Untuk melihat contoh kebijakan berbasis identitas Amazon Inspector, lihat Contoh kebijakan berbasis identitas untuk Amazon Inspector.

Sumber daya kebijakan untuk Amazon Inspector

Mendukung sumber daya kebijakan	Ya

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Yaitu, pengguna utama mana yang dapat melakukan tindakan pada sumber daya apa, dan dalam kondisi apa.

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

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

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

Untuk melihat daftar jenis sumber daya Amazon Inspector dan ARNnya, lihat Sumber daya yang ditentukan oleh Amazon Inspector di Referensi Otorisasi Layanan. Untuk mempelajari tindakan mana yang dapat Anda tentukan ARN dari setiap sumber daya, lihat Tindakan yang ditentukan oleh Amazon Inspector.

Untuk melihat contoh kebijakan berbasis identitas Amazon Inspector, lihat Contoh kebijakan berbasis identitas untuk Amazon Inspector.

Kunci kondisi kebijakan untuk Amazon Inspector

Mendukung kunci kondisi kebijakan spesifik layanan	Ya

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Yaitu, pengguna utama mana yang dapat melakukan tindakan pada sumber daya apa, dan dalam kondisi apa.

Elemen `Condition` (atau blok `Condition`) memungkinkan Anda menentukan kondisi di mana suatu pernyataan akan diterapkan. Elemen `Condition` bersifat opsional. Anda dapat membuat ekspresi kondisional yang menggunakan operator kondisi, misalnya sama dengan atau kurang dari, untuk mencocokkan kondisi dalam kebijakan dengan nilai-nilai yang diminta.

Jika Anda menentukan beberapa elemen `Condition` dalam satu pernyataan, atau beberapa kunci dalam satu elemen `Condition`, AWS akan mengevaluasinya dengan menggunakan operasi `AND` logis. Jika Anda menentukan beberapa nilai untuk satu kunci kondisi, AWS mengevaluasi kondisi menggunakan `OR` operasi logis. Semua kondisi harus dipenuhi sebelum izin pernyataan diberikan.

Anda juga dapat menggunakan variabel placeholder saat menentukan kondisi. Sebagai contoh, Anda dapat memberikan izin kepada pengguna IAM untuk mengakses sumber daya hanya jika izin tersebut mempunyai tanda yang sesuai dengan nama pengguna IAM mereka. Untuk informasi selengkapnya, silakan lihat Elemen kebijakan IAM: variabel dan tanda di Panduan Pengguna IAM.

AWS mendukung kunci kondisi global dan kunci kondisi khusus layanan. Untuk melihat semua kunci kondisi AWS global, lihat kunci konteks kondisi AWS global di Panduan Pengguna IAM.

Untuk melihat daftar kunci kondisi Amazon Inspector, lihat Kunci kondisi untuk Amazon Inspector di Referensi Otorisasi Layanan. Untuk mempelajari tindakan dan sumber daya yang dapat Anda gunakan kunci kondisi, lihat Tindakan yang ditentukan oleh Amazon Inspector.

Untuk melihat contoh kebijakan berbasis identitas Amazon Inspector, lihat Contoh kebijakan berbasis identitas untuk Amazon Inspector.

ACL di Amazon Inspector

Mendukung ACL	Tidak

Daftar kontrol akses (ACL) mengontrol pengguna utama (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACL sama dengan kebijakan berbasis sumber daya, meskipun tidak menggunakan format dokumen kebijakan JSON.

ABAC dengan Amazon Inspector

Mendukung ABAC (tanda dalam kebijakan)	Parsial

Kontrol akses berbasis atribut (ABAC) adalah strategi otorisasi yang menentukan izin berdasarkan atribut. Dalam AWS, atribut ini disebut tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke banyak AWS sumber daya. Pemberian tanda ke entitas dan sumber daya adalah langkah pertama dari ABAC. Kemudian rancanglah kebijakan ABAC untuk mengizinkan operasi-operasi ketika tanda milik pengguna utama cocok dengan tanda yang ada di sumber daya yang ingin diakses.

ABAC sangat berguna di lingkungan yang berkembang dengan cepat dan berguna dalam situasi di mana pengelolaan kebijakan menjadi rumit.

Untuk mengendalikan akses berdasarkan tag, berikan informasi tentang tanda di elemen syarat dari sebuh kebijakan dengan menggunakan kunci-kunci persyaratan `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`*, atau `aws:TagKeys`.

Jika sebuah layanan mendukung ketiga kunci kondisi untuk setiap jenis sumber daya, nilainya adalah Ya untuk layanan tersebut. Jika suatu layanan mendukung ketiga kunci kondisi hanya untuk beberapa jenis sumber daya, nilainya adalah Parsial.

Untuk informasi selengkapnya tentang ABAC, lihat Apa itu ABAC? di Panduan Pengguna IAM. Untuk melihat tutorial terkait langkah-langkah penyiapan ABAC, lihat Menggunakan kontrol akses berbasis atribut (ABAC) di Panduan Pengguna IAM.

Menggunakan kredensial sementara dengan Amazon Inspector

Mendukung kredensial sementara	Ya

Beberapa Layanan AWS tidak berfungsi saat Anda masuk menggunakan kredensi sementara. Untuk informasi tambahan, termasuk yang Layanan AWS bekerja dengan kredensi sementara, lihat Layanan AWS yang bekerja dengan IAM di Panduan Pengguna IAM.

Anda menggunakan kredensi sementara jika Anda masuk AWS Management Console menggunakan metode apa pun kecuali nama pengguna dan kata sandi. Misalnya, ketika Anda mengakses AWS menggunakan tautan masuk tunggal (SSO) perusahaan Anda, proses tersebut secara otomatis membuat kredensil sementara. Anda juga akan membuat kredensial sementara secara otomatis saat masuk ke konsol sebagai pengguna dan kemudian beralih peran. Untuk informasi selengkapnya tentang cara beralih peran, lihat Beralih peran (konsol) di Panduan Pengguna IAM.

Anda dapat membuat kredensyal sementara secara manual menggunakan API AWS CLI atau AWS . Anda kemudian dapat menggunakan kredensi sementara tersebut untuk mengakses. AWS AWS merekomendasikan agar Anda secara dinamis menghasilkan kredensi sementara alih-alih menggunakan kunci akses jangka panjang. Untuk informasi selengkapnya, lihat Kredensial keamanan sementara di IAM.

Izin utama lintas layanan untuk Amazon Inspector

Mendukung sesi akses maju (FAS)	Ya

Saat Anda menggunakan pengguna atau peran IAM untuk melakukan tindakan AWS, Anda dianggap sebagai prinsipal. Ketika Anda menggunakan beberapa layanan, Anda mungkin melakukan tindakan yang kemudian memulai tindakan lain di layanan yang berbeda. FAS menggunakan izin dari pemanggilan utama Layanan AWS, dikombinasikan dengan permintaan Layanan AWS untuk membuat permintaan ke layanan hilir. Permintaan FAS hanya dibuat ketika layanan menerima permintaan yang memerlukan interaksi dengan orang lain Layanan AWS atau sumber daya untuk menyelesaikannya. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan ketika mengajukan permintaan FAS, lihat Meneruskan sesi akses.

Peran layanan untuk Amazon Inspector

Mendukung peran layanan	Tidak

Peran layanan adalah sebuah peran IAM yang diambil oleh sebuah layanan untuk melakukan tindakan atas nama Anda. Administrator IAM dapat membuat, mengubah, dan menghapus peran

layanan dari dalam IAM. Untuk informasi selengkapnya, lihat Membuat peran untuk mendelegasikan izin ke Layanan AWS dalam Panduan pengguna IAM.

> **Warning**
>
> Mengubah izin untuk peran layanan dapat merusak fungsionalitas Amazon Inspector. Edit peran layanan hanya jika Amazon Inspector memberikan panduan untuk melakukannya.

Peran terkait layanan untuk Amazon Inspector

Mendukung peran yang terkait layanan	Ya

Peran terkait layanan adalah jenis peran layanan yang ditautkan ke. Layanan AWS Layanan tersebut dapat mengambil peran untuk melakukan sebuah tindakan atas nama Anda. Peran terkait layanan muncul di Anda Akun AWS dan dimiliki oleh layanan. Administrator IAM dapat melihat, tetapi tidak dapat mengedit izin untuk peran terkait layanan.

Untuk detail tentang membuat atau mengelola peran terkait layanan, lihat Layanan AWS bahwa bekerja dengan IAM. Temukan sebuah layanan dalam tabel yang memiliki `Yes` di kolom Peran terkait layanan. Pilih tautan Ya untuk melihat dokumentasi peran terkait layanan untuk layanan tersebut.

Contoh kebijakan berbasis identitas untuk Amazon Inspector

Secara default, pengguna dan peran tidak memiliki izin untuk membuat atau memodifikasi sumber daya Amazon Inspector. Mereka juga tidak dapat melakukan tugas dengan menggunakan AWS Management Console, AWS Command Line Interface (AWS CLI), atau AWS API. Untuk memberikan izin kepada pengguna untuk melakukan tindakan pada sumber daya yang mereka perlukan, administrator IAM dapat membuat kebijakan IAM. Administrator kemudian dapat menambahkan kebijakan IAM ke peran, dan pengguna dapat menjalankan peran.

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

Untuk detail tentang tindakan dan jenis sumber daya yang ditentukan oleh Amazon Inspector, termasuk format ARN untuk setiap jenis sumber daya, lihat Kunci tindakan, sumber daya, dan kondisi untuk Amazon Inspector di Referensi Otorisasi Layanan.

Topik

Praktik terbaik kebijakan

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

- Mulailah dengan kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit — Untuk mulai memberikan izin kepada pengguna dan beban kerja Anda, gunakan kebijakan AWS terkelola yang memberikan izin untuk banyak kasus penggunaan umum. Mereka tersedia di Anda Akun AWS. Kami menyarankan Anda mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola AWS pelanggan yang khusus untuk kasus penggunaan Anda. Untuk informasi selengkapnya, lihat kebijakan yang dikelola AWS atau kebijakan yang dikelola AWS untuk fungsi pekerjaan di Panduan Pengguna IAM.
- Menerapkan izin dengan hak akses paling rendah – Ketika Anda menetapkan izin dengan kebijakan IAM, hanya berikan izin yang diperlukan untuk melakukan tugas. Anda melakukan ini dengan menentukan tindakan yang dapat diambil pada sumber daya tertentu dalam kondisi tertentu, juga dikenal sebagai izin hak akses paling rendah. Untuk informasi selengkapnya tentang cara menggunakan IAM untuk menerapkan izin, lihat Kebijakan dan izin di IAM di Panduan Pengguna IAM.
- Gunakan kondisi dalam kebijakan IAM untuk membatasi akses lebih lanjut – Anda dapat menambahkan kondisi ke kebijakan Anda untuk membatasi akses ke tindakan dan sumber daya. Misalnya, Anda dapat menulis syarat kebijakan untuk menentukan bahwa semua pengajuan harus dikirim menggunakan SSL. Anda juga dapat menggunakan ketentuan untuk memberikan akses ke tindakan layanan jika digunakan melalui yang spesifik Layanan AWS, seperti AWS CloudFormation. Untuk informasi selengkapnya, lihat Elemen kebijakan JSON IAM: Syarat di Panduan Pengguna IAM.

- Menggunakan IAM Access Analyzer untuk memvalidasi kebijakan IAM Anda guna memastikan izin yang aman dan berfungsi – IAM Access Analyzer memvalidasi kebijakan baru dan yang sudah ada sehingga kebijakan tersebut mematuhi bahasa kebijakan IAM (JSON) dan praktik terbaik IAM. IAM Access Analyzer menyediakan lebih dari 100 pemeriksaan kebijakan dan rekomendasi yang dapat ditindaklanjuti untuk membantu Anda membuat kebijakan yang aman dan fungsional. Untuk informasi selengkapnya, lihat validasi kebijakan Analizer Akses IAM di Panduan Pengguna IAM.
- Memerlukan otentikasi multi-faktor (MFA) - Jika Anda memiliki skenario yang mengharuskan pengguna IAM atau pengguna root di Anda, Akun AWS aktifkan MFA untuk keamanan tambahan. Untuk mewajibkan MFA saat operasi API dipanggil, tambahkan kondisi MFA pada kebijakan Anda. Untuk informasi selengkapnya, lihat Mengonfigurasi akses API yang dilindungi MFA di Panduan Pengguna IAM.

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

Menggunakan konsol Amazon Inspector

Untuk mengakses konsol Amazon Inspector tersebut, Anda harus memiliki rangkaian izin minimum. Izin ini harus memungkinkan Anda untuk membuat daftar dan melihat detail tentang sumber daya Amazon Inspector di Anda. Akun AWS Jika Anda membuat kebijakan berbasis identitas yang lebih ketat daripada izin minimum yang diperlukan, konsol tidak akan berfungsi sebagaimana mestinya untuk entitas (pengguna atau peran) dengan kebijakan tersebut.

Anda tidak perlu mengizinkan izin konsol minimum untuk pengguna yang melakukan panggilan hanya ke AWS CLI atau AWS API. Sebaliknya, izinkan akses hanya ke tindakan yang cocok dengan operasi API yang coba dilakukan.

Untuk memastikan bahwa pengguna dan peran masih dapat menggunakan konsol Amazon Inspector, lampirkan juga Amazon `ConsoleAccess` Inspector `ReadOnly` AWS atau kebijakan terkelola ke entitas. Untuk informasi selengkapnya, lihat Menambahkan izin ke pengguna di Panduan Pengguna IAM.

Izinkan pengguna melihat izin mereka sendiri

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

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Izinkan akses hanya-baca ke semua sumber daya Amazon Inspector

Contoh ini menunjukkan kebijakan yang memungkinkan akses hanya-baca ke semua sumber daya Amazon Inspector.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
```

```
            "Action": [
                "inspector2:Describe*",
                "inspector2:Get*",
                "inspector2:BatchGet*",
                "inspector2:List*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "organizations:ListDelegatedAdministrators",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization"
            ],
            "Resource": "*"
        }
    ]
}
```

Izinkan akses penuh ke semua sumber daya Amazon Inspector

Contoh ini menunjukkan kebijakan yang memungkinkan akses penuh ke semua sumber daya Amazon Inspector.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "inspector2:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "inspector2.amazonaws.com"
                }
```

```
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "organizations:EnableAWSServiceAccess",
                "organizations:RegisterDelegatedAdministrator",
                "organizations:ListDelegatedAdministrators",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS kebijakan terkelola untuk Amazon Inspector

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

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

Anda tidak dapat mengubah izin yang ditentukan dalam kebijakan AWS terkelola. Jika AWS memperbarui izin yang ditentukan dalam kebijakan AWS terkelola, pembaruan akan memengaruhi semua identitas utama (pengguna, grup, dan peran) yang dilampirkan kebijakan tersebut. AWS kemungkinan besar akan memperbarui kebijakan AWS terkelola saat baru Layanan AWS diluncurkan atau operasi API baru tersedia untuk layanan yang ada.

Untuk informasi selengkapnya, lihat Kebijakan yang dikelola AWS dalam Panduan Pengguna IAM.

AWS kebijakan terkelola: AmazonInspector2FullAccess

Anda dapat melampirkan kebijakan `AmazonInspector2FullAccess` ke identitas IAM Anda.

Kebijakan ini memberikan izin administratif yang memungkinkan akses penuh ke Amazon Inspector.

Detail izin

Kebijakan ini mencakup izin berikut.

- `inspector2`— Memungkinkan akses penuh ke fungsionalitas Amazon Inspector.
- `iam`— Memungkinkan Amazon Inspector untuk membuat peran terkait layanan,. `AmazonInspector2AgentlessServiceRole` Ini diperlukan agar Amazon Inspector dapat melakukan operasi seperti mengambil informasi tentang instans Amazon EC2 Anda dan repositori Amazon ECR serta gambar kontainer, menganalisis jaringan VPC Anda, dan menjelaskan akun yang terkait dengan organisasi Anda. Untuk informasi selengkapnya, lihat Menggunakan peran tertaut layanan untuk Amazon Inspector.
- `organizations`— Memungkinkan administrator menggunakan Amazon Inspector untuk organisasi di. AWS Organizations Setelah mengaktifkan akses tepercaya untuk Amazon Inspector AWS Organizations, anggota akun administrator yang didelegasikan dapat mengelola setelan dan melihat temuan di seluruh organisasi mereka.
- `codeguru-security`— Memungkinkan administrator menggunakan Amazon Inspector untuk mengambil cuplikan kode informasi dan mengubah pengaturan enkripsi untuk kode yang disimpan oleh Keamanan. CodeGuru Untuk informasi selengkapnya, lihat Enkripsi saat istirahat untuk kode dalam temuan Anda.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": "inspector2:*",
   "Resource": "*"
  },
  {
   "Effect": "Allow",
```

```
    "Action": [
     "codeguru-security:BatchGetFindings",
     "codeguru-security:GetAccountConfiguration",
     "codeguru-security:UpdateAccountConfiguration"
    ],
    "Resource": "*"
   },
   {
    "Effect": "Allow",
    "Action": "iam:CreateServiceLinkedRole",
    "Resource": "*",
    "Condition": {
     "StringEquals": {
      "iam:AWSServiceName": "inspector2.amazonaws.com"
     }
    }
   },
   {
    "Effect": "Allow",
    "Action": [
     "organizations:EnableAWSServiceAccess",
     "organizations:RegisterDelegatedAdministrator",
     "organizations:ListDelegatedAdministrators",
     "organizations:ListAWSServiceAccessForOrganization",
     "organizations:DescribeOrganizationalUnit",
     "organizations:DescribeAccount",
     "organizations:DescribeOrganization"
    ],
    "Resource": "*"
   }
  ]
}
```

AWS kebijakan terkelola: AmazonInspector2ReadOnlyAccess

Anda dapat melampirkan kebijakan `AmazonInspector2ReadOnlyAccess` ke identitas IAM Anda.

Kebijakan ini memberikan izin yang memungkinkan akses hanya-baca ke Amazon Inspector.

Detail izin

Kebijakan ini mencakup izin berikut.

- `inspector2`— Memungkinkan akses read-only ke fungsionalitas Amazon Inspector.
- `organizations`— Memungkinkan detail tentang cakupan Amazon Inspector untuk organisasi yang akan AWS Organizations dilihat.
- `codeguru-security`— Memungkinkan cuplikan kode diambil dari Keamanan. CodeGuru Juga memungkinkan pengaturan enkripsi untuk kode Anda yang disimpan di CodeGuru Keamanan untuk dilihat.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "organizations:ListDelegatedAdministrators",
    "organizations:ListAWSServiceAccessForOrganization",
    "organizations:DescribeOrganizationalUnit",
    "organizations:DescribeAccount",
    "organizations:DescribeOrganization",
    "inspector2:BatchGet*",
    "inspector2:List*",
    "inspector2:Describe*",
    "inspector2:Get*",
    "inspector2:Search*",
    "codeguru-security:BatchGetFindings",
    "codeguru-security:GetAccountConfiguration"
   ],
   "Resource": "*"
  }
 ]
}
```

AWS kebijakan terkelola: AmazonInspector2ManagedCisPolicy

Anda dapat melampirkan `AmazonInspector2ManagedCisPolicy` kebijakan ke entitas IAM Anda. Kebijakan ini harus dilampirkan ke peran yang memberikan izin ke instans Amazon EC2 Anda untuk menjalankan pemindaian CIS instance. Anda dapat menggunakan peran IAM untuk mengelola kredensional sementara untuk aplikasi yang berjalan pada instans EC2 dan membuat AWS CLI atau permintaan API. AWS Cara ini lebih dianjurkan daripada menyimpan kunci akses

dalam instans EC2. Untuk menetapkan AWS peran ke instans EC2 dan membuatnya tersedia untuk semua aplikasinya, Anda membuat profil instance yang dilampirkan ke instance. Profil instans berisi peran dan memungkinkan program yang berjalan di instans EC2 mendapatkan kredensial sementara. Untuk informasi selengkapnya, lihat Menggunakan peran IAM untuk memberikan izin ke aplikasi yang berjalan di instans Amazon EC2 dalam Panduan Pengguna IAM.

Detail izin

Kebijakan ini mencakup izin berikut.

- `inspector2`— Memungkinkan akses ke tindakan yang digunakan untuk menjalankan pemindaian CIS.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
            "inspector2:StartCisSession",
            "inspector2:StopCisSession",
            "inspector2:SendCisSessionTelemetry",
            "inspector2:SendCisSessionHealth"
            ],
            "Resource": "*",
        }
     ]
 }
```

AWS kebijakan terkelola: AmazonInspector2ServiceRolePolicy

Anda tidak dapat melampirkan kebijakan `AmazonInspector2ServiceRolePolicy` ke entitas IAM Anda. Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan Amazon Inspector melakukan tindakan atas nama Anda. Untuk informasi selengkapnya, lihat Menggunakan peran tertaut layanan untuk Amazon Inspector.

AWS kebijakan terkelola: AmazonInspector2AgentlessServiceRolePolicy

Anda tidak dapat melampirkan kebijakan `AmazonInspector2AgentlessServiceRolePolicy` ke entitas IAM Anda. Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan Amazon

Inspector melakukan tindakan atas nama Anda. Untuk informasi selengkapnya, lihat Menggunakan peran tertaut layanan untuk Amazon Inspector.

Amazon Inspector memperbarui kebijakan terkelola AWS

Lihat detail tentang pembaruan kebijakan AWS terkelola untuk Amazon Inspector sejak layanan ini mulai melacak perubahan ini. Untuk peringatan otomatis tentang perubahan pada halaman ini, berlangganan umpan RSS di halaman riwayat Dokumen Amazon Inspector.

Perubahan	Deskripsi	Tanggal
AmazonInspector2 ManagedCisPolicy — Kebijakan baru	Amazon Inspector telah menambahkan kebijakan terkelola baru yang dapat Anda gunakan sebagai bagian dari profil instans untuk mengizinkan pemindaian CIS pada instans.	23 Januari 2024
AmazonInspector2 ServiceRolePolicy - Pembaruan untuk kebijakan yang ada	Amazon Inspector telah menambahkan izin baru yang memungkinkan Amazon Inspector untuk memulai pemindaian CIS pada instance target.	23 Januari 2024
AmazonInspector2 AgentlessServiceRolePolicy — Kebijakan baru	Amazon Inspector telah menambahkan kebijakan peran terkait layanan baru untuk memungkinkan pemindaian instans EC2 tanpa agen.	27 November 2023
AmazonInspector2 ReadOnlyAccess -	Amazon Inspector telah menambahkan izin baru yang memungkinkan pengguna	September 22, 2023

Perubahan	Deskripsi	Tanggal
Pembaruan untuk kebijakan yang ada	hanya-baca untuk mengambil detail intelijen kerentanan untuk temuan kerentanan paket.	
AmazonInspector2 ServiceRolePolicy - Pembaruan untuk kebijakan yang ada	Amazon Inspector telah menambahkan izin baru yang memungkinkan Amazon Inspector memindai konfigurasi jaringan instans Amazon EC2 yang merupakan bagian dari grup target Elastic Load Balancing.	31 Agustus 2023
AmazonInspector2 ReadOnlyAccess - Pembaruan untuk kebijakan yang ada	Amazon Inspector telah menambahkan izin baru yang memungkinkan pengguna read-only untuk mengekspor Software Bill of Materials (SBOM) untuk sumber daya mereka.	29 Juni 2023
AmazonInspector2 ReadOnlyAccess - Pembaruan untuk kebijakan yang ada	Amazon Inspector telah menambahkan izin baru yang memungkinkan pengguna hanya-baca untuk mengambil detail pengaturan enkripsi untuk temuan pemindaian kode Lambda untuk akun mereka.	13 Juni 2023

Perubahan	Deskripsi	Tanggal
AmazonInspector2 FullAccess - Pembaruan untuk kebijakan yang ada	Amazon Inspector telah menambahkan izin baru yang memungkinkan pengguna mengonfigurasi kunci KMS yang dikelola pelanggan untuk mengenkripsi kode dalam temuan dari pemindaian kode Lambda.	13 Juni 2023
AmazonInspector2 ReadOnlyAccess - Pembaruan untuk kebijakan yang ada	Amazon Inspector telah menambahkan izin baru yang memungkinkan pengguna hanya-baca untuk mengambil detail status pemindaian kode Lambda dan temuan untuk akun mereka.	02 Mei 2023
AmazonInspector2 ServiceRolePolicy - Pembaruan untuk kebijakan yang ada	Amazon Inspector telah menambahkan izin baru yang memungkinkan Amazon Inspector membuat saluran AWS CloudTrail terkait layanan di akun Anda saat Anda mengaktifkan pemindaian Lambda. Hal ini memungkinkan Amazon Inspector untuk memantau CloudTrail peristiwa di akun Anda.	April 30, 2023
AmazonInspector2 FullAccess - Pembaruan untuk kebijakan yang ada	Amazon Inspector telah menambahkan izin baru yang memungkinkan pengguna untuk mengambil rincian temuan kerentanan kode dari pemindaian kode Lambda.	April 21, 2023

Perubahan	Deskripsi	Tanggal
AmazonInspector2 ServiceRolePolicy - Pembaruan untuk kebijakan yang ada	Amazon Inspector telah menambahkan izin baru yang memungkinkan Amazon Inspector mengirim informasi ke Amazon EC2 Systems Manager tentang jalur khusus yang telah ditentukan pelanggan untuk inspeksi mendalam Amazon EC2.	17 April 2023
AmazonInspector2 ServiceRolePolicy - Pembaruan untuk kebijakan yang ada	Amazon Inspector telah menambahkan izin baru yang memungkinkan Amazon Inspector membuat saluran AWS CloudTrail terkait layanan di akun Anda saat Anda mengaktifkan pemindaian Lambda. Hal ini memungkinkan Amazon Inspector untuk memantau CloudTrail peristiwa di akun Anda.	April 30, 2023

Perubahan	Deskripsi	Tanggal
AmazonInspector2 ServiceRolePolicy - Pembaruan untuk kebijakan yang ada	Amazon Inspector telah menambahkan izin baru yang memungkinkan Amazon Inspector untuk meminta pemindaian kode pengembang dalam AWS Lambda fungsi, dan menerima data pemindaian dari Amazon Security. CodeGuru Selain itu, Amazon Inspector telah menambahkan izin untuk meninjau kebijakan IAM. Amazon Inspector menggunakan informasi ini untuk memindai fungsi Lambda untuk kerentanan kode.	28 Februari 2023
AmazonInspector2 ServiceRolePolicy - Pembaruan untuk kebijakan yang ada	Amazon Inspector telah menambahkan pernyataan baru yang memungkinkan Amazon Inspector untuk mengambil informasi CloudWatch dari tentang kapan AWS Lambda fungsi terakhir dipanggil. Amazon Inspector menggunakan informasi ini untuk memfokuskan pemindaian pada fungsi Lambda di lingkungan Anda yang telah aktif dalam 90 hari terakhir.	Februari 20, 2023

Perubahan	Deskripsi	Tanggal
AmazonInspector2 ServiceRolePolicy - Pembaruan untuk kebijakan yang ada	Amazon Inspector telah menambahkan pernyataan baru yang memungkinkan Amazon Inspector untuk mengambil informasi AWS Lambda tentang fungsi, termasuk setiap versi lapisan yang terkait dengan setiap fungsi. Amazon Inspector menggunakan informasi ini untuk memindai fungsi Lambda untuk kerentanan keamanan.	28 November 2022
AmazonInspector2 ServiceRolePolicy - Pembaruan untuk kebijakan yang ada	Amazon Inspector telah menambahkan tindakan baru untuk memungkinkan Amazon Inspector menggamba rkan eksekusi asosiasi SSM. Selain itu, Amazon Inspector telah menambahk an pelingkupan sumber daya tambahan untuk memungkin kan Amazon Inspector membuat, memperbarui, menghapus, dan memulai asosiasi SSM dengan dokumen SSM yang dimiliki. `AmazonInspector2`	31 Agustus 2022

Perubahan	Deskripsi	Tanggal
AmazonInspector2 ServiceRolePolicy Pembaruan untuk kebijakan yang ada	Amazon Inspector telah memperbarui pelingkupan sumber daya kebijakan untuk memungkinkan Amazon Inspector mengumpulkan inventaris perangkat lunak di partisi lain. AWS	12 Agustus 2022
AmazonInspector2 ServiceRolePolicy - Pembaruan untuk kebijakan yang ada	Amazon Inspector telah merestrukturisasi pelingkup an sumber daya dari tindakan yang memungkinkan Amazon Inspector membuat, menghapus, dan memperbarui asosiasi SSM.	Agustus 10, 2022
AmazonInspector2 ReadOnlyAccess — Kebijakan baru	Amazon Inspector menambahkan kebijakan baru untuk mengizinkan akses hanya-baca ke fungsionalitas Amazon Inspector.	Januari 21, 2022
AmazonInspector2 FullAccess — Kebijakan baru	Amazon Inspector menambahkan kebijakan baru untuk memungkinkan akses penuh ke fungsionalitas Amazon Inspector.	29 November 2021
AmazonInspector2 ServiceRolePolicy — Kebijakan baru	Amazon Inspector menambahkan kebijakan baru untuk mengizinkan Amazon Inspector melakukan tindakan di layanan lain atas nama Anda.	29 November 2021

Perubahan	Deskripsi	Tanggal
Amazon Inspector mulai melacak perubahan	Amazon Inspector mulai melacak perubahan untuk kebijakan yang AWS dikelola.	29 November 2021

Menggunakan peran tertaut layanan untuk Amazon Inspector

Amazon Inspector menggunakan peran terkait layanan AWS Identity and Access Management (IAM) bernama. `AWSServiceRoleForAmazonInspector2` Peran terkait layanan ini adalah peran IAM yang ditautkan langsung ke Amazon Inspector. Ini telah ditentukan sebelumnya oleh Amazon Inspector dan mencakup semua izin yang diperlukan oleh Amazon Inspector untuk memanggil orang lain atas nama Anda. Layanan AWS

Peran tertaut layanan mempermudah pengaturan Amazon Inspector karena Anda tidak perlu menambahkan izin yang diperlukan secara manual. Amazon Inspector mendefinisikan izin peran terkait layanan dan, kecuali ditentukan lain, hanya Amazon Inspector yang dapat mengambil peran tersebut. Izin yang ditentukan mencakup kebijakan kepercayaan dan kebijakan izin, serta bahwa kebijakan izin tidak dapat dilampirkan ke entitas IAM lainnya.

Anda harus mengonfigurasi izin untuk mengizinkan entitas IAM (seperti grup atau peran) membuat, mengedit, atau menghapus peran terkait layanan. Untuk informasi selengkapnya, lihat Izin peran tertaut layanan dalam Panduan Pengguna IAM. Anda dapat menghapus peran terkait layanan hanya setelah menghapus sumber daya terkait. Ini melindungi sumber daya Amazon Inspector karena Anda tidak dapat secara tidak sengaja menghapus izin untuk mengakses sumber daya.

Untuk informasi tentang layanan lain yang mendukung peran terkait layanan, silakan lihat layanan AWS yang bisa digunakan dengan IAM dan carilah layanan yang memiliki opsi Ya di kolom Peran terkait layanan. Pilih Ya dengan tautan untuk meninjau dokumentasi peran terkait layanan untuk layanan tersebut.

Izin peran tertaut layanan untuk Amazon Inspector

Amazon Inspector menggunakan peran tertaut layanan bernama `AWSServiceRoleForAmazonInspector2`. Peran terkait layanan ini mempercayai `inspector2.amazonaws.com` layanan untuk mengambil peran tersebut.

Kebijakan izin untuk peran, yang diberi nama`AmazonInspector2ServiceRolePolicy`, memungkinkan Amazon Inspector untuk melakukan tugas-tugas seperti:

- Gunakan tindakan Amazon Elastic Compute Cloud (Amazon EC2) untuk mengambil informasi tentang instans dan jalur jaringan Anda.
- Gunakan AWS Systems Manager tindakan untuk mengambil inventaris dari instans Amazon EC2 Anda, dan untuk mengambil informasi tentang paket pihak ketiga dari jalur khusus.
- Gunakan AWS Systems Manager `SendCommand` tindakan untuk memanggil pemindaian CIS untuk instance target.
- Gunakan tindakan Amazon Elastic Container Registry untuk mengambil informasi tentang gambar kontainer Anda.
- Gunakan AWS Lambda tindakan untuk mengambil informasi tentang fungsi Lambda Anda.
- Gunakan AWS Organizations tindakan untuk mendeskripsikan akun terkait.
- Gunakan CloudWatch tindakan untuk mengambil informasi tentang terakhir kali fungsi Lambda Anda dipanggil.
- Gunakan tindakan IAM tertentu untuk mengambil informasi tentang kebijakan IAM Anda yang dapat membuat kerentanan keamanan dalam kode Lambda Anda.
- Gunakan tindakan CodeGuru Keamanan untuk melakukan pemindaian kode di fungsi Lambda Anda. Amazon Inspector menggunakan tindakan CodeGuru Keamanan berikut:
  - codeguru-security: CreateScan — Memberikan izin untuk membuat pemindaian Keamanan. CodeGuru
  - codeguru-security: GetScan — Memberikan izin untuk mengambil CodeGuru metadata pemindaian Keamanan.
  - codeguru-security: ListFindings — Memberikan izin untuk mengambil temuan yang dihasilkan oleh Keamanan. CodeGuru
  - codeguru-security: DeleteScansByCategory - Memberikan izin untuk CodeGuru Keamanan untuk menghapus pemindaian yang diprakarsai oleh Amazon Inspector.
  - codeguru-security: BatchGetFindings — Memberikan izin untuk mengambil sekumpulan temuan spesifik yang dihasilkan oleh Keamanan. CodeGuru
- Gunakan tindakan Elastic Load Balancing tertentu untuk membentuk pemindaian jaringan instans EC2 yang merupakan bagian dari kelompok target Elastic Load Balancing.

Peran dikonfigurasi dengan kebijakan izin berikut.

```
    {
"Version": "2012-10-17",
"Statement": [
 {
  "Sid": "TirosPolicy",
  "Effect": "Allow",
  "Action": [
   "directconnect:DescribeConnections",
   "directconnect:DescribeDirectConnectGatewayAssociations",
   "directconnect:DescribeDirectConnectGatewayAttachments",
   "directconnect:DescribeDirectConnectGateways",
   "directconnect:DescribeVirtualGateways",
   "directconnect:DescribeVirtualInterfaces",
   "ec2:DescribeAvailabilityZones",
   "ec2:DescribeCustomerGateways",
   "ec2:DescribeInstances",
   "ec2:DescribeInternetGateways",
   "ec2:DescribeManagedPrefixLists",
   "ec2:DescribeNatGateways",
   "ec2:DescribeNetworkAcls",
   "ec2:DescribeNetworkInterfaces",
   "ec2:DescribePrefixLists",
   "ec2:DescribeRegions",
   "ec2:DescribeRouteTables",
   "ec2:DescribeSecurityGroups",
   "ec2:DescribeSubnets",
   "ec2:DescribeTransitGatewayAttachments",
   "ec2:DescribeTransitGatewayConnects",
   "ec2:DescribeTransitGatewayPeeringAttachments",
   "ec2:DescribeTransitGatewayRouteTables",
   "ec2:DescribeTransitGatewayVpcAttachments",
   "ec2:DescribeTransitGateways",
   "ec2:DescribeVpcEndpointServiceConfigurations",
   "ec2:DescribeVpcEndpoints",
   "ec2:DescribeVpcPeeringConnections",
   "ec2:DescribeVpcs",
   "ec2:DescribeVpnConnections",
   "ec2:DescribeVpnGateways",
   "ec2:GetManagedPrefixListEntries",
   "ec2:GetTransitGatewayRouteTablePropagations",
   "ec2:SearchTransitGatewayRoutes",
   "elasticloadbalancing:DescribeListeners",
```

```
    "elasticloadbalancing:DescribeLoadBalancerAttributes",
    "elasticloadbalancing:DescribeLoadBalancers",
    "elasticloadbalancing:DescribeRules",
    "elasticloadbalancing:DescribeTags",
    "elasticloadbalancing:DescribeTargetGroups",
    "elasticloadbalancing:DescribeTargetGroupAttributes",
    "elasticloadbalancing:DescribeTargetHealth",
    "network-firewall:DescribeFirewall",
    "network-firewall:DescribeFirewallPolicy",
    "network-firewall:DescribeResourcePolicy",
    "network-firewall:DescribeRuleGroup",
    "network-firewall:ListFirewallPolicies",
    "network-firewall:ListFirewalls",
    "network-firewall:ListRuleGroups",
    "tiros:CreateQuery",
    "tiros:GetQueryAnswer"
   ],
   "Resource": [
    "*"
   ]
  },
  {
   "Sid": "PackageVulnerabilityScanning",
   "Effect": "Allow",
   "Action": [
    "ecr:BatchGetImage",
    "ecr:BatchGetRepositoryScanningConfiguration",
    "ecr:DescribeImages",
    "ecr:DescribeRegistry",
    "ecr:DescribeRepositories",
    "ecr:GetAuthorizationToken",
    "ecr:GetDownloadUrlForLayer",
    "ecr:GetRegistryScanningConfiguration",
    "ecr:ListImages",
    "ecr:PutRegistryScanningConfiguration",
    "organizations:DescribeAccount",
    "organizations:DescribeOrganization",
    "organizations:ListAccounts",
    "ssm:DescribeAssociation",
    "ssm:DescribeAssociationExecutions",
    "ssm:DescribeInstanceInformation",
    "ssm:ListAssociations",
    "ssm:ListResourceDataSync"
   ],
```

```
    "Resource": "*"
   },
   {
    "Sid": "LambdaPackageVulnerabilityScanning",
    "Effect": "Allow",
    "Action": [
     "lambda:ListFunctions",
     "lambda:GetFunction",
     "lambda:GetLayerVersion",
     "cloudwatch:GetMetricData"
    ],
    "Resource": "*"
   },
   {
    "Sid": "GatherInventory",
    "Effect": "Allow",
    "Action": [
     "ssm:CreateAssociation",
     "ssm:StartAssociationsOnce",
     "ssm:DeleteAssociation",
     "ssm:UpdateAssociation"
    ],
    "Resource": [
     "arn:aws:ec2:*:*:instance/*",
     "arn:aws:ssm:*:*:document/AmazonInspector2-*",
     "arn:aws:ssm:*:*:document/AWS-GatherSoftwareInventory",
     "arn:aws:ssm:*:*:managed-instance/*",
     "arn:aws:ssm:*:*:association/*"
    ]
   },
   {
    "Sid": "DataSyncCleanup",
    "Effect": "Allow",
    "Action": [
     "ssm:CreateResourceDataSync",
     "ssm:DeleteResourceDataSync"
    ],
    "Resource": [
     "arn:aws:ssm:*:*:resource-data-sync/InspectorResourceDataSync-do-not-delete"
    ]
   },
   {
    "Sid": "ManagedRules",
    "Effect": "Allow",
```

```
    "Action": [
     "events:PutRule",
     "events:DeleteRule",
     "events:DescribeRule",
     "events:ListTargetsByRule",
     "events:PutTargets",
     "events:RemoveTargets"
    ],
    "Resource": [
     "arn:aws:events:*:*:rule/DO-NOT-DELETE-AmazonInspector*ManagedRule"
    ]
   },
   {
    "Sid": "LambdaCodeVulnerabilityScanning",
    "Effect": "Allow",
    "Action": [
     "codeguru-security:CreateScan",
     "codeguru-security:GetAccountConfiguration",
     "codeguru-security:GetFindings",
     "codeguru-security:GetScan",
     "codeguru-security:ListFindings",
     "codeguru-security:BatchGetFindings",
     "codeguru-security:DeleteScansByCategory"
    ],
    "Resource": [
     "*"
    ]
   },
   {
    "Sid": "CodeGuruCodeVulnerabilityScanning",
    "Effect": "Allow",
    "Action": [
     "iam:GetRole",
     "iam:GetRolePolicy",
     "iam:GetPolicy",
     "iam:GetPolicyVersion",
     "iam:ListAttachedRolePolicies",
     "iam:ListPolicies",
     "iam:ListPolicyVersions",
     "iam:ListRolePolicies",
     "lambda:ListVersionsByFunction"
    ],
    "Resource": [
     "*"
```

```
    ],
    "Condition": {
     "ForAnyValue:StringEquals": {
      "aws:CalledVia": [
       "codeguru-security.amazonaws.com"
      ]
     }
    }
   },
   {
    "Sid": "Ec2DeepInspection",
    "Effect": "Allow",
    "Action": [
     "ssm:PutParameter",
     "ssm:GetParameters",
     "ssm:DeleteParameter"
    ],
    "Resource": [
     "arn:aws:ssm:*:*:parameter/inspector-aws/service/inspector-linux-application-paths"
    ],
    "Condition": {
     "StringEquals": {
      "aws:ResourceAccount": "${aws:PrincipalAccount}"
     }
    }
   },
   {
    "Sid": "AllowManagementOfServiceLinkedChannel",
    "Effect": "Allow",
    "Action": [
     "cloudtrail:CreateServiceLinkedChannel",
     "cloudtrail:DeleteServiceLinkedChannel"
    ],
    "Resource": [
     "arn:aws:cloudtrail:*:*:channel/aws-service-channel/inspector2/*"
    ],
    "Condition": {
     "StringEquals": {
      "aws:ResourceAccount": "${aws:PrincipalAccount}"
     }
    }
   },
   {
    "Sid": "AllowListServiceLinkedChannels",
```

```
    "Effect": "Allow",
    "Action": [
     "cloudtrail:ListServiceLinkedChannels"
    ],
    "Resource": [
     "*"
    ],
    "Condition": {
     "StringEquals": {
      "aws:ResourceAccount": "${aws:PrincipalAccount}"
     }
    }
   },
   {
    "Sid": "AllowToRunInvokeCisSpecificDocuments",
    "Effect": "Allow",
    "Action": [
     "ssm:SendCommand",
     "ssm:GetCommandInvocation"
    ],
    "Resource": [
     "arn:aws:ssm:*:*:document/AmazonInspector2-InvokeInspectorSsmPluginCIS"
    ]
   },
   {
    "Sid": "AllowToRunCisCommandsToSpecificResources",
    "Effect": "Allow",
    "Action": [
     "ssm:SendCommand"
    ],
    "Resource": [
     "arn:aws:ec2:*:*:instance/*"
    ],
    "Condition": {
     "StringEquals": {
      "aws:ResourceAccount": "${aws:PrincipalAccount}"
     }
    }
   },
   {
    "Sid": "AllowToPutCloudwatchMetricData",
    "Effect": "Allow",
    "Action": [
     "cloudwatch:PutMetricData"
```

```
    ],
    "Resource": [
     "*"
    ],
    "Condition": {
     "StringEquals": {
      "cloudwatch:namespace": "AWS/Inspector2"
     }
    }
   }
  ]
}
```

Membuat peran tertaut layanan untuk Amazon Inspector

Anda tidak perlu membuat peran tertaut layanan secara manual. Saat Anda mengaktifkan Amazon Inspector di, API AWS Management Console, atau AWS API AWS CLI, Amazon Inspector membuat peran terkait layanan untuk Anda.

Mengedit peran tertaut layanan untuk Amazon Inspector

Amazon Inspector tidak mengizinkan Anda untuk mengedit peran tertaut layanan `AWSServiceRoleForAmazonInspector2`. Setelah peran terkait layanan dibuat, Anda tidak dapat mengubah nama peran karena berbagai entitas mungkin mereferensikan peran tersebut. Namun, Anda dapat mengubah deskripsi peran dengan menggunakan IAM. Untuk informasi selengkapnya, silakan lihat Menyunting peran terkait layanan dalam Panduan Pengguna IAM.

Menghapus peran tertaut layanan untuk Amazon Inspector

Jika Anda tidak perlu lagi menggunakan Amazon Inspector, sebaiknya hapus peran terkait `AWSServiceRoleForAmazonInspector2` layanan. Sebelum Anda dapat menghapus peran, Anda harus menonaktifkan Amazon Inspector di Wilayah AWS setiap tempat itu diaktifkan. Saat Anda menonaktifkan Amazon Inspector, itu tidak menghapus peran untuk Anda. Oleh karena itu, jika Anda mengaktifkan Amazon Inspector lagi, itu dapat menggunakan peran yang ada. Dengan begitu Anda dapat menghindari entitas yang tidak terpakai yang tidak dipantau atau dipelihara secara aktif. Tetapi, Anda harus membersihkan sumber daya peran terkait layanan sebelum menghapusnya secara manual.

Jika Anda menghapus peran tertaut layanan ini dan ingin membuatnya lagi, Anda dapat mengulangi proses yang sama untuk membuat kembali peran tersebut di akun Anda. Saat Anda mengaktifkan Amazon Inspector, Amazon Inspector membuat ulang peran terkait layanan untuk Anda.

> **Note**
>
> Jika layanan Amazon Inspector menggunakan peran saat Anda mencoba menghapus sumber daya, penghapusan mungkin gagal. Jika itu terjadi, tunggu beberapa menit dan kemudian coba operasi lagi.

Anda dapat menggunakan konsol IAM, the AWS CLI, atau AWS API untuk menghapus peran `AWSServiceRoleForAmazonInspector2` terkait layanan. Untuk informasi selengkapnya, silakan lihat Menghapus peran terkait layanan di Panduan Pengguna IAM.

Izin peran terkait layanan untuk pemindaian tanpa agen Amazon Inspector

Pemindaian tanpa agen Amazon Inspector menggunakan peran terkait layanan bernama. `AWSServiceRoleForAmazonInspector2Agentless` SLR ini memungkinkan Amazon Inspector untuk membuat snapshot volume Amazon EBS di akun Anda, lalu mengakses data dari snapshot tersebut. Peran terkait layanan ini mempercayai `agentless.inspector2.amazonaws.com` layanan untuk mengambil peran tersebut.

> **Important**
>
> Pernyataan dalam peran terkait layanan ini mencegah Amazon Inspector melakukan pemindaian tanpa agen pada instans EC2 apa pun yang telah Anda kecualikan dari pemindaian menggunakan tag. `InspectorEc2Exclusion` Selain itu, pernyataan mencegah Amazon Inspector mengakses data terenkripsi dari volume ketika kunci KMS yang digunakan untuk mengenkripsi memiliki tag. `InspectorEc2Exclusion` Untuk informasi selengkapnya, lihat Mengecualikan instance dari pemindaian Amazon Inspector.

Kebijakan izin untuk peran, yang diberi nama`AmazonInspector2AgentlessServiceRolePolicy`, memungkinkan Amazon Inspector untuk melakukan tugas-tugas seperti:

- Gunakan tindakan Amazon Elastic Compute Cloud (Amazon EC2) untuk mengambil informasi tentang instans, volume, dan snapshot EC2 Anda.
  - Gunakan tindakan penandaan Amazon EC2 untuk menandai snapshot untuk pemindaian dengan kunci tag. `InspectorScan`

  - Gunakan tindakan snapshot Amazon EC2 untuk membuat snapshot, beri tag dengan kunci `InspectorScan` tag, lalu hapus snapshot volume Amazon EBS yang telah ditandai dengan kunci tag. `InspectorScan`
- Gunakan tindakan Amazon EBS untuk mengambil informasi dari snapshot yang ditandai dengan kunci tag. `InspectorScan`
- Gunakan tindakan AWS KMS dekripsi pilih untuk mendekripsi snapshot yang dienkripsi dengan kunci yang dikelola pelanggan. AWS KMS Amazon Inspector tidak mendekripsi snapshot ketika kunci KMS yang digunakan untuk mengenkripsi mereka ditandai dengan tag. `InspectorEc2Exclusion`

Peran dikonfigurasi dengan kebijakan izin berikut.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "InstanceIdentification",
   "Effect": "Allow",
   "Action": [
    "ec2:DescribeInstances",
    "ec2:DescribeVolumes",
    "ec2:DescribeSnapshots"
   ],
   "Resource": "*"
  },
  {
   "Sid": "GetSnapshotData",
   "Effect": "Allow",
   "Action": [
    "ebs:ListSnapshotBlocks",
    "ebs:GetSnapshotBlock"
   ],
   "Resource": "arn:aws:ec2:*:*:snapshot/*",
   "Condition": {
    "StringLike": {
     "aws:ResourceTag/InspectorScan": "*"
    }
   }
  },
```

```
{
 "Sid": "CreateSnapshotsAnyInstanceOrVolume",
 "Effect": "Allow",
 "Action": "ec2:CreateSnapshots",
 "Resource": [
  "arn:aws:ec2:*:*:instance/*",
  "arn:aws:ec2:*:*:volume/*"
 ]
},
{
 "Sid": "DenyCreateSnapshotsOnExcludedInstances",
 "Effect": "Deny",
 "Action": "ec2:CreateSnapshots",
 "Resource": "arn:aws:ec2:*:*:instance/*",
 "Condition": {
  "StringEquals": {
   "ec2:ResourceTag/InspectorEc2Exclusion": "true"
  }
 }
},
{
 "Sid": "CreateSnapshotsOnAnySnapshotOnlyWithTag",
 "Effect": "Allow",
 "Action": "ec2:CreateSnapshots",
 "Resource": "arn:aws:ec2:*:*:snapshot/*",
 "Condition": {
  "Null": {
   "aws:TagKeys": "false"
  },
  "ForAllValues:StringEquals": {
   "aws:TagKeys": "InspectorScan"
  }
 }
},
{
 "Sid": "CreateOnlyInspectorScanTagOnlyUsingCreateSnapshots",
 "Effect": "Allow",
 "Action": "ec2:CreateTags",
 "Resource": "arn:aws:ec2:*:*:snapshot/*",
 "Condition": {
  "StringLike": {
   "ec2:CreateAction": "CreateSnapshots"
  },
  "Null": {
```

```
      "aws:TagKeys": "false"
     },
     "ForAllValues:StringEquals": {
      "aws:TagKeys": "InspectorScan"
     }
    }
   },
   {
    "Sid": "DeleteOnlySnapshotsTaggedForScanning",
    "Effect": "Allow",
    "Action": "ec2:DeleteSnapshot",
    "Resource": "arn:aws:ec2:*:*:snapshot/*",
    "Condition": {
     "StringLike": {
      "ec2:ResourceTag/InspectorScan": "*"
     }
    }
   },
   {
    "Sid": "DenyKmsDecryptForExcludedKeys",
    "Effect": "Deny",
    "Action": "kms:Decrypt",
    "Resource": "arn:aws:kms:*:*:key/*",
    "Condition": {
     "StringEquals": {
      "aws:ResourceTag/InspectorEc2Exclusion": "true"
     }
    }
   },
   {
    "Sid": "DecryptSnapshotBlocksVolContext",
    "Effect": "Allow",
    "Action": "kms:Decrypt",
    "Resource": "arn:aws:kms:*:*:key/*",
    "Condition": {
     "StringEquals": {
      "aws:ResourceAccount": "${aws:PrincipalAccount}"
     },
     "StringLike": {
      "kms:ViaService": "ec2.*.amazonaws.com",
      "kms:EncryptionContext:aws:ebs:id": "vol-*"
     }
    }
   },
```

```
  {
   "Sid": "DecryptSnapshotBlocksSnapContext",
   "Effect": "Allow",
   "Action": "kms:Decrypt",
   "Resource": "arn:aws:kms:*:*:key/*",
   "Condition": {
    "StringEquals": {
     "aws:ResourceAccount": "${aws:PrincipalAccount}"
    },
    "StringLike": {
     "kms:ViaService": "ec2.*.amazonaws.com",
     "kms:EncryptionContext:aws:ebs:id": "snap-*"
    }
   }
  },
  {
   "Sid": "DescribeKeysForEbsOperations",
   "Effect": "Allow",
   "Action": "kms:DescribeKey",
   "Resource": "arn:aws:kms:*:*:key/*",
   "Condition": {
    "StringEquals": {
     "aws:ResourceAccount": "${aws:PrincipalAccount}"
    },
    "StringLike": {
     "kms:ViaService": "ec2.*.amazonaws.com"
    }
   }
  },
  {
   "Sid": "ListKeyResourceTags",
   "Effect": "Allow",
   "Action": "kms:ListResourceTags",
   "Resource": "arn:aws:kms:*:*:key/*"
  }
 ]
}
```

Membuat peran terkait layanan untuk pemindaian tanpa agen

Anda tidak perlu membuat peran tertaut layanan secara manual. Saat Anda mengaktifkan Amazon Inspector di, API AWS Management Console, atau AWS API AWS CLI, Amazon Inspector membuat peran terkait layanan untuk Anda.

Mengedit peran terkait layanan untuk pemindaian tanpa agen

Amazon Inspector tidak mengizinkan Anda untuk mengedit peran tertaut layanan `AWSServiceRoleForAmazonInspector2Agentless`. Setelah peran terkait layanan dibuat, Anda tidak dapat mengubah nama peran karena berbagai entitas mungkin mereferensikan peran tersebut. Namun, Anda dapat mengubah deskripsi peran dengan menggunakan IAM. Untuk informasi selengkapnya, silakan lihat Menyunting peran terkait layanan dalam Panduan Pengguna IAM.

Menghapus peran terkait layanan untuk pemindaian tanpa agen

Jika Anda tidak perlu lagi menggunakan fitur atau layanan yang memerlukan peran tertaut layanan, sebaiknya Anda menghapus peran tersebut. Dengan begitu, Anda tidak memiliki entitas yang tidak digunakan yang tidak dipantau atau dikelola secara aktif.

> **Important**
>
> Untuk menghapus `AWSServiceRoleForAmazonInspector2Agentless` peran, Anda harus mengatur mode pemindaian Anda ke berbasis agen di semua Wilayah di mana pemindaian tanpa agen tersedia. Untuk informasi lebih lanjut, lihat [Tautan mode pemindaian pengaturan TBD].

Untuk menghapus peran terkait layanan secara manual menggunakan IAM

Gunakan konsol IAM, the AWS CLI, atau AWS API untuk menghapus peran AWSServiceRoleForAmazonInspector2Agentless terkait layanan. Untuk informasi selengkapnya, silakan lihat Menghapus peran terkait layanan di Panduan Pengguna IAM.

Pemecahan masalah identitas dan akses Amazon Inspector

Gunakan informasi berikut untuk membantu Anda mendiagnosis dan mengatasi masalah umum yang mungkin Anda temui saat bekerja menggunakan Amazon Inspector dan IAM.

Topik

- Saya tidak berwenang untuk melakukan tindakan di Amazon Inspector
- Saya tidak berwenang untuk melakukan iam: PassRole
- Saya ingin mengizinkan orang di luar saya Akun AWS untuk mengakses sumber daya Amazon Inspector saya

Saya tidak berwenang untuk melakukan tindakan di Amazon Inspector

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

Contoh kesalahan berikut terjadi ketika pengguna IAM `mateojackson` mencoba menggunakan konsol untuk melihat detail tentang suatu sumber daya *`my-example-widget`* rekaan, tetapi tidak memiliki izin `inspector2:`*`GetWidget`* rekaan.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 inspector2:GetWidget on resource: my-example-widget
```

Dalam hal ini, kebijakan untuk pengguna `mateojackson` harus diperbarui untuk mengizinkan akses ke sumber daya *`my-example-widget`* dengan menggunakan tindakan `inspector2:`*`GetWidget`*.

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

Saya tidak berwenang untuk melakukan iam: PassRole

Jika Anda menerima kesalahan yang tidak diizinkan untuk melakukan `iam:PassRole` tindakan, kebijakan Anda harus diperbarui agar Anda dapat meneruskan peran ke Amazon Inspector.

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

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

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

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

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

Saya ingin mengizinkan orang di luar saya Akun AWS untuk mengakses sumber daya Amazon Inspector saya

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

Untuk mempelajari selengkapnya, periksa hal berikut:

- Untuk mempelajari apakah Amazon Inspector mendukung fitur ini, lihat Cara kerja Amazon Inspector dengan IAM.
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda di seluruh sumber daya Akun AWS yang Anda miliki, lihat Menyediakan akses ke pengguna IAM di pengguna lain Akun AWS yang Anda miliki di Panduan Pengguna IAM.
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda kepada pihak ketiga Akun AWS, lihat Menyediakan akses yang Akun AWS dimiliki oleh pihak ketiga dalam Panduan Pengguna IAM.
- Untuk mempelajari cara memberikan akses melalui federasi identitas, lihat Memberikan akses kepada pengguna eksternal yang sah (federasi identitas) dalam Panduan Pengguna IAM.
- Untuk mempelajari perbedaan antara penggunaan peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Perbedaan antara peran IAM dan kebijakan berbasis sumber daya di Panduan Pengguna IAM.

Memantau Amazon Inspector

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

- Amazon EventBridge adalah layanan bus acara tanpa server yang memudahkan untuk menghubungkan aplikasi Anda dengan data dari berbagai sumber. EventBridge memberikan aliran data real-time dari aplikasi Anda sendiri, aplikasi oftware-as-a S-Service (SaaS), dan AWS layanan serta rute data tersebut ke target seperti Lambda. Ini memungkinkan Anda memantau

peristiwa yang terjadi di layanan, dan membangun arsitektur berbasis peristiwa. Untuk informasi selengkapnya, lihat Panduan EventBridge Pengguna Amazon.

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

Mencatat panggilan Amazon Inspector API menggunakan AWS CloudTrail

Amazon Inspector terintegrasi dengan AWS CloudTrail, layanan yang menyediakan catatan tindakan yang diambil oleh pengguna atau peran IAM, atau, di Amazon Inspector. Layanan AWS CloudTrail menangkap semua panggilan API untuk Amazon Inspector sebagai peristiwa. Panggilan yang diambil termasuk panggilan dari konsol Amazon Inspector dan panggilan ke operasi Amazon Inspector API. Jika Anda membuat jejak, Anda dapat mengaktifkan pengiriman CloudTrail acara secara berkelanjutan ke bucket Amazon S3, termasuk acara untuk Amazon Inspector. Jika Anda tidak membuat konfigurasi jejak, Anda masih dapat melihat kejadian terbaru dalam konsol CloudTrail di Riwayat peristiwa. Dengan menggunakan informasi yang dikumpulkan oleh CloudTrail, Anda dapat menentukan:

- Permintaan yang diajukan ke Amazon Inspector.
- Alamat IP dari mana permintaan dibuat.
- Siapa yang membuat permintaan.
- Saat permintaan dibuat.

Untuk mempelajari selengkapnya CloudTrail, lihat Panduan AWS CloudTrail Pengguna.

Informasi Amazon Inspector di CloudTrail

CloudTrail diaktifkan pada Akun AWS saat Anda membuat akun. Ketika aktivitas terjadi di Amazon Inspector, aktivitas tersebut dicatat dalam suatu CloudTrail peristiwa bersama dengan Layanan AWS peristiwa lain dalam riwayat Acara. Anda dapat melihat, mencari, dan mengunduh acara terbaru di situs Anda Akun AWS. Untuk informasi selengkapnya, lihat Melihat peristiwa dengan Riwayat CloudTrail acara.

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

- Ikhtisar untuk membuat jejak
- CloudTrail layanan dan integrasi yang didukung
- Mengonfigurasi notifikasi Amazon SNS untuk CloudTrail
- Menerima file CloudTrail log dari beberapa akun
- Menerima file CloudTrail log dari berbagai wilayah

Semua tindakan Amazon Inspector dicatat oleh. CloudTrail Semua tindakan yang dapat dilakukan Amazon Inspector didokumentasikan dalam Referensi API Amazon Inspector. Misalnya, panggilan untuk tindakan `CreateFindingsReport`, `ListCoverage`, dan `UpdateOrganizationConfiguration` menghasilkan entri dalam file log CloudTrail .

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

- Apakah permintaan tersebut dibuat dengan kredensial pengguna root atau pengguna IAM.
- Apakah permintaan tersebut dibuat dengan kredensial keamanan sementara atau tidak untuk peran atau pengguna gabungan.
- Apakah permintaan tersebut dibuat oleh Layanan AWS lain.

Untuk informasi selengkapnya, lihat Elemen userIdentity CloudTrail .

Memahami entri file log Amazon Inspector

Trail adalah konfigurasi yang memungkinkan pengiriman peristiwa sebagai file log ke bucket Amazon S3 yang Anda tentukan. CloudTrail file log berisi satu atau lebih entri log. Peristiwa menunjukkan satu permintaan dari sumber mana pun. Acara mencakup informasi tentang tindakan yang diminta, tanggal dan waktu tindakan, parameter permintaan, dan sebagainya. CloudTrail file log bukanlah

jejak tumpukan yang diurutkan dari panggilan API publik, jadi file tersebut tidak muncul dalam urutan tertentu.

Informasi Amazon Inspector Scan di CloudTrail

Amazon Inspector Scan terintegrasi dengan. CloudTrail Semua operasi API Amazon Inspector Scan dicatat sebagai peristiwa manajemen. Untuk daftar operasi API Amazon Inspector Scan yang dicatat oleh Amazon Inspector, lihat Amazon Inspector CloudTrail Scan di Referensi Amazon Inspector API.

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan `ScanSbom` tindakan:


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROA123456789EXAMPLE:akua_mansa",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/akua_mansa",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROA123456789EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-10-17T15:22:59Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-10-17T16:02:34Z",
    "eventSource": "gamma-inspector-scan.amazonaws.com",
    "eventName": "ScanSbom",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "203.0.113.0",
    "userAgent": "aws-sdk-java/2.20.162 Mac_OS_X/13.5.2 OpenJDK_64-
Bit_Server_VM/17.0.8+7-LTS Java/17.0.8 vendor/Amazon.com_Inc. io/sync http/
UrlConnection cfg/retry-mode/legacy",
```

```
    "requestParameters": {
        "sbom": {
            "specVersion": "1.5",
            "metadata": {
                "component": {
                    "name": "debian",
                    "type": "operating-system",
                    "version": "9"
                }
            },
            "components": [
                {
                    "name": "packageOne",
                    "purl": "pkg:deb/debian/packageOne@1.0.0?arch=x86_64&distro=9",
                    "type": "application"
                }
            ],
            "bomFormat": "CycloneDX"
        }
    },
    "responseElements": null,
    "requestID": "f041a27f-f33e-4f70-b09b-5fbc5927282a",
    "eventID": "abc8d1e4-d214-4f07-bc56-8a31be6e36fe",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```


Validasi Kepatuhan untuk Amazon Inspector

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

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

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

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

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

- AWS Sumber Daya AWS — Kumpulan buku kerja dan panduan ini mungkin berlaku untuk industri dan lokasi Anda.
- AWS Panduan Kepatuhan Pelanggan - Memahami model tanggung jawab bersama melalui lensa kepatuhan. Panduan ini merangkum praktik terbaik untuk mengamankan Layanan AWS dan memetakan panduan untuk kontrol keamanan di berbagai kerangka kerja (termasuk Institut Standar dan Teknologi Nasional (NIST), Dewan Standar Keamanan Industri Kartu Pembayaran (PCI), dan Organisasi Internasional untuk Standardisasi (ISO)).
- Mengevaluasi Sumber Daya dengan Aturan dalam Panduan AWS Config Pengembang — AWS Config Layanan menilai seberapa baik konfigurasi sumber daya Anda mematuhi praktik internal, pedoman industri, dan peraturan.
- AWS Security Hub— Ini Layanan AWS memberikan pandangan komprehensif tentang keadaan keamanan Anda di dalamnya AWS. Security Hub menggunakan kontrol keamanan untuk mengevaluasi sumber daya AWS Anda dan memeriksa kepatuhan Anda terhadap standar industri keamanan dan praktik terbaik. Untuk daftar layanan dan kontrol yang didukung, lihat Referensi kontrol Security Hub.
- AWS Audit ManagerIni Layanan AWS membantu Anda terus mengaudit AWS penggunaan Anda untuk menyederhanakan cara Anda mengelola risiko dan kepatuhan terhadap peraturan dan standar industri.

Ketahanan di Amazon Inspector

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

Keamanan Infrastruktur di Amazon Inspector

Sebagai layanan terkelola, Amazon Inspector dilindungi oleh keamanan jaringan AWS global. Untuk informasi tentang layanan AWS keamanan dan cara AWS melindungi infrastruktur, lihat Keamanan AWS Cloud. Untuk mendesain AWS lingkungan Anda menggunakan praktik terbaik untuk keamanan infrastruktur, lihat Perlindungan Infrastruktur dalam Kerangka Kerja yang AWS Diarsiteksikan dengan Baik Pilar Keamanan.

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

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

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

Respons insiden di Amazon Inspector

Keamanan adalah prioritas tertinggi di AWS. Sebagai bagian dari model tanggung jawab bersama AWS Cloud, AWS mengelola pusat data, jaringan, dan arsitektur perangkat lunak yang memenuhi persyaratan organisasi yang paling sensitif terhadap keamanan. AWS bertanggung jawab atas setiap respons insiden sehubungan dengan AWS Config layanan itu sendiri. Selain itu, sebagai

AWS pelanggan, Anda berbagi tanggung jawab untuk menjaga keamanan di cloud. Ini berarti Anda mengontrol keamanan yang Anda pilih untuk diterapkan dari AWS alat dan fitur yang dapat Anda akses, dan bertanggung jawab atas respons insiden di pihak Anda dari model tanggung jawab bersama.

Dengan menetapkan garis dasar keamanan yang memenuhi tujuan aplikasi Anda yang berjalan di cloud, Anda dapat mendeteksi penyimpangan yang dapat Anda tanggapi. Karena respons insiden keamanan dapat menjadi topik yang kompleks, kami mendorong Anda untuk meninjau sumber daya berikut sehingga Anda lebih dapat memahami dampak respons insiden (IR) dan pilihan Anda terhadap tujuan perusahaan Anda: Panduan Respons Insiden AWS Keamanan, whitepaper Praktik AWS Keamanan Terbaik, dan white paper Perspektif Keamanan AWS Cloud Adoption Framework (CAF).

Amazon Inspector

Amazon Inspector terintegrasi dengan layanan lainAWS. Layanan ini dapat menyerap data dari Amazon Inspector untuk memungkinkan Anda melihat temuan Anda dengan cara baru. Tinjau opsi integrasi berikut untuk mempelajari selengkapnya tentang cara layanan tersebut diatur untuk digunakan dengan Amazon Inspector

Mengintegrasikan Amazon Inspector

Amazon Elastic Container Registry (Amazon ECR) adalah registri kontainer Docker sepenuhnya dikelola yang membuatnya mudah untuk menyimpan, berbagi, dan menyebarkan gambar kontainer. Registri pribadi Amazon ECR meng-host citra kontainer Anda dalam arsitektur yang sangat tersedia dan dapat diskalakan. Anda dapat menggunakan Amazon Inspector untuk memindai gambar kontainer yang berada di repositori Amazon ECR Anda untuk paket sistem operasi yang rentan dan paket bahasa pemrograman.

Untuk informasi selengkapnya tentang menggunakan Amazon Inspector Amazon Inspector, lihat. Integrasi Amazon Inspector dengan Amazon Elastic Container Registry (Amazon ECR)

Integrasi Amazon Inspector dengan AWS Security Hub

AWS Security Hubmengumpulkan data keamanan dari seluruh AWS akun, layanan, dan produk lain yang didukung untuk menilai kondisi keamanan lingkungan Anda sesuai dengan standar industri dan praktik terbaik. Selain mengevaluasi postur keamanan Anda, Security Hub menciptakan lokasi sentral untuk temuan di seluruh AWS layanan yang terintegrasi, dan produk Jaringan AWS Mitra. Mengaktifkan Security Hub dengan Amazon Inspector secara otomatis memungkinkan Security Hub untuk menyerap data temuan Amazon Inspector.

Untuk informasi selengkapnya tentang penggunaan Security Hub dengan Amazon Inspector Integrasi Amazon Inspector dengan AWS Security Hub

Integrasi Amazon Inspector dengan Amazon Elastic Container Registry (Amazon ECR)

Amazon ECR adalah registri kontainer yang dikelola sepenuhnya yang mendukung gambar dan artefak Docker dan OCI. AWS Jika Anda menggunakan Amazon ECR, Anda dapat mengaktifkan pemindaian yang disempurnakan untuk registri Anda agar Amazon Inspector mendeteksi gambar

kontainer Anda secara otomatis dan memindai mereka untuk paket sistem operasi dan paket bahasa pemrograman yang rentan.

Integrasi ini memungkinkan Anda untuk melihat temuan Amazon Inspector untuk gambar kontainer dalam konsol Amazon ECR. Selain itu, dari konsol Amazon ECR Anda dapat mengelola frekuensi pemindaian dan menyempurnakan cakupan pemindaian dengan membuat filter inklusi.

Mengaktifkan integrasi

Anda dapat mengaktifkan integrasi dengan mengaktifkan pemindaian Amazon Inspector melalui konsol Amazon Inspector atau API, atau dengan mengonfigurasi repositori Anda untuk menggunakan pemindaian yang ditingkatkan dengan Amazon Inspector melalui konsol Amazon ECR atau API.

Untuk informasi selengkapnya tentang mengaktifkan integrasi melalui Amazon Inspector, lihat. Pemindaian sumber daya otomatis dengan Amazon Inspector

Untuk informasi tentang mengaktifkan dan mengonfigurasi Pemindaian yang disempurnakan di Amazon ECR, lihat Pemindaian yang Disempurnakan di panduan pengguna Amazon ECR.

Menggunakan integrasi dengan lingkungan multi-akun

Jika Anda adalah anggota di lingkungan multi-akun, Anda dapat mengaktifkan pemindaian yang disempurnakan melalui Amazon ECR. Namun, setelah diaktifkan, itu hanya dapat dinonaktifkan oleh administrator delegasi Amazon Inspector Anda. Jika dinonaktifkan, itu kembali ke pemindaian dasar. Untuk informasi selengkapnya, lihat Menonaktifkan Amazon Inspector.

Integrasi Amazon Inspector dengan AWS Security Hub

Security Hub memberi gambaran menyeluruh tentang status keamanan Anda dalam AWS dan membantu Anda memeriksa lingkungan Anda sesuai standar industri dan praktik terbaik terkait keamanan. Security Hub mengumpulkan data keamanan dari seluruh AWS akun, layanan, dan produk tambahan yang didukung. Anda dapat menggunakan informasi yang diberikannya untuk menganalisis tren keamanan Anda dan mengidentifikasi masalah keamanan prioritas tertinggi.

Integrasi Amazon Inspector dengan Security Hub memungkinkan Anda untuk mengirimkan temuan dari Amazon Inspector ke Security Hub. Security Hub kemudian dapat menyertakan temuan tersebut dalam analisis postur keamanan Anda.

Di AWS Security Hub, masalah keamanan dilacak sebagai temuan. Beberapa temuan dihasilkan dari masalah yang terdeteksi oleh AWS layanan atau produk pihak ketiga. Security Hub juga memiliki

seperangkat aturan yang digunakan untuk mendeteksi masalah keamanan dan menghasilkan temuan. Security Hub menyediakan alat untuk mengelola temuan dari seluruh sumber tersebut. Anda dapat melihat dan mem-filter daftar temuan dan melihat detail temuan. Untuk informasi selengkapnya tentang temuan di Security Hub, lihat Melihat temuan di AWS Security HubPanduan Pengguna. Anda juga dapat melacak status penyelidikan ke temuan. Lihat Mengambil tindakan pada temuan di Panduan Pengguna AWS Security Hub.

Semua temuan di Security Hub menggunakan format JSON standar yang disebut Format Temuan Keamanan AWS (ASFF). ASFF mencakup detail tentang sumber masalah, sumber daya yang terdampak, dan status temuan saat ini. Lihat AWS Security Finding Format (ASFF) di Panduan Pengguna AWS Security Hub.

Security Hub akan mengarsipkan temuan Amazon Inspector setelah temuan tersebut telah ditangani dan ditutup di Amazon Inspector.

Melihat temuan Amazon Inspector tor di AWS Security Hub

Temuan dari Amazon Inspector Classic dan Amazon Inspector baru tersedia di panel yang sama di Security Hub. Namun, Anda dapat memfilter temuan dari Amazon Inspector baru dengan menambahkan a `"aws/inspector/ProductVersion": "2"` ke bilah filter. Menambahkan filter ini tidak termasuk temuan dari Amazon Inspector Classic dari dasbor Security Hub.

Temspector Amazon Inspector tor

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:inspector2:us-east-1:123456789012:finding/FINDING_ID",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/inspector",
  "ProductName": "Inspector",
  "CompanyName": "Amazon",
  "Region": "us-east-1",
  "GeneratorId": "AWSInspector",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Vulnerabilities/CVE"
  ],
  "FirstObservedAt": "2023-01-31T20:25:38Z",
  "LastObservedAt": "2023-05-04T18:18:43Z",
  "CreatedAt": "2023-01-31T20:25:38Z",
  "UpdatedAt": "2023-05-04T18:18:43Z",
  "Severity": {
    "Label": "HIGH",
```

```
    "Normalized": 70
   },
   "Title": "CVE-2022-34918 - kernel",
   "Description": "An issue was discovered in the Linux kernel through 5.18.9. A type
  confusion bug in nft_set_elem_init (leading to a buffer overflow) could be used by a
  local attacker to escalate privileges, a different vulnerability than CVE-2022-32250.
  (The attacker can obtain root access, but must start with an unprivileged user
  namespace to obtain CAP_NET_ADMIN access.) This can be fixed in nft_setelem_parse_data
  in net/netfilter/nf_tables_api.c.",
   "Remediation": {
     "Recommendation": {
       "Text": "Remediation is available. Please refer to the Fixed version in the
  vulnerability details section above. For detailed remediation guidance for each of the
  affected packages, refer to the vulnerabilities section of the detailed finding JSON."
     }
   },
   "ProductFields": {
     "aws/inspector/FindingStatus": "ACTIVE",
     "aws/inspector/inspectorScore": "7.8",
     "aws/inspector/resources/1/resourceDetails/awsEc2InstanceDetails/platform":
  "AMAZON_LINUX_2",
     "aws/inspector/ProductVersion": "2",
     "aws/inspector/instanceId": "i-0f1ed287081bdf0fb",
     "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/inspector/
arn:aws:inspector2:us-east-1:123456789012:finding/FINDING_ID",
     "aws/securityhub/ProductName": "Inspector",
     "aws/securityhub/CompanyName": "Amazon"
   },
   "Resources": [
     {
       "Type": "AwsEc2Instance",
       "Id": "arn:aws:ec2:us-east-1:123456789012:i-0f1ed287081bdf0fb",
       "Partition": "aws",
       "Region": "us-east-1",
       "Tags": {
         "Patch Group": "SSM",
         "Name": "High-SEv-Test"
       },
       "Details": {
         "AwsEc2Instance": {
           "Type": "t2.micro",
           "ImageId": "ami-0cff7528ff583bf9a",
           "IpV4Addresses": [
             "52.87.229.97",
```

```
            "172.31.57.162"
          ],
          "KeyName": "ACloudGuru",
          "IamInstanceProfileArn": "arn:aws:iam::123456789012:instance-profile/
AmazonSSMRoleForInstancesQuickSetup",
          "VpcId": "vpc-a0c2d7c7",
          "SubnetId": "subnet-9c934cb1",
          "LaunchedAt": "2022-07-26T21:49:46Z"
        }
      }
    }
  ],
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "Vulnerabilities": [
    {
      "Id": "CVE-2022-34918",
      "VulnerablePackages": [
        {
          "Name": "kernel",
          "Version": "5.10.118",
          "Epoch": "0",
          "Release": "111.515.amzn2",
          "Architecture": "X86_64",
          "PackageManager": "OS",
          "FixedInVersion": "0:5.10.130-118.517.amzn2",
          "Remediation": "yum update kernel"
        }
      ],
      "Cvss": [
        {
          "Version": "2.0",
          "BaseScore": 7.2,
          "BaseVector": "AV:L/AC:L/Au:N/C:C/I:C/A:C",
          "Source": "NVD"
        },
        {
          "Version": "3.1",
          "BaseScore": 7.8,
          "BaseVector": "CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H",
          "Source": "NVD"
```

```
        },
        {
          "Version": "3.1",
          "BaseScore": 7.8,
          "BaseVector": "CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H",
          "Source": "NVD",
          "Adjustments": []
        }
      ],
      "Vendor": {
        "Name": "NVD",
        "Url": "https://nvd.nist.gov/vuln/detail/CVE-2022-34918",
        "VendorSeverity": "HIGH",
        "VendorCreatedAt": "2022-07-04T21:15:00Z",
        "VendorUpdatedAt": "2022-10-26T17:05:00Z"
      },
      "ReferenceUrls": [
        "https://git.kernel.org/pub/scm/linux/kernel/git/netdev/net.git/commit/?
id=7e6bc1f6cabcd30aba0b11219d8e01b952eacbb6",
        "https://lore.kernel.org/netfilter-devel/cd9428b6-7ffb-dd22-d949-
d86f4869f452@randorisec.fr/T/",
        "https://www.debian.org/security/2022/dsa-5191"
      ],
      "FixAvailable": "YES"
    }
  ],
  "FindingProviderFields": {
    "Severity": {
      "Label": "HIGH"
    },
    "Types": [
      "Software and Configuration Checks/Vulnerabilities/CVE"
    ]
  },
  "ProcessedAt": "2023-05-05T20:28:38.822Z"
}
```


Mengaktifkan dan mengonfigurasikan integrasi

Untuk menggunakan integrasi Amazon Inspector tor denganAWS Security Hub, Anda harus mengaktifkan Security Hub. Untuk informasi tentang cara mengaktifkan Security Hub, lihat Menyiapkan Security Hub di Panduan AWS Security Hub Pengguna.

Saat Anda mengaktifkan Amazon Inspector dan Security Hub, integrasi diaktifkan secara otomatis, dan Amazon Inspector mulai mengirimkan temuan ke Security Hub. Amazon Inspector mengirimkan semua temuan yang dihasilkannya ke Security Hub menggunakan Format Temuan Amazon Inspector mengirimkan semua temuan yang dihasilkannya ke Security Hub menggunakan Format Temtor AWS Keamanan (ASFF).

Menghentikan publikasi temuan ke AWS Security Hub

Cara menghentikan pengiriman temuan

Untuk berhenti mengirim temuan ke Security Hub, Anda dapat menggunakan konsol Security Hub atau API.

Lihat Menonaktifkan dan mengaktifkan aliran temuan dari integrasi (konsol) atau Menonaktifkan aliran temuan dari integrasi (API Security Hub,) di Panduan Pengguna. AWS CLI AWS Security Hub

Sistem operasi dan bahasa pemrograman yang didukung oleh Amazon Inspector

Amazon Inspector dapat memindai aplikasi perangkat lunak yang diinstal pada instans Amazon Elastic Compute Cloud (Amazon EC2), gambar kontainer yang disimpan di repositori Amazon Elastic Container Registry (Amazon ECR), dan fungsi. AWS Lambda Untuk gambar kontainer ECR, Amazon Inspector dapat memindai kerentanan paket sistem operasi dan bahasa pemrograman. Untuk fungsi Lambda, Amazon Inspector dapat memindai kerentanan kode. Saat Amazon Inspector memindai sumber daya, Amazon menggunakan mesin pemindaian yang dibuat khusus dan sumber lebih dari 50 umpan data untuk menghasilkan temuan untuk Common Vulnerabilities and Exposures (CVE). Sumber termasuk penasihat keamanan vendor, NVD, MITRE, umpan sumber terbuka, penelitian internal, dan umpan data berlisensi.

Agar Amazon Inspector dapat memindai sumber daya, sumber daya harus menjalankan sistem operasi yang didukung atau menggunakan bahasa pemrograman yang didukung. Topik di bagian ini mencantumkan sistem operasi, runtime, dan bahasa pemrograman yang saat ini didukung Amazon Inspector untuk berbagai sumber daya dan jenis pemindaian. Mereka juga mencantumkan sistem operasi yang sebelumnya didukung Amazon Inspector, tetapi sejak itu dihentikan oleh vendor. Amazon Inspector hanya dapat memberikan dukungan terbatas untuk sistem operasi setelah vendor menghentikan dukungan untuk sistem operasi.

Topik

Sistem operasi yang didukung: Pemindaian Amazon EC2

Tabel berikut mencantumkan sistem operasi yang saat ini didukung Amazon Inspector untuk pemindaian instans Amazon EC2. Ini juga mencantumkan sumber penasihat keamanan vendor untuk masing-masing, dan apakah sistem operasi itu dapat dipindai menggunakan metode pemindaian berbasis agen atau tanpa agen. Untuk informasi selengkapnya tentang metode pemindaian, lihat Pemindaian berbasis agen danPemindaian tanpa agen.

> **Note**
>
> Deteksi sistem operasi Linux hanya didukung untuk repositori manajer paket default dan tidak termasuk aplikasi pihak ketiga, repositori dukungan yang diperluas (misalnya, BYOS RHEL, PAYG RHEL, dan RHEL untuk SAP), dan repositori opsional, seperti Red Hat Application Streams.

Sistem operasi	Versi	Penasihat keamanan vendor	Dukungan pemindaian tanpa agen	Dukungan pemindaian berbasis agen
AlmaLinux	8	ALSA	Ya	Ya
AlmaLinux	9	ALSA	Ya	Ya
Amazon Linux (AL2)	AL2	SAYANGNYA	Ya	Ya
Amazon Linux 2023 (AL2023)	AL2023	SAYANGNYA	Ya	Ya
Bottlerocket	1.7.0 dan yang lebih baru	GHSA, CVE	Tidak	Ya
CentOS Linux (CentOS)	7	CESA	Ya	Ya
Server Debian (Buster)	10	DSA	Ya	Ya

Sistem operasi	Versi	Penasihat keamanan vendor	Dukungan pemindaian tanpa agen	Dukungan pemindaian berbasis agen
Server Debian (Bullseye)	11	DSA	Ya	Ya
Server Debian (Kutu Buku)	12	DSA	Ya	Ya
Fedora	38	CVE	Ya	Ya
Fedora	39	CVE	Ya	Ya
OpenSUSE	15.5	CVE	Ya	Ya
Oracle Linux (Oracle)	7	ELSA	Ya	Ya
Oracle Linux (Oracle)	8	ELSA	Ya	Ya
Oracle Linux (Oracle)	9	ELSA	Ya	Ya
Red Hat Enterprise Linux (RHEL)	7	RHSA	Ya	Ya
Red Hat Enterprise Linux (RHEL)	8	RHSA	Ya	Ya
Red Hat Enterprise Linux (RHEL)	9	RHSA	Ya	Ya
Linux Rocky	8	RLSA	Ya	Ya
Linux Rocky	9	RLSA	Ya	Ya

Sistem operasi	Versi	Penasihat keamanan vendor	Dukungan pemindaian tanpa agen	Dukungan pemindaian berbasis agen
Server Perusahaan SUSE Linux (SLES)	12.4	SUSE CVE	Ya	Ya
Server Perusahaan SUSE Linux (SLES)	12,5	SUSE CVE	Ya	Ya
Server Perusahaan SUSE Linux (SLES)	15.3	SUSE CVE	Ya	Ya
Server Perusahaan SUSE Linux (SLES)	15.4	SUSE CVE	Ya	Ya
Server Perusahaan SUSE Linux (SLES)	15.5	SUSE CVE	Ya	Ya
Ubuntu (Terpercaya)	14.04 (ESM)	USN, Ubuntu Pro	Ya	Ya
Ubuntu (Xenial)	16.04 (ESM)	USN, Ubuntu Pro	Ya	Ya
Ubuntu (Bionik)	18.04 (ESM)	USN, Ubuntu Pro	Ya	Ya
Ubuntu (Fokus)	20.04 (LTS)	USN	Ya	Ya

Sistem operasi	Versi	Penasihat keamanan vendor	Dukungan pemindaian tanpa agen	Dukungan pemindaian berbasis agen
Ubuntu (Jammy)	22.04 (LTS)	USN	Ya	Ya
Ubuntu (Mantic Minotaur)	23.10	USN	Ya	Ya
Windows Server	2016	MSKB	Tidak	Ya
Windows Server	2019	MSKB	Tidak	Ya
Windows Server	2022	MSKB	Tidak	Ya
macOS (Mojave)	10.14	APEL-SA	Tidak	Ya
macOS (Catalina)	10.15	APEL-SA	Tidak	Ya
macOS (Big Sur)	11	APEL-SA	Tidak	Ya
macOS (Monterey)	12	APEL-SA	Tidak	Ya
macOS (Ventura)	13	APEL-SA	Tidak	Ya

Bahasa pemrograman yang didukung: Inspeksi mendalam Amazon EC2

Amazon Inspector saat ini mendukung bahasa pemrograman berikut saat memindai instans Amazon EC2 Linux untuk kerentanan dalam paket perangkat lunak pihak ketiga:

- Java
- JavaScript
- Python

Amazon Inspector menggunakan Systems Manager Distributor untuk menerapkan plugin yang digunakan untuk pemeriksaan mendalam di instans Amazon EC2 Anda. Systems Manager Distributor mendukung sistem operasi yang terdaftar sebagai platform dan arsitektur paket yang didukung dalam panduan Systems Manager. Sistem operasi instans Amazon EC2 Anda harus didukung oleh Systems Manager Distributor dan Amazon Inspector untuk Amazon Inspector untuk melakukan pemindaian inspeksi mendalam.

> **Note**
>
> Inspeksi mendalam tidak didukung untuk sistem operasi Bottlerocket.

Sistem operasi yang didukung: pemindaian CIS

Tabel berikut mencantumkan sistem operasi yang saat ini didukung Amazon Inspector untuk pemindaian CIS. Tabel ini juga mencakup versi benchmark CIS yang digunakan untuk melakukan pemindaian sistem operasi itu.

Sistem operasi	Versi	Versi benchmark CIS
Amazon Linux 2	AL2	2.0.0
Amazon Linux 2023	AL2023	1.0.0
Windows Server	2019	2.0.0
Windows Server	2022	2.0.0

Sistem operasi yang didukung: Pemindaian Amazon ECR dengan Amazon Inspector

Amazon Inspector saat ini mendukung pemindaian sistem operasi berikut saat memindai gambar kontainer di repositori Amazon ECR:. Tabel ini juga mencantumkan sumber penasihat keamanan vendor untuk setiap sistem operasi.

Sistem operasi	Versi	Penasihat keamanan vendor
Alpine Linux (Alpine)	3.16	Alpine SecDB
Alpine Linux (Alpine)	3.17	Alpine SecDB
Alpine Linux (Alpine)	3.18	Alpine SecDB
Alpine Linux (Alpine)	3.19	Alpine SecDB
AlmaLinux	8	ALSA
AlmaLinux	9	ALSA
Amazon Linux (AL2)	AL2	ALAS
Amazon Linux 2023 (AL2023)	AL2023	ALAS
CentOS Linux (CentOS)	7	CESA
Debian Server (Buster)	10	DSA
Debian Server (Bullseye)	11	DSA
Debian Server (Bookworm)	12	DSA
Fedora	38	CVE
Fedora	39	CVE
OpenSUSE	15.5	CVE
Oracle Linux (Oracle)	7	ELSA
Oracle Linux (Oracle)	8	ELSA
Oracle Linux (Oracle)	9	ELSA
Photon OS	3	PHSA
Photon OS	4	PHSA

Sistem operasi	Versi	Penasihat keamanan vendor
Photon OS	5	PHSA
Red Hat Enterprise Linux (RHEL)	7	RHSA
Red Hat Enterprise Linux (RHEL)	8	RHSA
Red Hat Enterprise Linux (RHEL)	9	RHSA
Rocky Linux	8	RLSA
Rocky Linux	9	RLSA
SUSE Linux Enterprise Server (SLES)	12.4	SUSE CVE
SUSE Linux Enterprise Server (SLES)	12.5	SUSE CVE
SUSE Linux Enterprise Server (SLES)	15.3	SUSE CVE
SUSE Linux Enterprise Server (SLES)	15.4	SUSE CVE
SUSE Linux Enterprise Server (SLES)	15.5	SUSE CVE
Ubuntu (Trusty)	14.04 (ESM)	USN, Ubuntu Pro
Ubuntu (Xenial)	16.04 (ESM)	USN, Ubuntu Pro
Ubuntu (Bionic)	18.04 (ESM)	USN, Ubuntu Pro
Ubuntu (Focal)	20.04 (LTS)	USN
Ubuntu (Jammy)	22.04 (LTS)	USN

Sistem operasi	Versi	Penasihat keamanan vendor
Ubuntu (Mantic Minotaur)	23.10	USN

Bahasa pemrograman yang didukung: Pemindaian Amazon ECR

Amazon Inspector saat ini mendukung bahasa pemrograman berikut saat memindai gambar kontainer di repositori Amazon ECR:

- C#
- Go
- Java
- JavaScript
- PHP
- Python
- Ruby
- Rust

Runtime yang didukung: Pemindaian standar Amazon Inspector Lambda

Pemindaian standar Amazon Inspector Lambda saat ini mendukung bahasa pemrograman berikut saat memindai fungsi Lambda untuk kerentanan dalam paket perangkat lunak pihak ketiga:

- Java
  - java8
  - java8.al2
  - java11
  - java17
- Node.js
  - nodejs12.x
  - nodejs14.x
  - nodejs16.x

- nodejs18.x
- nodejs20.x

- Python
  - python3.7
  - python3.8
  - python3.9
  - python3.10
  - python3.11
- Go
  - go1.x
- Ruby
  - ruby2.7
  - ruby3.2
- .NET
  - .NET 6

Runtime yang didukung: Pemindaian kode Amazon Inspector Lambda

Pemindaian kode Amazon Inspector Lambda saat ini mendukung bahasa pemrograman berikut saat memindai fungsi Lambda untuk kerentanan dalam kode:

- Java
  - java8
  - java8.al2
  - java11
  - java17
- Node.js
  - nodejs12.x
  - nodejs14.x
  - nodejs16.x

  - nodejs18.x
  - nodejs20.x
- Python
  - python3.7
  - python3.8
  - python3.9
  - python3.10
  - python3.11
- Ruby
  - ruby2.7
  - ruby3.2

Sistem operasi yang dihentikan

Dukungan vendor standar untuk sistem operasi yang tercantum dalam tabel berikut telah dihentikan oleh vendor. Dalam tabel, kolom Dihentikan menunjukkan kapan vendor menghentikan dukungan standar untuk sistem operasi.

Amazon Inspector sebelumnya memberikan dukungan penuh untuk sistem operasi ini dan akan terus memindai instans Amazon EC2 dan gambar wadah Amazon ECR yang menjalankannya. Namun, sesuai dengan kebijakan vendor, sistem operasi tidak lagi diperbarui dengan tambalan dan, dalam banyak kasus, nasihat keamanan baru tidak lagi dirilis untuk mereka. Selain itu, beberapa vendor menghapus penasihat dan deteksi keamanan yang ada dari feed mereka ketika sistem operasi yang terpengaruh mencapai akhir dukungan standar. Akibatnya, Amazon Inspector mungkin berhenti menghasilkan temuan untuk CVE yang diketahui. Setiap temuan yang dihasilkan Amazon Inspector untuk sistem operasi yang dihentikan harus digunakan hanya untuk tujuan informasi.

Sebagai praktik keamanan terbaik dan untuk cakupan Amazon Inspector yang berkelanjutan, kami mendorong Anda untuk beralih ke versi sistem operasi yang didukung saat ini.

Sistem operasi yang dihentikan: Pemindaian Amazon EC2

Sistem operasi	Versi	Dihentikan
Amazon Linux (AL1)	2012	Desember 31, 2021

Sistem operasi	Versi	Dihentikan
CentOS Linux (CentOS)	8	Desember 31, 2021
Server Debian (Peregangan)	9	30 Juni 2022
Fedora	35	13 Desember 2022
Fedora	36	16 Mei 2023
Fedora	37	5 Desember 2023
OpenSUSE	15.3	Desember 1, 2022
OpenSUSE	15.4	Desember 7, 2023
OpenSUSE Leap (Lompatan SUSE)	15.2	1 Desember 2021
Oracle Linux (Oracle)	6	1 Maret 2021
Server Perusahaan SUSE Linux (SLES)	12	1 Juli 2019
Server Perusahaan SUSE Linux (SLES)	12.1	Mei 31, 2020
Server Perusahaan SUSE Linux (SLES)	12.2	31 Maret 2021
Server Perusahaan SUSE Linux (SLES)	12.3	30 Juni 2022
Server Perusahaan SUSE Linux (SLES)	15	Desember 31, 2019
Server Perusahaan SUSE Linux (SLES)	15.1	Januari 31, 2021
Server Perusahaan SUSE Linux (SLES)	15.2	Desember 31, 2021

Sistem operasi	Versi	Dihentikan
Ubuntu (Groovy)	20.10	22 Juli 2021
Ubuntu (Banyak)	21.04	20 Januari 2022
Ubuntu (Impish)	21.10	Juli 31, 2022
Ubuntu (Kinetic)	22.10	July 20, 2023
Ubuntu (Lunar Lobster)	23.04	January 25, 2024
Windows Server	2012	10 Oktober 2023
Windows Server	2012 R2	10 Oktober 2023

Sistem operasi yang dihentikan: Pemindaian Amazon ECR

Sistem operasi	Versi	Dihentikan
Alpine Linux (Alpine)	3.12	1 Mei 2022
Alpine Linux (Alpine)	3.13	1 November 2022
Alpine Linux (Alpine)	3.14	May 1, 2023
Alpine Linux (Alpine)	3.15	November 1, 2023
Amazon Linux (AL1)	2012	Desember 31, 2021
CentOS Linux (CentOS)	8	Desember 31, 2021
Server Debian (Peregangan)	9	30 Juni 2022
Fedora	35	13 Desember 2022
Fedora	36	16 Mei 2023
OpenSUSE	15.3	Desember 1, 2022

Sistem operasi	Versi	Dihentikan
OpenSUSE	15.4	December 7, 2023
OpenSUSE Leap (Lompatan SUSE)	15.2	1 Desember 2021
Oracle Linux (Oracle)	6	1 Maret 2021
Server Perusahaan SUSE Linux (SLES)	12	1 Juli 2019
Server Perusahaan SUSE Linux (SLES)	12.1	Mei 31, 2020
Server Perusahaan SUSE Linux (SLES)	12.2	31 Maret 2021
Server Perusahaan SUSE Linux (SLES)	12.3	30 Juni 2022
Server Perusahaan SUSE Linux (SLES)	15	Desember 31, 2019
Server Perusahaan SUSE Linux (SLES)	15.1	Januari 31, 2021
Server Perusahaan SUSE Linux (SLES)	15.2	Desember 31, 2021
Ubuntu (Groovy)	20.10	22 Juli 2021
Ubuntu (Banyak)	21.04	20 Januari 2022
Ubuntu (Impish)	21.10	Juli 31, 2022
Ubuntu (Kinetic)	22.10	July 20, 2023
Ubuntu (Lunar Lobster)	23.04	January 25, 2024

Menonaktifkan Amazon Inspector

Anda dapat menonaktifkan Amazon Inspector di Wilayah AWS manapun dengan menggunakan konsol Amazon Inspector atau API. Ikuti petunjuk di akhir topik ini untuk menonaktifkan Amazon Inspector. Jika Anda menonaktifkan semua pemindaian Amazon Inspector, Akun AWS Amazon Inspector dinonaktifkan untuk akun ini secara otomatis. Untuk informasi tentang menonaktifkan jenis pemindaian untuk sumber daya yang berbeda, lihat. Pemindaian sumber daya otomatis dengan Amazon Inspector

Setelah Amazon Inspector dinonaktifkan untuk akun, semua jenis pemindaian dinonaktifkan untuk akun tersebut di Wilayah tersebut. Selain itu, semua setelan pemindaian Amazon Inspector, aturan penekanan, serta filter serta temuan untuk akun di Wilayah tersebut akan dihapus.

Anda tidak dikenakan biaya untuk menggunakan Amazon Inspector saat dinonaktifkan untuk akun Anda di Wilayah tersebut. Setelah Anda menonaktifkan Amazon Inspector, Anda dapat memilih untuk mengaktifkannya kembali di lain waktu.

> **Note**
>
> Sebelum Anda menonaktifkan Amazon Inspector, kami sarankan Anda mengekspor temuan Anda. Untuk informasi selengkapnya, lihat Mengekspor laporan temuan dari Amazon Inspector.

Saat Anda menonaktifkan pemindaian Amazon Inspector Amazon EC2, asosiasi SSM berikut yang digunakan oleh Amazon Inspector akan dihapus:

- `InspectorDistributor-do-not-delete`
- `InspectorInventoryCollection-do-not-delete`
- `InvokeInspectorSsmPlugin-do-not-delete`. Selain itu, plugin Amazon Inspector SSM yang diinstal melalui asosiasi ini dihapus dari semua host Anda. Windows Untuk informasi selengkapnya, lihat WindowsContoh pemindaian.

Prasyarat

Bergantung pada jenis akun Anda, Anda mungkin perlu mengambil langkah tambahan sebelum menonaktifkan Amazon Inspector sebagai berikut:

- Jika Anda memiliki akun Amazon Inspector mandiri, Anda dapat menonaktifkannya kapan saja.
- Jika Anda adalah akun anggota di lingkungan multi-akun Amazon Inspector, Anda tidak dapat menonaktifkan layanan Anda sendiri. Anda harus menghubungi administrator yang didelegasikan untuk organisasi Anda untuk menonaktifkan layanan Anda.
- Jika Anda adalah administrator yang didelegasikan, Anda harus memisahkan semua akun anggota Anda sebelum dapat menonaktifkan Amazon Inspector. Untuk informasi selengkapnya, lihat Memutuskan akun anggota di Amazon Inspector.

> **Note**
>
> Memutuskan hubungan akun tidak menonaktifkan Amazon Inspector untuk akun tersebut, sebagai gantinya, akun anggota yang tidak terkait menjadi akun mandiri.

> **Note**
>
> Saat Anda menonaktifkan Amazon Inspector sebagai administrator yang didelegasikan, fitur aktivasi otomatis akan dinonaktifkan untuk organisasi Anda.

Nonaktifkan Amazon Inspector

Console

Untuk menonaktifkan Amazon Inspector

1. Buka konsol Amazon Inspector di https://console.aws.amazon.com/inspector/v2/home.
2. Dengan menggunakan Wilayah AWS pemilih di sudut kanan atas halaman, pilih Wilayah tempat Anda ingin menonaktifkan Amazon Inspector.
3. Di panel navigasi, pilih Pengaturan umum.
4. Pilih Nonaktifkan Inspector.
5. Saat diminta konfirmasi, masukkan nonaktifkan di kotak teks, lalu pilih Nonaktifkan Inspector.
6. (Disarankan) Ulangi langkah-langkah ini di setiap Wilayah yang ingin Anda nonaktifkan Amazon Inspector.

API

Jalankan operasi Nonaktifkan API. Dalam permintaan, berikan ID akun yang Anda nonaktifkan, dan `EC2, ECR, LAMBDA` `resourceTypes` untuk menonaktifkan semua pemindaian, yang akan menonaktifkan akun.

Kuota untuk Amazon Inspector

AWSAkun Anda memiliki kuota berikut untuk Amazon Inspector per Wilayah.

Sumber daya	Default	Komentar
Aturan penekanan	500	Jumlah maksimum aturan penekanan yang disimpan per AWS akun per Wilayah. Anda tidak dapat meminta kenaikan kuota.
Temuan jaringan Amazon EC2	10.000	Jumlah maksimum temuan jaringan Amazon EC2 per AWS akun. Anda tidak dapat meminta kenaikan kuota.
Akun anggota	10000	Jumlah maksimum akun anggota yang terkait dengan akun administrator yang didelegasikan Amazon Inspector. Batas ini didasarkan padaAWS Organizations, lihat Kuota untuk AWS Organizations.

Sumber daya	Default	Komentar
Konfigurasi pemindaian CIS	500	Jumlah maksimum konfigurasi pemindaian CIS. Anda tidak dapat meminta kenaikan kuota.

Untuk daftar kuota yang terkait dengan Amazon Inspector Classic, lihat Kuota layanan Amazon Inspector di. Referensi Umum AWS

Untuk daftar kuota yang terkait dengan Organizations, lihat Kuota layanan Organizations di. Referensi Umum AWS

Wilayah dan titik akhir

Pemindaian tanpa agen Amazon Inspector untuk Amazon EC2 sedang dalam rilis pratinjau. Penggunaan Anda atas fitur pemindaian Amazon EC2 tanpa agen tunduk pada Bagian 2 dari AWS Ketentuan Layanan (“Beta dan Pratinjau”).

Untuk melihat Wilayah AWS lokasi Amazon Inspector tersedia, lihat titik akhir Amazon Inspector di bagian. Referensi Umum Amazon Web Services

Titik akhir untuk Amazon Inspector Scan API

Tabel berikut menunjukkan titik akhir Regional yang dapat digunakan saat memanggil Amazon Inspector Scan API. Saat menggunakan API, Anda harus menyediakan titik akhir dan itu adalah Wilayah yang sesuai untuk Wilayah yang saat ini Anda autentikasi. AWS

Konvensi penamaan untuk titik akhir Amazon Inspector Scan adalah. `inspector-scan.`*`region`*`.amazonaws.com` Misalnya, jika Anda diautentikasi`us-west-2`, Anda akan menggunakan titik akhir `inspector-scan.us-west-2.amazonaws.com` untuk memanggil API. `inspector-scan`

Nama Wilayah	wilayah	Titik akhir	Protokol
US East (Ohio)	us-east-2	inspector-scan.us-east-2.amazonaws.com inspector-scan-fips.us-east-2.amazonaws.com	HTTPS
US East (N. Virginia)	us-east-1	inspector-scan.us-east-1.amazonaws.com	HTTPS

Nama Wilayah	wilayah	Titik akhir	Protokol
		inspector-scan-fips.us-east-1.amazonaws.com	
US West (N. California)	us-west-1	inspector-scan.us-west-1.amazonaws.com inspector-scan-fips.us-west-1.amazonaws.com	HTTPS
US West (Oregon)	us-west-2	inspector-scan.us-west-2.amazonaws.com inspector-scan-fips.us-west-2.amazonaws.com	HTTPS
Africa (Cape Town)	af-south-1	inspector-scan.af-south-1.amazonaws.com	HTTPS
Asia Pacific (Hong Kong)	ap-east-1	inspector-scan.ap-east-1.amazonaws.com	HTTPS
Asia Pacific (Jakarta)	ap-southeast-3	inspector-scan.ap-southeast-3.amazonaws.com	HTTPS
Asia Pacific (Mumbai)	ap-south-1	inspector-scan.ap-south-1.amazonaws.com	HTTPS

Nama Wilayah	wilayah	Titik akhir	Protokol
Asia Pacific (Osaka)	ap-northeast-3	inspector-scan.ap-northeast-3.amazonaws.com	HTTPS
Asia Pacific (Seoul)	ap-northeast-2	inspector-scan.ap-northeast-2.amazonaws.com	HTTPS
Asia Pacific (Singapore)	ap-southeast-1	inspector-scan.ap-southeast-1.amazonaws.com	HTTPS
Asia Pacific (Sydney)	ap-southeast-2	inspector-scan.ap-southeast-2.amazonaws.com	HTTPS
Asia Pacific (Tokyo)	ap-northeast-1	inspector-scan.ap-northeast-1.amazonaws.com	HTTPS
Canada (Central)	ca-central-1	inspector-scan.ca-central-1.amazonaws.com	HTTPS
Europe (Frankfurt)	eu-central-1	inspector-scan.eu-central-1.amazonaws.com	HTTPS
Europe (Ireland)	eu-west-1	inspector-scan.eu-west-1.amazonaws.com	HTTPS
Europe (London)	eu-west-2	inspector-scan.eu-west-2.amazonaws.com	HTTPS

Nama Wilayah	wilayah	Titik akhir	Protokol
Europe (Milan)	eu-south-1	inspector-scan.eu-south-1.amazonaws.com	HTTPS
Europe (Paris)	eu-west-3	inspector-scan.eu-west-3.amazonaws.com	HTTPS
Europe (Stockholm)	eu-north-1	inspector-scan.eu-north-1.amazonaws.com	HTTPS
Europe (Zurich)	eu-central-2	inspector-scan.eu-central-2.amazonaws.com	HTTPS
Middle East (Bahrain)	me-south-1	inspector-scan.me-south-1.amazonaws.com	HTTPS
South America (São Paulo)	sa-east-1	inspector-scan.sa-east-1.amazonaws.com	HTTPS
AWS GovCloud (AS-Timur)	us-gov-east-1	pemindaian inspektur. us-gov-east-1.amazonaws.com inspector-scan-fips.us-gov-east-1.amazonaws.com	HTTPS

Nama Wilayah	wilayah	Titik akhir	Protokol
AWS GovCloud (AS-Barat)	us-gov-west-1	pemindaian inspektur . us-gov-west-1.amazonaws.com inspector-scan-fips. us-gov-west-1.amazonaws.com	HTTPS

Ketersediaan fitur khusus wilayah

Bagian ini menjelaskan ketersediaan fitur Amazon Inspector oleh. Wilayah AWS

Pemindaian EC2 tanpa agen untuk Wilayah Amazon EC2

Tabel berikut menunjukkan Wilayah AWS tempat pemindaian tanpa agen untuk Amazon EC2 saat ini tersedia.

Nama Wilayah	Kode Wilayah
US East (Northern Virginia)	us-east-1
AS Barat (Oregon)	us-west-2
Eropa (Irlandia)	eu-west-1

Wilayah pemindaian kode Lambda

Tabel berikut menunjukkan Wilayah AWS di mana pemindaian kode Lambda saat ini tersedia.

Nama Wilayah	Kode Wilayah
US East (Northern Virginia)	us-east-1
AS Barat (Oregon)	us-west-2
Timur AS (Ohio)	us-east-2

Nama Wilayah	Kode Wilayah
Asia Pasifik (Sydney)	ap-southeast-2
Asia Pacific (Tokyo)	ap-northeast-1
Eropa (Frankfurt)	eu-central-1
Europe (Ireland)	eu-west-1
Europe (London)	eu-west-2
Eropa (Stockholm)	eu-north-1
Asia Pasifik (Singapura)	ap-southeast-1

Wilayah AWS GovCloud (US)

Untuk informasi terbaru, lihat Amazon Inspector di AWS GovCloud (US)Panduan Pengguna.

Riwayat dokumen untuk Panduan Pengguna Amazon Inspector

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

Perubahan	Deskripsi	Tanggal
Fungsionalitas yang diperbarui	Amazon Inspector memperbarui periode retensi untuk temuan tertutup dari 30 hari hingga 7 hari. Untuk informasi selengkapnya, lihat Memahami temuan di Amazon Inspector.	Februari 12, 2024
Fungsionalitas yang diperbarui	Amazon Inspector menambahkan pernyataan baru pada kebijakan tersebut. AmazonInspector2ServiceRolePolicy Pernyataan baru ini memungkinkan Amazon Inspector untuk memulai pemindaian CIS untuk instans Anda.	23 Januari 2024
Kebijakan Baru	Amazon Inspector telah menambahkan kebijakan baru, AmazonInspector2ManagedCisPolicykebijakan, yang dapat Anda gunakan sebagai bagian dari dalam profil instans untuk mengizinkan pemindaian CIS pada sebuah instans.	23 Januari 2024

Fitur Baru	Amazon Inspector sekarang akan menyegarkan durasi pemindaian ulang ECR dari gambar kontainer saat Anda menariknya. Untuk mengubah durasi pemindaian ulang berdasarkan tanggal push atau pull, lihat Mengonfigurasi durasi pemindaian ulang ECR.	23 Januari 2024
Fitur Baru	Amazon Inspector sekarang dapat menjalankan pemindaian Center for Internet Security (CIS) pada instans EC2. Untuk informasi selengkapnya, lihat pemindaian Amazon Inspector CIS.	23 Januari 2024
Fitur Baru	Amazon Inspector sekarang dapat memindai gambar kontainer di pipeline CI/CD Anda. Untuk informasi selengkapnya, lihat Integrasi CI/CD dengan Amazon Inspector.	30 November 2023
Kebijakan Baru	Amazon Inspector telah menambahkan kebijakan baru yang memungkinkan Amazon Inspector memindai snapshot Amazon EBS dari instans EC2 Anda untuk pemindaian tanpa agen. Untuk informasi selengkapnya tentang kebijakan ini, lihat Pemindaian tanpa agen.	27 November 2023

Fitur Baru	Amazon Inspector sekarang mendukung pemindaian instans Amazon EC2 Linux yang didukung tanpa agen SSM melalui pemindaian tanpa agen. Untuk informasi lebih lanjut, lihat Pemindaian tanpa agen.	27 November 2023
Sumber daya baru yang didukung	Amazon Inspector sekarang mendukung pemindaian instans macOS Amazon EC2. Lihat Sistem operasi yang didukung: Pemindaian Amazon EC2 untuk versi macOS yang didukung.	5 Oktober 2023
Daerah Baru	Amazon Inspector sekarang tersedia di Asia Pasifik (Jakarta), Afrika (Cape Town), Asia Pasifik (Osaka), dan Eropa (Zurich).	September 29, 2023
Fitur baru	Anda sekarang dapat mengecualikan instans EC2 dari pemindaian Amazon Inspector menggunakan tag pengecualian.	14 September 2023
Fitur baru	Amazon Inspector telah menambahkan izin baru yang memungkinkan Amazon Inspector memindai konfigurasi jaringan instans Amazon EC2 yang merupakan bagian dari grup target Elastic Load Balancing.	31 Agustus 2023

Fitur baru	Amazon Inspector sekarang memberikan rincian intelijen kerentanan untuk temuan kerentanan paket.	31 Juli 2023
Fungsionalitas yang diperbarui	Amazon Inspector telah menambahkan izin baru yang memungkinkan pengguna read-only untuk mengekspo r Software Bill of Materials (SBOM) untuk sumber daya mereka.	29 Juni 2023
Fitur baru	Anda sekarang dapat mengekspor SBOM untuk sumber daya yang dipindai oleh Amazon Inspector.	13 Juni 2023
Fitur baru	Pemindaian kode Lambda sekarang tersedia secara umum. Fitur baru telah ditambahkan yang memungkin kan Anda mengenkripsi kode yang diidentifikasi dalam temuan pemindaian kode Lambda Anda. Selain itu, pemindaian kode Lambda sekarang menyediakan penulisan ulang remediasi yang disarankan untuk kode Anda.	13 Juni 2023

Fungsionalitas yang diperbarui	Amazon Inspector menambahkan pernyataan baru pada kebijakan tersebut. AmazonInspector2ReadOnlyAccess Pernyataan baru ini memungkinkan pengguna hanya-baca untuk mengambil detail status pemindaian kode Lambda dan temuan untuk akun mereka.	2 Mei 2023
Fitur baru	Amazon Inspector telah menambahkan pencarian database Vulnerability yang memungkinkan Anda memeriksa apakah Amazon Inspector mencakup CVE tertentu.	1 Mei 2023
Fungsionalitas yang diperbarui	Amazon Inspector telah menambahkan izin baru ke AmazonInspector2ServiceRolePolicykebijakan yang memungkinkan Amazon Inspector membuat saluran AWS CloudTrail terkait layanan di akun Anda saat Anda mengaktifkan pemindaian Lambda. Ini memungkinkan Amazon Inspector untuk memantau CloudTrail peristiwa di akun Anda.	April 30, 2023

Fungsionalitas yang diperbarui	Amazon Inspector menambahkan pernyataan baru pada kebijakan tersebut. AmazonInspector2FullAccess Pernyataan baru ini memungkinkan pengguna untuk mengambil rincian temuan kerentanan kode dari pemindaian kode Lambda.	17 April 2023
Fungsionalitas yang diperbarui	Amazon Inspector menambahkan pernyataan baru pada kebijakan tersebut. AmazonInspector2ServiceRolePolicy Pernyataan baru ini memungkinkan Amazon Inspector untuk mengirim informasi ke Amazon EC2 Systems Manager tentang jalur kustom yang telah Anda tentukan untuk inspeksi mendalam Amazon EC2.	17 April 2023
Fitur baru	Amazon Inspector menambahkan dukungan tambahan untuk instans Linux EC2 dalam bentuk inspeksi mendalam Amazon Inspector , yang memindai instans Anda untuk kerentanan paket dalam paket bahasa pemrograman aplikasi.	17 April 2023

Fungsionalitas yang diperbarui	Amazon Inspector menambahkan pernyataan baru pada kebijakan tersebut. AmazonInspector2ServiceRolePolicy Pernyataan baru memungkinkan Amazon Inspector untuk meminta pemindaian kode pengembang dalam AWS Lambda fungsi, dan menerima data pemindaian dari Amazon Security. CodeGuru Selain itu Amazon Inspector telah menambahkan izin untuk meninjau kebijakan IAM. Amazon Inspector menggunakan informasi ini untuk memindai fungsi Lambda untuk kerentanan kode.	28 Februari 2023
Fitur baru	Amazon Inspector menambahkan dukungan tambahan untuk fungsi Lambda dalam bentuk pemindaian kode Lambda, yang memindai kode pengembang fungsi Lambda Anda untuk kerentanan keamanan.	28 Februari 2023

Fungsionalitas yang diperbarui	Amazon Inspector menambahkan pernyataan baru pada kebijakan tersebut. AmazonInspector2ServiceRolePolicy Pernyataan baru ini memungkinkan Amazon Inspector untuk mengambil informasi dari CloudWatch tentang kapan AWS Lambda fungsi terakhir digunakan . menggunakan informasi ini untuk memfokuskan pemindaian pada fungsi Lambda di lingkungan Anda yang telah aktif dalam 90 hari terakhir.	Februari 20, 2023
Fungsionalitas yang diperbarui	Amazon Inspector menambahkan pernyataan baru pada kebijakan tersebut. AmazonInspector2ServiceRolePolicy Pernyataan baru ini memungkinkan Amazon Inspector untuk mengambil informasi tentang fungsi Anda. AWS Lambda Amazon Inspector menggunakan informasi ini untuk memindai fungsi Lambda Anda untuk mencari kerentanan keamanan.	28 November 2022
Fitur baru	Amazon Inspector menambahkan dukungan untuk fungsi Scanning AWS Lambda.	28 November 2022

Konten yang diperbarui	Menambahkan prosedur, contoh kebijakan, dan tip untuk mengekspor laporan temuan dari Amazon Inspector ke bucket Amazon Simple Storage Service (Amazon S3).	14 Oktober 2022
Konten baru	Menambahkan informasi tentang menilai cakupan Amazon Inspector lingkungan AWS Anda dengan menggunakan konsol Amazon Inspector. Informasi tersebut mencakup deskripsi nilai Status untuk sumber daya individu di lingkungan Anda.	Oktober 7, 2022
Fitur baru	Amazon Inspector sekarang memberikan rincian tambahan tentang cara memulihkan kerentanan paket. Bidang baru telah ditambahkan untuk menemukan detail. Bidang baru menyediakan konteks tentang apakah perbaikan tersedia melalui pembaruan paket. Jika perbaikan tersedia, bagian Remediasi yang disarankan dari temuan menunjukkan perintah yang dapat Anda jalankan untuk memperbaiki.	September 2, 2022

Fungsionalitas yang diperbarui	Amazon Inspector menambahkan tindakan baru ke kebijakan tersebut. AmazonInspector2ServiceRolePolicy Tindakan baru ini memungkinkan Amazon Inspector untuk menggambarkan eksekusi asosiasi SSM. Amazon Inspector juga menambahkan pelingkupan sumber daya tambahan untuk memungkinkan Amazon Inspector membuat, memperbarui, menghapus, dan memulai asosiasi SSM dengan dokumen SSM yang dimiliki. `AmazonInspector2`	31 Agustus 2022
Fitur baru	Amazon Inspector sekarang mendukung pemindaian untuk instance. Windows Amazon Inspector sekarang dapat memindai instans terkelola SSM yang menjalankan sistem operasi yang didukung. Windows Pemindaian Windows host dilakukan oleh plugin Amazon Inspector SSM, yang diinstal dan dipanggil melalui asosiasi SSM baru yang secara otomatis dibuat oleh Amazon Inspector.	31 Agustus 2022

Fungsionalitas yang diperbarui	Amazon Inspector memperbarui pelingkupan sumber daya AmazonInspector2ServiceRolePolicykebijakan untuk memungkinkan Amazon Inspector mengumpulkan inventaris perangkat lunak di partisi lain. AWS	12 Agustus 2022
Fungsionalitas yang diperbarui	Dalam AmazonInspector2ServiceRolePolicykebijakan tersebut, Amazon Inspector merestrukturisasi pelingkupan sumber daya dari tindakan yang memungkinkan Amazon Inspector membuat, menghapus, dan memperbarui asosiasi SSM.	Agustus 10, 2022

Fitur baru	Amazon Inspector sekarang mendukung perubahan pengaturan durasi pemindaian ulang otomatis ECR Anda. Pengaturan durasi pemindaian ulang otomatis Amazon ECR menentukan berapa lama Amazon Inspector terus memantau gambar yang didorong ke repositori. Ketika gambar lebih tua dari durasi pemindaian, Amazon Inspector tidak akan lagi memindai gambar dan menutup semua temuan yang ada untuknya. Semua akun baru akan secara otomatis memiliki durasi pemindaian ulang otomatis ECR yang disetel ke seumur hidup. Akun yang dibuat sebelumnya memiliki durasi pemindaian ulang otomatis ECR 30 hari, tetapi sekarang Anda dapat memilih dari 30 hari, 180 hari, atau durasi seumur hidup untuk pemindaian.	Juni 25, 2022
Fungsionalitas baru	Amazon Inspector menambahkan kebijakan AWS terkelola baru, AmazonInspector2ReadOnlyAccesskebijakan, untuk mengizinkan akses hanya-baca ke fungsionalitas Amazon Inspector.	Januari 21, 2022

Ketersediaan umum	Ini adalah rilis publik awal dari Panduan Pengguna Amazon Inspector.	29 November 2021

AWSGlosarium

Untuk AWS terminologi terbaru, lihat AWSglosarium di Referensi. Glosarium AWS

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