aws

Panduan Pengguna

# Amazon Inspector Klasik

Versi Latest

# Amazon Inspector Klasik: Panduan Pengguna

# Table of Contents

Ini adalah panduan pengguna untuk Amazon Inspector Classic. Untuk informasi tentang Amazon Inspector yang baru, lihat Panduan Pengguna Amazon Inspector. Untuk mengakses konsol Amazon Inspector Classic, buka konsol Amazon Inspector https://console.aws.amazon.com/inspector/di, lalu pilih Amazon Inspector Classic di panel navigasi.

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

# Apa itu Amazon Inspector Classic?

> **Note**
>
> Amazon Inspector baru, versi Amazon Inspector Classic yang sepenuhnya direkonstruksi dan didesain ulang, sekarang tersedia di seluruh dunia. Wilayah AWS Amazon Inspector baru telah memperluas cakupan untuk menambahkan dukungan untuk gambar kontainer yang berada di Amazon Elastic Container Registry (Amazon ECR) Registry (Amazon ECR) selain instans EC2. Amazon Inspector baru menawarkan dukungan multi-akun melalui integrasi dengan AWS Organizations, dan kerentanan perangkat lunak berkelanjutan dan pemindaian jangkauan jaringan berdasarkan kerentanan dan eksposur umum (CVE). Kami mendorong Anda untuk menjelajahi dan menggunakan fitur ini dan fitur baru dan lebih baik lainnya, dan untuk mendapatkan keuntungan dari nilai keamanan yang ditingkatkan secara signifikan. Untuk mempelajari fitur dan harga Amazon Inspector baru, lihat Amazon Inspector. Untuk mempelajari cara pindah ke Amazon Inspector baru, lihat. Pindah ke Amazon Inspector baru

Amazon Inspector Classic menguji aksesibilitas jaringan instans Amazon EC2 Anda dan status keamanan aplikasi Anda yang berjalan pada instans tersebut. Amazon Inspector Classic menilai aplikasi untuk eksposur, kerentanan, dan penyimpangan dari praktik terbaik. Setelah melakukan penilaian, Amazon Inspector Classic menghasilkan daftar rinci temuan keamanan yang diatur berdasarkan tingkat keparahan.

Dengan Amazon Inspector Classic, Anda dapat mengotomatiskan penilaian kerentanan keamanan di seluruh pipeline pengembangan dan penerapan atau untuk sistem produksi statis. Hal ini memungkinkan Anda untuk membuat pengujian keamanan bagian reguler dari pengembangan dan operasi IT.

Amazon Inspector Classic juga menawarkan perangkat lunak standar yang disebut agen yang dapat Anda instal secara opsional di sistem operasi instans EC2 yang ingin Anda nilai. Agen memonitor perilaku instans EC2, termasuk jaringan, sistem file, dan aktivitas proses. Hal ini juga mengumpulkan seperangkat perilaku dan data konfigurasi (telemetri).

> **Important**
>
> AWS tidak menjamin bahwa mengikuti rekomendasi yang diberikan akan menyelesaikan setiap masalah keamanan potensial. Temuan yang dihasilkan oleh Amazon Inspector Classic

bergantung pada pilihan paket aturan yang disertakan dalam setiap templat penilaian, keberadaan AWS non-komponen dalam sistem Anda, dan faktor lainnya. Anda bertanggung jawab atas keamanan aplikasi, proses, dan alat yang berjalan pada AWS layanan. Untuk informasi selengkapnya, lihat Model Tanggung Jawab AWS Bersama untuk keamanan.

> **Note**
>
> AWS bertanggung jawab untuk melindungi infrastruktur global yang menjalankan layanan yang ditawarkan di AWS Cloud. Infrastruktur ini terdiri dari perangkat keras, perangkat lunak, jaringan, dan fasilitas yang menjalankan AWS layanan. AWS menyediakan beberapa laporan dari auditor pihak ketiga yang telah memverifikasi kepatuhan kami terhadap berbagai standar dan peraturan keamanan komputer. Untuk informasi selengkapnya, lihat Kepatuhan AWS Cloud.

Untuk informasi tentang terminologi Amazon Inspector Classic, lihat. Terminologi dan konsep Amazon Inspector

## Manfaat Amazon Inspector Classic

Berikut adalah beberapa manfaat utama Amazon Inspector Classic:

- Integrasikan pemeriksaan keamanan otomatis ke dalam proses penerapan dan produksi reguler Anda — Nilai keamanan AWS sumber daya Anda untuk tujuan forensik, pemecahan masalah, atau audit aktif. Menjalankan penilaian selama proses pengembangan, atau menjalankan mereka dalam lingkungan produksi yang stabil.
- Menemukan masalah keamanan aplikasi – Mengotomatiskan penilaian keamanan aplikasi Anda dan mengidentifikasi kelemahan secara proaktif. Hal ini memungkinkan Anda untuk mengembangkan dan mengulangi aplikasi baru dengan cepat, dan menilai kepatuhan terhadap kebijakan dan praktik terbaik.
- Dapatkan pemahaman yang lebih dalam tentang AWS sumber daya Anda — Tetap terinformasi tentang aktivitas dan data konfigurasi AWS sumber daya Anda dengan meninjau temuan yang dihasilkan Amazon Inspector Classic.

# Fitur Amazon Inspector Classic

Berikut adalah beberapa fitur utama Amazon Inspector Classic:

- Pemindaian konfigurasi dan mesin pemantauan aktivitas — Amazon Inspector Classic menyediakan agen yang menganalisis konfigurasi sistem dan sumber daya. Hal ini juga memantau aktivitas untuk menentukan target penilaian terlihat seperti apa, bagaimana perilakunya, dan komponen dependennya. Kombinasi telemetri ini memberikan gambaran lengkap target dan potensi masalah keamanan atau kepatuhannya.
- Pustaka konten bawaan — Amazon Inspector Classic menyertakan pustaka aturan dan laporan bawaan. Hal ini termasuk pemeriksaan terhadap praktik terbaik, standar kepatuhan umum, dan kelemahan. Pemeriksaan mencakup langkah-langkah yang direkomendasikan secara detail untuk menyelesaikan masalah keamanan yang potensial.
- Otomatisasi melalui API — Amazon Inspector Classic dapat sepenuhnya otomatis melalui API. Hal ini memungkinkan Anda untuk menggabungkan pengujian keamanan ke dalam proses pengembangan dan desain, termasuk memilih, mengeksekusi, dan melaporkan hasil tes tersebut.

# Mengakses Amazon Inspector Classic

Anda dapat bekerja dengan layanan Amazon Inspector Classic dengan salah satu cara berikut:

Konsol Amazon Inspector Classic

Masuk ke AWS Management Console dan buka konsol Amazon Inspector Classic di https://console.aws.amazon.com/inspector/.

Konsol adalah antarmuka berbasis browser yang memungkinkan Anda mengakses dan menggunakan layanan Amazon Inspector Classic.

AWS SDK

AWS menyediakan perangkat pengembangan perangkat lunak (SDK) yang terdiri dari perpustakaan dan kode sampel untuk berbagai bahasa dan platform pemrograman. Hal ini termasuk Java, Python, Ruby, .NET, iOS, Android, dan banyak lagi. SDK menyediakan cara mudah untuk membuat akses terprogram ke layanan Amazon Inspector Classic. Untuk informasi tentang AWS SDK, termasuk cara mengunduh dan menginstalnya, lihat Alat untuk Amazon Web Services.

Amazon Inspector Classic HTTPS API

Anda dapat mengakses Amazon Inspector Classic dan AWS secara terprogram menggunakan Amazon Inspector Classic HTTPS API, yang memungkinkan Anda mengeluarkan permintaan HTTPS langsung ke layanan. Untuk informasi selengkapnya, lihat Referensi API Amazon Inspector Classic.

AWS Alat Baris Perintah

Anda dapat menggunakan alat baris AWS perintah untuk menjalankan perintah di baris perintah sistem Anda untuk melakukan tugas Amazon Inspector Classic. Alat baris perintah juga berguna jika Anda ingin membangun skrip yang melakukan AWS tugas. Untuk informasi selengkapnya, lihat Antarmuka Baris AWS Perintah Amazon Inspector Classic.

# Terminologi dan konsep Amazon Inspector

Ketika Anda memulai dengan Amazon Inspector, Anda bisa mendapatkan keuntungan dari mempelajari konsep-konsep kuncinya.

Agen Amazon Inspector

Agen perangkat lunak yang dapat Anda instal pada instans EC2 yang termasuk dalam target penilaian. Agen mengumpulkan seperangkat data konfigurasi (telemetri). Untuk informasi selengkapnya, lihat Agen Amazon Inspector Classic.

Penilaian berjalan

Proses menemukan potensi masalah keamanan melalui analisis konfigurasi target penilaian Anda terhadap paket aturan tertentu. Selama penilaian berjalan, Amazon Inspector memonitor, mengumpulkan, dan menganalisis data konfigurasi (telemetri) dari sumber daya dalam target yang ditentukan. Selanjutnya, Amazon Inspector menganalisis data dan membandingkannya dengan seperangkat paket aturan keamanan yang ditentukan dalam templat penilaian yang digunakan selama penilaian berjalan. Penilaian berjalan yang telah selesai menghasilkan daftar temuan, yang merupakan potensi masalah keamanan dari berbagai tingkat kepelikan. Untuk informasi selengkapnya, lihat Templat penilaian Amazon Inspector Classic dan penilaian berjalan.

Target penilaian

Dalam konteks Amazon Inspector, kumpulan sumber daya AWS yang bekerja sama sebagai suatu unit untuk membantu Anda mencapai tujuan bisnis Anda. Amazon Inspector mengevaluasi keadaan keamanan sumber daya yang merupakan target penilaian.

> **Important**
>
> Saat ini, target penilaian Amazon Inspector Anda hanya dapat terdiri dari instans EC2. Untuk informasi selengkapnya, lihatBatas layanan Amazon Inspector Classic

Untuk membuat target penilaian Amazon Inspector, Anda harus terlebih dahulu menandai instans EC2 Anda dengan pasangan nilai-kunci pilihan Anda. Selanjutnya, Anda dapat membuat tampilan instans EC2 yang ditandai ini yang memiliki kunci umum atau nilai umum. Untuk informasi selengkapnya, lihat Target penilaian Amazon Inspector.

Templat penilaian

Konfigurasi yang digunakan selama menjalankan penilaian Anda. Templat mencakup hal-hal berikut:

- Paket aturan yang digunakan Amazon Inspector untuk mengevaluasi target penilaian Anda
- Topik Amazon SNS yang Anda inginkan untuk mengirim notifikasi Amazon Inspector untuk mengirim pemberitahuan tentang kondisi dan temuan berjalan
- Tanda (pasangan nilai-kunci) yang dapat Anda tetapkan ke temuan yang dihasilkan oleh penilaian berjalan
- Durasi penilaian berjalan

Temuan

Potensi masalah keamanan yang ditemukan Amazon Inspector selama penilaian berjalan untuk target yang ditentukan. Temuan ditampilkan di konsol Amazon Inspector atau diambil melalui API. Mereka berisi uraian detail tentang masalah keamanan dan rekomendasi tentang cara memperbaikinya. Untuk informasi selengkapnya, lihat Temuan Amazon Inspector Classic.

Rule

Dalam konteks Amazon Inspector, pemeriksaan keamanan yang dilakukan selama penilaian berjalan. Ketika aturan mendeteksi potensi masalah keamanan, Amazon Inspector menghasilkan temuan yang menjelaskan masalah tersebut.

Paket aturan

Dalam konteks Amazon Inspector, kumpulan berbagai aturan. Paket aturan sesuai dengan tujuan keamanan yang mungkin Anda miliki. Anda dapat menentukan tujuan keamanan Anda dengan

memilih paket aturan yang sesuai ketika Anda membuat templat penilaian Amazon Inspector. Untuk informasi selengkapnya, lihat Amazon Inspector Classic mengatur paket dan aturan.

Telemetri

Informasi paket yang diinstal dan konfigurasi perangkat lunak untuk instans EC2. Amazon Inspector mengumpulkan data selama penilaian berjalan.

# Batas layanan Amazon Inspector Classic

Tabel berikut menunjukkan batas Amazon Inspector Classic untuk akun AWS.

> **Important**
>
> Saat ini, target penilaian Anda hanya dapat terdiri dari instans EC2.

Berikut ini adalah batas Amazon Inspector Classic per akun AWS per wilayah:

| Resource | Batas Default | Comments |
|---|---|---|
| Instans dalam menjalankan penilaian | 500 | Jumlah maksimum instans EC2 yang dapat dimasukkan di semua penilaian berjalan per akun per wilayah. |
| Penilaian berjalan | 50000 | Jumlah maksimum penilaian berjalan yang dapat Anda buat per akun per wilayah. Anda dapat memiliki beberapa penilaian berjalan yang terjadi pada waktu yang sama selama target penilaian yang |

| Resource | Batas Default | Comments |
| --- | --- | --- |
| | | digunakan untuk proses ini tidak mengandung instans EC2 yang tumpang tindih. |
| Templat Penilaian | 500 | Jumlah maksimum templat penilaian yang dapat Anda miliki pada waktu tertentu per akun per wilayah. |
| Target Penilaian | 50 | Jumlah maksimum target penilaian yang dapat Anda miliki pada waktu tertentu per akun per wilayah. |

Kecuali dinyatakan lain, batas ini dapat ditingkatkan berdasarkan permintaan dengan menghubungi AWS Dukungan Center.

# Harga Amazon Inspector Classic

Harga Amazon Inspector Classic didasarkan pada jumlah instans EC2 yang disertakan dalam setiap penilaian dan paket aturan yang digunakan dalam penilaian tersebut.

## Harga untuk paket aturan jangkauan jaringan

Penilaian Amazon Inspector Classic dengan paket aturan jangkauan jaringan diberi harga per instans per penilaian (penilaian instans) per bulan. Misalnya, jika Anda menjalankan 1 penilaian terhadap 1 instance, itu adalah 1 instance-assessment. Jika Anda menjalankan 1 penilaian terhadap 10 instans, itu adalah 10 penilaian instans. Harga mulai dari $0.15 per instance-assessment per bulan dengan diskon volume untuk mencapai serendah $0.04 per instance-assessment per bulan.

### Detail uji coba gratis

| 90 hari pertama menggunakan Amazon Inspector Classic | Harga penilaian per instans |
|---|---|
| 250 penilaian contoh pertama | $0,00 |

### Detail harga

| Dalam bulan tertentu | Harga penilaian per instans |
|---|---|
| 250 penilaian contoh pertama | $0,15 |
| Berikutnya 750 instance-assessment | $0,13 |
| Selanjutnya 4.000 penilaian instans | $0,10 |
| Selanjutnya 45.000 penilaian instans | $0,07 |
| Semua penilaian contoh lainnya | $0,04 |

## Harga untuk paket aturan penilaian tuan rumah

Untuk kombinasi Common Vulnerabilities and Exposures (CVE), tolok ukur Center for Internet Security (CIS), Security Best Practices, dan Runtime Behavior Analysis yang disertakan dalam penilaian

Paket aturan penilaian host Amazon Inspector Classic menggunakan agen yang diterapkan di Instans Amazon EC2 yang menjalankan aplikasi yang ingin Anda nilai. Penilaian dengan paket aturan tuan rumah diberi harga per agen per penilaian (penilaian agen) per bulan. Misalnya, jika Anda menjalankan 1 penilaian terhadap 1 agen, itu adalah penilaian agen 1. Jika Anda menjalankan 1 penilaian terhadap 10 agen, itu adalah 10 penilaian agen. Harga mulai dari $0,30 per penilaian agen per bulan dengan diskon volume untuk mencapai serendah $0,05 per penilaian agen per bulan.

### Detail uji coba gratis

| 90 hari pertama menggunakan Amazon Inspector Classic | Harga per agen-penilaian |
|---|---|
| 250 penilaian agen pertama | $0,00 |

### Detail harga

| Dalam bulan tertentu | Harga per agen-penilaian |
|---|---|
| 250 penilaian agen pertama | $0,30 |
| Selanjutnya 750 penilaian agen | $0,25 |
| Selanjutnya 4.000 penilaian agen | $0,15 |
| Selanjutnya 45.000 penilaian agen | $0,10 |
| Semua penilaian agen lainnya | $0,05 |

## Amazon Inspector Classic mendukung sistem operasi dan Wilayah

Bab ini memberikan informasi tentang sistem operasi dan Wilayah AWS yang didukung Amazon Inspector Classic.

> **Important**
>
> Saat ini, target penilaian Amazon Inspector Classic hanya dapat terdiri dari instans EC2. Anda dapat menjalankan penilaian tanpa agen dengan paket aturan Keterjangkauan Jaringan pada setiap instans EC2 terlepas dari apa pun sistem operasinya.

Untuk informasi tentang paket aturan Amazon Inspector Classic yang tersedia di seluruh sistem operasi yang didukung, lihat. Paket aturan Amazon Inspector Classic untuk sistem operasi yang didukung

Topik



## Sistem operasi berbasis Linux yang didukung untuk agen Amazon Inspector Classic

Anda dapat menggunakan agen Amazon Inspector Classic pada instans 64-bit x86 dan Arm EC2. Agen tersebut kompatibel dengan versi sistem operasi berbasis Linux berikut ini:

- Contoh 64-bit x86
  - Amazon Linux 2
  - Amazon Linux (2018.03, 2017.09, 2017.03, 2016.09, 2016.03, 2015.09, 2015.03, 2014.09, 2014.03, 2013.09, 2013.03, 2012.09, 2012.03)
  - Ubuntu (20.04 LTS, 18.04 LTS, 16.04 LTS, 14.04 LTS)
  - Debian (10.x, 9.0 - 9.5, 8.0 - 8.7)
  - Red Hat Enterprise Linux (8.x, 7.2 - 7.x, 6.2 - 6.9)
  - CentOS (7.2 - 7.x, 6.2 - 6.9)
- Contoh lengan
  - Amazon Linux 2
  - Red Hat Enterprise Linux (7.6 - 7.x)
  - Ubuntu (18.04 LTS, 16.04 LTS)

## Sistem operasi berbasis Windows yang didukung untuk agen Amazon Inspector Classic

Anda dapat menggunakan agen Amazon Inspector Classic hanya pada instans EC2 yang menjalankan versi 64-bit dari sistem operasi berbasis Windows berikut:

- Windows Server 2019 Base
- Windows Server 2016 Base
- Windows Server 2012 R2

- Windows Server 2012
- Server Windows 2008 R2

## Wilayah AWS yang Didukung

Amazon Inspector Classic didukung di Wilayah AWS berikut:

- US East (Ohio) us-east-2
- US East (N. Virginia) us-east-1
- US West (N. California) us-west-1
- US West (Oregon) us-west-2
- Asia Pacific (Mumbai) ap-south-1
- Asia Pacific (Seoul) ap-northeast-2
- Asia Pacific (Sydney) ap-southeast-2
- Asia Pacific (Tokyo) ap-northeast-1
- Europe (Frankfurt) eu-central-1
- Europe (Ireland) eu-west-1
- Europe (London) eu-west-2
- Europe (Stockholm) eu-north-1
- AWS GovCloud (AS-Timur) -1 gov-us-east
- AWS GovCloud (AS-Barat) -1 gov-us-west

> **Note**
>
> Paket aturan Network Reachability tidak tersedia di Wilayah AWS GovCloud (AS).

# Pindah ke Amazon Inspector baru

Amazon Inspector baru sekarang tersedia secara global di. Wilayah AWS Amazon Inspector yang baru adalah versi yang sepenuhnya direkonstruksi dan didesain ulang dari Amazon Inspector yang ada, sekarang disebut Amazon Inspector Classic. Kemampuan berikut adalah penyempurnaan utama Amazon Inspector:

- Dibangun untuk skala - Amazon Inspector baru dibuat untuk skala dan lingkungan cloud yang dinamis. Tidak ada batasan jumlah instance atau gambar yang dapat dipindai di akun.
- Support untuk gambar kontainer - Amazon Inspector baru juga memindai gambar kontainer yang berada di Amazon Elastic Container Registry (Amazon ECR) untuk kerentanan perangkat lunak.
- Support untuk manajemen multi-akun - Amazon Inspector baru terintegrasi dengan Organizations. Ini memungkinkan Anda untuk mendelegasikan akun administrator untuk Amazon Inspector dari organisasi Anda. Akun administrator yang didelegasikan adalah akun terpusat yang menggabungkan semua temuan dan dapat mengonfigurasi semua akun anggota.
- Menggunakan AWS Systems Manager Agen (Agen SSM) - Dengan Amazon Inspector baru, Anda tidak perlu lagi menginstal dan memelihara agen Amazon Inspector yang berdiri sendiri di semua instans EC2 Anda. Amazon Inspector baru memanfaatkan Agen SSM yang digunakan secara luas.
- Pemindaian otomatis dan berkelanjutan — Dengan Amazon Inspector Classic, Anda secara manual mengatur target penilaian, templat penilaian, dan mengonfigurasi frekuensi penilaian. Namun, versi baru Amazon Inspector secara otomatis mendeteksi semua instans EC2 yang baru diluncurkan dan gambar kontainer yang memenuhi syarat yang didorong ke Amazon ECR dan segera memindai mereka untuk kerentanan perangkat lunak dan paparan jaringan yang tidak diinginkan. Sumber daya secara otomatis dipindai ulang berdasarkan beberapa pemicu, termasuk instans EC2 baru yang diluncurkan, gambar kontainer didorong ke Amazon ECR, pemasangan paket baru dalam instans EC2, pemasangan tambalan, atau publikasi Common Vulnerabilities and Exposure (CVE) baru yang memengaruhi sumber daya.
- Skor risiko Amazon Inspector - Amazon Inspector baru menghitung skor risiko Amazon Inspector untuk membantu memprioritaskan temuan Anda. Skor risiko dikalkuasi dengan menghubungkan informasi up-to-date CVE dengan faktor temporal dan lingkungan seperti aksesibilitas jaringan dan informasi eksploitasi.
- Integrasi lainnya — Semua temuan dikumpulkan dalam konsol Amazon Inspector yang baru dirancang dan didorong ke AWS Security Hub dan EventBridge Amazon untuk mengotomatiskan alur kerja, seperti tiket. Temuan terkait gambar kontainer juga didorong ke Amazon ECR.

Untuk mempelajari semua fitur dan harga Amazon Inspector baru, lihat Panduan Pengguna Amazon Inspector.

Meskipun kami akan terus mendukung Amazon Inspector Classic untuk beberapa waktu, dan pelanggan dapat menggunakan Amazon Inspector dan Amazon Inspector Classic baru di akun yang sama, kami sangat menyarankan Anda untuk bermigrasi ke Amazon Inspector yang baru. Bagian berikut memandu Anda melalui proses perpindahan dari Amazon Inspector Classic ke Amazon Inspector yang baru.

Topik



# Langkah 1: (Opsional) Laporan dan temuan penilaian ekspor

Untuk menyimpan laporan penilaian dan temuan di Amazon Inspector Classic, buat laporan penilaian.

Membuat laporan penilaian

1. Pada halaman Penilaian berjalan, cari penilaian berjalan yang ingin Anda buat laporannya. Pastikan statusnya adalah Analisis selesai.
2. Pada kolom Laporan untuk penilaian berjalan ini, pilih ikon laporan.

> **Important**
>
> Ikon laporan ada di kolom Laporan hanya untuk penilaian berjalan yang berlangsung atau akan berlangsung setelah 25 April 2017. Saat itulah laporan penilaian di Amazon Inspector Classic tersedia.

3. Di kotak dialog Laporan penilaian, pilih jenis laporan yang ingin Anda lihat (baik laporan temuan atau laporan lengkap) dan format laporan (HTML atau PDF). Kemudian pilih Buat laporan.

## Langkah 2: Hapus semua penilaian terjadwal yang berjalan di Amazon Inspector Classic

Untuk menonaktifkan Amazon Inspector Classic, hapus semua templat penilaian di akun Anda secara aktif. Wilayah AWS Menghapus templat penilaian menghentikan semua proses penilaian masa depan yang dijadwalkan.

Untuk menghapus templat penilaian

- Pada halaman Templat Penilaian, pilih templat yang ingin Anda hapus, lalu pilih Hapus. Ketika diminta konfirmasi, pilih Ya.

> **Important**
>
> Ketika Anda menghapus templat penilaian, semua penilaian berjalan, temuan, dan versi laporan yang terkait dengan templat ini juga akan dihapus.

## Langkah 3: Aktifkan Amazon Inspector baru

Anda dapat mengaktifkan Amazon Inspector baru menggunakan Amazon Inspector API AWS Management Console atau Amazon Inspector baru. Untuk memulai dengan Amazon Inspector baru, lihat Memulai di Panduan Pengguna Amazon Inspector.

# Memulai dengan Amazon Inspector Classic

Tutorial ini menunjukkan cara kepada Anda cara mengatur Amazon Inspector Classic dan memulai dengan membuat dan menjalankan penilaian pertama Anda.

## Pengaturan dalam satu klik

Prosedur berikut menunjukkan cara untuk membuat dan menjalankan penilaian otomatis menggunakan templat yang telah dibuat dan parameter penjadwalan yang telah ditentukan (seminggu sekali atau satu kali saja) pada semua instans Amazon Elastic Compute Cloud (Amazon EC2) yang tersedia di saat iniAkun AWS danWilayah AWS.

1. Masuk keAWS Management Console dan buka konsol Amazon Inspector Classic di https://console.aws.amazon.com/inspector/.
2. Pada halaman Selamat Datang, pilih jenis penilaian yang ingin Anda jalankan. Penilaian Jaringan menganalisis konfigurasi jaringanAWS lingkungan Anda untuk kelemahan, dan tidak memerlukan agen Amazon Inspector Classic. Penilaian Host menganalisis perangkat lunak pada host dan konfigurasi instans EC2 Anda untuk kelemahan, dan memerlukan agen untuk diinstal pada instans EC2.

   Pilih salah satu Jalankan mingguan (disarankan) atau Jalankan sekali. Segera setelah Anda memilih, layanan secara otomatis membuat penilaian untuk Anda. Secara khusus, layanan ini melakukan hal-hal berikut:

   a. Membuat peran tertaut layanan.

      > **Note**
      >
      > Untuk mengidentifikasi instans EC2 yang ditentukan dalam target penilaian, Amazon Inspector Classic perlu menghitung tanda dan instans EC2 Anda. Amazon Inspector Classic mendapat akses ke sumber daya ini di peran terkait layanan yang disebut`AWSServiceRoleForAmazonInspector`.Akun AWS Untuk informasi lebih lanjut tentang peran tertaut layanan, lihat Menggunakan peran terkait layanan untuk Amazon Inspector Classic dan Menggunakan Peran Tertaut Layanan.

   b. Jika berlaku, instal agen Amazon Inspector Classic pada semua instans EC2 yang tersedia di Wilayah AndaAkun AWS.

> **Note**
>
> Layanan menginstal agen Amazon Inspector Classic hanya pada instans EC2 yang memungkinkanAWS Systems Manager Run Command. Untuk menggunakan opsi ini, pastikan bahwa semua instans EC2 Anda dalam saat iniAkun AWS danWilayah AWS memiliki SSM Agent terinstal dan memiliki IAM role yang memungkinkan Run Command. Untuk informasi selengkapnya, lihat Menginstal agen pada beberapa EC2 instance menggunakan Systems Manager Run Command.

c. Menambahkan instans tersebut ke target penilaian.

d. Memasukkan target tersebut dalam templat penilaian dengan seperangkat standar paket aturan.

e. Menjalankan penilaian mingguan atau hanya sekali, tergantung pada apakah Anda memilih Jalankan mingguan (disarankan) atau Jalankan sekali.

3. Di kotak dialog Konfirmasi, pilih OK. Amazon Inspector Classic secara otomatis menjalankan penilaian Anda.

## Pengaturan lanjutan

Prosedur berikut menunjukkan cara untuk memilih instans Amazon EC2, paket aturan, dan parameter penjadwalan tertentu untuk dimasukkan ke target penilaian dan templat.

1. Pada halaman Selamat Datang, pilih Pengaturan lanjutan.
2. Pada halaman Tentukan target penilaian, masukkan nama target penilaian Anda.
3. Untuk Semua Instans, Anda dapat menyimpan kotak centang yang dipilih untuk memasukkan semua instans EC2 di WilayahAkun AWS dan Anda dalam target penilaian. Jika Anda ingin memilih instans EC2 mana yang akan dimasukkan, hapus kotak centang Semua Instans, dan masukkan tanda Kunci dan Nilai yang terkait dengan instans EC2 target. Untuk informasi lebih lanjut tentang penandaan instans EC2, lihat Penandaan Sumber Daya Amazon EC2 Anda.
4. Untuk Instal Agen, Anda dapat menyimpan kotak centang yang dipilih secara default jika instans Anda mengizinkan Systems Manager Run Command. Layanan menginstal agen Amazon Inspector Classic pada semua instans EC2 dalam target penilaian yang memungkinkanAWS Systems Manager. Untuk menggunakan opsi ini, pastikan bahwa semua instans EC2 Anda dalam saat iniAkun AWS danWilayah AWS memiliki SSM Agent terinstal dan memiliki IAM role yang memungkinkan Run Command. Untuk informasi selengkapnya, lihat Menginstal agen

pada beberapa EC2 instance menggunakan Systems Manager Run Command. Jika Anda ingin menginstal agen secara manual, lihat Menginstal Agen Amazon Inspector.

5. Pilih Selanjutnya.
6. Pada halaman Tentukan templat penilaian, masukkan nama templat penilaian Anda.
7. Untuk Paket aturan, pilih paket aturan yang akan dimasukkan di templat penilaian ini. Untuk informasi lebih lanjut tentang paket aturan, lihat Aturan dan Paket Aturan Amazon Inspector.
8. Untuk Durasi, pilih durasi penilaian berjalan Anda.
9. (Opsional) Untuk Jadwal Penilaian, atur jadwal untuk penilaian berjalan yang berulang.
10. Pilih Selanjutnya.
11. Pada halaman Tinjauan, tinjau pilihan Anda untuk target dan templat penilaian. Jika Anda puas dengan konfigurasinya, pilih Buat. Jika Anda menetapkan jadwal penilaian untuk templat penilaian Anda, penilaian berjalan secara otomatis setelah Anda memilih Buat.

> **Note**
>
> Untuk mengidentifikasi instans EC2 yang ditentukan dalam target penilaian, Amazon Inspector Classic perlu menghitung tanda dan instans EC2 Anda. Amazon Inspector Classic mendapat akses ke sumber daya ini di peran terkait layanan yang disebut`AWSServiceRoleForAmazonInspector`.Akun AWS Untuk informasi selengkapnya tentang penggunaan peran yang terhubung dengan lingkungan di Amazon Inspector Classic, lihatMenggunakan peran terkait layanan untuk Amazon Inspector Classic. Untuk informasi selengkapnya tentang penggunaan peran yang terhubung dengan layanan, lihat Menggunakan peran yang terhubung dengan layanan di PanduanAWS Identity and Access Management Pengguna.

12. Jika Anda tidak mengatur jadwal penilaian, arahkan ke templat penilaian Anda melalui konsol, lalu pilih Jalankan.
13. Untuk melacak progres penilaian berjalan, di panel navigasi konsol, pilih Penilaian berjalan, lalu pilih Temuan. Untuk informasi lebih lanjut tentang temuan, lihat Temuan Amazon Inspector Classic.

# Tutorial untuk Amazon Inspector Classic

Tutorial berikut menunjukkan cara melakukan penilaian Amazon Inspector Classic yang berjalan pada sistem operasi Red Hat Enterprise Linux dan Ubuntu.

Tutorial

- Tutorial: Menggunakan Amazon Inspector Classic dengan Red Hat Enterprise Linux
- Tutorial: Menggunakan Amazon Inspector Classic dengan Ubuntu Server

# Tutorial Amazon Inspector - Red Hat Enterprise Linux

Sebelum Anda mengikuti petunjuk di tutorial ini, kami merekomendasikan agar Anda terbiasa dengan Terminologi dan konsep Amazon Inspector.

Tutorial ini menunjukkan bagaimana menggunakan Amazon Inspector Classic untuk menganalisis perilaku instans EC2 yang menjalankan sistem operasi Red Hat Enterprise Linux 7.5. Ini memberikan petunjuk langkah demi langkah tentang cara menavigasi alur kerja Amazon Inspector Classic. Alur kerja termasuk mempersiapkan instans Amazon EC2, menjalankan templat penilaian, dan melakukan perbaikan keamanan yang direkomendasikan yang dihasilkan dalam temuan penilaian. Jika Anda adalah pengguna pertama kali dan ingin mengatur dan menjalankan penilaian Amazon Inspector Classic dengan satu klik, lihatMembuat Penilaian Dasar.

Topik

- Langkah 1: Mengatur instans Amazon EC2 untuk digunakan dengan Amazon Inspector Classic
- Langkah 2: Mengubah instans Amazon EC2
- Langkah 3: Membuat target penilaian dan menginstal agen pada instans EC2
- Langkah 4: Membuat dan menjalankan templat penilaian Anda
- Langkah 5: Mencari dan menganalisis temuan Anda
- Langkah 6: Menerapkan perbaikan yang direkomendasikan ke target penilaian Anda

## Langkah 1: Mengatur instans Amazon EC2 untuk digunakan dengan Amazon Inspector Classic

Untuk tutorial ini, buat satu instans EC2 yang menjalankan Red Hat Enterprise Linux 7.5, dan tandai menggunakan kunci Nama dan nilai **`InspectorEC2InstanceLinux`**.

> **Note**
>
> Untuk informasi lebih lanjut tentang penandaan instans EC2, lihat Sumber Daya dan Tanda.

## Langkah 2: Mengubah instans Amazon EC2

Untuk tutorial ini, Anda memodifikasi instans target EC2 Anda agar terekspos ke potensi masalah keamanan CVE-2018-1111. Untuk informasi lebih lanjut, lihat https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1111 dan Kelemahan dan eksposur umum.

Hubungkan ke instans Anda, **`InspectorEC2InstanceLinux`**, dan jalankan perintah berikut:

```
sudo yum install dhclient-12:4.2.5-68.el7
```

Untuk petunjuk tentang cara menghubungkan ke instans EC2, lihat Menghubungkan ke Instans Anda di Panduan Pengguna Amazon EC2.

## Langkah 3: Membuat target penilaian dan menginstal agen pada instans EC2

Amazon Inspector Classic menggunakan target penilaian untuk menunjuk sumber daya AWS yang ingin Anda evaluasi.

Untuk membuat target penilaian dan menginstal agen pada instans EC2

1. Masuk keAWS Management Consoledan buka konsol Amazon Inspector Classic dihttps://console.aws.amazon.com/inspector/.
2. Di panel navigasi, pilih Target penilaian, lalu pilih Buat.

   Lakukan hal berikut:

   a. Untuk Nama, masukkan nama untuk target penilaian Anda.

Untuk tutorial ini, masukkan **`MyTargetLinux`**.

b. Untuk Gunakan Tanda, pilih instans EC2 yang ingin Anda sertakan dalam target penilaian ini dengan memasukkan nilai untuk bidang Kunci dan Nilai.

   Untuk tutorial ini, pilih instans EC2 yang Anda buat pada langkah sebelumnya dengan memasukkan **`Name`** dalam bidang Kunci dan **`InspectorEC2InstanceLinux`** dalam bidang Nilai.

   Untuk menyertakan semua instans EC2 di akun AWS dan Daerah Anda di target penilaian, pilih kotak centang Semua Instans.

c. Pilih Save (Simpan).

d. Instal agen Amazon Inspector pada instans EC2 yang Anda tandai. Untuk menginstal agen pada semua instans EC2 yang termasuk dalam target penilaian, pilih kotak centang Instal Agen.

> **Note**
>
> Anda juga dapat menginstal agen Amazon Inspector menggunakanPerintah Operasi Pengelola Sistem AWS. Untuk menginstal agen pada semua instans dalam target penilaian, Anda dapat menentukan tanda yang sama yang Anda gunakan saat membuat target penilaian. Atau Anda dapat menginstal agen Amazon Inspector pada instans EC2 Anda secara manual. Untuk informasi lebih lanjut, lihat Menginstal agen Amazon Inspector Classic.

e. Pilih Simpan.

> **Note**
>
> Pada titik ini, Amazon Inspector membuat peran tertaut layanan yang disebut`AWSServiceRoleForAmazonInspector`. Peran tersebut memberikan Amazon Inspector Classic akses yang diperlukan untuk sumber daya Anda. Untuk informasi selengkapnya, lihat Membuat peran terkait layanan untuk Amazon Inspector Classic.

## Langkah 4: Membuat dan menjalankan templat penilaian Anda

Untuk membuat dan menjalankan templat Anda

1. Di panel navigasi, pilih Templat Penilaian, lalu pilih Buat.
2. Untuk Nama, masukkan nama untuk templat penilaian Anda. Untuk tutorial ini, masukkan **`MyFirstTemplateLinux`**.
3. Untuk Nama target, pilih target penilaian yang Anda buat di atas, **`MyTargetLinux`**.
4. Untuk Paket aturan, pilih paket aturan yang ingin Anda gunakan di templat penilaian ini.

   Untuk tutorial ini, pilih Kelemahan dan Eksposur Umum-1.1.
5. Untuk Durasi, tentukan durasi untuk templat penilaian Anda.

   Untuk tutorial ini, pilih 15 menit.
6. Pilih Buat dan jalankan.

## Langkah 5: Mencari dan menganalisis temuan Anda

Penilaian berjalan menghasilkan serangkaian temuan, atau potensi masalah keamanan yang ditemukan Amazon Inspector Classic dalam target penilaian Anda. Anda dapat meninjau temuan dan mengikuti langkah-langkah yang direkomendasikan untuk menyelesaikan potensi masalah keamanan.

Dalam tutorial ini, jika Anda menyelesaikan langkah-langkah sebelumnya, penilaian berjalan Anda menghasilkan temuan terhadap kelemahan umum CVE-2018-1111.

Untuk mencari dan menganalisis temuan Anda

1. Di panel navigasi, pilih Penilaian berjalan. Verifikasi bahwa status berjalan untuk templat penilaian yang disebut MyFirstTemplateLinux diatur ke Mengumpulkan data. Hal ini menunjukkan bahwa penilaian berjalan saat ini sedang berlangsung, dan data telemetri untuk target Anda sedang dikumpulkan dan dianalisis terhadap paket aturan yang dipilih.
2. Anda tidak dapat melihat temuan yang dihasilkan oleh penilaian berjalan saat masih berlangsung. Biarkan penilaian berjalan menyelesaikan seluruh durasinya. Namun, untuk tutorial ini, Anda bisa menghentikan prosesnya setelah beberapa menit.

Status MyFirstTemplateLinux berubah terlebih dahulu ke Menghentikan, kemudian dalam beberapa menit ke Menganalisis, dan akhirnya ke Analisis selesai. Untuk melihat perubahan status ini, pilih ikon Segarkan.

3. Di panel navigasi, pilih Temuan.

   Anda dapat melihat temuan baru untuk kepelikan Tinggi yang disebut Instans InspectorEC2InstanceLinux rentan terhadap CVE-2018-1111.

   > **Note**
   >
   > Jika Anda tidak melihat temuan baru, pilih ikon Segarkan.

   Untuk memperluas tampilan dan melihat detail temuan ini, pilih panah ke arah kiri temuan. Detail temuan tersebut mencakup hal-hal berikut:

   - ARN temuan
   - Nama penilaian berjalan yang menghasilkan temuan ini
   - Nama target penilaian yang menghasilkan temuan ini
   - Nama templat penilaian yang menghasilkan temuan ini
   - Waktu mulai penilaian berjalan
   - Waktu henti penilaian berjalan
   - Status penilaian berjalan
   - Nama paket aturan yang mencakup aturan yang memicu temuan ini
   - ID agen Amazon Inspector
   - Nama temuan
   - Kepelikan temuan
   - Deskripsi temuan
   - Rekomendasi langkah-langkah perbaikan yang dapat Anda selesaikan untuk memperbaiki potensi masalah keamanan yang diuraikan oleh temuan

## Langkah 6: Menerapkan perbaikan yang direkomendasikan ke target penilaian Anda

Untuk tutorial ini, Anda memodifikasi target penilaian Anda agar terekspos ke potensi masalah keamanan CVE-2018-1111. Dalam prosedur ini, Anda menerapkan perbaikan yang direkomendasikan untuk masalah tersebut.

Untuk menerapkan perbaikan ke target Anda

1. Terhubunglah ke instans **`InspectorEC2InstanceLinux`** yang Anda buat di bagian sebelumnya, dan jalankan perintah berikut:

   ```
   sudo yum update dhclient-12:4.2.5-68.el7
   ```

2. Pada halaman Templat penilaian, pilih MyFirstTemplateLinux, lalu pilih Jalankan untuk memulai penilaian berjalan baru menggunakan templat ini.
3. Ikuti langkah-langkah di Langkah 5: Mencari dan menganalisis temuan Anda untuk melihat temuan yang dihasilkan dari templat MyFirstTemplateLinux yang berjalan berikutnya.

   Karena Anda mengatasi masalah keamanan CVE-2018-1111, Anda seharusnya tidak lagi melihat temuan untuk hal ini.

# Tutorial Amazon Inspector

Sebelum Anda mengikuti petunjuk di tutorial ini, kami merekomendasikan agar Anda terbiasa dengan Terminologi dan konsep Amazon Inspector.

Tutorial ini menunjukkan bagaimana menggunakan Amazon Inspector Classic untuk menganalisis perilaku instans EC2 yang menjalankan sistem operasi Ubuntu Server 16.04 LTS. Ini memberikan petunjuk langkah demi langkah tentang cara menavigasi alur kerja Amazon Inspector.

Jika Anda adalah pengguna pertama kali dan ingin mengatur dan menjalankan penilaian Amazon Inspector dengan satu klik, lihatMembuat Penilaian Dasar.

Topik

- Langkah 1: Mengatur instans Amazon EC2 untuk digunakan dengan Amazon Inspector Classic
- Langkah 2: Membuat target penilaian dan menginstal agen pada instans EC2
- Langkah 3: Membuat dan menjalankan templat penilaian Anda

- Langkah 4: Mencari dan menganalisis temuan yang dihasilkan
- Langkah 5: Menerapkan perbaikan yang direkomendasikan ke target penilaian Anda

## Langkah 1: Mengatur instans Amazon EC2 untuk digunakan dengan Amazon Inspector Classic

Untuk mengatur instans EC2

- Untuk tutorial ini, membuat satu instans EC2 menjalankan Ubuntu Server 16.04 LTS dan menandainya menggunakan kunci Nama dan nilai **`InspectorEC2InstanceUbuntu`**.

> **Note**
>
> Untuk informasi lebih lanjut tentang penandaan instans EC2, lihat Sumber Daya dan Tanda.

## Langkah 2: Membuat target penilaian dan menginstal agen pada instans EC2

Amazon Inspector menggunakan target penilaian untuk menunjuk sumber daya AWS yang akan dievaluasi.

Untuk membuat target penilaian dan menginstal agen pada instans EC2

1. Masuk keAWS Management Consoledan buka konsol Amazon Inspector Classic dihttps://console.aws.amazon.com/inspector/.
2. Di panel navigasi, pilih Target penilaian, lalu pilih Buat.
3. Untuk Nama, masukkan nama untuk target penilaian Anda.

   Untuk tutorial ini, ketikkan **`MyTargetUbuntu`**.
4. Untuk Gunakan Tanda, pilih instans EC2 yang ingin Anda sertakan dalam target penilaian ini dengan memasukkan nilai untuk bidang Kunci dan Nilai.

   Untuk tutorial ini, pilih instans EC2 yang Anda buat pada langkah sebelumnya dengan memasukkan **`Name`** dalam bidang Kunci dan **`InspectorEC2InstanceUbuntu`** dalam bidang Nilai.

Untuk menyertakan semua instans EC2 di akun AWS dan Daerah Anda di target penilaian, pilih kotak Semua Instans.

5. Instal Agen Amazon Inspector pada instans EC2 yang Anda tandai. Untuk menginstal agen pada semua instans EC2 yang termasuk dalam target penilaian, pilih kotak Instal Agen.

> **Note**
>
> Anda juga dapat menginstal Agen Amazon Inspector menggunakan Systems Manager Run Command. Untuk menginstal agen pada semua instans dalam target penilaian, Anda dapat menentukan tanda yang sama yang digunakan untuk membuat target penilaian. Atau Anda dapat menginstal Agen Amazon Inspector pada instans EC2 Anda secara manual. Untuk informasi lebih lanjut, lihat Menginstal agen Amazon Inspector Classic.

6. Pilih Simpan.

> **Note**
>
> Pada titik ini, peran tertaut layanan yang disebut`AWSServiceRoleForAmazonInspector`dibuat untuk memberi Amazon Inspector akses ke sumber daya Anda. Untuk informasi selengkapnya, lihat Membuat peran terkait layanan untuk Amazon Inspector Classic.

## Langkah 3: Membuat dan menjalankan templat penilaian Anda

Untuk membuat dan menjalankan templat Anda

1. Jika Anda menggunakan Pengaturan lanjutan, Anda akan diarahkan ke halaman Tentukan templat penilaian. Jika tidak, navigasikan ke halaman Templat penilaian, lalu pilih Buat.
2. Untuk Nama, masukkan nama untuk templat penilaian Anda. Untuk tutorial ini, masukkan **`MyFirstTemplateUbuntu`**.
3. Untuk Nama target, pilih target penilaian yang Anda buat di atas, **`MyTargetUbuntu`**.
4. Untuk Paket aturan, gunakan menu tarik turun untuk memilih paket aturan yang ingin Anda gunakan di templat penilaian ini.

Untuk tutorial ini, pilih Kelemahan dan Eksposur Umum-1.1.

5. Untuk Durasi, tentukan durasi untuk templat penilaian Anda.

   Untuk tutorial ini, pilih 15 menit.

6. Jika Anda menggunakan Pengaturan lanjutan, pilih Selanjutnya. Pada halaman Tinjauan berikut, pilih Buat. Atau, pilih Buat dan jalankan.

## Langkah 4: Mencari dan menganalisis temuan yang dihasilkan

Penilaian berjalan yang telah selesai menghasilkan serangkaian temuan, atau potensi masalah keamanan yang ditemukan Amazon Inspector di target penilaian Anda. Anda dapat meninjau temuan dan mengikuti langkah-langkah yang direkomendasikan untuk menyelesaikan potensi masalah keamanan.

1. Navigasikan ke halaman Penilaian Berjalan. Verifikasi bahwa status berjalan untuk templat penilaian yang disebut MyFirstTemplateUbuntu yang Anda buat dalam langkah sebelumnya telah diatur ke Mengumpulkan data. Hal ini menunjukkan bahwa penilaian berjalan saat ini sedang berlangsung, dan data telemetri untuk target Anda sedang dikumpulkan dan dianalisis terhadap paket aturan yang dipilih.
2. Anda tidak dapat melihat temuan yang dihasilkan oleh penilaian berjalan saat masih berlangsung. Biarkan penilaian berjalan menyelesaikan seluruh durasinya.

   Status MyFirstTemplateUbuntu berubah terlebih dahulu ke Menghentikan, kemudian dalam beberapa menit ke Menganalisis, dan akhirnya ke Analisis selesai. Untuk melihat perubahan status ini, pilih ikon Segarkan.

3. Navigasikan ke halaman Temuan.

   Untuk memperluas tampilan dan melihat detail temuan, pilih panah ke arah kiri temuan. Detail temuan tersebut mencakup hal-hal berikut:

   - ARN temuan
   - Nama penilaian berjalan yang menghasilkan temuan ini
   - Nama target penilaian yang menghasilkan temuan ini
   - Nama templat penilaian yang menghasilkan temuan ini
   - Waktu mulai penilaian berjalan

- Waktu henti penilaian berjalan
- Status penilaian berjalan
- Nama paket aturan yang mencakup aturan yang memicu temuan
- ID agen Amazon Inspector
- Nama temuan
- Kepelikan temuan
- Deskripsi temuan
- Rekomendasi langkah-langkah perbaikan yang dapat Anda selesaikan untuk memperbaiki potensi masalah keamanan yang diuraikan oleh temuan

## Langkah 5: Menerapkan perbaikan yang direkomendasikan ke target penilaian Anda

Dalam prosedur ini, Anda menerapkan pembaruan untuk memperbaiki masalah yang ditemukan.

1. Hubungkan ke instans **`InspectorEC2InstanceUbuntu`** Anda, dan lakukan pembaruan paket.
2. Pada halaman Templat penilaian, MyFirstTemplateUbuntu, lalu pilih Jalankan untuk memulai proses berjalan baru menggunakan templat ini.
3. Ikuti langkah-langkah di Langkah 4: Mencari dan menganalisis temuan yang dihasilkan untuk melihat temuan yang dihasilkan dari templat MyFirstTemplateUbuntu yang berjalan berikutnya.

   Pembaruan paket harus telah menyelesaikan temuan dari proses berjalan pertama templat.

# Keamanan di Amazon Inspector Classic

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

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

- Keamanan cloud — AWS bertanggung jawab untuk melindungi infrastruktur yang menjalankan AWS layanan di AWS Cloud. AWS juga memberi Anda layanan yang dapat Anda gunakan dengan aman. Auditor pihak ketiga secara teratur menguji dan memverifikasi efektivitas keamanan kami sebagai bagian dari Program AWS Kepatuhan Program AWS Kepatuhan . Untuk mempelajari tentang program kepatuhan yang berlaku untuk Amazon Inspector Classic, lihat AWSLayanan 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 Classic. Topik berikut menunjukkan cara mengonfigurasi Amazon Inspector Classic 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 Classic Anda.

Topik

- Praktik terbaik keamanan untuk Amazon Inspector Classic

# Perlindungan data di Amazon Inspector Classic

Model tanggung jawab AWS bersama model berlaku untuk perlindungan data di Amazon Inspector Classic. Seperti yang dijelaskan dalam model AWS ini, bertanggung jawab untuk melindungi infrastruktur global yang menjalankan semua AWS Cloud. Anda bertanggung jawab untuk mempertahankan kendali atas konten yang di-host pada infrastruktur ini. Anda juga bertanggung jawab atas tugas-tugas konfigurasi dan manajemen keamanan untuk Layanan AWS yang Anda gunakan. Untuk informasi selengkapnya tentang privasi data, lihat Privasi Data FAQ. Untuk informasi tentang perlindungan data di Eropa, lihat Model Tanggung Jawab AWS Bersama dan posting GDPR blog di Blog AWS Keamanan.

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 otentikasi multi-faktor (MFA) dengan setiap akun.
- GunakanSSL/TLSuntuk berkomunikasi dengan AWS sumber daya. Kami membutuhkan TLS 1.2 dan merekomendasikan TLS 1.3.
- Siapkan API dan pencatatan aktivitas pengguna dengan AWS CloudTrail. Untuk informasi tentang penggunaan CloudTrail jejak untuk menangkap AWS aktivitas, lihat Bekerja dengan CloudTrail jejak di AWS CloudTrail Panduan Pengguna.
- Gunakan solusi AWS enkripsi, bersama dengan semua kontrol keamanan default di dalamnya Layanan AWS.
- Gunakan layanan keamanan terkelola tingkat lanjut seperti Amazon Macie, yang membantu menemukan dan mengamankan data sensitif yang disimpan di Amazon S3.
- Jika Anda memerlukan FIPS 140-3 modul kriptografi yang divalidasi saat mengakses AWS melalui antarmuka baris perintah atau, gunakan titik akhir. API FIPS Untuk informasi selengkapnya tentang FIPS titik akhir yang tersedia, lihat Federal Information Processing Standard (FIPS) 140-3.

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 Classic atau lainnya Layanan AWS menggunakan konsol,, API AWS CLI, atau. AWS SDKs 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. Jika Anda memberikan URL ke server eksternal, kami sangat menyarankan agar Anda tidak menyertakan informasi kredensil dalam URL untuk memvalidasi permintaan Anda ke server tersebut.

Topik



## Enkripsi data saat tidak digunakan

Data telemetri yang dihasilkan agen Amazon Inspector Classic selama penilaian dijalankan diformat dalam file. JSON File-file ini dikirim near-real-time TLS ke Amazon Inspector Classic, di mana mereka dienkripsi dengan kunci turunan fana. per-assessment-run AWS KMS

File disimpan dengan aman di bucket S3 yang didedikasikan untuk Amazon Inspector Classic. Mesin aturan Amazon Inspector Classic melakukan hal berikut:

- Mengakses data telemetri terenkripsi dalam bucket S3
- Mendekripsi dalam memori
- Memproses data terhadap aturan penilaian yang dikonfigurasi untuk menghasilkan temuan

## Mengenkripsi data saat transit

Sebagai layanan terkelola, Amazon Inspector Classic 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 API panggilan yang AWS dipublikasikan untuk mengakses Amazon Inspector Classic melalui jaringan. Klien harus mendukung hal-hal berikut:

- Keamanan Lapisan Transportasi (TLS). Kami membutuhkan TLS 1.2 dan merekomendasikan TLS 1.3.

- Suite cipher dengan kerahasiaan maju yang sempurna (PFS) seperti (Ephemeral Diffie-Hellman) atau DHE (Elliptic Curve Ephemeral Diffie-Hellman). ECDHE Sebagian besar sistem modern seperti Java 7 dan setelahnya mendukung mode ini.

Selain itu, permintaan harus ditandatangani menggunakan access key ID dan secret access key yang terkait dengan IAM utama. Atau Anda dapat menggunakan AWS Security Token Service (AWS STS) untuk membuat kredensial keamanan sementara untuk menandatangani permintaan.

# Identity and Access Management untuk Amazon Inspector Classic

AWS Identity and Access Management (IAM) adalah Layanan AWS yang membantu administrator mengontrol akses ke AWS sumber daya dengan aman. IAMadministrator mengontrol siapa yang dapat diautentikasi (masuk) dan diberi wewenang (memiliki izin) untuk menggunakan sumber daya Amazon Inspector. IAMadalah Layanan AWS yang dapat Anda gunakan tanpa biaya tambahan.

Topik

- Menggunakan peran terkait layanan untuk Amazon Inspector Classic
- Memecahkan masalah identitas dan akses Amazon Inspector Classic

## 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 Memecahkan masalah identitas dan akses Amazon Inspector Classic.

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. Anda kemudian harus mengirimkan permintaan ke administrator IAM Anda untuk mengubah izin pengguna layanan Anda. Tinjau informasi di halaman ini untuk memahami konsep basic IAM. Untuk mempelajari lebih lanjut tentang bagaimana perusahaan Anda dapat menggunakan IAM Amazon Inspector, lihat. Bagaimana Amazon Inspector Classic bekerja dengan IAM

IAMadministrator - Jika Anda seorang IAM administrator, Anda mungkin ingin mempelajari detail tentang cara menulis kebijakan untuk mengelola akses ke Amazon Inspector. Untuk melihat contoh kebijakan berbasis identitas Amazon Inspector yang dapat Anda gunakan, lihat. IAM Contoh kebijakan berbasis identitas untuk Amazon Inspector Classic

## Mengautentikasi dengan identitas

Otentikasi adalah cara Anda masuk AWS menggunakan kredensi identitas Anda. Anda harus diautentikasi (masuk ke AWS) sebagai Pengguna root akun AWS, sebagai IAM pengguna, atau dengan mengambil peranIAM.

Anda dapat masuk AWS sebagai identitas federasi dengan menggunakan kredensi yang disediakan melalui sumber identitas. AWS IAM Identity Center Pengguna (Pusat IAM Identitas), autentikasi masuk tunggal perusahaan Anda, dan kredensi Google atau Facebook Anda adalah contoh identitas federasi. Saat Anda masuk sebagai identitas federasi, administrator Anda sebelumnya menyiapkan

federasi identitas menggunakan IAM peran. Ketika Anda mengakses AWS dengan menggunakan federasi, Anda secara tidak langsung mengambil peran.

Bergantung pada jenis pengguna Anda, Anda dapat masuk ke AWS Management Console atau portal AWS akses. Untuk informasi selengkapnya tentang masuk AWS, lihat Cara masuk ke Panduan AWS Sign-In Pengguna Anda Akun AWS.

Jika Anda mengakses AWS secara terprogram, AWS sediakan kit pengembangan perangkat lunak (SDK) dan antarmuka baris perintah (CLI) untuk menandatangani permintaan Anda secara kriptografis dengan menggunakan kredensil Anda. Jika Anda tidak menggunakan AWS alat, Anda harus menandatangani permintaan sendiri. Untuk informasi selengkapnya tentang menggunakan metode yang disarankan untuk menandatangani permintaan sendiri, lihat Versi AWS Tanda Tangan 4 untuk API permintaan di Panduan IAM Pengguna.

Apa pun metode autentikasi yang digunakan, Anda mungkin diminta untuk menyediakan informasi keamanan tambahan. Misalnya, AWS merekomendasikan agar Anda menggunakan otentikasi multi-faktor (MFA) untuk meningkatkan keamanan akun Anda. Untuk mempelajari selengkapnya, lihat Autentikasi multi-faktor di Panduan AWS IAM Identity Center Pengguna dan Autentikasi AWS multi-faktor IAM di 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. Lindungi kredensial pengguna root Anda dan gunakan kredensial tersebut untuk melakukan tugas yang hanya dapat dilakukan pengguna root. Untuk daftar lengkap tugas yang mengharuskan Anda masuk sebagai pengguna root, lihat Tugas yang memerlukan kredensi pengguna root di IAMPanduan Pengguna.

### Identitas gabungan

Sebagai praktik terbaik, mewajibkan pengguna manusia, termasuk pengguna yang memerlukan akses administrator, untuk menggunakan federasi dengan penyedia identitas untuk mengakses Layanan AWS dengan menggunakan kredensi sementara.

Identitas federasi adalah pengguna dari direktori pengguna perusahaan Anda, penyedia identitas web, direktori Pusat Identitas AWS Directory Service, atau pengguna mana pun yang mengakses Layanan AWS dengan menggunakan kredensil yang disediakan melalui sumber identitas. Ketika

identitas federasi mengakses Akun AWS, mereka mengambil peran, dan peran memberikan kredensi sementara.

Untuk manajemen akses terpusat, kami sarankan Anda menggunakan AWS IAM Identity Center. Anda dapat membuat pengguna dan grup di Pusat IAM Identitas, 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 IAM Identitas, lihat Apa itu Pusat IAM Identitas? dalam AWS IAM Identity Center User Guide.

## Pengguna dan grup IAM

IAMPengguna adalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus untuk satu orang atau aplikasi. Jika memungkinkan, sebaiknya mengandalkan kredensi sementara daripada membuat IAM pengguna yang memiliki kredensi jangka panjang seperti kata sandi dan kunci akses. Namun, jika Anda memiliki kasus penggunaan khusus yang memerlukan kredensil jangka panjang dengan IAM pengguna, kami sarankan Anda memutar kunci akses. Untuk informasi selengkapnya, lihat Memutar kunci akses secara teratur untuk kasus penggunaan yang memerlukan kredensi jangka panjang di IAMPanduan Pengguna.

IAMGrup adalah identitas yang menentukan kumpulan IAM pengguna. Anda tidak dapat masuk sebagai grup. Anda dapat menggunakan grup untuk menentukan izin bagi beberapa pengguna sekaligus. Grup mempermudah manajemen izin untuk sejumlah besar pengguna sekaligus. Misalnya, Anda dapat memiliki grup bernama IAMAdminsdan memberikan izin grup tersebut untuk mengelola sumber dayaIAM.

Pengguna berbeda dari peran. Pengguna secara unik terkait dengan satu orang atau aplikasi, tetapi peran dimaksudkan untuk dapat digunakan oleh siapa pun yang membutuhkannya. Pengguna memiliki kredensial jangka panjang permanen, tetapi peran memberikan kredensial sementara. Untuk mempelajari selengkapnya, lihat Kasus penggunaan untuk IAM pengguna di Panduan IAM Pengguna.

## Peran IAM

IAMPeran adalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus. Ini mirip dengan IAM pengguna, tetapi tidak terkait dengan orang tertentu. Untuk mengambil IAM peran sementara di dalam AWS Management Console, Anda dapat beralih dari pengguna ke IAM peran (konsol). Anda dapat mengambil peran dengan memanggil AWS CLI atau AWS API operasi atau dengan menggunakan kustomURL. Untuk informasi selengkapnya tentang metode penggunaan peran, lihat Metode untuk mengambil peran dalam Panduan IAM Pengguna.

IAMperan dengan kredensi sementara berguna dalam situasi berikut:

- Akses pengguna terfederasi – Untuk menetapkan izin ke identitas terfederasi, Anda membuat peran dan menentukan izin untuk peran tersebut. Ketika identitas terfederasi mengautentikasi, identitas tersebut terhubung dengan peran dan diberi izin yang ditentukan oleh peran. Untuk informasi tentang peran untuk federasi, lihat Membuat peran untuk penyedia identitas pihak ketiga (federasi) di Panduan IAM Pengguna. Jika Anda menggunakan Pusat IAM Identitas, Anda mengonfigurasi set izin. Untuk mengontrol apa yang dapat diakses identitas Anda setelah diautentikasi, Pusat IAM Identitas mengkorelasikan izin yang disetel ke peran. IAM Untuk informasi tentang set izin, lihat Set izin dalam Panduan Pengguna AWS IAM Identity Center .
- Izin IAM pengguna sementara — IAM Pengguna atau peran dapat mengambil IAM peran untuk sementara mengambil izin yang berbeda untuk tugas tertentu.
- Akses lintas akun — Anda dapat menggunakan IAM peran untuk memungkinkan seseorang (prinsipal tepercaya) di akun lain mengakses sumber daya di akun Anda. Peran adalah cara utama untuk memberikan akses lintas akun. Namun, dengan beberapa Layanan AWS, Anda dapat melampirkan kebijakan secara langsung ke sumber daya (alih-alih menggunakan peran sebagai proxy). Untuk mempelajari perbedaan antara peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Akses sumber daya lintas akun di IAM Panduan Pengguna. IAM
- Akses lintas layanan — Beberapa Layanan AWS menggunakan fitur lain Layanan AWS. Misalnya, saat Anda melakukan panggilan dalam suatu layanan, biasanya layanan tersebut menjalankan aplikasi di Amazon EC2 atau menyimpan objek di Amazon S3. Sebuah layanan mungkin melakukannya menggunakan izin prinsipal yang memanggil, menggunakan peran layanan, atau peran terkait layanan.
  - Sesi akses teruskan (FAS) — Saat Anda menggunakan IAM pengguna atau peran 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. FASmenggunakan izin dari pemanggilan utama Layanan AWS, dikombinasikan dengan permintaan Layanan AWS untuk membuat permintaan ke layanan hilir. FASPermintaan 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 saat membuat FAS permintaan, lihat Meneruskan sesi akses.
  - Peran layanan — Peran layanan adalah IAMperan yang diasumsikan layanan untuk melakukan tindakan atas nama Anda. IAMAdministrator dapat membuat, memodifikasi, dan menghapus peran layanan dari dalamIAM. Untuk informasi selengkapnya, lihat Membuat peran untuk mendelegasikan izin ke Layanan AWS dalam IAMPanduan Pengguna.

  - Peran terkait layanan — Peran terkait layanan adalah jenis peran layanan yang ditautkan ke peran layanan. Layanan AWS Layanan tersebut dapat menjalankan peran untuk melakukan tindakan atas nama Anda. Peran terkait layanan muncul di Anda Akun AWS dan dimiliki oleh layanan. IAMAdministrator dapat melihat, tetapi tidak mengedit izin untuk peran terkait layanan.
- Aplikasi yang berjalan di Amazon EC2 — Anda dapat menggunakan IAM peran untuk mengelola kredenal sementara untuk aplikasi yang berjalan pada EC2 instance dan membuat AWS CLI atau AWS API meminta. Ini lebih baik untuk menyimpan kunci akses dalam EC2 instance. Untuk menetapkan AWS peran ke EC2 instance dan membuatnya tersedia untuk semua aplikasinya, Anda membuat profil instance yang dilampirkan ke instance. Profil instance berisi peran dan memungkinkan program yang berjalan pada EC2 instance untuk mendapatkan kredensi sementara. Untuk informasi selengkapnya, lihat Menggunakan IAM peran untuk memberikan izin ke aplikasi yang berjalan di EC2 instans Amazon di IAMPanduan Pengguna.

## 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 JSON dokumen. Untuk informasi selengkapnya tentang struktur dan isi dokumen JSON kebijakan, lihat Ringkasan JSON kebijakan di Panduan IAM Pengguna.

Administrator dapat menggunakan AWS JSON kebijakan untuk menentukan siapa yang memiliki akses ke apa. Yaitu, principal dapat melakukan tindakan pada suatu sumber daya, dan dalam suatu syarat.

Secara default, pengguna dan peran tidak memiliki izin. Untuk memberikan izin kepada pengguna untuk melakukan tindakan pada sumber daya yang mereka butuhkan, IAM administrator dapat membuat IAM kebijakan. Administrator kemudian dapat menambahkan IAM kebijakan ke peran, dan pengguna dapat mengambil peran.

Kebijakan IAM mendefinisikan izin untuk tindakan terlepas dari metode yang Anda gunakan untuk melakukan operasi. Misalnya, anggaplah Anda memiliki kebijakan yang mengizinkan tindakan `iam:GetRole`. Pengguna dengan kebijakan itu bisa mendapatkan informasi peran dari AWS Management Console, AWS CLI, atau AWS API.

## Kebijakan berbasis identitas

Kebijakan berbasis identitas adalah dokumen kebijakan JSON izin yang dapat Anda lampirkan ke identitas, seperti pengguna, grup IAM pengguna, atau peran. Kebijakan ini mengontrol jenis tindakan yang dapat dilakukan oleh pengguna dan peran, di sumber daya mana, dan berdasarkan kondisi seperti apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat Menentukan IAM izin khusus dengan kebijakan yang dikelola pelanggan di Panduan Pengguna. IAM

Kebijakan berbasis identitas dapat dikategorikan lebih lanjut sebagai kebijakan inline atau kebijakan yang dikelola. Kebijakan inline disematkan langsung ke satu pengguna, grup, atau peran. Kebijakan terkelola adalah kebijakan mandiri yang dapat Anda lampirkan ke beberapa pengguna, grup, dan peran dalam. Akun AWS Kebijakan AWS terkelola mencakup kebijakan terkelola dan kebijakan yang dikelola pelanggan. Untuk mempelajari cara memilih antara kebijakan terkelola atau kebijakan sebaris, lihat Memilih antara kebijakan terkelola dan kebijakan sebaris di IAMPanduan Pengguna.

## Kebijakan berbasis sumber daya

Kebijakan berbasis sumber daya adalah dokumen JSON kebijakan yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah kebijakan kepercayaan IAM peran dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Untuk sumber daya tempat kebijakan dilampirkan, kebijakan menentukan tindakan apa yang dapat dilakukan oleh prinsipal tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus menentukan prinsipal dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau. Layanan AWS

Kebijakan berbasis sumber daya merupakan kebijakan inline yang terletak di layanan tersebut. Anda tidak dapat menggunakan kebijakan AWS terkelola IAM dalam kebijakan berbasis sumber daya.

## Daftar kontrol akses (ACLs)

Access control lists (ACLs) mengontrol prinsipal mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACLsmirip dengan kebijakan berbasis sumber daya, meskipun mereka tidak menggunakan format dokumen kebijakan. JSON

Amazon S3, AWS WAF, dan Amazon VPC adalah contoh layanan yang mendukung. ACLs Untuk mempelajari selengkapnyaACLs, lihat Ikhtisar daftar kontrol akses (ACL) di Panduan Pengembang Layanan Penyimpanan Sederhana Amazon.

## Jenis-jenis kebijakan lain

AWS mendukung jenis kebijakan tambahan yang kurang umum. Jenis-jenis kebijakan ini dapat mengatur izin maksimum yang diberikan kepada Anda oleh jenis kebijakan yang lebih umum.

- Batas izin — Batas izin adalah fitur lanjutan tempat Anda menetapkan izin maksimum yang dapat diberikan oleh kebijakan berbasis identitas kepada entitas (pengguna atau peran). IAM IAM Anda dapat menetapkan batasan izin untuk suatu entitas. Izin yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas milik entitas dan batasan izinnya. Kebijakan berbasis sumber daya yang menentukan pengguna atau peran dalam bidang `Principal` tidak dibatasi oleh batasan izin. Penolakan eksplisit dalam salah satu kebijakan ini akan menggantikan pemberian izin. Untuk informasi selengkapnya tentang batas izin, lihat Batas izin untuk IAM entitas di IAMPanduan Pengguna.
- Kebijakan kontrol layanan (SCPs) — SCPs adalah JSON kebijakan 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 (SCPs) ke salah satu atau semua akun Anda. SCPMembatasi izin untuk entitas di akun anggota, termasuk masing-masing Pengguna root akun AWS. Untuk informasi selengkapnya tentang Organizations danSCPs, lihat Kebijakan kontrol layanan di Panduan AWS Organizations Pengguna.
- Kebijakan kontrol sumber daya (RCPs) — RCPs adalah JSON kebijakan yang dapat Anda gunakan untuk menetapkan izin maksimum yang tersedia untuk sumber daya di akun Anda tanpa memperbarui IAM kebijakan yang dilampirkan ke setiap sumber daya yang Anda miliki. RCPMembatasi izin untuk sumber daya di akun anggota dan dapat memengaruhi izin efektif untuk identitas, termasuk Pengguna root akun AWS, terlepas dari apakah itu milik organisasi Anda. Untuk informasi selengkapnya tentang Organizations danRCPs, termasuk daftar dukungan Layanan AWS tersebutRCPs, lihat Kebijakan kontrol sumber daya (RCPs) di Panduan AWS Organizations Pengguna.
- Kebijakan sesi – Kebijakan sesi adalah kebijakan lanjutan yang Anda berikan sebagai parameter ketika Anda membuat sesi sementara secara programatis untuk peran atau pengguna terfederasi. Izin sesi yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas pengguna atau peran dan kebijakan sesi. Izin juga bisa datang dari kebijakan berbasis sumber daya. Penolakan secara tegas dalam salah satu kebijakan ini membatalkan izin. Untuk informasi selengkapnya, lihat Kebijakan sesi di Panduan IAM Pengguna.

### Berbagai jenis kebijakan

Ketika beberapa jenis kebijakan berlaku pada suatu permintaan, izin yang dihasilkan lebih rumit untuk dipahami. Untuk mempelajari cara AWS menentukan apakah akan mengizinkan permintaan saat beberapa jenis kebijakan terlibat, lihat Logika evaluasi kebijakan di Panduan IAM Pengguna.

## Bagaimana Amazon Inspector Classic bekerja dengan IAM

Sebelum Anda menggunakan IAM untuk mengelola akses ke Amazon Inspector, pelajari IAM fitur apa saja yang tersedia untuk digunakan dengan Amazon Inspector.

IAMfitur yang dapat Anda gunakan dengan Amazon Inspector Classic

| IAMfitur | 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 |
| ACLs | Tidak |
| ABAC(tag dalam kebijakan) | Parsial |
| Kredensial sementara | Ya |
| Izin principal | Ya |
| Peran layanan | Tidak |
| Peran terkait layanan | Ya |

Untuk mendapatkan tampilan tingkat tinggi tentang cara kerja Amazon Inspector dan layanan AWS lainnya dengan IAM sebagian besar fitur, AWS lihat layanan yang berfungsi di IAM Panduan PenggunaIAM.

## Kebijakan berbasis identitas untuk Amazon Inspector

Mendukung kebijakan berbasis identitas: Ya

Kebijakan berbasis identitas adalah dokumen kebijakan JSON izin yang dapat Anda lampirkan ke identitas, seperti pengguna, grup IAM pengguna, atau peran. Kebijakan ini mengontrol jenis tindakan yang dapat dilakukan oleh pengguna dan peran, di sumber daya mana, dan berdasarkan kondisi seperti apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat Menentukan IAM izin khusus dengan kebijakan yang dikelola pelanggan di Panduan Pengguna. IAM

Dengan kebijakan IAM berbasis identitas, Anda dapat menentukan tindakan dan sumber daya yang diizinkan atau ditolak serta kondisi di mana tindakan diizinkan atau ditolak. Anda tidak dapat menentukan secara spesifik prinsipal dalam sebuah kebijakan berbasis identitas karena prinsipal berlaku bagi pengguna atau peran yang melekat kepadanya. Untuk mempelajari semua elemen yang dapat Anda gunakan dalam JSON kebijakan, lihat referensi elemen IAM JSON kebijakan di Panduan IAM Pengguna.

Contoh kebijakan berbasis identitas untuk Amazon Inspector

Untuk melihat contoh kebijakan berbasis identitas Amazon Inspector, lihat Contoh kebijakan berbasis identitas untuk Amazon Inspector Classic.

## Kebijakan berbasis sumber daya dalam Amazon Inspector

Mendukung kebijakan berbasis sumber daya: Tidak

Kebijakan berbasis sumber daya adalah dokumen JSON kebijakan yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah kebijakan kepercayaan IAM peran dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Untuk sumber daya tempat kebijakan dilampirkan, kebijakan menentukan tindakan apa yang dapat dilakukan oleh prinsipal tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus menentukan prinsipal dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau. Layanan AWS

Untuk mengaktifkan akses lintas akun, Anda dapat menentukan seluruh akun atau entitas IAM di akun lain sebagai penanggung jawab kebijakan berbasis sumber daya. Menambahkan prinsipal akun silang ke kebijakan berbasis sumber daya hanya setengah dari membangun hubungan kepercayaan. Ketika prinsipal dan sumber daya berbeda Akun AWS, IAM administrator di akun tepercaya juga harus memberikan izin entitas utama (pengguna atau peran) untuk mengakses sumber daya. Mereka memberikan izin dengan melampirkan kebijakan berbasis identitas kepada entitas. Namun, jika kebijakan berbasis sumber daya memberikan akses ke principal dalam akun yang sama, tidak diperlukan kebijakan berbasis identitas tambahan. Untuk informasi selengkapnya, lihat Akses sumber daya lintas akun IAM di Panduan IAM Pengguna.

## Tindakan kebijakan untuk Amazon Inspector

Mendukung tindakan kebijakan: Ya

Administrator dapat menggunakan AWS JSON kebijakan untuk menentukan siapa yang memiliki akses ke apa. Yaitu, principal dapat melakukan tindakan pada suatu sumber daya, dan dalam suatu syarat.

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

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

Untuk melihat daftar tindakan Amazon Inspector, lihat Tindakan yang ditentukan oleh Amazon Inspector Classic di Referensi Otorisasi Layanan.

Tindakan kebijakan di Amazon Inspector menggunakan awalan berikut sebelum tindakan:

```
inspector
```

Untuk menetapkan secara spesifik beberapa tindakan dalam satu pernyataan, pisahkan tindakan tersebut dengan koma.

```
"Action": [
      "inspector:action1",
      "inspector:action2"
```

```
        ]
```

Kebijakan izin berikut memberikan izin pengguna untuk menjalankan semua operasi yang dimulai dengan `Describe` dan `List`. Operasi ini menunjukkan informasi tentang sumber daya Amazon Inspector, seperti target penilaian atau temuan. Karakter wildcard (*) di elemen `Resource` menunjukkan bahwa operasi diperbolehkan untuk semua sumber daya Amazon Inspector milik akun tersebut:

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action": [
            "inspector:Describe*",
            "inspector:List*"
            ],
         "Resource":"*"
      }
   ]
}
```

## Contoh 2: Memungkinkan pengguna untuk melakukan setiap penjelasan dan daftar operasi hanya pada temuan Amazon Inspector

Kebijakan izin berikut memberikan izin pengguna untuk menjalankan operasi `ListFindings` dan `DescribeFindings` saja. Operasi ini menunjukkan informasi tentang temuan Amazon Inspector. Karakter wildcard (*) di elemen `Resource` menunjukkan bahwa operasi diperbolehkan untuk semua sumber daya Amazon Inspector milik akun tersebut.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action": [
                  "inspector:DescribeFindings",
                  "inspector:ListFindings"
         ],
```

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

Untuk melihat contoh kebijakan berbasis identitas Amazon Inspector, lihat Contoh kebijakan berbasis identitas untuk Amazon Inspector Classic.

## Sumber daya kebijakan untuk Amazon Inspector

Mendukung sumber daya kebijakan: Ya

Administrator dapat menggunakan AWS JSON kebijakan untuk menentukan siapa yang memiliki akses ke apa. Yaitu, principal dapat melakukan tindakan pada suatu sumber daya, dan dalam suatu syarat.

Elemen `Resource` JSON kebijakan menentukan objek atau objek yang tindakan tersebut berlaku. Pernyataan harus menyertakan elemen `Resource` atau `NotResource`. Sebagai praktik terbaik, tentukan sumber daya menggunakan Amazon Resource Name (ARN). Anda dapat melakukan ini untuk tindakan yang mendukung jenis sumber daya tertentu, yang dikenal sebagai izin tingkat sumber daya.

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

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

Untuk melihat daftar jenis sumber daya Amazon Inspector dan jenisnyaARNs, lihat Sumber daya yang ditentukan oleh Amazon Inspector Classic dalam Referensi Otorisasi Layanan. Untuk mempelajari tindakan yang dapat Anda tentukan ARN dari setiap sumber daya, lihat Tindakan yang ditentukan oleh Amazon Inspector Classic.

Untuk melihat contoh kebijakan berbasis identitas Amazon Inspector, lihat Contoh kebijakan berbasis identitas untuk Amazon Inspector Classic.

## Kunci kondisi kebijakan untuk Amazon Inspector

Mendukung kunci kondisi kebijakan khusus layanan: Yes

Administrator dapat menggunakan AWS JSON kebijakan untuk menentukan siapa yang memiliki akses ke apa. Yaitu, di mana utama dapat melakukan tindakan pada sumber daya, dan dalam kondisi apa.

Elemen `Condition` (atau blok `Condition`) akan memungkinkan Anda menentukan kondisi yang menjadi dasar suatu pernyataan berlaku. Elemen `Condition` bersifat opsional. Anda dapat membuat ekspresi bersyarat 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 sebuah pernyataan, atau beberapa kunci dalam elemen `Condition` tunggal, maka AWS akan mengevaluasinya 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. Misalnya, Anda dapat memberikan izin IAM pengguna untuk mengakses sumber daya hanya jika ditandai dengan nama IAM pengguna mereka. Untuk informasi selengkapnya, lihat elemen IAM kebijakan: variabel dan tag di Panduan IAM Pengguna.

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 IAM Pengguna.

Untuk melihat daftar kunci kondisi Amazon Inspector, lihat Kunci kondisi untuk Amazon Inspector Classic di Referensi Otorisasi Layanan. Untuk mempelajari tindakan dan sumber daya yang dapat Anda gunakan kunci kondisi, lihat Tindakan yang ditentukan oleh Amazon Inspector Classic.

Untuk melihat contoh kebijakan berbasis identitas Amazon Inspector, lihat Contoh kebijakan berbasis identitas untuk Amazon Inspector Classic.

## ACLsdi Amazon Inspector

MendukungACLs: Tidak

Access control lists (ACLs) mengontrol prinsipal mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACLsmirip dengan kebijakan berbasis sumber daya, meskipun mereka tidak menggunakan format dokumen kebijakan. JSON

## ABACdengan Amazon Inspector

Mendukung ABAC (tag dalam kebijakan): Sebagian

Attribute-based access control (ABAC) adalah strategi otorisasi yang mendefinisikan izin berdasarkan atribut. Dalam AWS, atribut ini disebut tag. Anda dapat melampirkan tag ke IAM entitas (pengguna atau peran) dan ke banyak AWS sumber daya. Menandai entitas dan sumber daya adalah langkah pertama dari. ABAC Kemudian Anda merancang ABAC kebijakan untuk mengizinkan operasi ketika tag prinsipal cocok dengan tag pada sumber daya yang mereka coba akses.

ABACmembantu dalam lingkungan yang berkembang pesat dan membantu dengan situasi di mana manajemen kebijakan menjadi rumit.

Untuk mengendalikan akses berdasarkan tanda, berikan informasi tentang tanda di elemen kondisi dari kebijakan menggunakan kunci kondisi `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 untuk hanya beberapa jenis sumber daya, nilainya adalah Parsial.

Untuk informasi selengkapnyaABAC, lihat Menentukan izin dengan ABAC otorisasi di IAMPanduan Pengguna. Untuk melihat tutorial dengan langkah-langkah penyiapanABAC, lihat Menggunakan kontrol akses berbasis atribut (ABAC) di IAMPanduan Pengguna.

## Menggunakan kredensial sementara dengan Amazon Inspector

Mendukung kredensial sementara: Ya

Beberapa Layanan AWS tidak berfungsi saat Anda masuk menggunakan kredensil sementara. Untuk informasi tambahan, termasuk yang Layanan AWS bekerja dengan kredensi sementara, lihat Layanan AWS yang berfungsi IAM di IAMPanduan Pengguna.

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 link sign-on (SSO) tunggal perusahaan Anda, proses tersebut secara otomatis membuat kredensi sementara. Anda juga akan secara otomatis membuat kredensial sementara ketika Anda masuk ke konsol sebagai seorang pengguna lalu beralih peran. Untuk informasi selengkapnya tentang beralih peran, lihat Beralih dari pengguna ke IAM peran (konsol) di Panduan IAM Pengguna.

Anda dapat secara manual membuat kredensil sementara menggunakan atau. AWS CLI AWS API Anda kemudian dapat menggunakan kredensil 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 Kredensi keamanan sementara di. IAM

## Izin utama lintas layanan untuk Amazon Inspector

Mendukung sesi akses maju (FAS): Ya

Saat Anda menggunakan IAM pengguna atau peran 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. FASmenggunakan izin dari pemanggilan utama Layanan AWS, dikombinasikan dengan permintaan Layanan AWS untuk membuat permintaan ke layanan hilir. FASPermintaan 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 saat membuat FAS permintaan, lihat Meneruskan sesi akses.

## Peran layanan untuk Amazon Inspector

Mendukung peran layanan: Tidak

Peran layanan adalah IAMperan yang diasumsikan layanan untuk melakukan tindakan atas nama Anda. IAMAdministrator dapat membuat, memodifikasi, dan menghapus peran layanan dari dalamIAM. Untuk informasi selengkapnya, lihat Membuat peran untuk mendelegasikan izin ke Layanan AWS dalam IAMPanduan Pengguna.

> **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 terkait layanan: Ya

Peran terkait layanan adalah jenis peran layanan yang ditautkan ke. Layanan AWS Layanan tersebut dapat menjalankan peran untuk melakukan tindakan atas nama Anda. Peran terkait layanan muncul di Anda Akun AWS dan dimiliki oleh layanan. IAMAdministrator dapat melihat, tetapi tidak mengedit izin untuk peran terkait layanan.

Untuk detail tentang cara membuat atau mengelola peran tertaut layanan Amazon Inspector, lihat Menggunakan peran terkait layanan untuk Amazon Inspector Classic.

## Contoh kebijakan berbasis identitas untuk Amazon Inspector Classic

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 butuhkan, IAM administrator dapat membuat IAM kebijakan. Administrator kemudian dapat menambahkan IAM kebijakan ke peran, dan pengguna dapat mengambil peran.

Untuk mempelajari cara membuat kebijakan IAM berbasis identitas menggunakan contoh dokumen kebijakan ini, lihat Membuat JSON IAM kebijakan (konsol) di Panduan Pengguna. IAM

Untuk detail tentang tindakan dan jenis sumber daya yang ditentukan oleh Amazon Inspector, termasuk format ARNs untuk setiap jenis sumber daya, lihat Kunci tindakan, sumber daya, dan kondisi untuk Amazon Inspector Classic dalam Referensi Otorisasi Layanan.

Topik

- Praktik terbaik kebijakan
- Menggunakan konsol Amazon Inspector
- Mengizinkan pengguna melihat izin mereka sendiri
- Izinkan pengguna untuk melakukan deskripsi dan daftar operasi hanya pada temuan Amazon Inspector

### Praktik terbaik kebijakan

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

- Mulailah dengan kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit — Untuk mulai memberikan izin kepada pengguna dan beban kerja Anda, gunakan kebijakan AWS terkelola yang memberikan izin untuk banyak kasus penggunaan umum. Mereka tersedia di Anda Akun AWS. Kami menyarankan Anda mengurangi izin lebih lanjut dengan menentukan kebijakan

yang dikelola AWS pelanggan yang khusus untuk kasus penggunaan Anda. Untuk informasi selengkapnya, lihat kebijakan AWSAWS terkelola atau kebijakan terkelola untuk fungsi pekerjaan di Panduan IAM Pengguna.

- Menerapkan izin hak istimewa paling sedikit — Saat Anda menetapkan izin dengan IAM kebijakan, berikan hanya izin yang diperlukan untuk melakukan tugas. Anda melakukannya dengan mendefinisikan tindakan yang dapat diambil pada sumber daya tertentu dalam kondisi tertentu, yang juga dikenal sebagai izin dengan hak akses paling rendah. Untuk informasi selengkapnya tentang penggunaan IAM untuk menerapkan izin, lihat Kebijakan dan izin IAM di IAM Panduan Pengguna.
- Gunakan ketentuan dalam IAM kebijakan untuk membatasi akses lebih lanjut — Anda dapat menambahkan kondisi ke kebijakan Anda untuk membatasi akses ke tindakan dan sumber daya. Misalnya, Anda dapat menulis kondisi kebijakan untuk menentukan bahwa semua permintaan harus dikirim menggunakanSSL. 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 IAM JSON kebijakan: Kondisi dalam Panduan IAM Pengguna.
- Gunakan IAM Access Analyzer untuk memvalidasi IAM kebijakan Anda guna memastikan izin yang aman dan fungsional — IAM Access Analyzer memvalidasi kebijakan baru dan yang sudah ada sehingga kebijakan mematuhi bahasa IAM kebijakan () 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 Memvalidasi kebijakan dengan IAM Access Analyzer di IAMPanduan Pengguna.
- Memerlukan otentikasi multi-faktor (MFA) - Jika Anda memiliki skenario yang mengharuskan IAM pengguna atau pengguna root di Anda Akun AWS, aktifkan MFA untuk keamanan tambahan. Untuk meminta MFA kapan API operasi dipanggil, tambahkan MFA kondisi ke kebijakan Anda. Untuk informasi selengkapnya, lihat APIAkses aman dengan MFA di Panduan IAM Pengguna.

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

## Menggunakan konsol Amazon Inspector

Untuk mengakses konsol Amazon Inspector Classic, Anda harus memiliki set 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 Sebagai gantinya, izinkan akses hanya ke tindakan yang cocok dengan API operasi yang mereka coba lakukan.

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 IAM Pengguna.

### Mengizinkan pengguna melihat izin mereka sendiri

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

```
{
    "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 pengguna untuk melakukan deskripsi dan daftar operasi hanya pada temuan Amazon Inspector

Kebijakan izin berikut memberikan izin pengguna untuk menjalankan operasi `ListFindings` dan `DescribeFindings` saja. Operasi ini menunjukkan informasi tentang temuan Amazon Inspector. Karakter wildcard (*) di elemen `Resource` menunjukkan bahwa operasi diperbolehkan untuk semua sumber daya Amazon Inspector milik akun tersebut.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action": [
                  "inspector:DescribeFindings",
                  "inspector:ListFindings"
         ],
         "Resource":"*"
      }
   ]
}
```

## Menggunakan peran terkait layanan untuk Amazon Inspector Classic

Amazon Inspector Classic menggunakan AWS Identity and Access Management (IAM) peran terkait layanan. Peran terkait layanan adalah jenis peran unik yang ditautkan langsung ke Amazon Inspector Classic. IAM Peran terkait layanan telah ditentukan sebelumnya oleh Amazon Inspector Classic dan menyertakan semua izin yang diperlukan layanan untuk memanggil orang lain atas nama Anda. Layanan AWS

Peran terkait layanan membuat pengaturan Amazon Inspector Classic lebih mudah karena Anda tidak perlu menambahkan izin yang diperlukan secara manual. Amazon Inspector Classic mendefinisikan izin peran terkait layanannya, dan kecuali ditentukan lain, hanya Amazon Inspector Classic yang dapat menjalankan perannya. Izin yang ditentukan mencakup kebijakan kepercayaan dan kebijakan izin, serta kebijakan izin tidak dapat dilampirkan ke entitas IAM IAM lainnya.

Anda dapat menghapus peran tertaut layanan hanya setelah terlebih dahulu menghapus sumber dayanya yang terkait. Ini melindungi sumber daya Amazon Inspector Classic karena Anda tidak dapat secara tidak sengaja menghapus izin untuk mengakses sumber daya.

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

## Izin peran terkait layanan untuk Amazon Inspector Classic

Amazon Inspector Classic menggunakan peran terkait layanan bernama —. AWSServiceRoleForAmazonInspector ServiceLinkedRoleDescription

Peran AWSServiceRoleForAmazonInspector terkait layanan mempercayai layanan berikut untuk mengambil peran:

- `inspector.amazonaws.com`

Kebijakan izin peran bernama AmazonInspectorServiceRolePolicy memungkinkan Amazon Inspector Classic menyelesaikan tindakan berikut pada sumber daya yang ditentukan:

- Tindakan: `iam:CreateServiceLinkedRole` pada `arn:aws:iam::*:role/aws-service-role/inspector.amazonaws.com/AWSServiceRoleForAmazonInspector`

Anda harus mengonfigurasi izin untuk mengizinkan IAM entitas (seperti IAM pengguna, grup, atau peran) membuat, mengedit, atau menghapus peran terkait layanan. Untuk informasi selengkapnya, lihat Izin peran terkait layanan di Panduan Pengguna. IAM

## Membuat peran terkait layanan untuk Amazon Inspector Classic

Anda tidak perlu membuat peran terkait layanan secara manual. Saat Anda CompleteThisCreateActionInThisService berada di AWS Management Console, Amazon Inspector

Classic AWS CLI AWS API, atau Amazon Inspector Classic membuat peran terkait layanan untuk Anda.

## Mengedit peran terkait layanan untuk Amazon Inspector Classic

Amazon Inspector Classic tidak mengizinkan Anda mengedit peran terkait AWSServiceRoleForAmazonInspector layanan. Setelah membuat peran tertaut layanan, Anda tidak dapat mengubah nama peran karena berbagai entitas mungkin mengacu ke peran tersebut. Namun, Anda dapat menyunting deskripsi peran menggunakan IAM. Untuk informasi selengkapnya, lihat Mengedit peran terkait layanan di IAMPanduan Pengguna.

## Menghapus peran terkait layanan untuk Amazon Inspector Classic

Jika Anda tidak perlu lagi menggunakan fitur atau layanan yang memerlukan peran terkait layanan, kami merekomendasikan Anda menghapus peran tersebut. Dengan begitu, Anda tidak memiliki entitas yang tidak digunakan yang tidak dipantau atau dipelihara secara aktif. Tetapi, Anda harus membersihkan sumber daya peran terkait layanan sebelum menghapusnya secara manual.

> **Note**
>
> Jika layanan Amazon Inspector Classic menggunakan peran saat Anda mencoba menghapus sumber daya, maka penghapusan mungkin gagal. Jika hal itu terjadi, tunggu beberapa menit dan coba mengoperasikannya lagi.

Untuk menghapus sumber daya Amazon Inspector Classic yang digunakan oleh **`AWSServiceRoleForAmazonInspector`**

- Hapus target penilaian Anda untuk ini Akun AWS di semua Wilayah AWS tempat Anda menjalankan Amazon Inspector Classic. Untuk informasi selengkapnya, lihat Target penilaian Amazon Inspector.

Untuk menghapus peran terkait layanan secara manual menggunakan IAM

Gunakan IAM konsol, AWS CLI, atau AWS API untuk menghapus peran AWSServiceRoleForAmazonInspector terkait layanan. Untuk informasi selengkapnya, lihat Menghapus peran terkait layanan di Panduan Pengguna. IAM

### Wilayah yang Didukung untuk peran terkait layanan Amazon Inspector Classic

Amazon Inspector Classic mendukung penggunaan peran terkait layanan di semua Wilayah tempat layanan tersedia. Untuk informasi selengkapnya, silakan lihat Wilayah AWS dan titik akhir.

## Memecahkan masalah identitas dan akses Amazon Inspector Classic

Gunakan informasi berikut untuk membantu Anda mendiagnosis dan memperbaiki masalah umum yang mungkin Anda temui saat bekerja dengan 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 `mateojackson` IAM pengguna mencoba menggunakan konsol untuk melihat detail tentang *`my-example-widget`* sumber daya fiksi tetapi tidak memiliki izin `inspector:`*`GetWidget`* fiksi.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 inspector: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 `inspector:`*`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 ketika IAM pengguna bernama `marymajor` mencoba menggunakan konsol 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 orang-orang di luar organisasi Anda untuk mengakses sumber daya Anda. Anda dapat menentukan siapa saja yang dipercaya untuk mengambil peran tersebut. Untuk layanan yang mendukung kebijakan berbasis sumber daya atau daftar kontrol akses (ACLs), Anda dapat menggunakan kebijakan tersebut untuk memberi orang akses ke sumber daya Anda.

Untuk mempelajari selengkapnya, periksa referensi berikut:

- Untuk mempelajari apakah Amazon Inspector mendukung fitur ini, lihat Bagaimana Amazon Inspector Classic bekerja dengan IAM.
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda di seluruh sumber daya Akun AWS yang Anda miliki, lihat Menyediakan akses ke IAM pengguna lain Akun AWS yang Anda miliki di Panduan IAM Pengguna.
- 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 IAM Pengguna.
- Untuk mempelajari cara menyediakan akses melalui federasi identitas, lihat Menyediakan akses ke pengguna yang diautentikasi secara eksternal (federasi identitas) di Panduan Pengguna. IAM

- Untuk mempelajari perbedaan antara menggunakan peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Akses sumber daya lintas akun di IAM Panduan Pengguna. IAM

# Pencatatan dan pemantauan di Amazon Inspector Classic

Amazon Inspector Classic terintegrasi dengan AWS CloudTrail, layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atau AWS layanan di Amazon Inspector Classic. CloudTrail menangkap semua API panggilan untuk Amazon Inspector Classic sebagai acara, termasuk panggilan dari konsol Amazon Inspector Classic dan panggilan kode ke operasi Amazon Inspector Classic. API

Untuk informasi tentang penggunaan CloudTrail login di Amazon Inspector Classic, lihat. Mencatat panggilan API Amazon Inspector denganAWS CloudTrail

Anda dapat memantau Amazon Inspector Classic menggunakan Amazon CloudWatch, yang mengumpulkan dan memproses data mentah menjadi metrik waktu hampir nyata yang dapat dibaca. Secara default, Amazon Inspector Classic mengirimkan data metrik ke CloudWatch dalam periode 5 menit.

Untuk informasi tentang penggunaan CloudWatch dengan Amazon Inspector Classic, lihat. Memantau Amazon Inspector Classic menggunakan Amazon CloudWatch

# Tanggapan insiden di Amazon Inspector Classic

Respons insiden untuk Amazon Inspector Classic adalah AWS tanggung jawab. AWS memiliki kebijakan dan program formal yang terdokumentasi yang mengatur respons insiden.

AWS Masalah operasional dengan dampak luas diposting di AWS Service Health Dashboard.

Masalah operasional juga di-posting ke akun individu melalui AWS Health Dashboard. Untuk informasi tentang cara menggunakan AWS Health Dashboard, lihat Panduan AWS Health Pengguna.

# Validasi kepatuhan untuk Amazon Inspector Classic

Auditor pihak ketiga menilai keamanan dan kepatuhan Amazon Inspector Classic sebagai bagian dari AWS beberapa program kepatuhan. Ini termasukSOC,PCI, Fed RAMPHIPAA, dan lainnya.

Untuk daftar AWS layanan dalam lingkup program kepatuhan tertentu, lihat AWSLayanan dalam Lingkup oleh AWS Layanan Program Kepatuhan . Untuk informasi umum, lihat Program AWS Kepatuhan Program AWS .

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

Tanggung jawab kepatuhan Anda saat menggunakan Amazon Inspector Classic ditentukan oleh sensitivitas data Anda, tujuan kepatuhan perusahaan Anda, serta undang-undang dan peraturan yang berlaku. AWS menyediakan sumber daya berikut untuk membantu kepatuhan:

- Panduan Quick Start Keamanan dan Kepatuhan – Panduan deployment ini membahas pertimbangan arsitektur dan menyediakan langkah–langkah untuk melakukan deployment terhadap lingkungan dasar di AWS yang menjadi fokus keamanan dan kepatuhan.
- Arsitektur untuk HIPAA Keamanan dan Kepatuhan di Amazon Web Services — Whitepaper ini menjelaskan bagaimana perusahaan dapat menggunakannya AWS untuk membuat HIPAA aplikasi yang sesuai.
- AWS Sumber Daya AWS — Kumpulan buku kerja dan panduan ini mungkin berlaku untuk industri dan lokasi Anda.
- 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— AWS Layanan ini memberikan pandangan komprehensif tentang keadaan keamanan Anda di dalamnya AWS yang membantu Anda memeriksa kepatuhan Anda terhadap standar industri keamanan dan praktik terbaik.

# Ketahanan di Amazon Inspector Classic

Infrastruktur AWS global dibangun di sekitar AWS Wilayah dan Zona Ketersediaan. AWS Wilayah menyediakan beberapa Availability Zone yang terpisah secara fisik dan terisolasi, yang terhubung dengan latensi rendah, throughput tinggi, dan jaringan yang sangat redundan. Dengan Zona Ketersediaan, Anda dapat merancang serta mengoperasikan aplikasi dan basis data yang secara otomatis melakukan fail over di antara zona tanpa gangguan. Zona Ketersediaan memiliki ketersediaan dan toleransi kesalahan yang lebih baik, dan dapat diskalakan dibandingkan infrastruktur pusat data tunggal atau multi tradisional.

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

Amazon Inspector Classic sangat tersedia dan mengeksekusi kueri menggunakan sumber daya komputasi di beberapa Availability Zone. Hal ini secara otomatis merutekan permintaan secara tepat jika Availability Zone tertentu tidak terjangkau.

Amazon Inspector Classic menggunakan Amazon S3 sebagai penyimpanan data dasarnya, yang membuat data Anda sangat tersedia dan tahan lama. Amazon S3 menyediakan infrastruktur tahan lama untuk menyimpan data penting. Ini dirancang untuk daya tahan objek sebesar 99,999999999%. Data Anda disimpan secara redundan di berbagai fasilitas dan beberapa perangkat di setiap fasilitas.

## Keamanan infrastruktur di Amazon Inspector Classic

Sebagai layanan terkelola, Amazon Inspector Classic 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 API panggilan yang AWS dipublikasikan untuk mengakses Amazon Inspector Classic melalui jaringan. Klien harus mendukung hal-hal berikut:

- Keamanan Lapisan Transportasi (TLS). Kami membutuhkan TLS 1.2 dan merekomendasikan TLS 1.3.
- Suite cipher dengan kerahasiaan maju yang sempurna (PFS) seperti (Ephemeral Diffie-Hellman) atau DHE (Elliptic Curve Ephemeral Diffie-Hellman). ECDHE Sebagian besar sistem modern seperti Java 7 dan setelahnya mendukung mode ini.

Selain itu, permintaan harus ditandatangani menggunakan access key ID dan secret access key yang terkait dengan IAM utama. Atau Anda dapat menggunakan AWS Security Token Service (AWS STS) untuk membuat kredensial keamanan sementara untuk menandatangani permintaan.

Untuk informasi selengkapnya tentang jaringan Amazon Inspector Classic dan keamanan agen, lihat. the section called “Keamanan agen Jaringan dan Amazon Inspector Classic”

# Analisis konfigurasi dan kerentanan di Amazon Inspector Classic

Amazon Inspector Classic menawarkan perangkat lunak standar yang disebut agen yang dapat Anda instal secara opsional di sistem operasi EC2 instance yang ingin Anda nilai. Agen mengumpulkan seperangkat data konfigurasi yang dikenal sebagai telemetri. Untuk informasi selengkapnya tentang agen Amazon Inspector Classic, lihat. Agen Amazon Inspector Classic

# Praktik terbaik keamanan untuk Amazon Inspector Classic

Amazon Inspector Classic menyediakan sejumlah fitur keamanan untuk dipertimbangkan saat Anda mengembangkan dan menerapkan kebijakan keamanan Anda sendiri. Praktik terbaik ini adalah pedoman umum dan tidak mewakili solusi keamanan yang lengkap. Karena praktik terbaik ini mungkin tidak sesuai atau tidak memadai untuk lingkungan Anda, perlakukan itu sebagai pertimbangan yang bermanfaat, bukan sebagai resep.

Untuk daftar praktik terbaik keamanan Amazon Inspector Classic, lihat. the section called “Praktik terbaik keamanan untuk Amazon Inspector Classic”

# Agen Amazon Inspector Classic

Agen Amazon Inspector Classic adalah entitas yang mengumpulkan informasi paket yang diinstal dan konfigurasi perangkat lunak untuk instans Amazon EC2. Meskipun tidak diperlukan dalam semua kasus, Anda harus menginstal agen Amazon Inspector Classic pada setiap instans Amazon EC2 target Anda untuk menilai keamanannya sepenuhnya.

Untuk informasi lebih lanjut tentang cara menginstal, menghapus instalasi, dan menginstal ulang agen, cara memverifikasi apakah agen terinstal berjalan, dan cara mengonfigurasi dukungan proksi untuk agen, lihat Bekerja dengan agen Amazon Inspector Classic pada sistem operasi berbasis Linux dan Bekerja dengan agen Amazon Inspector pada sistem operasi berbasis Windows.

> **Note**
>
> Agen Amazon Inspector Classic tidak diperlukan untuk menjalankan paket aturan Network Reachability.

> **Important**
>
> Agen Amazon Inspector Classic mengandalkan metadata instans Amazon EC2 agar berfungsi dengan benar. Hal ini mengakses metadata instans yang menggunakan versi 1 atau versi 2 Layanan Metadata Instans (IMDSv1 atau IMDSv2). Lihat Metadata Instans dan Data Pengguna untuk mempelajari lebih lanjut tentang metadata instans EC2 dan metode akses.

Topik

- Menginstal agen Amazon Inspector Classic
- Bekerja dengan agen Amazon Inspector Classic pada sistem operasi berbasis Linux
- Bekerja dengan agen Amazon Inspector pada sistem operasi berbasis Windows
- (Opsional) Verifikasi tanda tangan skrip instalasi agen Amazon Inspector pada sistem operasi berbasis Linux
- (Opsional) Verifikasi tanda tangan skrip instalasi agen Amazon Inspector pada sistem operasi berbasis Windows

## Hak istimewa agen Amazon Inspector Classic

Anda harus memiliki izin administratif atau root untuk menginstal agen Amazon Inspector Classic. Pada sistem operasi berbasis Linux yang didukung, agen terdiri dari mode pengguna dapat dijalankan yang berjalan dengan akses root. Pada sistem operasi berbasis Windows yang didukung, agen terdiri dari layanan pembaru dan layanan agen, masing-masing berjalan dalam mode pengguna dengan hak istimewa `LocalSystem`.

## Keamanan agen Jaringan dan Amazon Inspector Classic

Agen Amazon Inspector Classic memulai semua komunikasi dengan layanan Amazon Inspector Classic. Hal ini berarti bahwa agen harus memiliki jalur jaringan keluar ke titik akhir publik sehingga dapat mengirim data telemetri. Sebagai contoh, agen mungkin terhubung ke `arsenal.<region>.amazonaws.com`, atau titik akhirnya mungkin bucket Amazon S3 di `s3.dualstack.<region>.amazonaws.com`. Pastikan untuk mengganti `<region>` dengan AWS Wilayah sebenarnya tempat Anda menjalankan Amazon Inspector Classic. Untuk informasi lebih lanjut, lihat Rentang Alamat IP AWS. Karena semua koneksi dari agen dibuat keluar, tidak perlu membuka port di grup keamanan Anda untuk memungkinkan komunikasi masuk ke agen dari Amazon Inspector Classic.

Agen berkomunikasi secara berkala dengan Amazon Inspector Classic melalui saluran yang dilindungi TLS, yang diautentikasi menggunakan identitas yang terkait dengan peran instans EC2, atau, jika tidak ada peran yang ditetapkan, dengan dokumen metadata instans. AWS Ketika diautentikasi, agen mengirimkan pesan detak jantung ke layanan dan menerima instruksi dari layanan sebagai tanggapan. Jika penilaian telah dijadwalkan, agen menerima instruksi untuk penilaian tersebut. Instruksi ini adalah file JSON terstruktur, dan mereka memberi tahu agen untuk mengaktifkan atau menonaktifkan sensor yang telah dikonfigurasi tertentu di agen. Setiap tindakan instruksi telah ditetapkan dalam agen. Instruksi sewenang-wenang tidak dapat dijalankan.

Selama penilaian, agen mengumpulkan data telemetri dari sistem untuk dikirim kembali ke Amazon Inspector Classic melalui saluran yang dilindungi TLS. Agen tidak membuat perubahan pada sistem tempatnya mengumpulkan data. Setelah agen mengumpulkan data telemetri, ia mengirimkan data kembali ke Amazon Inspector Classic untuk diproses. Di luar data telemetri yang dihasilkannya, agen tidak mampu mengumpulkan atau mentransmisikan data lain tentang sistem atau target penilaian. Saat ini, tidak ada metode yang terekspos untuk mencegat dan memeriksa data telemetri di agen.

# Pembaruan agen Amazon Inspector Classic

Saat pembaruan untuk agen Amazon Inspector Classic tersedia, pembaruan tersebut diunduh secara otomatis dari Amazon S3 dan diterapkan. Hal ini juga memperbarui dependensi yang diperlukan. Fitur pembaruan otomatis menghilangkan kebutuhan untuk melacak dan secara manual mempertahankan versioning agen yang telah Anda instal pada instans EC2 Anda. Semua pembaruan tunduk pada proses kontrol perubahan Amazon yang diaudit untuk memastikan kepatuhan terhadap standar keamanan yang berlaku.

Untuk lebih memastikan keamanan agen, semua komunikasi antara agen dan situs rilis pembaruan otomatis (S3) dilakukan melalui koneksi TLS, dan server diautentikasi. Semua biner yang terlibat dalam proses pembaruan otomatis ditandatangani secara digital, dan tanda tangan diverifikasi oleh pembaru sebelum instalasi. Proses pembaruan otomatis dijalankan hanya selama periode non-penilaian. Jika ada kesalahan yang terdeteksi, proses pembaruan dapat melakukan rollback dan kembali mencoba pembaruan. Akhirnya, proses pembaruan agen berfungsi untuk meningkatkan kemampuan agen saja. Tak satu pun dari informasi spesifik Anda yang pernah dikirim dari agen ke Amazon Inspector Classic sebagai bagian dari alur kerja pembaruan. Satu-satunya informasi yang dikomunikasikan sebagai bagian dari proses pembaruan adalah keberhasilan instalasi dasar atau gagal telemetri dan, jika berlaku, informasi diagnostik kegagalan pembaruan.

# Siklus hidup data telemetri

Data telemetri yang dihasilkan oleh agen Amazon Inspector Classic selama penilaian dijalankan diformat dalam file JSON. File dikirimkan near-real-time melalui TLS ke Amazon Inspector Classic, di mana file tersebut dienkripsi dengan kunci turunan KMS per-assessment-run sesaat. File disimpan dengan aman di bucket Amazon S3 yang didedikasikan untuk Amazon Inspector Classic. Mesin aturan Amazon Inspector Classic mengakses data telemetri terenkripsi di bucket S3, mendekripsi dalam memori, dan memproses data berdasarkan aturan penilaian yang dikonfigurasi untuk menghasilkan temuan. Data telemetri yang disimpan di S3 dipertahankan hanya untuk memungkinkan bantuan dengan permintaan dukungan. Hal ini tidak digunakan atau dikumpulkan

oleh Amazon untuk tujuan lain. Setelah 30 hari, data telemetri dihapus secara permanen sesuai dengan kebijakan siklus hidup bucket S3 standar untuk data Amazon Inspector Classic. Saat ini, Amazon Inspector Classic tidak menyediakan API atau mekanisme akses bucket S3 ke telemetri yang dikumpulkan.

## Kontrol akses dari Amazon Inspector Classic ke dalam akun AWS

Sebagai layanan keamanan, Amazon Inspector Classic mengakses AWS akun dan sumber daya Anda hanya jika perlu menemukan instans EC2 untuk dinilai dengan menanyakan tag. Ini dilakukan melalui akses IAM standar melalui peran yang dibuat selama penyiapan awal layanan Amazon Inspector Classic. Selama penilaian, semua komunikasi dengan lingkungan Anda dimulai oleh agen Amazon Inspector Classic yang diinstal secara lokal pada instans EC2. Objek layanan Amazon Inspector Classic yang dibuat, seperti target penilaian, templat penilaian, dan temuan yang dihasilkan oleh layanan, disimpan dalam database yang dikelola oleh dan hanya dapat diakses oleh Amazon Inspector Classic.

## Batas agen Amazon Inspector Classic

Untuk informasi tentang batas agen Amazon Inspector Classic, lihat. Batas layanan Amazon Inspector Classic

## Menginstal agen Amazon Inspector Classic

Anda dapat menginstal agen Amazon Inspector Classic menggunakan Systems Manager Run Command pada beberapa instance (termasuk instance berbasis Linux dan berbasis Windows). Atau, Anda dapat menginstal agen satu per satu dengan masuk ke setiap EC2 instance. Prosedur dalam bab ini memberikan instruksi untuk kedua metode.

Sebagai opsi lain, Anda dapat dengan cepat menginstal agen di semua EC2 instans Amazon yang disertakan dalam target penilaian dengan memilih kotak centang Instal Agen pada halaman Tentukan target Penilaian di konsol.

Topik

- Menginstal agen pada beberapa EC2 instance menggunakan Systems Manager Run Command
- Menginstal agen pada instance berbasis Linux EC2
- Menginstal agen pada instance berbasis Windows EC2

> **Note**
>
> Prosedur dalam Bab ini berlaku untuk semua AWS Wilayah yang didukung oleh Amazon Inspector Classic.

## Menginstal agen pada beberapa EC2 instance menggunakan Systems Manager Run Command

Anda dapat menginstal agen Amazon Inspector Classic pada EC2 instans Anda menggunakan Perintah Systems Manager Run. Hal ini memungkinkan Anda untuk menginstal agen dari jarak jauh dan pada beberapa instans (baik instans berbasis Linux maupun berbasis Windows dengan perintah yang sama) sekaligus.

> **Important**
>
> Menginstal agen menggunakan Systems Manager Run Command saat ini tidak didukung untuk sistem operasi Debian.

> **Important**
>
> Untuk menggunakan opsi ini, pastikan EC2 instans Anda telah menginstal SSM Agen dan memiliki IAM peran yang memungkinkan Run Command. SSMAgen diinstal, secara default, pada instans Amazon EC2 Windows dan instans Amazon Linux. Amazon EC2 Systems Manager memerlukan IAM peran untuk EC2 instance yang memproses perintah dan peran terpisah untuk pengguna yang menjalankan perintah. Untuk informasi selengkapnya, lihat Menginstal dan mengonfigurasi peran keamanan SSM Agen dan Mengonfigurasi peran keamanan. SSM

Untuk menginstal agen pada beberapa EC2 instance menggunakan Systems Manager Run Command

1. Buka AWS Systems Manager konsol di https://console.aws.amazon.com/systems-manager/.
2. Di panel navigasi di bawah Node Tools, pilih Run Command.
3. Pilih Run a command (Jalankan perintah).

4. Untuk dokumen Command, pilih dokumen bernama AmazonInspector-M anageAWSAgent yang dimiliki oleh Amazon. Dokumen ini berisi skrip untuk menginstal agen Amazon Inspector Classic pada EC2 instance.
5. Untuk Target, Anda dapat memilih EC2 instance menggunakan metode yang berbeda. Untuk menginstal agen pada semua instans dalam target penilaian, Anda dapat menentukan tanda yang digunakan untuk membuat target penilaian.
6. Berikan pilihan Anda untuk sisa pilihan yang tersedia menggunakan petunjuk di Menjalankan perintah dari konsol, lalu pilih Jalankan.

> **Note**
>
> Anda juga dapat menginstal agen pada beberapa EC2 instance (berbasis Linux dan berbasis Windows) saat membuat target penilaian, atau Anda dapat menggunakan tombol Install Agents with Run Command untuk target yang ada. Untuk informasi selengkapnya, lihat Membuat target penilaian.

## Menginstal agen pada instance berbasis Linux EC2

Lakukan prosedur berikut untuk menginstal agen Amazon Inspector Classic pada instance berbasis LinuxEC2.

Untuk menginstal agen pada instance berbasis Linux EC2

1. Masuk ke EC2 instans Anda yang menjalankan sistem operasi berbasis Linux tempat Anda ingin menginstal agen Amazon Inspector Classic.

   > **Note**
   >
   > Untuk informasi tentang sistem operasi yang didukung Amazon Inspector Classic, lihat. Amazon Inspector Classic mendukung sistem operasi dan Wilayah

2. Unduh skrip instalasi agen dengan menjalankan salah satu dari perintah berikut ini:

   - wget https://inspector-agent.amazonaws.com/linux/latest/install
   - curl -O https://inspector-agent.amazonaws.com/linux/latest/install

3. (Opsional) Verifikasi bahwa skrip instalasi agen tidak diubah atau rusak. Untuk informasi selengkapnya, lihat (Opsional) Verifikasi tanda tangan skrip instalasi agen Amazon Inspector pada sistem operasi berbasis Linux.
4. Untuk menginstal agen, jalankan sudo bash install.

> **Note**
>
> Jika Anda menginstal agen di SELinux lingkungan, Amazon Inspector Classic dapat dideteksi sebagai daemon yang tidak terbatas. Anda dapat menghindari hal ini dengan mengubah domain proses agen dari default `initrc_t` ke `bin_t`. Gunakan perintah berikut untuk menetapkan `bin_t` konteks ke skrip run Amazon Inspector Classic sebelum menginstal agen untuk: SELinux
> sudo semanage fcontext -a -t bin_t /etc/rc\.d/init\.d/awsagent
> sudo semanage fcontext -a -t bin_t /etc/init\.d/awsagent

> **Note**
>
> Ketika pembaruan untuk agen tersedia, mereka secara otomatis diunduh dari Amazon S3 dan diterapkan. Untuk informasi selengkapnya, lihat Pembaruan agen Amazon Inspector Classic.
> Jika Anda ingin melewati proses pembaruan otomatis ini, jalankan perintah berikut ketika Anda menginstal agen:
> sudo bash install -u false

> **Note**
>
> (Opsional) Untuk menghapus skrip instalasi agen, jalankan rm install.

5. Verifikasi bahwa file-file yang diperlukan agar agen berhasil diinstal dan berfungsi dengan benar berikut ini telah diinstal:

   - `libcurl4` (diperlukan untuk menginstal agen di Ubuntu 18.04)
   - `libcurl3`
   - `libgcc1`

- `libc6`
- `libstdc++6`
- `libssl1.0.1`
- `libssl1.0.2` (diperlukan untuk menginstal agen di Debian 9)
- `libssl1.1`(diperlukan untuk menginstal agen di Ubuntu 20.04) LTS
- `libpcap0.8`

## Menginstal agen pada instance berbasis Windows EC2

Lakukan prosedur berikut untuk menginstal agen Amazon Inspector Classic pada instance berbasis WindowsEC2.

Untuk menginstal agen pada instance berbasis Windows EC2

1. Masuk ke EC2 instans Anda menjalankan sistem operasi berbasis Windows tempat Anda ingin menginstal agen.

   > **Note**
   >
   > Untuk informasi selengkapnya tentang sistem operasi yang didukung Amazon Inspector Classic, lihat. Amazon Inspector Classic mendukung sistem operasi dan Wilayah

2. Unduh file .exe berikut ini:

   `https://inspector-agent.amazonaws.com/windows/installer/latest/AWSAgentInstall.exe`

3. Buka jendela perintah (dengan izin administratif), arahkan ke lokasi tempat Anda menyimpan unduhan `AWSAgentInstall.exe`, dan jalankan file .exe untuk menginstal agen.

   > **Note**
   >
   > Ketika pembaruan untuk agen tersedia, mereka secara otomatis diunduh dari Amazon S3 dan diterapkan. Untuk informasi selengkapnya, lihat Pembaruan agen Amazon Inspector Classic.
   >
   > Jika Anda ingin melewati proses pembaruan otomatis ini, jalankan perintah berikut ketika Anda menginstal agen:

```
AWSAgentInstall.exe AUTOUPDATE=No
```

# Bekerja dengan agen Amazon Inspector Classic pada sistem operasi berbasis Linux

Anda dapat menginstal, menghapus, memverifikasi, dan memodifikasi perilaku agen Amazon Inspector Classic. Masuk ke instans Amazon EC2 Anda yang menjalankan sistem operasi berbasis Linux, dan jalankan salah satu prosedur berikut. Untuk informasi selengkapnya tentang sistem operasi yang didukung Amazon Inspector Classic, lihat. Amazon Inspector Classic mendukung sistem operasi dan Wilayah

**Important**

Agen Amazon Inspector Classic mengandalkan metadata instans Amazon EC2 agar berfungsi dengan benar. Hal ini mengakses metadata instans yang menggunakan versi 1 atau versi 2 Layanan Metadata Instans (IMDSv1 atau IMDSv2). Lihat Metadata Instans dan Data Pengguna untuk mempelajari lebih lanjut tentang metadata instans EC2 dan metode akses.

**Note**

Perintah di bagian ini berfungsi di semua AWS Wilayah yang didukung oleh Amazon Inspector Classic.

Topik

## Memverifikasi bahwa agen Amazon Inspector Classic sedang berjalan

- Untuk memverifikasi bahwa agen diinstal dan berjalan, masuk ke instans EC2 Anda, dan jalankan perintah berikut:

  sudo /opt/aws/awsagent/bin/awsagent status

  Perintah ini mengembalikan status agen yang sedang berjalan, atau kesalahan yang menyatakan bahwa agen tidak dapat dihubungi.

## Menghentikan agen Amazon Inspector Classic

- Untuk menghentikan agen, jalankan perintah berikut:

  sudo /etc/init.d/awsagent stop

## Memulai agen Amazon Inspector Classic

- Untuk memulai agen, jalankan perintah berikut:

  sudo /etc/init.d/awsagent start

## Memodifikasi pengaturan agen Amazon Inspector Classic

Setelah agen Amazon Inspector Classic diinstal dan dijalankan pada instans EC2, Anda dapat mengubah pengaturan dalam `agent.cfg` file untuk mengubah perilaku agen. Pada sistem operasi berbasis Linux, file `agent.cfg` terletak di direktori `/opt/aws/awsagent/etc`. Setelah Anda memodifikasi dan menyimpan file `agent.cfg`, Anda harus menghentikan dan memulai agen untuk menerapkan perubahan.

> **Important**
>
> Kami sangat merekomendasikan Anda memodifikasi file `agent.cfg` hanya dengan bimbingan AWS Support.

# Mengkonfigurasi dukungan proxy untuk agen Amazon Inspector Classic

Untuk mendapatkan dukungan proksi untuk agen pada sistem operasi berbasis Linux, gunakan file konfigurasi spesifik agen dengan variabel lingkungan tertentu. Untuk informasi lebih lanjut, lihat https://wiki.archlinux.org/index.php/proxy_settings.

Lengkapi salah satu prosedur berikut:

Untuk menginstal agen pada instans EC2 yang menggunakan server proksi

1. Buat file bernama `awsagent.env` dan simpan di direktori `/etc/init.d/`.
2. Edit `awsagent.env` untuk memasukkan variabel lingkungan ini dalam format berikut:

   - `export https_proxy=hostname:port`
   - `export http_proxy=hostname:port`
   - `export no_proxy=169.254.169.254`

   > **Note**
   >
   > Ganti nilai dalam contoh sebelumnya hanya dengan nama host dan kombinasi nomor port yang valid. Tentukan alamat IP dari titik akhir metadata instans (169.254.169.254) untuk variabel `no_proxy`.

3. Instal agen Amazon Inspector Classic dengan menyelesaikan langkah-langkah dalam prosedur. Menginstal agen pada instance berbasis Linux EC2

Untuk mengonfigurasi dukungan proksi pada instans EC2 dengan agen berjalan

1. Untuk mengonfigurasi dukungan proksi, versi agen yang berjalan pada instans EC2 Anda harus 1.0.800.1 atau yang lebih baru. Jika Anda mengaktifkan proses pembaruan otomatis untuk agen, Anda dapat memverifikasi bahwa versi agen adalah 1.0.800.1 atau yang lebih baru dengan menggunakan prosedur Memverifikasi bahwa agen Amazon Inspector Classic sedang berjalan. Jika Anda tidak mengaktifkan proses pembaruan otomatis untuk agen, Anda harus menginstal kembali agen pada instans EC2 ini dengan mengikuti prosedur Menginstal agen pada instance berbasis Linux EC2.
2. Buat file bernama `awsagent.env`, dan simpan di direktori `/etc/init.d/`.
3. Edit `awsagent.env` untuk memasukkan variabel lingkungan ini dalam format berikut:

- `export https_proxy=hostname:port`
- `export http_proxy=hostname:port`
- `export no_proxy=169.254.169.254`

> **Note**
>
> Ganti nilai dalam contoh sebelumnya hanya dengan nama host dan kombinasi nomor port yang valid. Tentukan alamat IP dari titik akhir metadata instans (169.254.169.254) untuk variabel `no_proxy`.

4. Mulai ulang agen dengan terlebih dahulu menghentikannya menggunakan perintah berikut:

   ```
   sudo /etc/init.d/awsagent restart
   ```

   Pengaturan proksi diambil dan digunakan oleh agen dan proses pembaruan otomatis.

## Menghapus instalasi agen Amazon Inspector Classic

Untuk menghapus instalasi agen

1. Masuk ke instans EC2 Anda yang menjalankan sistem operasi berbasis Linux di mana Anda ingin menghapus instalasi agen.

   > **Note**
   >
   > Untuk informasi selengkapnya tentang sistem operasi yang didukung Amazon Inspector Classic, lihat. Amazon Inspector Classic mendukung sistem operasi dan Wilayah

2. Untuk menghapus instalasi agen, gunakan salah satu perintah berikut:

   - Pada Amazon Linux, CentOS, dan Red Hat, jalankan perintah berikut:

     ```
     sudo yum remove 'AwsAgent*'
     ```

   - Pada Ubuntu Server, jalankan perintah berikut:

     ```
     sudo apt-get purge 'awsagent*'
     ```

# Bekerja dengan agen Amazon Inspector pada sistem operasi berbasis Windows

Anda dapat memulai, menghentikan, dan memodifikasi perilaku agen Amazon Inspector. Masuk ke instans EC2 Anda yang menjalankan sistem operasi berbasis Windows dan lakukan salah satu prosedur dalam bab ini. Untuk informasi lebih lanjut tentang sistem operasi yang didukung untuk Amazon Inspector untuk Amazon Inspector untuk informasi lebih lanjut tentang sistem operasi yang didukung untuk Amazon Inspector untuk AmazonAmazon Inspector Classic mendukung sistem operasi dan Wilayah Inspector untuk

**Important**

Agen Amazon Inspector bergantung pada metadata instans Amazon Inspector bergantung pada metadata instans Amazon EC2 Inspector bergantung pada metadata instans Amazon Inspector bergantung pada metadata Hal ini mengakses metadata instans yang menggunakan versi 1 atau versi 2 Layanan Metadata Instans (IMDSv1 atau IMDSv2). Lihat Metadata Instans dan Data Pengguna untuk mempelajari lebih lanjut tentang metadata instans EC2 dan metode akses.

**Note**

Perintah di bagian ini berfungsi di semua Wilayah yang didukung oleh Amazon Inspector di semuaAWS Wilayah yang didukung oleh Amazon Inspector pada semua Wilayah yang didukung oleh Amazon Inspector pada semua Wilayah

Topik

## Memulai atau menghentikan agen Amazon Inspector atau memverifikasi bahwa agen berjalan

Untuk memulai, menghentikan, atau memverifikasi agen

1. Pada instans EC2 Anda, pilih Mulai, Jalankan, lalu masukkan **`services.msc`**.
2. Jika agen berhasil berjalan, dua layanan terdaftar dengan status mereka yang diatur ke Dimulai atau Berjalan dalam jendela Layanan: Layanan Agen AWS dan Layanan Pembaru Agen AWS.
3. Untuk memulai agen, klik kanan Layanan Agen AWS, lalu pilih Mulai. Jika layanan berhasil dimulai, status diperbarui ke Dimulai atau Berjalan.
4. Untuk menghentikan agen, klik kanan Layanan Agen AWS, lalu pilih Hentikan. Jika layanan berhasil berhenti, status dihapus (muncul sebagai kosong). Kami tidak merekomendasikan untuk menghentikan Layanan Pembaru Agen AWS karena hal ini menonaktifkan instalasi semua perangkat tambahan masa depan dan perbaikan untuk agen.
5. Untuk memverifikasi bahwa agen diinstal dan berjalan, masuk ke instans EC2 Anda, dan buka jendela perintah menggunakan izin administratif. Arahkan ke `C:\Program Files\Amazon Web Services\AWS Agent`, lalu jalankan perintah berikut:

   AWSAgentStatus.exe

   Perintah ini mengembalikan status agen yang sedang berjalan, atau kesalahan yang menyatakan bahwa agen tidak dapat dihubungi.

## Memodifikasi pengaturan agen Amazon Inspector

Setelah agen Amazon Inspector diinstal dan berjalan pada instans EC2, Anda dapat memodifikasi pengaturan di`agent.cfg` file untuk mengubah perilaku agen. Pada sistem operasi berbasis Windows, file terletak di direktori `C:\ProgramData\Amazon Web Services\AWS Agent`. Setelah Anda memodifikasi dan menyimpan file `agent.cfg`, Anda harus menghentikan dan memulai agen untuk menerapkan perubahan.

> **Important**
>
> Kami sangat merekomendasikan Anda memodifikasi file `agent.cfg` hanya dengan bimbingan AWS Support.

# Mengonfigurasi dukungan proksi untuk agen Amazon Inspector

Untuk mendapatkan dukungan proksi untuk agen pada sistem operasi berbasis Windows, gunakan proksi `WinHTTP`. Untuk mengatur proksi `WinHTTP` menggunakan utilitas `netsh`, lihat Netsh Commands for Windows Hypertext Transfer Protocol (WINHTTP).

> **Important**
>
> Hanya proksi HTTPS yang didukung untuk instans berbasis Windows.

Lengkapi salah satu prosedur berikut:

Untuk menginstal agen pada instans EC2 yang menggunakan server proksi

1. Unduh file .exe berikut: `https://d1wk0tztpsntt1.cloudfront.net/windows/installer/latest/AWSAgentInstall.exe`
2. Buka jendela atau PowerShell jendela perintah (menggunakan izin administratif). Navigasi ke lokasi tempat Anda menyimpan `AWSAgentInstall.exe` yang sudah diunduh, lalu jalankan perintah berikut:

   ```
   .\AWSAgentInstall.exe /install USEPROXY=1
   ```

Untuk mengonfigurasi dukungan proksi pada instans EC2 dengan agen berjalan

1. Untuk mengonfigurasi dukungan proksi, versi agen Amazon Inspector yang berjalan pada instans EC2 Anda harus 1.0.0.59 atau yang lebih baru. Jika Anda mengaktifkan proses pembaruan otomatis untuk agen, Anda dapat memverifikasi bahwa versi agen adalah 1.0.0.59 atau yang lebih baru dengan menggunakan prosedur Memulai atau menghentikan agen Amazon Inspector atau memverifikasi bahwa agen berjalan. Jika Anda tidak mengaktifkan proses pembaruan otomatis untuk agen, Anda harus menginstal kembali agen pada instans EC2 ini dengan mengikuti prosedur Menginstal agen pada instance berbasis Windows EC2.
2. Buka editor registri (`regedit.exe`).
3. Navigasi ke kunci registri berikut: `"HKEY_LOCAL_MACHINE/SOFTWARE/Amazon Web Services/AWS Agent Updater"`.
4. Di dalam kunci registri ini, buat nilai `DWORD(32bit)` registri yang disebut `"UseProxy"`.
5. Klik dua kali pada nilai tersebut, dan tetapkan nilai ke 1.

6. Masukkan **`services.msc`**, temukan Layanan Agen AWS dan Layanan Pembaru Agen AWS dalam jendela Layanan, dan mulai ulang setiap proses. Setelah kedua proses berhasil dimulai ulang, jalankan file `AWSAgentStatus.exe` (lihat langkah 5 di Memulai atau menghentikan agen Amazon Inspector atau memverifikasi bahwa agen berjalan). Melihat status agen Anda dan memverifikasi bahwa statusnya menggunakan proksi dikonfigurasi.

## Menghapus instalasi agen Amazon Inspector

Untuk menghapus instalasi agen

1. Masuk ke instans EC2 Anda yang menjalankan sistem operasi berbasis Windows di mana Anda ingin menghapus instalasi agen Amazon Inspector yang Anda inginkan untuk menghapus instalasi agen Amazon Inspector Anda yang menjalankan sistem operasi berbasis Windows di mana Anda ingin menghapus instalasi agen Amazon Inspector Anda.

   > **Note**
   >
   > Untuk informasi lebih lanjut tentang sistem operasi yang didukung untuk Amazon Inspector untuk Amazon Inspector untuk informasi lebih lanjut tentang sistem operasi yang didukung untuk Amazon Inspector untuk AmazonAmazon Inspector Classic mendukung sistem operasi dan Wilayah Inspector untuk

2. Pada instans EC2 Anda, arahkan ke Panel Kontrol, Tambah/Hapus Program.
3. Dalam daftar program yang terinstal, pilih agen AWS, lalu pilih Hapus instalasi.

# (Opsional) Verifikasi tanda tangan skrip instalasi agen Amazon Inspector pada sistem operasi berbasis Linux

Topik ini menjelaskan proses yang direkomendasikan untuk memverifikasi validitas skrip instalasi agen Amazon Inspector untuk sistem operasi berbasis Linux.

Saat Anda mengunduh aplikasi dari internet, kami merekomendasikan Anda untuk mengautentikasi identitas penerbit perangkat lunak dan memeriksa apakah aplikasi tersebut belum diubah atau rusak setelah diterbitkan. Ini akan melindungi Anda agar tidak menginstal versi aplikasi yang berisi virus atau kode berbahaya lainnya.

Jika setelah menjalankan langkah-langkah dalam topik ini, Anda menganggap bahwa perangkat lunak untuk agen Amazon Inspector telah diubah atau rusak, JANGAN menjalankan file instalasi file instalasi. Alih-alih, hubungi AWS Support.

File agen Amazon Inspector untuk sistem operasi berbasis Linux ditandatangani menggunakanGnuPG, yaitu implementasi sumber terbuka dari standar Pretty Good Privacy (OpenPGP) untuk tanda tangan digital yang aman. GnuPG(juga dikenal sebagaiGPG) menyediakan pemeriksaan autentikasi dan integritas melalui tanda tangan digital. Amazon EC2 menerbitkan kunci publik dan tanda tangan yang dapat Anda gunakan untuk memverifikasi alat Amazon EC2 CLI yang diunduh. Untuk informasi lebih lanjut tentang PGP dan GnuPG (GPG), lihat http://www.gnupg.org.

Langkah pertamanya adalah membangun kepercayaan dengan penerbit perangkat lunak. Unduh kunci publik dari penerbit perangkat lunak, periksa apakah pemilik kunci publik adalah benar-benar pemiliknya, lalu tambahkan kunci publik ke dalam keyring Anda. Keyring adalah kumpulan kunci publik yang diketahui. Setelah menetapkan autentikasi kunci publik, Anda dapat menggunakannya untuk memverifikasi tanda tangan aplikasi.

Topik



## Menginstal alat GPG

Jika sistem operasi Anda adalah Linux atau Unix, alat GPG mungkin sudah terinstal. Untuk menguji apakah alat ini sudah terinstal di sistem Anda, ketikkan gpg pada jendela perintah. Jika alat GPG telah teriinstal, Anda akan melihat perintah command prompt GPG. Jika alat GPG belum terinstal, Anda akan melihat pesan kesalahan yang menyatakan bahwa perintah tidak dapat ditemukan. Anda dapat menginstal paket GnuPG dari repositori.

Untuk menginstal alat GPG pada Linux berbasis Debian

- Dari terminal, jalankan perintah berikut:apt-get install gnupg.

Untuk menginstal alat GPG pada Linux berbasis Red Hat

- Dari terminal, jalankan perintah berikut:yum install gnupg.

# Mengautentikasi dan mengimpor kunci publik

Langkah berikutnya dalam proses ini adalah mengautentikasi kunci publik Amazon Inspector dan menambahkannya sebagai kunci tepercaya di dalamGPG keyring Anda.

Untuk mengautentikasi dan mengimpor kunci publik Amazon Inspector

1. Dapatkan salinan kunci build GPG publik kami dengan melakukan salah satu langkah berikut:

   - Unduh dari https://d1wk0tztpsntt1.cloudfront.net/linux/latest/inspector.gpg.
   - Salin kunci dari teks berikut dan tempelkan ke file bernama `inspector.gpg`. Pastikan untuk memasukkan semua hal berikut ini:

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v2.0.18 (GNU/Linux)

mQINBFYDlfEBEADFpfNt/mdCtsmfDoga+PfHY9bdXAD68yhp2m9NyH3BOzle/MXI
8siNfoRgzDwuWnIaezHwwLWkDw2paRxp1NMQ9qRe8Phq0ewheLrQu95dwDgMcw90
gf9m1iKVHjdVQ9qNHlB2OFknPDxMDRHcrmlJYDKYCX3+MODEHnlK25tIH2KWezXP
FPSU+TkwjLRzSMYH1L8IwjFUIIi78jQS9a31R/cOl4zuC5fOVghYlSomLI8irfoD
JSa3csVRujSmOAf9o3beiMR/kNDMpgDOxgiQTu/Kh39cl6o8AKe+QKK48kqO7hra
h1dpzLbfeZEVU6dWMZtlUksG/zKxuzD6d8vXYH7Z+x09POPFALQCQQMC3WisIKgj
zJEFhXMCCQ3NLC3CeyMq3vP7MbVRBYE7t3d2uDREkZBgIf+mbUYfYPhrzy0qT9Tr
PgwcnUvDZuazxuuPzucZGOJ5kbptat3DcUpstjdkMGAId3JawBbps77qRZdA+swr
o9o3jbowgmf0y5ZS6KwvZnC6XyTAkXy2io7mSrAIRECrANrzYzfp5v7uD7w8Dk0X
1OrfOm1VufMzAyTu0YQGBWaQKzSB8tCkvFw54PrRuUTcV826XU7SIJNzmNQo58uL
bKyLVBSCVabfs0lkECIesq8PT9xMYfQJ421uATHyYUnFTU2TYrCQEab7oQARAQAB
tCdBbWF6b24gSW5zcGVjdG9yIDxpbnNwZWN0b3JAYW1hem9uLmNvbT6JAjgEEwEC
ACIFAlYDlfECGwMGCwkIBwMCBhUIAgkKCwQWAgMBAh4BAheAAAoJECR0CWBYNgQY
8yUP/2GpIl40f3mKBUiSTe0XQLvwiBCHmY+V9fOuKqDTinxssjEMCnz0vsKeCZF/
L35pwNa/oW0OJa8D7sCkKG+8LuyMpcPDyqptLrYPprUWtz2+qLCHgpWsrku7ateF
x4hWS0jUVeHPaBzI9V1NTHsCx9+nbpWQ5Fk+7VJI8hbMDY7NQx6fcse8WTlP/0r/
HIkKzzqQQaaOf5t9zc5DKwi+dFmJbRUyaq22xs8C81UODjHunhjHdZ21cnsgk91S
fviuaum9aR4/uVIYOTVWnjC5J3+VlczyUt5FaYrrQ5ov0dM+biTUXwve3X8Q85Nu
DPnO/+zxb7Jz3QCHXnuTbxZTjvvl60Oi8//uRTnPXjz4wZLwQfibgHmk1++hzND7
wOYA02Js6v5FZQlLQAod7q2wuA1pq4MroLXzziDfy/9ea8B+tzyxlmNVRpVZY4Ll
DOHyqGQhpkyV3drjjNZlEofwbfu7m6ODwsgMl5ynzhKklJzwPJFfB3mMc7qLi+qX
MJtEX8KJ/iVUQStHHAG7daL1bxpWSI3BRuaHsWbBGQ/mcHBgUUOQJyEp5LAdg9Fs
VP55gWtF7pIqifiqlcfgG0Ov+A3NmVbmiGKSZvfrc5KsF/k43rCGqDx1RV6gZvyI
LfO9+3sEIlNrsMib0KRLDeBt3EuDsaBZgOkqjDhgJUesqiCy
=iEhB
-----END PGP PUBLIC KEY BLOCK-----
```

2. Pada jendela perintah di direktori tempat Anda menyimpan inspector.gpg, gunakan perintah berikut untuk mengimpor kunci publik Amazon Inspector ke dalam keyring Anda:

```
gpg --import inspector.gpg
```

Perintah tersebut mengembalikan hasil yang serupa dengan berikut ini:

```
gpg: key 58360418: public key "Amazon Inspector <inspector@amazon.com>" imported
                   gpg: Total number processed: 1
                   gpg:               imported: 1  (RSA: 1)
```

Catat nilai utama; Anda membutuhkannya pada langkah berikutnya. Dalam contoh sebelumnya, nilai utama adalah `58360418`.

3. Verifikasi sidik jari dengan menjalankan perintah berikut, mengganti key-value dengan nilai dari langkah sebelumnya:

```
gpg --fingerprint key-value
```

Perintah ini mengembalikan hasil yang serupa dengan berikut ini:

```
pub   4096R/58360418 2015-09-24
                Key fingerprint = DDA0 D4C5 10AE 3C20 6F46  6DC0 2474 0960 5836
 0418
                uid                  Amazon Inspector <inspector@amazon.com>
```

Selain itu, string sidik jari harus identik dengan `DDA0 D4C5 10AE 3C20 6F46 6DC0 2474 0960 5836 0418`, seperti yang ditunjukkan dalam contoh sebelumnya. Bandingkan sidik jari kunci yang dikembalikan dengan yang dipublikasikan di halaman ini. Mereka harus cocok. Jika mereka tidak cocok, jangan instal skrip instalasi agen Amazon Inspector, dan hubungi AWS Support.

## Memverifikasi tanda tangan paket

Setelah Anda menginstal`GPG` alat, mengautentikasi dan mengimpor kunci publik Amazon Inspector, dan memverifikasi bahwa kunci publik tersebut dapat dipercaya, Anda siap untuk memverifikasi tanda tangan skrip instalasi.

Untuk memverifikasi tanda tangan skrip instalasi

1. Pada perintah command prompt, jalankan perintah berikut untuk mengunduh file tanda tangan untuk skrip instalasi:

   ```
   curl -O https://inspector-agent.amazonaws.com/linux/latest/install.sig
   ```

2. Verifikasi tanda tangan dengan menjalankan perintah berikut pada jendela perintah di direktori tempat Anda menyimpan`install.sig` dan file instalasi klasik Amazon Inspector. Kedua file harus ada.

   ```
   gpg --verify ./install.sig
   ```

   Outputnya akan terlihat seperti berikut ini:

   ```
   gpg: Signature made Thu 24 Sep 2015 03:19:09 PM UTC using RSA key ID 58360418
   gpg: Good signature from "Amazon Inspector <inspector@amazon.com>" [unknown]
   gpg: WARNING: This key is not certified with a trusted signature!
   gpg:          There is no indication that the signature belongs to the owner.
   Primary key fingerprint: DDA0 D4C5 10AE 3C20 6F46  6DC0 2474 0960 5836 0418
   ```

   Jika output berisi frasa`Good signature from "Amazon Inspector <inspector@amazon.com>"`, itu berarti bahwa tanda tangan telah berhasil diverifikasi, dan Anda dapat melanjutkan untuk menjalankan skrip instalasi Amazon Inspector Classic.

   Jika output mencakup frasa `BAD signature`, periksa apakah Anda melakukan prosedur dengan benar. Jika Anda terus mendapatkan respons ini, jangan jalankan file instalasi yang Anda unduh sebelumnya, dan hubungi AWS Support.

Berikut ini adalah detail tentang peringatan yang mungkin Anda lihat:

- PERINGATAN: Kunci ini tidak disertifikasi dengan tanda tangan tepercaya! Tidak ada indikasi bahwa tanda tangan ini adalah milik pemiliknya. Ini mengacu pada tingkat kepercayaan pribadi Anda dalam keyakinan bahwa Anda memiliki kunci publik yang autentik untuk Amazon Inspector. Idealnya, Anda harus mendatangi kantor AWS dan menerima kunci secara langsung. Namun, kemungkinan besar Anda akan mengunduhnya dari situs web. Dalam hal ini, situs web tersebut adalah situs web AWS.

- gpg: tidak ditemukan kunci yang benar-benar tepercaya. Hal ini berarti Anda (atau orang lain yang Anda percaya) tidak "benar-benar memercayai" kunci tersebut.

Untuk informasi lebih lanjut, lihat http://www.gnupg.org.

# (Opsional) Verifikasi tanda tangan skrip instalasi agen Amazon Inspector pada sistem operasi berbasis Windows

Topik ini menjelaskan proses yang direkomendasikan untuk memverifikasi validitas skrip instalasi agen Amazon Inspector untuk sistem operasi berbasis Windows.

Saat Anda mengunduh aplikasi dari internet, kami merekomendasikan Anda untuk mengautentikasi identitas penerbit perangkat lunak dan memeriksa apakah aplikasi tersebut belum diubah atau rusak setelah diterbitkan. Ini akan melindungi Anda agar tidak menginstal versi aplikasi yang berisi virus atau kode berbahaya lainnya.

Jika setelah menjalankan langkah-langkah dalam topik ini, Anda merasa bahwa perangkat lunak untuk agen Amazon Inspector telah diubah atau rusak, JANGAN menjalankan file instalasi. Alih-alih, hubungi AWS Support.

Untuk memverifikasi validitas skrip instalasi agen yang diunduh pada sistem operasi berbasis Windows, pastikan bahwa cap jempol sertifikat signer Amazon Services LLC sama dengan nilai ini:

E8 83 C5 3A F7 8C BA 7C F5 A2 47 E9 B8 86 FC E9 68 EE 0B 36

Untuk memverifikasi nilai ini, lakukan prosedur berikut:

1. Klik kanan `AWSAgentInstall.exe` yang diunduh, dan buka jendela Properti.
2. Pilih tab Tanda Tangan Digital.
3. Dari Daftar Tanda Tangan, pilih Amazon Web Services, Inc., lalu pilih Detail.
4. Pilih tab Umum, jika belum dipilih, lalu pilih Lihat Sertifikat.
5. Pilih tab Detail, dan kemudian pilih Semua di Tampilkan daftar tarik turun, jika belum dipilih.
6. Gulir ke bawah sampai Anda melihat bidang Cap Jempol lalu pilih Cap Jempol. Ini menampilkan seluruh nilai cap jempol di jendela bawah.

    - Jika nilai cap jempol di jendela bawah identik dengan nilai berikut:

      E8 83 C5 3A F7 8C BA 7C F5 A2 47 E9 B8 86 FC E9 68 EE 0B 36

skrip instalasi agen yang diunduh milik Anda bersifat autentik dan dapat diinstal dengan aman.

- Jika nilai cap jempol di jendela detail bawah tidak identik dengan nilai di atas, jangan jalankan `AWSAgentInstall.exe`.

# Target penilaian Amazon Inspector

Anda dapat menggunakan Amazon Inspector Classic untuk mengevaluasi apakahAWStarget penilaian (koleksiAWSsumber daya) memiliki potensi masalah keamanan yang harus Anda atasi.

> **Important**
>
> Saat ini, target penilaian Anda hanya dapat terdiri dari instans EC2 yang berjalan pada sistem operasi yang didukung. Untuk informasi tentang sistem operasi yang didukung dan Wilayah AWS yang didukung, lihat the section called “Sistem operasi dan Wilayah yang didukung”.

> **Note**
>
> Untuk informasi tentang meluncurkan instans EC2, lihat Amazon Elastic Compute Cloud documentation.

Topik



## Menandai sumber daya untuk membuat target penilaian

Untuk membuat target penilaian untuk Amazon Inspector untuk menilai, Anda memulai dengan penandaan instans EC2 yang ingin Anda sertakan di target Anda. Tanda adalah kata atau frasa yang bertindak sebagai metadata untuk mengidentifikasi dan mengatur instans Anda dan sumber daya AWS lainnya. Amazon Inspector menggunakan tanda yang Anda buat untuk mengidentifikasi instans milik target Anda.

Setiap tanda AWS terdiri dari pasangan kunci dan nilai pilihan Anda. Misalnya, Anda dapat memilih untuk memberi nama “Name” untuk kunci Anda dan “MyFirstInstance” untuk nilai Anda. Setelah

menandai instans, Anda menggunakan konsol Amazon Inspector untuk menambahkan instans ke target penilaian Anda. Setiap instans tidak perlu cocok dengan lebih dari satu tanda pasangan nilai-kunci.

Ketika Anda menandai instans EC2 Anda untuk membangun target penilaian, Anda dapat membuat kunci tanda kustom Anda sendiri atau menggunakan tombol tanda yang dibuat oleh orang lain dalam akun AWS yang sama. Anda juga dapat menggunakan kunci tanda yang AWS buat secara otomatis. Misalnya, AWS secara otomatis membuat kunci tanda Nama untuk instans EC2 yang Anda luncurkan.

Anda dapat menambahkan tanda ke instans EC2 ketika Anda membuatnya, atau Anda dapat menambahkan, mengubah, atau menghapus tanda tersebut satu per satu pada halaman konsol untuk setiap instans EC2. Anda juga dapat menambahkan tanda ke beberapa instans EC2 sekaligus menggunakan Editor Tanda.

Untuk informasi lebih lanjut, lihat Editor Tanda. Untuk informasi lebih lanjut tentang penandaan instans EC2, lihat Sumber Daya dan Tanda.

## Batas target penilaian Amazon Inspector

Anda dapat membuat hingga 50 target penilaian per akun AWS. Untuk informasi selengkapnya, lihat Batas layanan Amazon Inspector Classic.

## Membuat target penilaian

Anda dapat menggunakan konsol Amazon Inspector untuk membuat target penilaian.

Untuk membuat target penilaian

1. Masuk keAWS Management Consoledan buka konsol Amazon Inspector Classic dihttps://console.aws.amazon.com/inspector/.
2. Di panel navigasi, pilih Target Penilaian, lalu pilih Buat.
3. Untuk Nama, masukkan nama untuk target penilaian Anda.
4. Lakukan salah satu dari berikut:

   - Untuk memasukkan semua instans EC2 dalam akun AWS ini dan Wilayah dalam target penilaian ini, pilih kotak centang Semua instans.

> **Note**
>
> Batas jumlah maksimum agen yang dapat Anda sertakan dalam penilaian berjalan berlaku ketika Anda menggunakan opsi ini. Untuk informasi selengkapnya, lihat Batas layanan Amazon Inspector Classic.

- Untuk memilih instans EC2 yang ingin Anda sertakan dalam target penilaian ini, untuk Gunakan Tag, masukkan nama kunci tanda dan pasangan nilai-kunci.

5. (Opsional) Saat menciptakan target, Anda dapat memilih kotak centang Instal Agen untuk menginstal agen pada semua instans EC2 dalam target ini. Untuk menggunakan opsi ini, instans EC2 Anda harus memiliki SSM Agent terinstal dan IAM role yang memungkinkan Run Command. SSM Agent terinstal, secara default, pada instans Windows Amazon EC2 dan instans Amazon Linux. Amazon EC2 Systems Manager memerlukan IAM role untuk instans EC2 yang memproses perintah dan peran terpisah bagi pengguna yang menjalankan perintah. Untuk informasi lebih lanjut, lihat Menginstal dan Mengonfigurasi SSM Agent dan Mengonfigurasi Peran Keamanan untuk System Manager.

> **Important**
>
> Jika instans EC2 sudah memiliki agen berjalan, menggunakan opsi ini menggantikan agen yang saat ini berjalan pada instans dengan versi agen terbaru.

> **Note**
>
> Untuk target penilaian yang ada, Anda dapat memilih Menginstal Agen dengan tombol Run Command untuk menginstal agen pada semua instans EC2 dalam target ini.

> **Note**
>
> Anda juga dapat menginstal agen pada beberapa instans EC2 (baik instans berbasis Linux dan berbasis Windows dengan perintah yang sama) secara jarak jauh dengan menggunakan Systems Manager Run Command. Untuk informasi selengkapnya, lihat

Menginstal Agen Amazon Inspector pada Beberapa Instans EC2 Menggunakan Systems Manager Run Command.

6. Pilih Save (Simpan).

> **Note**
>
> Anda dapat menggunakan tombol Tinjau Target pada halaman Target Penilaian untuk meninjau semua instans EC2 yang termasuk dalam target penilaian. Untuk setiap instans EC2, Anda dapat meninjau nama host, ID instans, alamat IP, dan, jika berlaku, status agen. Status agen dapat memiliki nilai berikut: SEHAT,TIDAK SEHAT, danTIDAK DIKETAHUI. Amazon Inspector Classic menampilkanTIDAK DIKETAHUIstatus ketika tidak dapat menentukan apakah ada agen yang berjalan pada instans EC2.

## Menghapus target penilaian

Untuk menghapus target penilaian, lakukan prosedur berikut ini.

Untuk menghapus target penilaian

- Pada halaman Target penilaian, pilih target yang ingin Anda hapus, lalu pilih Hapus. Ketika diminta konfirmasi, pilih Ya.

> **Important**
>
> Ketika Anda menghapus target penilaian, semua templat penilaian, penilaian berjalan, temuan, dan versi laporan yang terkait dengan target ini juga akan dihapus.

Anda juga dapat menghapus target penilaian dengan menggunakan API `DeleteAssessmentTarget`.

# Amazon Inspector Classic mengatur paket dan aturan

Anda dapat menggunakan Amazon Inspector Classic untuk menilai target penilaian Anda (kumpulan sumber daya AWS) untuk potensi masalah keamanan dan kerentanan. Amazon Inspector Classic membandingkan perilaku dan konfigurasi keamanan target penilaian dengan paket aturan keamanan yang dipilih. Dalam konteks Amazon Inspector Classic, aturannya adalah pemeriksaan keamanan yang dilakukan Amazon Inspector Classic selama penilaian dijalankan.

Di Amazon Inspector Classic, aturan dikelompokkan ke dalam paket aturan yang berbeda baik berdasarkan kategori, tingkat keparahan, atau harga. Hal ini memberi Anda pilihan untuk jenis analisis yang dapat Anda lakukan. Misalnya, Amazon Inspector Classic menawarkan sejumlah besar aturan yang dapat Anda gunakan untuk menilai aplikasi Anda. Akan tetapi, Anda mungkin ingin menyertakan subset yang lebih kecil dari aturan yang tersedia untuk menargetkan area tertentu yang menjadi perhatian atau untuk menemukan masalah keamanan tertentu. Perusahaan dengan departemen IT besar mungkin ingin menentukan apakah aplikasi mereka terekspos ancaman keamanan. Perusahaan lain mungkin ingin fokus hanya pada masalah dengan tingkat kepelikan Tinggi.



## Tingkat keparahan untuk aturan di Amazon Inspector Classic

Setiap aturan Amazon Inspector Classic memiliki tingkat keparahan yang ditetapkan. Hal ini mengurangi kebutuhan untuk memprioritaskan satu aturan di atas aturan lain dalam analisis Anda. Hal ini juga dapat membantu Anda menentukan respons Anda ketika aturan menyoroti potensi masalah.

Semua tingkat Tinggi, Medium, dan Rendah menunjukkan masalah keamanan yang dapat mengakibatkan pembobolan kerahasiaan, integritas, dan ketersediaan informasi dalam target penilaian Anda. Tingkat ini dibedakan oleh seberapa besar kemungkinan masalah ini menyebabkan pembobolan dan seberapa mendesak untuk memperbaiki masalah ini.

Tingkat Informasi hanya menyoroti detail konfigurasi keamanan target penilaian Anda.

Berikut adalah cara yang disarankan untuk merespons masalah berdasarkan tingkat kepelikannya:

- Tinggi – Masalah dengan tingkat kepelikan tinggi bersifat sangat mendesak. Amazon Inspector Classic merekomendasikan agar Anda memperlakukan masalah keamanan ini sebagai keadaan darurat dan segera menerapkan perbaikan.
- Medium – Masalah dengan tingkat kepelikan medium bersifat agak mendesak. Amazon Inspector Classic merekomendasikan agar Anda memperbaiki masalah ini pada kesempatan berikutnya, misalnya, selama pembaruan layanan berikutnya.
- Rendah – Masalah dengan tingkat kepelikan rendah bersifat kurang mendesak. Amazon Inspector Classic merekomendasikan agar Anda memperbaiki masalah ini sebagai bagian dari salah satu pembaruan layanan future Anda.
- Informasi – Masalah ini murni bersifat informatif. Berdasarkan tujuan bisnis dan organisasi Anda, Anda dapat dengan mudah membuat catatan informasi ini atau menggunakannya untuk meningkatkan keamanan target penilaian Anda.

# Aturan paket di Amazon Inspector Classic

Penilaian Amazon Inspector dapat menggunakan kombinasi dari paket aturan berikut:

Penilaian jaringan:

- Keterjangkauan Jaringan

Penilaian tuan rumah:

- Kelemahan dan eksposur umum
- Patokan Pusat Keamanan Internet (CIS)
- Praktik terbaik keamanan untuk Amazon Inspector Classic

# Keterjangkauan Jaringan

Aturan dalam paket Keterjangkauan Jaringan menganalisis konfigurasi jaringan Anda untuk menemukan kelemahan keamanan instans EC2 Anda. Temuan yang dihasilkan Amazon Inspector juga memberikan panduan tentang membatasi akses yang tidak aman.

Paket aturan Network Reachability menggunakan teknologi terbaru dari inisiatif AWS Provable Security.

Temuan yang dihasilkan oleh aturan ini menunjukkan apakah port Anda dapat dijangkau dari internet melalui gateway internet (termasuk instans di balik Application Load Balancer atau Classic Load Balancer), koneksi peering VPC, atau VPN melalui gateway virtual. Temuan ini juga menyoroti konfigurasi jaringan yang memungkinkan akses yang berpotensi berbahaya, seperti grup keamanan yang salah dikelola, ACL, IGW, dan sebagainya.

Aturan-aturan ini membantu mengotomatiskan pemantauan jaringan AWS Anda dan mengidentifikasi di mana akses jaringan ke instans EC2 Anda mungkin salah dikonfigurasi. Dengan memasukkan paket ini dalam penilaian berjalan Anda, Anda dapat menerapkan pemeriksaan keamanan jaringan detail tanpa harus menginstal pemindai dan mengirim paket, yang kompleks dan mahal untuk dipelihara, terutama di koneksi peering VPC dan VPN.

> **Important**
>
> Agen Amazon Inspector Classic tidak diharuskan untuk menilai instans EC2 Anda dengan paket aturan ini. Namun, agen yang diinstal dapat memberikan informasi tentang adanya proses yang didengarkan pada port. Jangan menginstal agen pada sistem operasi yang tidak didukung Amazon Inspector Classic. Jika agen hadir pada instans yang menjalankan sistem operasi yang tidak didukung, paket aturan Keterjangkauan Jaringan tidak akan bekerja pada instans tersebut.

Untuk informasi selengkapnya, lihat Paket aturan Amazon Inspector Classic untuk sistem operasi yang didukung.

## Konfigurasi yang dianalisis

Aturan Keterjangkauan Jaringan menganalisis konfigurasi entitas berikut untuk kelemahan:

- Instans Amazon EC2
- Penyeimbang Beban Aplikasi
- Connect Langsung
- Penyeimbang Beban Elastis
- Antarmuka Jaringan Elastis
- Gerbang Internet (IGW)
- Daftar Kontrol Akses Jaringan (ACL)
- Tabel Rute

- Grup Keamanan (SGs)
- Subnet
- Awan Pribadi Virtual (VPC)
- Gateway Pribadi Virtual (VGW)
- Koneksi peering VPC

## Rute keterjangkauan

Aturan Keterjangkauan Jaringan memeriksa rute keterjangkauan berikut, yang sesuai dengan cara di mana port Anda dapat diakses dari luar VPC Anda:

- **`Internet`** - Gateway Internet (termasuk Application Load Balancer dan Classic Load Balancer)
- **`PeeredVPC`** - Koneksi peering VPC
- **`VGW`** - Virtual private gateway

## Jenis temuan

Penilaian yang mencakup paket aturan Keterjangkauan Jaringan dapat mengembalikan jenis temuan berikut untuk setiap rute keterjangkauan:

- `RecognizedPort`
- `UnrecognizedPortWithListener`
- `NetworkExposure`

### `RecognizedPort`

Port yang biasanya digunakan untuk layanan yang dikenal dapat dicapai. Jika agen terdapat pada instans EC2 target, temuan yang dihasilkan juga akan menunjukkan apakah ada proses mendengarkan aktif pada port. Temuan jenis ini diberi tingkat kepelikan berdasarkan dampak keamanan dari layanan yang dikenal:

- **`RecognizedPortWithListener`** – Sebuah port yang dikenal secara eksternal dapat dijangkau dari internet publik melalui komponen jaringan tertentu, dan proses mendengarkan pada port.
- **`RecognizedPortNoListener`** – Sebuah port dapat dijangkau secara eksternal dari internet publik melalui komponen jaringan tertentu, dan tidak ada proses mendengarkan pada port.

- **`RecognizedPortNoAgent`** – Sebuah port dapat dijangkau secara eksternal dari internet publik melalui komponen jaringan tertentu. Adanya proses mendengarkan pada port tidak dapat ditentukan tanpa menginstal agen pada instans target.

Tabel berikut menunjukkan daftar port yang dikenal:

| Layanan | Port TCP | Port UDP |
|---|---|---|
| SMB | 445 | 445 |
| NetBIOS | 137, 139 | 137, 138 |
| LDAP | 389 | 389 |
| LDAP melalui TLS | 636 | |
| Katalog global LDAP | 3268 | |
| Katalog global LDAP melalui TLS | 3269 | |
| NFS | 111, 2049, 4045, 1110 | 111, 2049, 4045, 1110 |
| Kerberos | 88, 464, 543, 544, 749, 751 | 88, 464, 749, 750, 751, 752 |
| RPC | 111, 135, 530 | 111, 135, 530 |
| WINS | 1512, 42 | 1512, 42 |
| DHCP | 67, 68, 546, 547 | 67, 68, 546, 547 |
| Syslog | 601 | 514 |
| Layanan cetak | 515 | |
| Telnet | 23 | 23 |
| FTP | 21 | 21 |
| SSH | 22 | 22 |

| Layanan | Port TCP | Port UDP |
| --- | --- | --- |
| RDP | 3389 | 3389 |
| MongoDB | 27017, 27018, 27019, 28017 | |
| SQL Server | 1433 | 1434 |
| MySQL | 3306 | |
| PostgreSQL | 5432 | |
| Oracle | 1521, 1630 | |
| Elasticsearch | 9300, 9200 | |
| HTTP | 80 | 80 |
| HTTPS | 443 | 443 |

### `UnrecogizedPortWithListener`

Port yang tidak tercantum dalam tabel sebelumnya bersifat dapat dijangkau dan memiliki proses mendengarkan aktif. Karena temuan jenis ini menunjukkan informasi tentang proses mendengarkan, mereka dapat dihasilkan hanya ketika agen Amazon Inspector diinstal pada instans EC2 target. Temuan jenis ini diberi kepelikan Rendah.

### `NetworkExposure`

Temuan jenis ini menunjukkan informasi agregat pada port yang dapat dijangkau pada instans EC2 Anda. Untuk setiap kombinasi dari antarmuka jaringan elastis dan grup keamanan pada instans EC2, temuan ini menunjukkan set dapat dijangkau rentang TCP dan UDP port. Temuan jenis ini memiliki tingkat kepelikan Informasi.

## Kelemahan dan eksposur umum

Aturan dalam paket ini membantu memverifikasi apakah instans EC2 dalam target penilaian Anda terekspos kelemahan dan eksposur umum (CVE). Serangan dapat mengeksploitasi kelemahan yang

tidak di-patch untuk membobol kerahasiaan, integritas, atau ketersediaan layanan atau data Anda. Sistem CVE menyediakan metode referensi untuk kelemahan dan eksposur keamanan informasi yang diketahui secara umum. Untuk informasi lebih lanjut, lihat https://cve.mitre.org/.

Jika CVE tertentu muncul dalam temuan yang dihasilkan oleh penilaian Amazon Inspector Classic, Anda dapat mencari https://cve.mitre.org/ untuk ID CVE (misalnya,). **CVE-2009-0021** Hasil pencarian dapat memberikan informasi detail tentang CVE ini, tingkat kepelikan, dan cara menguranginya.

Untuk paket aturan Common Vulnerabilities & Exploits (CVE), Amazon Inspector telah memetakan level CVSS Base Scoring dan ALAS Severity yang disediakan:

| Keparahan Amazon Inspector | Skor Dasar CVSS | ALAS Keparahan (jika CVSS tidak mencetak gol) |
|---|---|---|
| Tinggi | >= 5 | Kritis atau Penting |
| Sedang | < 5 and >= 2,1 | Sedang |
| Rendah | < 2.1 and >= 0.8 | Rendah |
| Informasi | < 0,8 | N/A |

Aturan yang disertakan dalam paket ini membantu Anda menilai apakah instans EC2 Anda terekspos ke CVE dalam daftar wilayah berikut:

- AS Timur (Virginia N.)
- AS Timur (Ohio)
- AS Barat (California N.)
- AS Barat (Oregon)
- Uni Eropa (Irlandia)
- Uni Eropa (Frankfurt am Main)
- Uni Eropa (London)
- Uni Eropa (Stockholm)
- Asia Pasifik (Tokyo)
- Asia Pasifik (Seoul)

- Asia Pasifik (Mumbai)
- Asia Pasifik (Sydney)
- AWS GovCloud West (AS)
- AWS GovCloud Timur (AS)

Paket aturan CVE diperbarui secara berkala; daftar ini mencakup CVE yang termasuk dalam penilaian berjalan yang terjadi pada waktu yang sama dengan saat daftar ini diambil.

Untuk informasi selengkapnya, lihat Paket aturan Amazon Inspector Classic untuk sistem operasi yang didukung.

## Patokan Pusat Keamanan Internet (CIS)

Program Tolok Ukur Keamanan CIS menyediakan praktik terbaik industri berbasis konsensus yang terdefinisi dengan baik, tidak bias, untuk membantu organisasi menilai dan meningkatkan keamanan mereka. AWS adalah perusahaan Anggota Tolok Ukur Keamanan CIS. Untuk daftar sertifikasi Amazon Inspector Classic, lihat halaman Amazon Web Services di situs web CIS.

Amazon Inspector Classic saat ini menyediakan paket aturan Bersertifikat CIS berikut untuk membantu menetapkan postur konfigurasi yang aman untuk sistem operasi berikut:

Amazon Linux

- `CIS Benchmark for Amazon Linux 2 Benchmark v1.0.0 Level 1`
- `CIS Benchmark for Amazon Linux 2 Benchmark v1.0.0 Level 2`
- `CIS Benchmark for Amazon Linux Benchmark v2.1.0 Level 1`
- `CIS Benchmark for Amazon Linux Benchmark v2.1.0 Level 2`
- `CIS Benchmark for Amazon Linux 2014.09-2015.03 v1.1.0 Level 1`

CentOS Linux

- `CIS Benchmark for CentOS Linux 7 Benchmark v2.2.0 Level 1 Server`
- `CIS Benchmark for CentOS Linux 7 Benchmark v2.2.0 Level 2 Server`
- `CIS Benchmark for CentOS Linux 7 Benchmark v2.2.0 Level 1 Workstation`
- `CIS Benchmark for CentOS Linux 7 Benchmark v2.2.0 Level 2 Workstation`
- `CIS Benchmark for CentOS Linux 6 Benchmark v2.0.2 Level 1 Server`

- CIS Benchmark for CentOS Linux 6 Benchmark v2.0.2 Level 2 Server
- CIS Benchmark for CentOS Linux 6 Benchmark v2.0.2 Level 1 Workstation
- CIS Benchmark for CentOS Linux 6 Benchmark v2.0.2 Level 2 Workstation

### Perusahaan Topi Merah Linux

- CIS Benchmark for Red Hat Enterprise Linux 7 Benchmark v2.1.1 Level 1 Server
- CIS Benchmark for Red Hat Enterprise Linux 7 Benchmark v2.1.1 Level 2 Server
- CIS Benchmark for Red Hat Enterprise Linux 7 Benchmark v2.1.1 Level 1 Workstation
- CIS Benchmark for Red Hat Enterprise Linux 7 Benchmark v2.1.1 Level 2 Workstation
- CIS Benchmark for Red Hat Enterprise Linux 6 Benchmark v2.0.2 Level 1 Server
- CIS Benchmark for Red Hat Enterprise Linux 6 Benchmark v2.0.2 Level 2 Server
- CIS Benchmark for Red Hat Enterprise Linux 6 Benchmark v2.0.2. Level 1 Workstation
- CIS Benchmark for Red Hat Enterprise Linux 6 Benchmark v2.0.2 Level 2 Workstation

### Ubuntu

- CIS Benchmark for Ubuntu Linux 18.04 LTS Benchmark v1.0.0 Level 1 Server
- CIS Benchmark for Ubuntu Linux 18.04 LTS Benchmark v1.0.0 Level 2 Server
- CIS Benchmark for Ubuntu Linux 18.04 LTS Benchmark v1.0.0 Level 1 Workstation
- CIS Benchmark for Ubuntu Linux 18.04 LTS Benchmark v1.0.0 Level 2 Workstation
- CIS Benchmark for Ubuntu Linux 16.04 LTS Benchmark v1.1.0 Level 1 Server
- CIS Benchmark for Ubuntu Linux 16.04 LTS Benchmark v1.1.0 Level 2 Server

- CIS Benchmark for Ubuntu Linux 16.04 LTS Benchmark v1.1.0 Level 1 Workstation
- CIS Benchmark for Ubuntu Linux 16.04 LTS Benchmark v1.1.0 Level 2 Workstation
- CIS Benchmark for Ubuntu Linux 14.04 LTS Benchmark v2.0.0 Level 1 Server
- CIS Benchmark for Ubuntu Linux 14.04 LTS Benchmark v2.0.0 Level 2 Server
- CIS Benchmark for Ubuntu Linux 14.04 LTS Benchmark v2.0.0 Level 1 Workstation
- CIS Benchmark for Ubuntu Linux 14.04 LTS Benchmark v2.0.0 Level 2 Workstation

### Windows

- Windows Server 2016 (CIS Benchmark for Microsoft Windows 2016 RTM (Release 1607), v1.1.0, Level 1 Member Server Profile)
- Windows Server 2016 (CIS Benchmark for Microsoft Windows 2016 RTM (Release 1607), v1.1.0, Level 2 Member Server Profile)
- Windows Server 2016 (CIS Benchmark for Microsoft Windows 2016 RTM (Release 1607), v1.1.0, Level 1 Domain Controller Profile)
- Windows Server 2016 (CIS Benchmark for Microsoft Windows 2016 RTM (Release 1607), v1.1.0, Level 2 Domain Controller Profile)
- Windows Server 2016 (CIS Benchmark for Microsoft Windows 2016 RTM (Release 1607), v1.1.0, Next Generation Windows Security Profile)
- Windows Server 2012 R2 (CIS Benchmark for Microsoft Windows 2012 R2, v2.2.0, Level 1 Domain Controller Profile)
- Windows Server 2012 R2 (CIS Benchmark for Microsoft Windows 2012 R2, v2.2.0, Level 2 Domain Controller Profile)
- Windows Server 2012 R2 (CIS Benchmark for Microsoft Windows 2012 R2, v2.2.0, Level 1 Member Server Profile)
- Windows Server 2012 R2 (CIS Benchmark for Microsoft Windows 2012 R2, v2.2.0, Level 2 Member Server Profile)
- Windows Server 2012 (CIS Benchmark for Microsoft Windows 2012 non-R2, v2.0.0, Level 1 Member Server Profile)

- Windows Server 2012 (CIS Benchmark for Microsoft Windows 2012 non-R2, v2.0.0, Level 2 Member Server Profile)
- Windows Server 2012 (CIS Benchmark for Microsoft Windows 2012 non-R2, v2.0.0, Level 1 Domain Controller Profile)
- Windows Server 2012 (CIS Benchmark for Microsoft Windows 2012 non-R2, v2.0.0, Level 2 Domain Controller Profile)
- Windows Server 2008 R2 (CIS Benchmark for Microsoft Windows 2008 R2, v3.0.0, Level 1 Domain Controller Profile)
- Windows Server 2008 R2 (CIS Benchmark for Microsoft Windows 2008 R2, v3.0.0, Level 1 Member Server Profile)

Jika tolok ukur CIS tertentu muncul dalam temuan yang dihasilkan oleh penilaian Amazon Inspector Classic, Anda dapat mengunduh deskripsi PDF terperinci dari tolok ukur dari https://benchmarks.cisecurity.org/ (pendaftaran gratis diperlukan). Dokumen patokan menyediakan informasi detail tentang patokan CIS ini, tingkat kepelikan, dan cara menguranginya.

Untuk informasi selengkapnya, lihat Paket aturan Amazon Inspector Classic untuk sistem operasi yang didukung.

## Praktik terbaik keamanan untuk Amazon Inspector Classic

Gunakan aturan Amazon Inspector Classic untuk membantu menentukan apakah sistem Anda dikonfigurasi dengan aman.

> **Important**
>
> Saat ini, Anda dapat menyertakan dalam target penilaian instans EC2 yang menjalankan baik sistem operasi berbasis Linux ataupun berbasis Windows.
> Selama menjalankan penilaian, aturan yang dijelaskan dalam bagian ini menghasilkan temuan hanya untuk instans EC2 yang menjalankan sistem operasi berbasis Linux. Aturan tidak menghasilkan temuan untuk instans EC2 yang menjalankan sistem operasi berbasis Windows.
> Untuk informasi selengkapnya, lihat Paket aturan Amazon Inspector Classic untuk sistem operasi yang didukung.

Topik



## Menonaktifkan login root melalui SSH

Aturan ini membantu menentukan apakah daemon SSH dikonfigurasi untuk mengizinkan masuk ke instans EC2 Anda sebagai root.

Kepelikan

Medium

Temuan

Ada instans EC2 dalam target penilaian Anda yang dikonfigurasi untuk memungkinkan pengguna untuk masuk ke kredensial root melalui SSH. Hal ini meningkatkan kemungkinan serangan brute-force yang sukses.

Resolusi

Kami merekomendasikan Anda untuk mengonfigurasi instans EC2 Anda untuk mencegah login akun root melalui SSH. Alih-alih, masuklah sebagai pengguna non-root dan gunakan `sudo` untuk meningkatkan hak istimewa bila diperlukan. Untuk menonaktifkan login akun root SSH, atur `PermitRootLogin` ke no di file `/etc/ssh/sshd_config`, lalu mulai ulang `sshd`.

## Mendukung SSH versi 2 saja

Aturan ini membantu menentukan apakah instans EC2 Anda dikonfigurasi untuk mendukung protokol SSH versi 1.

Kepelikan

Medium

Temuan

Instans EC2 dalam target penilaian Anda dikonfigurasi untuk mendukung SSH-1, yang berisi kekurangan desain inheren yang sangat mengurangi keamanannya.

Resolusi

Kami merekomendasikan Anda mengonfigurasi instans EC2 dalam target penilaian Anda untuk mendukung hanya SSH-2 dan yang lebih baru. Untuk OpenSSH, Anda bisa mencapainya dengan mengatur `Protocol 2` di file `/etc/ssh/sshd_config`. Untuk informasi selengkapnya, lihat `man sshd_config`.

## Menonaktifkan autentikasi kata sandi Melalui SSH

Aturan ini membantu menentukan apakah instans EC2 Anda dikonfigurasi untuk mendukung autentikasi kata sandi melalui protokol SSH.

Kepelikan

Medium

Temuan

Instans EC2 dalam target penilaian Anda dikonfigurasi untuk mendukung autentikasi kata sandi melalui SSH. Autentikasi kata sandi rentan terhadap serangan brute-force dan harus dinonaktifkan untuk mendukung autentikasi berbasis kunci jika memungkinkan.

Resolusi

Kami merekomendasikan Anda menonaktifkan autentikasi kata sandi melalui SSH pada instans EC2 Anda dan mengaktifkan dukungan untuk autentikasi berbasis kunci sebagai gantinya. Hal ini secara signifikan mengurangi kemungkinan serangan brute-force yang berhasil. Untuk informasi selengkapnya, lihathttps://aws.amazon.com/articles/1233/. Jika autentikasi kata sandi didukung, penting untuk membatasi akses ke server SSH ke alamat IP tepercaya.

## Mengonfigurasi usia maksimum kata sandi

Aturan ini membantu menentukan apakah usia maksimum untuk kata sandi dikonfigurasi pada instans EC2 Anda.

Kepelikan

Medium

Temuan

Instans EC2 dalam target penilaian Anda tidak dikonfigurasi untuk usia maksimum untuk kata sandi.

Resolusi

Jika Anda menggunakan kata sandi, kami merekomendasikan Anda mengonfigurasi usia maksimum untuk kata sandi pada semua instans EC2 di target penilaian Anda. Hal ini mengharuskan pengguna untuk secara teratur mengubah kata sandi mereka dan mengurangi kemungkinan serangan menebak kata sandi yang sukses. Untuk memperbaiki masalah ini bagi pengguna yang sudah ada, gunakan perintah chage. Untuk mengonfigurasi usia maksimum untuk sandi untuk semua pengguna di masa mendatang, edit bidang `PASS_MAX_DAYS` di file `/etc/login.defs`.

## Mengonfigurasi panjang minimum kata sandi

Aturan ini membantu menentukan apakah panjang minimum untuk kata sandi dikonfigurasi pada instans EC2 Anda.

Kepelikan

Medium

Temuan

Instans EC2 dalam target penilaian Anda tidak dikonfigurasi untuk panjang minimum untuk kata sandi.

Resolusi

Jika Anda menggunakan kata sandi, kami merekomendasikan Anda mengonfigurasi panjang minimum untuk kata sandi pada semua instans EC2 di target penilaian Anda. Mengatur panjang

minimum kata sandi mengurangi risiko serangan menebak kata sandi yang sukses. Anda dapat melakukan ini dengan menggunakan opsi berikut dipwquality.confberkas: minlen. Untuk informasi selengkapnya, lihathttps://linux.die.net/man/5/pwquality.conf.

Jika pwquality.conf tidak tersedia pada instans Anda, Anda dapat mengatur opsi minlen menggunakan modul pam_cracklib.so. Untuk informasi selengkapnya, lihat man pam_cracklib.

Opsi minlen harus diatur ke 14 atau lebih besar.

## Mengonfigurasi kompleksitas kata sandi

Aturan ini membantu menentukan apakah mekanisme kompleksitas kata sandi dikonfigurasi pada instans EC2 Anda.

Kepelikan

Medium

Temuan

Tidak ada mekanisme kompleksitas atau pembatasan kata sandi dikonfigurasi pada instans EC2 di target penilaian Anda. Hal ini memungkinkan pengguna untuk mengatur kata sandi sederhana, yang meningkatkan kemungkinan pengguna tidak sah mendapatkan akses dan menyalahgunakan akun.

Resolusi

Jika Anda menggunakan kata sandi, kami merekomendasikan Anda mengonfigurasi semua instans EC2 di target penilaian Anda untuk memerlukan tingkat kompleksitas sandi. Anda dapat melakukan ini dengan menggunakan opsi berikut di file pwquality.conf: lcredit, ucredit, dcredit, dan ocredit. Untuk informasi lebih lanjut, lihat https://linux.die.net/man/5/pwquality.conf .

Jika pwquality.conf tidak tersedia pada instans Anda, Anda dapat mengatur opsi lcredit, ucredit, dcredit, dan ocredit menggunakan modul pam_cracklib.so. Untuk informasi selengkapnya, lihat man pam_cracklib.

Nilai yang diharapkan untuk masing-masing pilihan ini kurang dari atau sama dengan -1, seperti yang ditunjukkan di bawah ini:

```
lcredit <= -1, ucredit <= -1, dcredit<= -1, ocredit <= -1
```

Selain itu,opsi `remember` harus diatur ke 12 atau lebih besar. Untuk informasi selengkapnya, lihat `man pam_unix`.

## Mengaktifkan ASLR

Aturan ini membantu menentukan apakah pengacakan tata letak ruang alamat (ASLR) diaktifkan pada sistem operasi instans EC2 di target penilaian Anda.

Kepelikan

Medium

Temuan

Instans EC2 dalam target penilaian Anda tidak memiliki ASLR aktif.

Resolusi

Untuk meningkatkan keamanan target penilaian Anda, kami merekomendasikan Anda mengaktifkan ASLR pada sistem operasi dari semua instans EC2 di target Anda dengan menjalankan echo 2 | sudo tee /proc/sys/kernel/randomize_va_space.

## Mengaktifkan DEP

Aturan ini membantu menentukan apakah Pencegahan Eksekusi Data (DEP) diaktifkan pada sistem operasi dari instans EC2 di target penilaian Anda.

> **Note**
>
> Aturan ini tidak didukung untuk instans EC2 dengan prosesor ARM.

Kepelikan

Medium

Temuan

Instans EC2 dalam target penilaian Anda tidak memiliki DEP aktif.

Resolusi

Kami merekomendasikan agar Anda mengaktifkan DEP pada sistem operasi dari semua instans EC2 dalam target penilaian Anda. Mengaktifkan DEP melindungi instans Anda dari bahaya keamanan menggunakan teknik buffer-overflow.

## Mengonfigurasi izin untuk direktori sistem

Aturan ini memeriksa izin pada direktori sistem yang berisi biner dan informasi konfigurasi sistem. Ia memeriksa bahwa hanya pengguna root (pengguna yang masuk menggunakan kredensial akun root) memiliki izin menulis untuk direktori ini.

Kepelikan

Tinggi

Temuan

Instans EC2 dalam target penilaian Anda berisi direktori sistem yang dapat ditulis oleh pengguna non-root.

Resolusi

Untuk meningkatkan keamanan target penilaian Anda dan untuk mencegah eskalasi hak istimewa oleh pengguna lokal jahat, konfigurasikan semua direktori sistem pada semua instans EC2 target Anda untuk dapat ditulis hanya oleh pengguna yang masuk dengan menggunakan kredensial akun root.

# Templat penilaian Amazon Inspector Classic dan penilaian berjalan

Amazon Inspector Classic membantu Anda menemukan potensi masalah keamanan dengan menggunakan aturan keamanan untuk menganalisis sumber daya Anda AWS . Amazon Inspector Classic memantau dan mengumpulkan data perilaku (telemetri) tentang sumber daya Anda. Data tersebut mencakup informasi tentang penggunaan saluran aman, lalu lintas jaringan di antara proses yang berjalan, dan detail komunikasi dengan AWS layanan. Selanjutnya, Amazon Inspector Classic menganalisis dan membandingkan data dengan seperangkat paket aturan keamanan. Terakhir, Amazon Inspector Classic menghasilkan daftar temuan yang mengidentifikasi potensi masalah keamanan dari berbagai tingkat keparahan.

Untuk memulai, Anda membuat target penilaian (kumpulan AWS sumber daya yang ingin dianalisis Amazon Inspector Classic). Berikutnya, Anda membuat templat penilaian (cetak biru yang Anda gunakan untuk mengonfigurasi penilaian Anda). Anda menggunakan templat untuk memulai penilaian berjalan, yang merupakan proses pemantauan dan analisis yang menghasilkan satu set temuan.

Topik



## Templat penilaian Amazon Inspector Classic

Templat penilaian memungkinkan Anda untuk menentukan konfigurasi untuk penilaian berjalan Anda, termasuk yang berikut ini:

- Paket aturan yang digunakan Amazon Inspector Classic untuk mengevaluasi target penilaian Anda

- Durasi penilaian berjalan – Anda dapat mengatur durasi penilaian berjalan antara 3 menit hingga 24 jam. Kami merekomendasikan pengaturan durasi penilaian berjalan hingga 1 jam.
- Topik Amazon SNS yang dikirimkan oleh Amazon Inspector Classic tentang status dan temuan penilaian Anda
- Atribut Amazon Inspector Classic (pasangan nilai kunci) yang dapat Anda tetapkan ke temuan yang dihasilkan oleh proses penilaian yang menggunakan templat penilaian ini

Setelah Amazon Inspector Classic membuat template penilaian, Anda dapat menandainya seperti sumber daya lainnya AWS . Untuk informasi lebih lanjut, lihat Editor Tanda. Menandai templat penilaian memungkinkan Anda untuk mengaturnya dan mendapatkan pengawasan yang lebih baik dari strategi keamanan Anda. Misalnya, Amazon Inspector Classic menawarkan sejumlah besar aturan yang dapat Anda menilai target penilaian Anda. Anda mungkin ingin menyertakan berbagai subset dari aturan yang tersedia dalam templat penilaian Anda untuk menargetkan area tertentu yang menjadi perhatian atau untuk mengungkap masalah keamanan tertentu. Menandai templat penilaian memungkinkan Anda untuk menemukan dan menjalankannya dengan cepat setiap saat sesuai dengan strategi dan tujuan keamanan Anda.

> **Important**
>
> Setelah membuat templat penilaian, Anda tidak dapat memodifikasinya.

## Batas templat penilaian Amazon Inspector Classic

Anda dapat membuat hingga 500 templat penilaian untuk setiap AWS akun.

Untuk informasi selengkapnya, lihat Batas layanan Amazon Inspector Classic.

## Membuat templat penilaian

Untuk membuat templat penilaian

1. Masuk ke AWS Management Console dan buka konsol Amazon Inspector Classic di https://console.aws.amazon.com/inspector/.
2. Di panel navigasi, pilih Templat Penilaian, lalu pilih Buat.
3. Untuk Nama, masukkan nama untuk templat penilaian Anda.

4. Untuk Nama target, pilih target penilaian untuk dianalisis.

> **Note**
>
> Ketika Anda membuat templat penilaian, Anda dapat menggunakan tombol Pratinjau Target pada halaman Templat Penilaian untuk meninjau semua instans EC2 yang termasuk dalam target penilaian. Untuk setiap instans EC2, Anda dapat meninjau nama host, ID instans, alamat IP, dan, jika berlaku, status agen. Status agen dapat memiliki nilai-nilai berikut: SEHAT, TIDAK SEHAT, dan TIDAK DIKETAHUI. Amazon Inspector Classic menampilkan status UNKNOWN ketika tidak dapat menentukan apakah ada agen yang berjalan pada instans EC2.
> Anda juga dapat menggunakan tombol Pratinjau Target pada halaman Templat Penilaian untuk meninjau instans EC2 yang membentuk target penilaian yang dimasukkan dalam templat yang Anda buat sebelumnya.

5. Untuk Paket aturan, pilih satu atau lebih paket aturan yang akan dimasukkan di templat penilaian ini.
6. Untuk Durasi, tentukan durasi untuk templat penilaian Anda.
7. (Opsional) Untuk topik SNS, tentukan topik SNS yang Anda inginkan Amazon Inspector Classic untuk mengirim notifikasi tentang status dan temuan proses penilaian. Amazon Inspector Classic dapat mengirim pemberitahuan SNS tentang peristiwa berikut:

   - Penilaian berjalan telah dimulai
   - Penilaian berjalan telah berakhir
   - Status penilaian berjalan telah berubah
   - Temuan dihasilkan

   Untuk informasi lebih lanjut tentang pengaturan topik SNS, lihat Menyiapkan topik SNS untuk notifikasi Amazon Inspector Classic.
8. (Opsional) Untuk Tanda, masukkan nilai untuk Kunci dan Nilai. Anda dapat menambahkan beberapa tanda ke templat penilaian.
9. (Opsional) Untuk Atribut yang ditambahkan ke temuan, masukkan nilai untuk Kunci dan Nilai. Amazon Inspector Classic menerapkan atribut ke semua temuan yang dihasilkan oleh template penilaian. Anda dapat menambahkan beberapa atribut ke templat penilaian. Untuk informasi lebih lanjut tentang temuan dan penandaan temuan, lihat Temuan Amazon Inspector Classic.

10. (Opsional) Untuk mengatur jadwal untuk penilaian berjalan Anda menggunakan templat ini, pilih kotak centang Mengatur pengulangan penilaian berjalan sekali setiap <number_of_days>, mulai sekarang dan tentukan pola pengulangan (jumlah hari) menggunakan panah atas dan bawah.

> **Note**
>
> Bila Anda menggunakan kotak centang ini, Amazon Inspector Classic secara otomatis membuat aturan Amazon CloudWatch Events untuk jadwal penilaian berjalan yang Anda siapkan. Amazon Inspector Classic kemudian juga secara otomatis membuat peran IAM bernama. `AWS_InspectorEvents_Invoke_Assessment_Template` Peran ini memungkinkan CloudWatch Events melakukan panggilan API terhadap resource Amazon Inspector Classic. Untuk informasi selengkapnya, lihat Apa itu CloudWatch Acara Amazon? dan Menggunakan Kebijakan Berbasis Sumber Daya untuk Acara. CloudWatch

> **Note**
>
> Anda juga dapat mengatur penilaian berjalan otomatis melalui fungsi AWS Lambda . Untuk informasi selengkapnya, lihat Mengatur penilaian berjalan otomatis melalui fungsi Lambda.

11. Pilih Buat dan jalankan atau Buat.

## Menghapus templat penilaian

Untuk menghapus templat penilaian, lakukan prosedur berikut.

Untuk menghapus templat penilaian

- Pada halaman Templat Penilaian, pilih templat yang ingin Anda hapus, lalu pilih Hapus. Ketika diminta konfirmasi, pilih Ya.

> **Important**
>
> Ketika Anda menghapus templat penilaian, semua penilaian berjalan, temuan, dan versi laporan yang terkait dengan templat ini juga akan dihapus.

Anda juga dapat menghapus templat penilaian dengan menggunakan API `DeleteAssessmentTemplate`.

# Penilaian berjalan

Setelah membuat templat penilaian, Anda dapat menggunakannya untuk memulai penilaian berjalan. Anda dapat memulai beberapa proses menggunakan template yang sama selama Anda tetap dalam batas run untuk setiap AWS akun. Untuk informasi selengkapnya, lihat Penilaian Amazon Inspector Classic menjalankan batas .

Jika Anda menggunakan konsol Amazon Inspector Classic, Anda harus memulai proses pertama template penilaian baru Anda dari halaman template Penilaian. Setelah memulai proses, Anda dapat menggunakan halaman Penilaian berjalan untuk memantau progres yang berjalan. Gunakan tombol Jalankan, Batalkan, dan Hapus untuk memulai, membatalkan, atau menghapus proses berjalan. Anda juga dapat melihat detail proses, termasuk ARN proses, paket aturan yang dipilih untuk proses tersebut, tanda dan atribut yang Anda terapkan ke proses, dan banyak lagi.

Untuk proses berikutnya dari templat penilaian, Anda dapat menggunakan tombol Jalankan, Batalkan, dan Hapus pada halaman Templat penilaian atau halaman Penilaian berjalan.

## Menghapus penilaian berjalan

Untuk menghapus penilaian berjalan, lakukan prosedur berikut.

Untuk menghapus proses

- Pada halaman Penilaian berjalan, pilih proses yang ingin Anda hapus, lalu pilih Hapus. Ketika diminta konfirmasi, pilih Ya.

> **Important**
>
> Ketika Anda menghapus proses, semua temuan dan semua versi laporan dari proses tersebut juga dihapus.

Anda juga dapat menghapus proses dengan menggunakan API `DeleteAssessmentRun`.

# Penilaian Amazon Inspector Classic menjalankan batas

Anda dapat membuat hingga 50.000 proses penilaian untuk setiap AWS akun.

Anda dapat memiliki beberapa proses yang terjadi pada waktu yang sama selama target yang digunakan untuk proses ini tidak mengandung instans EC2 yang tumpang tindih.

Untuk informasi selengkapnya, lihat Batas layanan Amazon Inspector Classic.

# Mengatur penilaian berjalan otomatis melalui fungsi Lambda

Jika Anda ingin mengatur jadwal berulang untuk penilaian Anda, Anda dapat mengonfigurasi templat penilaian Anda untuk berjalan secara otomatis dengan membuat fungsi Lambda menggunakan konsol AWS Lambda . Untuk informasi lebih lanjut, lihat Fungsi Lambda.

Untuk mengatur penilaian otomatis berjalan menggunakan AWS Lambda konsol, lakukan prosedur berikut.

Untuk mengatur proses otomatis melalui fungsi Lambda

1. Masuk ke AWS Management Console, dan buka AWS Lambda konsol.
2. Di panel navigasi, pilih Dasbor atau Fungsi, lalu pilih Buat Fungsi Lambda.
3. Pada halaman Buat fungsi, pilihJelajahi repositori aplikasi tanpa server, lalu masukkan **`inspector`** di bidang pencarian.
4. Pilih inspector-scheduled-runcetak biru.
5. Pada halaman Tinjau, konfigurasikan, dan terapkan, siapkan jadwal berulang untuk menjalankan otomatis dengan menentukan CloudWatch peristiwa yang memicu fungsi Anda. Untuk melakukannya, masukkan nama aturan dan deskripsi, lalu pilih ekspresi jadwal. Ekspresi jadwal menentukan seberapa sering proses terjadi, misalnya setiap 15 menit atau sekali dalam sehari. Untuk informasi selengkapnya tentang CloudWatch acara dan konsep, lihat Apa itu CloudWatch Acara Amazon?

   Jika Anda memilih kotak centang Aktifkan pemicu, proses dimulai segera setelah Anda selesai membuat fungsi Anda. Proses otomatis berikutnya mengikuti pola berulang yang Anda tentukan di bidang Ekspresi jadwal. Jika Anda tidak memilih kotak centang Aktifkan pemicu saat membuat fungsi, Anda dapat mengedit fungsi nanti untuk mengaktifkan pemicu ini.
6. Pada halaman Konfigurasi fungsi, tentukan hal berikut:

- Untuk Nama, masukkan nama untuk fungsi Anda.
- (Opsional) Untuk Deskripsi, masukkan deskripsi yang akan membantu Anda mengidentifikasi fungsi Anda nanti.
- Untuk runtime, pertahankan nilai default. **`Node.js 8.10`** AWS Lambda mendukung inspector-scheduled-runcetak biru hanya untuk runtime. **`Node.js 8.10`**
- Templat penilaian yang ingin Anda jalankan secara otomatis menggunakan fungsi ini. Anda melakukan ini dengan memberikan nilai untuk variabel lingkungan yang dipanggil assessmentTemplateArn.
- Tetap atur handler ke nilai default **`index.handler`**.
- Izin untuk fungsi Anda yang menggunakan bidang Role. Untuk informasi lebih lanjut, lihat Model Izin AWS Lambda.

  Untuk menjalankan fungsi ini, Anda memerlukan peran IAM yang memungkinkan AWS Lambda untuk memulai proses dan menulis pesan log tentang proses, termasuk kesalahan apa pun, ke Amazon CloudWatch Logs. AWS Lambda mengasumsikan peran ini untuk setiap proses otomatis berulang. Misalnya, Anda dapat melampirkan kebijakan sampel berikut ke IAM role ini:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "inspector:StartAssessmentRun",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource": "*"
    }
  ]
}
```

7. Tinjau pilihan Anda, lalu pilih Buat fungsi.

# Menyiapkan topik SNS untuk notifikasi Amazon Inspector Classic

Amazon Simple Notification Service (Amazon SNS) adalah layanan web yang mengirimkan pesan untuk berlangganan titik akhir atau klien. Anda dapat menggunakan Amazon SNS untuk mengatur notifikasi untuk Amazon Inspector Classic.

Untuk mengatur topik SNS untuk pemberitahuan

1. Membuat sebuah topik SNS. Lihat Tutorial: Membuat Topik Amazon SNS. Ketika Anda membuat topik, perluas bagian Kebijakan akses - opsional. Kemudian lakukan hal berikut untuk mengizinkan penilaian untuk mengirimkan pesan ke topik:

   a. Untuk Pilih metode, pilih Dasar.

   b. Untuk Menentukan siapa yang dapat mempublikasikan pesan ke topik, pilih Hanya AWS akun yang ditentukan, lalu masukkan ARN untuk akun di Wilayah tempat Anda membuat topik:

      - `US East (Ohio)` - arn:aws:iam::646659390643:root
      - `US East (N. Virginia)` - arn:aws:iam::316112463485:root
      - `US West (N. California)` - arn:aws:iam::166987590008:root
      - `US West (Oregon)` - arn:aws:iam::758058086616:root
      - `Asia Pacific (Mumbai)` - arn:aws:iam::162588757376:root
      - `Asia Pacific (Seoul)` - arn:aws:iam::526946625049:root
      - `Asia Pacific (Sydney)` - arn:aws:iam::454640832652:root
      - `Asia Pacific (Tokyo)` - arn:aws:iam::406045910587:root
      - `Europe (Frankfurt)` - arn:aws:iam::537503971621:root
      - `Europe (Ireland)` - arn:aws:iam::357557129151:root
      - `Europe (London)` - arn:aws:iam::146838936955:root
      - `Europe (Stockholm)` - arn:aws:iam::453420244670:root
      - `AWS GovCloud (US-East)`- arn ::iam: :206278770380:root aws-us-gov
      - `AWS GovCloud (US-West)`- arn ::iam: :850862329162:akar aws-us-gov

   c. Untuk Tentukan siapa yang dapat berlangganan topik ini, pilih Hanya AWS akun yang ditentukan, lalu masukkan ARN untuk akun di Wilayah tempat Anda membuat topik.

d. Untuk melindungi diri Anda dari Inspector yang digunakan sebagai wakil yang bingung seperti yang dijelaskan dalam masalah Deputi Bingung di Panduan Pengguna IAM, lakukan hal berikut:

   i. Pilih Lanjutan. Ini akan mengarahkan Anda ke editor JSON.

   ii. Tambahkan kondisi berikut:

```
"Condition": {
   "StringEquals": {
     "aws:SourceAccount": <your account Id here>,
     "aws:SourceArn": "arn:aws:inspector:*:*:*"
   }
 }
```

e. (Opsional) Untuk informasi tambahan tentang aws: SourceAccount dan aws:SourceArn, lihat Kunci konteks kondisi global di Panduan Pengguna IAM.

f. Perbarui pengaturan lain untuk topik yang diperlukan, lalu pilih Buat topik.

2. (Opsional) Untuk membuat topik SNS terenkripsi, lihat Enkripsi saat istirahat di Panduan Pengembang SNS.

3. Untuk melindungi diri Anda dari Inspector yang digunakan sebagai wakil bingung untuk kunci KMS Anda, ikuti langkah-langkah tambahan di bawah ini:

   a. Buka CMK Anda di konsol KMS.

   b. Pilih Edit.

   c. Tambahkan kondisi berikut:

```
"Condition": {
   "StringEquals": {
     "aws:SourceAccount": <your account Id here>,
     "aws:SourceArn": "arn:aws:sns:*:*:*"
   }
 }
```

4. Buat langganan untuk topik yang Anda buat. Untuk informasi lebih lanjut, lihat Tutorial: Berlangganan Titik Akhir untuk Topik Amazon SNS.

5. Untuk mengonfirmasi bahwa langganan dikonfigurasi dengan benar, publikasikan pesan untuk topik. Untuk informasi lebih lanjut, lihat Tutorial: Memublikasikan Pesan untuk Topik Amazon SNS.

# Temuan Amazon Inspector Classic

Temuan adalah masalah keamanan potensial yang ditemukan Amazon Inspector Classic selama penilaian target penilaian Anda. Temuan ditampilkan di konsol Amazon Inspector Classic atau melalui API. Temuan berisi deskripsi detail tentang masalah keamanan dan rekomendasi untuk menyelesaikannya.

Setelah Amazon Inspector menghasilkan temuan, Anda dapat melacaknya dengan menetapkan atribut Amazon Inspector Classic kepada mereka. Atribut ini terdiri dari pasangan nilai-kunci.

Melacak temuan Anda dengan atribut dapat berguna untuk mengelola alur kerja strategi keamanan Anda. Misalnya, setelah Anda membuat dan menjalankan penilaian, hal ini menghasilkan daftar temuan dari berbagai tingkat kepelikan, urgensi, dan minat kepada Anda, berdasarkan tujuan keamanan dan pendekatan Anda. Anda mungkin ingin segera mengikuti langkah-langkah rekomendasi suatu temuan untuk menyelesaikan masalah keamanan yang berpotensi mendesak. Atau Anda mungkin ingin menunda penyelesaian temuan lain hingga pembaruan layanan yang akan datang berikutnya. Misalnya, untuk melacak temuan untuk menyelesaikan segera, Anda dapat membuat dan menetapkan atribut ke temuan dengan sepasang kunci-nilai **`Status`** / **`Urgent`**. Anda juga dapat menggunakan atribut untuk mendistribusikan beban kerja penyelesaian potensi masalah keamanan. Misalnya, untuk memberi Bob (yang adalah seorang teknisi keamanan di tim Anda) tugas menyelesaikan temuan, Anda dapat menetapkan atribut untuk temuan dengan sepasang kunci-nilai **`Assigned Engineer`** / **`Bob`**.

## Bekerja dengan temuan

Selesaikan prosedur berikut pada salah satu temuan Amazon Inspector Classic yang dihasilkan.

Untuk menemukan, menganalisis, dan menetapkan atribut untuk temuan

1. Masuk ke AWS Management Console dan buka konsol Amazon Inspector Classic di https://console.aws.amazon.com/inspector/.
2. Setelah menjalankan penilaian, buka halaman Temuan di konsol Amazon Inspector Classic untuk melihat temuan Anda.

   Anda juga dapat melihat temuan Anda di bagian Temuan Terkemuka di halaman Dasbor konsol Amazon Inspector Classic.

> **Note**
>
> Anda tidak dapat melihat temuan yang dihasilkan oleh penilaian berjalan saat prosesnya masih berlangsung. Namun, Anda dapat melihat subset temuan jika Anda menghentikan penilaian sebelum menyelesaikan durasinya. Dalam lingkungan produksi, kami menyarankan agar Anda membiarkan setiap penilaian berjalan selama seluruh durasinya sehingga dapat menghasilkan satu set temuan yang lengkap.

3. Untuk melihat detail temuan tertentu, pilih widget Perluas di samping temuan tersebut. Detail temuan tersebut mencakup hal-hal berikut:

   - Nama target penilaian yang mencakup instans EC2 tempat temuan ini terdaftar.
   - Nama templat penilaian yang digunakan untuk menghasilkan temuan ini.
   - Waktu mulai penilaian berjalan.
   - Waktu henti penilaian berjalan.
   - Status penilaian berjalan.
   - Nama paket aturan yang mencakup aturan yang memicu temuan ini.
   - Nama temuan.
   - Kepelikan temuan.
   - Detail kepelikan asli dari Sistem Penilaian Kepelikan Umum (Common Vulnerability Scoring System/CVSS). Hal ini termasuk vektor CVSS dan metrik skor CVSS (termasuk CVSS versi 2.0 dan 3.0) untuk temuan yang dipicu oleh aturan dalam paket aturan Kelemahan dan Eksposur Umum. Untuk detail tentang CVSS, lihat https://www.first.org/cvss/.
   - Detail tingkat keparahan asli dari Pusat Keamanan Internet (CIS). Hal ini termasuk metrik berat CIS untuk temuan yang dipicu oleh aturan dalam paket Patokan CIS. Untuk informasi lebih lanjut tentang metrik berat CIS, lihat https://www.cisecurity.org/.
   - Deskripsi temuan.
   - Rekomendasi langkah-langkah yang dapat Anda selesaikan untuk memperbaiki potensi masalah keamanan yang diuraikan oleh temuan.

4. Untuk menetapkan atribut ke temuan, pilih temuan, lalu pilih Tambah/Edit Atribut.

   Anda juga dapat menetapkan atribut untuk temuan saat Anda membuat templat penilaian. Untuk melakukannya, Anda mengonfigurasi templat baru untuk secara otomatis menetapkan atribut untuk semua temuan yang dihasilkan oleh penilaian berjalan. Anda dapat menggunakan

bidang Kunci dan Nilai dari bidang Tanda untuk temuan dari penilaian ini. Untuk informasi selengkapnya, lihat Templat penilaian Amazon Inspector Classic dan penilaian berjalan.

5. Untuk mengekspor temuan ke spreadsheet, pilih panah bawah di sudut kanan atas halaman Temuan. Di kotak dialog, pilih Ekspor semua kolom atau Ekspor kolom yang terlihat.

   Perhatikan bahwa dalam konten yang diekspor, semua nilai datetime adalah stempel waktu jangka waktu.

6. Untuk memfilter temuan Anda saat ini, masukkan string tunggal yang ingin Anda filter, seperti ID instans atau nomor CVE, di bilah filter di atas tabel temuan. Untuk menampilkan atau menyembunyikan kolom informasi tambahan, pilih ikon pengaturan di sudut kanan atas halaman Temuan.
7. Untuk menghapus temuan, navigasikan ke halaman Penilaian berjalan dan pilih proses yang menghasilkan temuan yang ingin Anda hapus. Lalu pilih Hapus. Ketika diminta konfirmasi, pilih Ya.

   > **Important**
   >
   > Anda tidak dapat menghapus temuan individual di Amazon Inspector Classic. Ketika Anda menghapus penilaian berjalan, semua temuan dan semua versi laporan dari proses tersebut juga dihapus.

   Anda juga dapat menghapus penilaian yang dijalankan dengan menggunakan DeleteAssessmentRunAPI.

# Laporan penilaian

Amazon InspectorLaporan penilaianadalah dokumen yang memerinci apa yang diuji dalam penilaian berjalan dan hasil penilaian. Anda dapat menyimpan laporan, membagikannya dengan tim Anda untuk tindakan perbaikan, atau menggunakannya untuk menambah data audit kepatuhan Anda. Anda dapat membuat laporan untuk penilaian berjalan setelah proses berhasil diselesaikan.

> **Note**
>
> Anda dapat membuat laporan hanya untuk penilaian berjalan yang terjadi setelah 25 April 2017, yaitu ketika laporan penilaian di Amazon Inspector menjadi tersedia.

Anda dapat melihat jenis laporan penilaian berikut:

- Laporan temuan – laporan ini berisi informasi berikut:
  - Ringkasan penilaian
  - Instans EC2 yang dievaluasi selama penilaian berjalan
  - Paket aturan yang termasuk dalam penilaian berjalan
  - Informasi detail tentang setiap temuan, termasuk semua instans EC2 yang memiliki temuan
- Laporan lengkap – laporan ini berisi semua informasi yang disertakan dalam laporan temuan, dan juga menyediakan daftar aturan yang diperiksa terhadap instans dalam target penilaian.

Membuat laporan penilaian

1. Pada halaman Penilaian berjalan, cari penilaian berjalan yang ingin Anda buat laporannya. Pastikan statusnya diatur ke Analisis selesai.
2. Pada kolom Laporan untuk penilaian berjalan ini, pilih ikon laporan.

> **Important**
>
> Ikon laporan ada di kolom Laporan hanya untuk penilaian berjalan yang berlangsung atau akan berlangsung setelah 25 April 2017. Saat itulah laporan penilaian di Amazon Inspector menjadi tersedia.

3. Di kotak dialog Laporan penilaian, pilih jenis laporan yang ingin Anda lihat (baik Temuan ataupun laporan Penuh) dan format laporan (HTML atau PDF). Kemudian pilih Buat laporan.

Anda juga dapat membuat laporan penilaian melalui API GetAssessmentReport.

Untuk menghapus laporan penilaian, lakukan prosedur berikut.

Untuk menghapus laporan

- Pada halaman Penilaian berjalan, pilih proses yang ingin Anda hapus laporannya, lalu pilih Hapus. Ketika diminta konfirmasi, pilih Ya.

  > **Important**
  >
  > Di Amazon Inspector Classic, Anda tidak dapat menghapus laporan individu. Ketika Anda menghapus penilaian berjalan, semua versi laporan dari proses tersebut dan semua temuan juga dihapus.

  Anda juga dapat menghapus penilaian berjalan dengan menggunakan API DeleteAssessmentRun.

# Pengecualian di Amazon Inspector

Pengecualian adalah output dari penilaian berjalan Amazon Inspector. Pengecualian menunjukkan pemeriksaan keamanan mana yang tidak dapat diselesaikan dan cara menyelesaikan masalah. Sebagai contoh, masalah dapat disebabkan oleh tidak adanya agen pada instans EC2 target tertentu, penggunaan sistem operasi yang tidak didukung, atau kesalahan tak terduga.

Anda dapat melihat pengecualian di halaman Penilaian berjalan di konsol. Untuk informasi selengkapnya, lihat Melihat pengecualian pasca-penilaian.

Untuk menghindari menimbulkan tidak perluAWSAmazon Inspector memungkinkan Anda untuk melakukan pratinjau pengecualian sebelum menjalankan penilaian. Anda dapat menemukan pratinjau di halaman Templat penilaian di konsol. Untuk informasi selengkapnya, lihat Pratinjau pengecualian.

> **Note**
>
> Anda dapat membuat pengecualian pasca-penilaian hanya untuk proses yang terjadi setelah 25 Juni 2018. Saat itulah pengecualian di Amazon Inspector menjadi tersedia. Namun, pratinjau pengecualian tersedia untuk semua templat penilaian pada tanggal berapa pun.

Topik



## Jenis pengecualian

Amazon Inspector dapat menghasilkan jenis pengecualian berikut.

| Jenis Pengecualian | Deskripsi | Rekomendasi |
| --- | --- | --- |
| Tidak ada | Tidak ada instans | Periksa bahwa |

| Jenis Pengecualian | Deskripsi | Rekomendasi |
| --- | --- | --- |
| instan dalam target | EC2 dengan tanda yang ditentukan dalam target penilaian. | tanda dalam target penilaian Anda cocok dengan tanda instans EC2 target Anda. |
| Agen sudah berjala | Penilaian berjalan sudah berlangsung pada instans EC2 target. | Tunggu sampai penilaian yang saat ini berjalan pada instans EC2 target telah selesai. |

| Jenis Pengecualian | Deskripsi | Rekomendasi |
| --- | --- | --- |
| Agen tidak ditemu | Agen Amazon Inspector tidak ditemukan pada instans EC2 target. | Menginstal atau menginstal ulang agen Amazon Inspector pada instans EC2 target. Untuk informasi selengkapnya, lihat Menginstal agen Amazon Inspector Classic. |

| Jenis Pengecualian | Deskripsi | Rekomendasi |
| --- | --- | --- |
| Agen tidak sehat | Agen Amazon Inspector Classic pada instans EC2 target sedang dalam keadaan tidak sehat. | Periksa status agen Amazon Inspector pada instans ini dan lakukan tindakan yang diperlukan. Untuk informasi lebih lanjut, lihat Agen Inspector. |

| Jenis Pengecualian | Deskripsi | Rekomendasi |
| --- | --- | --- |
| Versi OS yang tidak diduku | Sistem operasi instans EC2 target tidak didukung untuk penilaian Amazon Inspector. | Hapus instans EC2 target dari target penilaian, atau buat target yang tidak termasuk instans ini. Untuk daftar sistem operasi yang didukung, lihatSistem Operasi dan Wilayah yang Didukung Amazon Inspector Classic. |

| Jenis Pengecualian | Deskripsi | Rekomendasi |
| --- | --- | --- |
| Paket aturan yang tidak digunakan lagi | Templat penilaian mencakup paket aturan yang tidak digunakan lagi. | Buat templat penilaian tanpa paket aturan yang tidak digunakan lagi, dan gunakan untuk penilaian berjalan di masa mendatang. |

| Jenis Pengecualian | Deskripsi | Rekomendasi |
| --- | --- | --- |
| Paket aturan yang tidak didukung oleh OS | Sistem operasi instans EC2 target tidak didukung oleh paket aturan yang disertakan dalam templat penilaian. | Buat templat penilaian tanpa paket aturan yang bertentangan atau hapus instans EC2 target dari templat penilaian. Untuk daftar paket aturan yang didukung oleh sistem operasi, lihat Ketersediaan Paket Aturan yang Tersedia di Seluruh Sistem Operasi |

| Jenis Pengecualian | Deskripsi | Rekomendasi |
| --- | --- | --- |
| | | yang Didukung. |
| Kesalahan evaluasi aturan untuk instans tunggal | Kesalahan internal telah menyebabkan kegagalan evaluasi aturan untuk instans ini. | Cobalah untuk menjalankan penilaian Anda lagi. Hubungi support jika pengecualian tetap ada saat Anda menjalankan kembali penilaian. |

| Jenis Pengecualian | Deskripsi | Rekomendasi |
| --- | --- | --- |
| Kesalahan evaluasi aturan | Kesalahan internal telah menyebabkan kegagalan evaluasi aturan untuk penilaian Anda. | Cobalah untuk menjalankan penilaian lagi. Hubungi support jika pengecualian tetap ada saat Anda menjalankan kembali penilaian. |

| Jenis Pengecualian | Deskripsi | Rekomendasi |
| --- | --- | --- |
| Kesal Keterj kauar Jaring – intern | Kesalahan internal telah menyebabkan kegagalan evaluasi Keterjangkauan Jaringan pada pemeriksaan untuk port yang dapat dijangkau dari internet. Anda mungkin mendapatkan temuan untuk jenis Keterjangkauan Jaringan lainnya. | Cobalah untuk menjalankan penilaian lagi. Hubungi support jika pengecualian tetap ada saat Anda menjalankan kembali penilaian. |

| Jenis Pengecualian | Deskripsi | Rekomendasi |
| --- | --- | --- |
| Kesalahan Keterjangkauan Jaringan – internal melalui Application Load Balancer | Kesalahan internal telah menyebabkan kegagalan evaluasi Keterjangkauan Jaringan pada pemeriksaan untuk port yang dapat dijangkau dari internet melalui Application Load Balancer. Anda mungkin mendapatkan temuan untuk jenis Keterjangkauan Jaringan lainnya. | Cobalah untuk menjalankan penilaian lagi. Hubungi support jika pengecualian tetap ada saat Anda menjalankan kembali penilaian. |

| Jenis Pengecualian | Deskripsi | Rekomendasi |
| --- | --- | --- |
| Kesalahan Keterjangkauan Jaringan – internal melalui penyeimbang beban Elastic Load Balancing | Kesalahan internal telah menyebabkan kegagalan evaluasi Keterjangkauan Jaringan pada pemeriksaan untuk port yang dapat dijangkau dari internet melalui penyeimbang beban Elastic Load Balancing. Anda mungkin mendapatkan temuan untuk jenis Keterjangkauan | Cobalah untuk menjalankan penilaian lagi. Hubungi support jika pengecualian tetap ada saat Anda menjalankan kembali penilaian. |

| Jenis Pengecualian | Deskripsi | Rekomendasi |
| --- | --- | --- |
| | Jaringan lainnya. | |
| Kesalahan Keterjangkauan Jaringan – VPN | Kesalahan internal telah menyebabkan kegagalan evaluasi Keterjangkauan Jaringan pada pemeriksaan untuk port yang dapat dijangkau dari VPN. Anda mungkin mendapatkan temuan untuk jenis Keterjangkauan Jaringan lainnya. | Cobalah untuk menjalankan penilaian lagi. Hubungi support jika pengecualian tetap ada saat Anda menjalankan kembali penilaian. |

| Jenis Pengecualian | Deskripsi | Rekomendasi |
| --- | --- | --- |
| Kesalahan Keterjangkauan Jaringan – AWS Direct Connect | Kesalahan internal telah menyebabkan kegagalan evaluasi Keterjangkauan Jaringan pada pemeriksaan untuk port yang dapat dijangkau melalui AWS Direct Connect. Anda mungkin mendapatkan temuan untuk jenis Keterjangkauan Jaringan lainnya. | Cobalah untuk menjalankan penilaian lagi. Hubungi support jika pengecualian tetap ada saat Anda menjalankan kembali penilaian. |

| Jenis Pengecualian | Deskripsi | Rekomendasi |
| --- | --- | --- |
| Kesalahan Keterjangkauan Jaringan – peering VPC | Kesalahan internal telah menyebabkan kegagalan evaluasi Keterjangkauan Jaringan pada pemeriksaan untuk port yang dapat dijangkau dari peering VPC. Anda mungkin mendapatkan temuan untuk jenis Keterjangkauan Jaringan lainnya. | Cobalah untuk menjalankan penilaian lagi. Hubungi support jika pengecualian tetap ada saat Anda menjalankan kembali penilaian. |

# Pratinjau pengecualian

Amazon Inspector memungkinkan Anda untuk melakukan pratinjau potensi pengecualian sebelum menjalankan penilaian.

Untuk melakukan pratinjau pengecualian penilaian

1. Masuk keAWS Management Consoledan buka konsol Amazon Inspector Classic dihttps://console.aws.amazon.com/inspector/.
2. Di panel navigasi, pilih Templat Penilaian.
3. Perluas templat, dan dalam bagian Templat penilaian, pilih Pratinjau pengecualian.
4. Tinjau deskripsi semua pengecualian yang terdeteksi dan rekomendasi untuk mengatasinya.

   Anda juga dapat membuat daftar dan menguraikan pengecualian dengan menggunakan operasi `ListExclusions` dan `DescribeExclusions`.

## Melihat pengecualian pasca-penilaian

Setelah penilaian berjalan, Anda dapat melihat detail tentang setiap pengecualian.

Untuk melihat detail tentang pengecualian

1. Masuk keAWS Management Consoledan buka konsol Amazon Inspector Classic dihttps://console.aws.amazon.com/inspector/.
2. Di panel navigasi, pilih Penilaian berjalan.
3. Di kolom Pengecualian, pilih tautan aktif yang terkait dengan penilaian berjalan.
4. Tinjau deskripsi semua pengecualian yang terdeteksi dan rekomendasi untuk mengatasinya.

   Anda juga dapat membuat daftar dan menguraikan pengecualian dengan menggunakan operasi `ListExclusions` dan `DescribeExclusions`.

# Paket aturan Amazon Inspector Classic untuk sistem operasi yang didukung

Anda dapat menjalankan paket aturan Amazon Inspector Classic pada instans EC2 yang termasuk dalam target penilaian Anda. Tabel berikut menunjukkan ketersediaan paket aturan untuk sistem operasi yang didukung.

**Important**

Anda dapat menjalankan penilaian tanpa agen dengan paket aturan Keterjangkauan Jaringan pada setiap instans EC2 terlepas dari apa pun sistem operasinya.

**Note**

Untuk informasi lebih lanjut tentang sistem operasi yang didukung, lihat Amazon Inspector Classic mendukung sistem operasi dan Wilayah.

| Sistem Operasi yang Didukung | Kelemahan dan Eksposur Umum | Patokan CIS | Keterjangkauan Jaringan | Praktik Terbaik Keamanan | Analisis Perilaku Waktu Aktif |
|---|---|---|---|---|---|
| Amazon Linux 2 | Didukung | Didukung | Didukung | Didukung | Telah usang |
| Amazon Linux 2018, | Didukung | Didukung | Didukung | Didukung | Telah usang |
| Amazon Linux 2017, | Didukung | Didukung | Didukung | Didukung | Telah usang |

| Sister Opera yang Diduk | Kelemahan dan Eksposur Umum | Patokan CIS | Keterjangkauan Jaringan | Praktik Terbaik Keamanan | Analisis Perilaku Waktu Aktif |
|---|---|---|---|---|---|
| Amaz Linux 2017, | Didukung | Didukung | Didukung | Didukung | Telah usang |
| Amaz Linux 2016, | Didukung | Didukung | Didukung | Didukung | Telah usang |
| Amaz Linux 2016, | Didukung | Didukung | Didukung | Didukung | Telah usang |
| Amaz Linux 2015, | Didukung | Didukung | Didukung | Didukung | Telah usang |
| Amaz Linux 2015, | Didukung | Didukung | Didukung | Didukung | Telah usang |
| Amaz Linux 2014, | Didukung | | Didukung | Didukung | |
| Amaz Linux 2014, | Didukung | | Didukung | Didukung | |
| Amaz Linux 2013, | Didukung | | Didukung | Didukung | |

| Sister Opera yang Diduk | Kelemahan dan Eksposur Umum | Patokan CIS | Keterjangkauan Jaringan | Praktik Terbaik Keamanan | Analisis Perilaku Waktu Aktif |
|---|---|---|---|---|---|
| Amaz Linux 2013, | Didukung | | Didukung | Didukung | |
| Amaz Linux 2012, | Didukung | | Didukung | Didukung | |
| Amaz Linux 2012, | Didukung | | Didukung | Didukung | |
| Ubun 20.04 LTS | Didukung | | Didukung | Didukung | |
| Ubun 18.04 LTS | Didukung | Didukung | Didukung | Didukung | Telah usang |
| Ubun 16.04 LTS | Didukung | Didukung | Didukung | Didukung | Telah usang |
| Ubun 14.04 LTS | Didukung | Didukung | Didukung | Didukung | Telah usang |

| Sister Opera yang Diduk | Kelemahan dan Eksposur Umum | Patokan CIS | Keterjangkauan Jaringan | Praktik Terbaik Keamanan | Analisis Perilaku Waktu Aktif |
|---|---|---|---|---|---|
| Debia 10.x, 9.0 - 9.5, 8.0 - 8.7 | Didukung | | Didukung | Didukung | |
| RHEL 8.x | Didukung | | Didukung | Didukung | |
| RHEL 7.6 - 7.x | Didukung | Didukung | Didukung | Didukung | |
| RHEL 6.2 - 6.9, 7.2 - 7.5 | Didukung | Didukung | Didukung | Didukung | Telah usang |
| Cent( 7.6 - 7.X | Didukung | Didukung | Didukung | Didukung | |

| Sistem Operasi yang Diduk | Kelemahan dan Eksposur Umum | Patokan CIS | Keterjangkauan Jaringan | Praktik Terbaik Keamanan | Analisis Perilaku Waktu Aktif |
|---|---|---|---|---|---|
| CentO 6.2 - 6.9, 7.2 - 7.5 | Didukung | Didukung | Didukung | Didukung | Telah usang |
| Windo Serve 2019 Base | Didukung | | Didukung | | |
| Windo Serve 2016 Base | Didukung | Didukung | Didukung | | Telah usang |
| Windo Serve 2012 R2 | Didukung | Didukung | Didukung | | Telah usang |
| Windo Serve 2012 | Didukung | Didukung | Didukung | | Telah usang |
| Windo Serve 2008 R2 | Didukung | Didukung | Didukung | | Telah usang |

# Mencatat panggilan API Amazon Inspector denganAWS CloudTrail

Amazon Inspector Classic terintegrasi denganAWS CloudTrail, layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atauAWSlayanan di Amazon Inspector. CloudTrail menangkap semua panggilan API untuk Amazon Inspector sebagai kejadian, termasuk panggilan dari konsol Amazon Inspector dan panggilan kode ke operasi API Amazon Inspector. Jika membuat jejak, Anda dapat mengaktifkan pengiriman kejadian CloudTrail berkelanjutan ke bucket Amazon S3, termasuk kejadian untuk Amazon Inspector. Jika Anda tidak mengonfigurasi jejak, Anda masih dapat melihat kejadian terbaru dalam konsol CloudTrail di Riwayat peristiwa. Dengan informasi yang dikumpulkan oleh CloudTrail, Anda dapat menentukan permintaan yang dibuat ke Amazon Inspector, alamat IP asal permintaan dibuat, siapa yang membuat permintaan, kapan permintaan dibuat, dan lainnya.

Untuk mempelajari selengkapnya tentang CloudTrail, lihat Panduan Pengguna AWS CloudTrail. Untuk daftar lengkap operasi API Amazon Inspector, lihatTindakandi dalamReferensi API Amazon Inspector Classic.

## Informasi Amazon Inspector di CloudTrail

CloudTrail diaktifkan pada akun AWS Anda saat Anda membuat akun tersebut. Saat aktivitas terjadi di Amazon Inspector, aktivitas tersebut dicatat di kejadian CloudTrail bersama aktivitas lainnyaAWSPeristiwa layanan diRiwayat peristiwa. Anda dapat melihat, mencari, dan mengunduh peristiwa terbaru di akun AWS Anda. Untuk informasi selengkapnya, lihat Melihat Peristiwa dengan Riwayat Peristiwa CloudTrail.

Untuk catatan berkelanjutan tentang peristiwa diAWSakun, termasuk acara untuk Amazon Inspector Classic, membuatjejak. Jejak memungkinkan CloudTrail mengirim file log ke bucket Amazon S3. Secara default, ketika Anda membuat jejak di konsol, jejak akan diterapkan ke semua Wilayah AWS. Jejak mencatat peristiwa dari semua Wilayah di partisi AWS dan mengirimkan file log ke bucket Amazon S3 yang Anda tentukan. Selain itu, Anda dapat mengonfigurasi layanan AWS lainnya untuk menganalisis lebih lanjut dan bertindak berdasarkan data peristiwa yang dikumpulkan di log CloudTrail. Untuk informasi selengkapnya, lihat yang berikut:

- Ikhtisar untuk Membuat Jejak
- Layanan yang Didukung dan Integrasi CloudTrail

- Mengonfigurasi Notifikasi Amazon SNS untuk CloudTrail
- Menerima Berkas Log CloudTrail dari Berbagai Wilayah dan Menerima Berkas Log CloudTrail dari Berbagai Akun

CloudTrail mencatat semua operasi Amazon Inspector Classic, termasuk operasi hanya-baca, sepertiListAssessmentRunsdanDescribeAssessmentTargets, dan operasi manajemen, sepertiAddAttributesToFindingsdanCreateAssessmentTemplate.

> **Note**
>
> CloudTrail hanya mencatat informasi permintaan operasi baca-saja Amazon Inspector. Kedua informasi permintaan dan respons dicatat untuk semua operasi Amazon Inspector lainnya.

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

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

Untuk informasi selengkapnya, lihat Elemen userIdentity CloudTrail.

## Memahami entri berkas log Amazon Inspector

Jejak adalah konfigurasi yang memungkinkan pengiriman peristiwa sebagai berkas log ke bucket Amazon S3 yang telah Anda tentukan. File log CloudTrail berisi satu atau beberapa entri log. Sebuah kejadian mewakili satu permintaan dari sumber apa pun dan mencakup informasi tentang tindakan yang diminta, tanggal dan waktu tindakan, dan parameter permintaan lainnya. File log CloudTrail bukan jejak tumpukan terurut dari panggilan API publik, sehingga berkas tersebut tidak muncul dalam urutan tertentu.

Contoh berikut menampilkan entri log CloudTrail yang menunjukkan Amazon InspectorCreateResourceGroupOperasi:

```
{
    "eventVersion": "1.03",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::444455556666:user/Alice",
        "accountId": "444455556666",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2016-04-14T17:05:54Z"
            },
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::444455556666:user/Alice",
                "accountId": "444455556666",
                "userName": "Alice"
            }
        }
    },
    "eventTime": "2016-04-14T17:12:34Z",
    "eventSource": "inspector.amazonaws.com",
    "eventName": "CreateResourceGroup",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "205.251.233.179",
    "userAgent": "console.amazonaws.com",
    "requestParameters": {
        "resourceGroupTags": [
            {
                "key": "Name",
                "value": "ExampleEC2Instance"
            }
        ]
    },
    "responseElements": {
        "resourceGroupArn": "arn:aws:inspector:us-west-2:444455556666:resourcegroup/0-
oclRMp8B"
    },
    "requestID": "148256d2-0264-11e6-a9b5-b98a7d3b840f",
    "eventID": "e5ea533e-eede-46cc-94f6-0d08e6306ff0",
    "eventType": "AwsApiCall",
```

```
    "apiVersion": "v20160216",
    "recipientAccountId": "444455556666"
}
```

# Memantau Amazon Inspector Classic menggunakan Amazon CloudWatch

Anda dapat memantau Amazon Inspector Classic menggunakan AmazonCloudWatch, yang mengumpulkan dan memproses data mentah menjadi mudah dibaca, mendekati metrik waktu nyata. Secara default, Amazon Inspector Classic mengirimkan data metrik ke CloudWatch dalam periode 5 menit. Anda dapat menggunakanAWS Management Console,AWS CLI, atau API untuk melihat metrik yang dikirim Amazon Inspector Classic. CloudWatch

Untuk informasi lebih lanjut tentang Amazon CloudWatch, lihat Panduan Pengguna Amazon CloudWatch.

## Metrik Amazon Inspector Classic CloudWatch

Namespace Amazon Inspector Classic menyertakan metrik berikut.

**`AssessmentTargetARN`**metrik:

| Metrik | Deskripsi |
| --- | --- |
| `TotalMatchingAgents` | Jumlah agen sesuai dengan target ini |
| `TotalHealthyAgents` | Jumlah agen yang sehat sesuai dengan target ini |
| `TotalAssessmentRuns` | Jumlah penilaian berjalan untuk target ini |
| `TotalAssessmentRun Findings` | Jumlah temuan untuk target ini |

**`AssessmentTemplateARN`**metrik:

| Metrik | Deskripsi |
| --- | --- |
| `TotalMatchingAgents` | Jumlah agen sesuai dengan templat ini |
| `TotalHealthyAgents` | Jumlah agen yang sehat sesuai dengan templat ini |

| Metrik | Deskripsi |
| --- | --- |
| `TotalAssessmentRuns` | Jumlah penilaian berjalan untuk templat ini |
| `TotalAssessmentRunFindings` | Jumlah temuan untuk templat ini |

Metrik agregat

| Metrik | Deskripsi |
| --- | --- |
| `TotalAssessmentRuns` | Jumlah penilaian berjalan dalam akun AWS ini |

# Mengonfigurasi Amazon Inspector Classic menggunakanAWS CloudFormation

Untuk informasi referensi tentang sumber daya Amazon Inspector Classic yang didukung olehAWS CloudFormation, lihat topik berikut:

- `AWS::Inspector::AssessmentTarget`
- `AWS::Inspector::AssessmentTemplate`
- `AWS::Inspector::ResourceGroup`

> **Important**
>
> Untuk daftar ARN paket aturan Amazon Inspector Classic yang didukungAWSDaerah, lihatARN Amazon Inspector untuk paket aturan.

# Integrasi dengan AWS Security Hub

AWS Security Hub memberi Anda gambaran menyeluruh tentang status keamanan Anda dalam AWS dan membantu Anda memeriksa lingkungan Anda terhadap standar industri keamanan dan praktik terbaik. Security Hub mengumpulkan data keamanan dari seluruh akun AWS, layanan, dan produk mitra pihak ketiga yang didukung serta membantu Anda menganalisis tren keamanan 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.

Daftar Isi



## Bagaimana Amazon Inspector mengirimkan temuan ke Security Hub

Di Security Hub, masalah keamanan dilacak sebagai temuan. Beberapa temuan berasal dari masalah yang terdeteksi oleh layanan AWS atau mitra 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 memfilter daftar temuan dan melihat detail untuk temuan. Lihat Melihat temuan di Panduan Pengguna AWS Security Hub. 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 terpengaruh, dan status temuan saat ini. Lihat Format Temuan Keamanan AWS (ASFF) di Panduan Pengguna AWS Security Hub.

Amazon Inspector adalah salah satu layanan AWS yang mengirimkan temuan ke Security Hub.

## Jenis temuan yang dikirimkan Amazon Inspector

Amazon Inspector mengirimkan semua temuan yang dihasilkannya ke Security Hub.

Amazon Inspector mengirimkan temuan ke Security Hub menggunakan Format Temuan Keamanan AWS (ASFF). Dalam ASFF, bidang `Types` menyediakan jenis temuan. Temuan dari Amazon Inspector dapat memiliki nilai berikut untuk `Types`.

- Pemeriksaan Perangkat Lunak dan Konfigurasi/Kelemahan/CVE
- Pemeriksaan Perangkat Lunak dan Konfigurasi/Praktik Terbaik Keamanan AWS/Keterjangkauan Jaringan
- Pemeriksaan Perangkat Lunak dan Konfigurasi/Standar Industri dan Regulasi/Patokan Pengerasan Host CIS

## Latensi untuk mengirim temuan

Ketika Amazon Inspector membuat temuan baru, temuan biasanya dikirim ke Security Hub dalam waktu lima menit.

## Mencoba kembali saat Security Hub tidak tersedia

Jika Security Hub tidak tersedia, Amazon Inspector mencoba kembali mengirimkan temuan sampai mereka diterima.

## Memperbarui temuan yang ada di Security Hub

Setelah mengirimkan temuan ke Security Hub, Amazon Inspector memperbarui temuan untuk mencerminkan pengamatan tambahan dari aktivitas temuan. Hal ini akan menghasilkan lebih sedikit temuan Amazon Inspector di Security Hub daripada di Amazon Inspector.

# Temuan umum dari Amazon Inspector

Amazon Inspector mengirimkan temuan ke Security Hub menggunakan Format Temuan Keamanan AWS (ASFF).

Berikut adalah contoh temuan umum dari Amazon Inspector.


```
{
  "SchemaVersion": "2018-10-08",
  "Id": "inspector/us-east-1/111122223333/629ff13fbbb44c872f7bba3e7f79f60cb6d443d8",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/inspector",
  "GeneratorId": "arn:aws:inspector:us-east-1:316112463485:rulespackage/0-PmNV0Tcd",
  "AwsAccountId": "111122223333",
  "Types": [
    "Software and Configuration Checks/AWS Security Best Practices/Network Reachability
 - Recognized port reachable from internet"
  ],
  "CreatedAt": "2020-08-19T17:36:22.169Z",
  "UpdatedAt": "2020-11-04T16:36:06.064Z",
  "Severity": {
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "6.0"
  },
  "Confidence": 10,
  "Title": "On instance i-0c10c2c7863d1a356, TCP port 22 which is associated with 'SSH'
is reachable from the internet",
  "Description": "On this instance, TCP port 22, which is associated with SSH, is
reachable from the internet. You can install the Inspector agent on this instance
and re-run the assessment to check for any process listening on this port. The
instance i-0c10c2c7863d1a356 is located in VPC vpc-a0c2d7c7 and has an attached ENI
eni-078eac9d6ad9b20d1 which uses network ACL acl-154b8273. The port is reachable from
the internet through Security Group sg-0af64c8a5eb30ca75 and IGW igw-e209d785",
  "Remediation": {
    "Recommendation": {
      "Text": "You can edit the Security Group sg-0af64c8a5eb30ca75 to remove access
from the internet on port 22"
    }
  },
  "ProductFields": {
    "attributes/VPC": "vpc-a0c2d7c7",
    "aws/inspector/id": "Recognized port reachable from internet",
```

```
    "serviceAttributes/schemaVersion": "1",
    "aws/inspector/arn": "arn:aws:inspector:us-east-1:111122223333:target/0-8zh1cWkg/
template/0-rqtRV0u0/run/0-Ck2F6tY9/finding/0-B458MQWe",
    "attributes/ACL": "acl-154b8273",
    "serviceAttributes/assessmentRunArn": "arn:aws:inspector:us-
east-1:111122223333:target/0-8zh1cWkg/template/0-rqtRV0u0/run/0-Ck2F6tY9",
    "attributes/PROTOCOL": "TCP",
    "attributes/RULE_TYPE": "RecognizedPortNoAgent",
    "aws/inspector/RulesPackageName": "Network Reachability",
    "attributes/INSTANCE_ID": "i-0c10c2c7863d1a356",
    "attributes/PORT_GROUP_NAME": "SSH",
    "attributes/IGW": "igw-e209d785",
    "serviceAttributes/rulesPackageArn": "arn:aws:inspector:us-
east-1:111122223333:rulespackage/0-PmNV0Tcd",
    "attributes/SECURITY_GROUP": "sg-0af64c8a5eb30ca75",
    "attributes/ENI": "eni-078eac9d6ad9b20d1",
    "attributes/REACHABILITY_TYPE": "Internet",
    "attributes/PORT": "22",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/inspector/
inspector/us-east-1/111122223333/629ff13fbbb44c872f7bba3e7f79f60cb6d443d8",
    "aws/securityhub/ProductName": "Inspector",
    "aws/securityhub/CompanyName": "Amazon"
  },
  "Resources": [
    {
      "Type": "AwsEc2Instance",
      "Id": "arn:aws:ec2:us-east-1:193043430472:instance/i-0c10c2c7863d1a356",
      "Partition": "aws",
      "Region": "us-east-1",
      "Tags": {
        "Name": "kubectl"
      },
      "Details": {
        "AwsEc2Instance": {
          "ImageId": "ami-02354e95b39ca8dec",
          "IpV4Addresses": [
            "172.31.43.6"
          ],
          "VpcId": "vpc-a0c2d7c7",
          "SubnetId": "subnet-4975b475"
        }
      }
    }
  ],
```

```
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE"
}
```

## Mengaktifkan dan mengonfigurasi integrasi

Untuk menggunakan integrasi dengan Security Hub, Anda harus mengaktifkan Security Hub. Untuk informasi tentang cara mengaktifkan Security Hub, lihat Menyiapkan Security Hub di Panduan Pengguna AWS Security Hub.

Bila Anda mengaktifkan Amazon Inspector dan Security Hub, integrasi diaktifkan secara otomatis. Amazon Inspector mulai mengirim temuan ke Security Hub.

## Bagaimana 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 (Security Hub API, AWS CLI) di Panduan Pengguna AWS Security Hub.

# ARN Amazon Inspector

Setiap jenis sumber daya dan paket aturan di Amazon Inspector Classic memiliki Amazon Resource Name (ARN) unik yang terkait dengannya.

Daftar Isi



## ARN untuk sumber daya Amazon Inspector

Di Amazon Inspector Classic, sumber daya utama adalah grup sumber daya, target penilaian, templat penilaian, penilaian berjalan, dan temuan. Sumber daya ini memiliki Amazon Resource Name (ARN) yang unik dan terkait dengan sumber daya, seperti yang ditunjukkan di tabel berikut.

| Tipe Sumber Daya | Format ARN |
| --- | --- |
| Grup sumber daya | `arn:aws:inspector:region:account-id:resourcegroup/ID` |
| Target penilaian | `arn:aws:inspector:region:account-id:target/ID` |
| Templat penilaian | `arn:aws:inspector:region:account-id:target/ID:template:ID` |
| Penilaian berjalan | `arn:aws:inspector:region:account-id:target/ID/template/ID/run/ID` |
| Temuan | `arn:aws:inspector:region:account-id:target/ID/template/ID/run/ID/finding/ID` |

# ARN Amazon Inspector untuk paket aturan

Tabel berikut menunjukkan ARN untuk paket aturan Amazon Inspector di semua Wilayah yang didukung.

Topik

- US East (Ohio)
- US East (N. Virginia)
- US West (N. California)
- US West (Oregon)
- Asia Pacific (Mumbai)
- Asia Pacific (Seoul)
- Asia Pacific (Sydney)
- Asia Pacific (Tokyo)
- Europe (Frankfurt)
- Europe (Ireland)
- Europe (London)
- Europe (Stockholm)

- AWS GovCloud (US-East)
- AWS GovCloud (US-West)

## US East (Ohio)

| Nama Paket Aturan | ARN |
| --- | --- |
| Kelemahan dan Eksposur Umum | `arn:aws:inspector:us-east-2:646659390643:rulespackage/0-JnA8Zp85` |
| Patokan Konfigurasi Keamanan Sistem Operasi CIS | `arn:aws:inspector:us-east-2:646659390643:rulespackage/0-m8r61nnh` |
| Keterjangkauan Jaringan | `arn:aws:inspector:us-east-2:646659390643:rulespackage/0-cE4kTR30` |
| Praktik Terbaik Keamanan | `arn:aws:inspector:us-east-2:646659390643:rulespackage/0-AxKmMHPX` |

## US East (N. Virginia)

| Nama Paket Aturan | ARN |
| --- | --- |
| Kelemahan dan Eksposur Umum | `arn:aws:inspector:us-east-1:316112463485:rulespackage/0-gEjTy7T7` |

| Nama Paket Aturan | ARN |
| --- | --- |
| Patokan Konfigurasi Keamanan Sistem Operasi CIS | arn:aws:inspector:us-east-1:316112463485:rulespackage/0-rExsr2X8 |
| Keterjangkauan Jaringan | arn:aws:inspector:us-east-1:316112463485:rulespackage/0-PmNV0Tcd |
| Praktik Terbaik Keamanan | arn:aws:inspector:us-east-1:316112463485:rulespackage/0-R01qwB5Q |

## US West (N. California)

| Nama Paket Aturan | ARN |
| --- | --- |
| Kelemahan dan Eksposur Umum | arn:aws:inspector:us-west-1:166987590008:rulespackage/0-TKgzoVOa |
| Patokan Konfigurasi Keamanan Sistem Operasi CIS | arn:aws:inspector:us-west-1:166987590008:rulespackage/0-xUY8iRqX |
| Keterjangkauan Jaringan | arn:aws:inspector:us-west-1:166987590008:rulespackage/0-TxmXimXF |

| Nama Paket Aturan | ARN |
| --- | --- |
| Praktik Terbaik Keamanan | `arn:aws:inspector:us-west-1:166987590008:rulespackage/0-byoQRFYm` |

## US West (Oregon)

| Nama Paket Aturan | ARN |
| --- | --- |
| Kelemahan dan Eksposur Umum | `arn:aws:inspector:us-west-2:758058086616:rulespackage/0-9hgA516p` |
| Patokan Konfigurasi Keamanan Sistem Operasi CIS | `arn:aws:inspector:us-west-2:758058086616:rulespackage/0-H5hpSawc` |
| Keterjangkauan Jaringan | `arn:aws:inspector:us-west-2:758058086616:rulespackage/0-rD1z6dpl` |
| Praktik Terbaik Keamanan | `arn:aws:inspector:us-west-2:758058086616:rulespackage/0-JJOtZiqQ` |

## Asia Pacific (Mumbai)

| Nama Paket Aturan | ARN |
| --- | --- |
| Kelemahan dan Eksposur Umum | arn:aws:inspector:ap-south-1:162588757376:rulespackage/0-LqnJE9dO |
| Patokan Konfigurasi Keamanan Sistem Operasi CIS | arn:aws:inspector:ap-south-1:162588757376:rulespackage/0-PSUlX14m |
| Keterjangkauan Jaringan | arn:aws:inspector:ap-south-1:162588757376:rulespackage/0-YxKfjFu1 |
| Praktik Terbaik Keamanan | arn:aws:inspector:ap-south-1:162588757376:rulespackage/0-fs0IZZBj |

## Asia Pacific (Seoul)

| Nama Paket Aturan | ARN |
| --- | --- |
| Kelemahan dan Eksposur Umum | arn:aws:inspector:ap-northeast-2:526946625049:rulespackage/0-PoGHMznc |
| Patokan Konfigurasi Keamanan Sistem Operasi CIS | arn:aws:inspector:ap-northeast-2:526 |

| Nama Paket Aturan | ARN |
| --- | --- |
| | 946625049:rulespac kage/0-T9srhg1z |
| Keterjangkauan Jaringan | arn:aws:inspector: ap-northeast-2:526 946625049:rulespac kage/0-s3OmLzhL |
| Praktik Terbaik Keamanan | arn:aws:inspector: ap-northeast-2:526 946625049:rulespac kage/0-2WRpmi4n |

## Asia Pacific (Sydney)

| Nama Paket Aturan | ARN |
| --- | --- |
| Kelemahan dan Eksposur Umum | arn:aws:inspector: ap-southeast-2:454 640832652:rulespac kage/0-D5TGAxiR |
| Patokan Konfigurasi Keamanan Sistem Operasi CIS | arn:aws:inspector: ap-southeast-2:454 640832652:rulespac kage/0-Vkd2Vxjq |
| Keterjangkauan Jaringan | arn:aws:inspector: ap-southeast-2:454 640832652:rulespac kage/0-FLcuV4Gz |
| Praktik Terbaik Keamanan | arn:aws:inspector: ap-southeast-2:454 |

| Nama Paket Aturan | ARN |
| --- | --- |
| | 640832652:rulespac kage/0-asL6HRgN |

## Asia Pacific (Tokyo)

| Nama Paket Aturan | ARN |
| --- | --- |
| Kelemahan dan Eksposur Umum | arn:aws:inspector: ap-northeast-1:406 045910587:rulespac kage/0-gHP9oWNT |
| Patokan Konfigurasi Keamanan Sistem Operasi CIS | arn:aws:inspector: ap-northeast-1:406 045910587:rulespac kage/0-7WNjqgGu |
| Keterjangkauan Jaringan | arn:aws:inspector: ap-northeast-1:406 045910587:rulespac kage/0-YI95DVd7 |
| Praktik Terbaik Keamanan | arn:aws:inspector: ap-northeast-1:406 045910587:rulespac kage/0-bBUQnxMq |

## Europe (Frankfurt)

| Nama Paket Aturan | ARN |
| --- | --- |
| Kelemahan dan Eksposur Umum | arn:aws:inspector: eu-central-1:53750 |

| Nama Paket Aturan | ARN |
| --- | --- |
| | 3971621:rulespackage/0-wNqHa8M9 |
| Patokan Konfigurasi Keamanan Sistem Operasi CIS | arn:aws:inspector:eu-central-1:537503971621:rulespackage/0-nZrAVuv8 |
| Keterjangkauan Jaringan | arn:aws:inspector:eu-central-1:537503971621:rulespackage/0-6yunpJ91 |
| Praktik Terbaik Keamanan | arn:aws:inspector:eu-central-1:537503971621:rulespackage/0-ZujVHEPB |

## Europe (Ireland)

| Nama Paket Aturan | ARN |
| --- | --- |
| Kelemahan dan Eksposur Umum | arn:aws:inspector:eu-west-1:357557129151:rulespackage/0-ubA5XvBh |
| Patokan Konfigurasi Keamanan Sistem Operasi CIS | arn:aws:inspector:eu-west-1:357557129151:rulespackage/0-sJBhCr0F |
| Keterjangkauan Jaringan | arn:aws:inspector:eu-west-1:35755712 |

| Nama Paket Aturan | ARN |
| --- | --- |
| | 9151:rulespackage/0-SPzU33xe |
| Praktik Terbaik Keamanan | arn:aws:inspector:eu-west-1:357557129151:rulespackage/0-SnojL3Z6 |

## Europe (London)

| Nama Paket Aturan | ARN |
| --- | --- |
| Kelemahan dan Eksposur Umum | arn:aws:inspector:eu-west-2:146838936955:rulespackage/0-kZGCqcE1 |
| Patokan Konfigurasi Keamanan Sistem Operasi CIS | arn:aws:inspector:eu-west-2:146838936955:rulespackage/0-IeCjwf1W |
| Keterjangkauan Jaringan | arn:aws:inspector:eu-west-2:146838936955:rulespackage/0-AizSYyNq |
| Praktik Terbaik Keamanan | arn:aws:inspector:eu-west-2:146838936955:rulespackage/0-XApUiSaP |

## Europe (Stockholm)

| Nama Paket Aturan | ARN |
| --- | --- |
| Kelemahan dan Eksposur Umum | `arn:aws:inspector:eu-north-1:453420244670:rulespackage/0-IgdgIewd` |
| Patokan Konfigurasi Keamanan Sistem Operasi CIS | `arn:aws:inspector:eu-north-1:453420244670:rulespackage/0-Yn8jlX7f` |
| Keterjangkauan Jaringan | `arn:aws:inspector:eu-north-1:453420244670:rulespackage/0-52Sn74uu` |
| Praktik Terbaik Keamanan | `arn:aws:inspector:eu-north-1:453420244670:rulespackage/0-HfBQSbSf` |

## AWS GovCloud (US-East)

| Nama Paket Aturan | ARN |
| --- | --- |
| Kelemahan dan Eksposur Umum | `arn:aws-us-gov:inspector:us-gov-east-1:206278770380:rulespackage/0-3IFKFu0b` |
| Patokan Konfigurasi Keamanan Sistem Operasi CIS | `arn:aws-us-gov:inspector:us-gov-east` |

| Nama Paket Aturan | ARN |
| --- | --- |
| | -1:206278770380:rulespackage/0-pTLCdIww |
| Praktik Terbaik Keamanan | arn:aws-us-gov:inspector:us-gov-east-1:206278770380:rulespackage/0-vlgEGcVD |

## AWS GovCloud (US-West)

| Nama Paket Aturan | ARN |
| --- | --- |
| Kelemahan dan Eksposur Umum | arn:aws-us-gov:inspector:us-gov-west-1:850862329162:rulespackage/0-4oQgcI4G |
| Patokan Konfigurasi Keamanan Sistem Operasi CIS | arn:aws-us-gov:inspector:us-gov-west-1:850862329162:rulespackage/0-Ac4CFOuc |
| Praktik Terbaik Keamanan | arn:aws-us-gov:inspector:us-gov-west-1:850862329162:rulespackage/0-rOTGqe5G |

# Riwayat dokumen

Tabel berikut menjelaskan riwayat rilis dokumentasi Amazon Inspector Classic setelah Mei 2018.

| Perubahan | Deskripsi | Tanggal |
| --- | --- | --- |
| Praktik terbaik keamanan yang diperbarui untuk kata sandi | Persyaratan praktik terbaik keamanan Amazon Inspector Classic untuk panjang kata sandi instans EC2 dan kompleksitas kata sandi telah diperbarui. Lihat Mengonfigurasi panjang minimum kata sandi dan Mengonfigurasi kompleksitas kata sandi | Selasa, 08 Maret 2021 |
| Menambahkan dukungan untuk versi sistem operasi yang lebih baru | Amazon Inspector Classic sekarang mendukung versi sistem operasi berikut: Ubunti 20.4 LTS, Debian 10.x, RHEL 8.x, dan Windows Server 2019 Base. | 15 Oktober 2020 |
| Informasi keamanan dikonsolidasikan ke dalam babak keamanan baru | Informasi keamanan untuk Amazon Inspector Classic, termasuk informasi tentang pengelolaan identitas dan manajemen akses, dikonsolidasikan ke dalam bagian keamanan. Lihat Keamanan di Amazon Inspector Classic. | 7 April 2020 |
| Dokumentasi yang diperbarui untuk menghapus dukungan untuk paket aturan Analisis Perilaku Runtime. | Beberapa topik diperbarui untuk menghapus informasi tentang paket aturan Analisis Perilaku Waktu Aktif, yang tidak lagi didukung. | Selasa, 05 September 2019 |

| | | |
|---|---|---|
| Ditambahkan OS Support | Menambahkan dukungan Amazon Inspector Classic untuk CentOS 7.6. Untuk informasi selengkapnya, lihat Amazon Inspector Classic Supported Operating Systems and Regions and Rules Packages Availability Across Supported Operating Systems. | Selasa, 03 Desember 2018 |
| Konten baru | Menambahkan paket aturan Amazon Inspector Classic Network Reachability, yang memungkinkan pengguna menjalankan penilaian tanpa agen yang menganalisis konfigurasi jaringan untuk kerentanan keamanan. Untuk informasi lebih lanjut, lihat Keterjangkauan Jaringan . | 9 November 2018 |
| Ditambahkan OS Support | Menambahkan dukungan Amazon Inspector Classic untuk RHEL 7.6. Untuk informasi selengkapnya, lihat Amazon Inspector Classic Supported Operating Systems and Regions and Rules Packages Availability Across Supported Operating Systems. | 30 Oktober 2018 |

| | | |
|---|---|---|
| Menambahkan dukungan OS | Dukungan ditambahkan untuk berbagai sistem operasi ke paket aturan Patokan CIS. Untuk informasi lebih lanjut, lihat Patokan Pusat Keamanan Internet (CIS) dan Ketersediaan Paket Aturan di Seluruh Sistem Operasi yang Didukung. | 13 Agustus 2018 |
| Ditambahkan dukungan Wilayah | Dukungan Wilayah ditambahkan untuk `AWS GovCloud (US)`. | 13 Juni 2018 |

Tabel berikut menjelaskan riwayat rilis dokumentasi Amazon Inspector Classic sebelum Juni 2018.

| Perubahan | Deskripsi | Tanggal |
|---|---|---|
| Konten baru | Ditambahkan kemampuan untuk menargetkan semua instans Amazon EC2 di suatu akun. Untuk informasi selengkapnya, lihat Target penilaian Amazon Inspector. | 24 Mei 2018 |
| Dukungan OS ditambahkan | Menambahkan dukungan Amazon Inspector Classic untuk Amazon Linux 2018.03 dan Ubuntu 18.04. | 15 Mei 2018 |
| Konten baru | Menambahkan kemampuan untuk mengatur penilaian Amazon Inspector Classic berulang. | 30 April 2018 |
| Konten baru | Menambahkan kemampuan untuk menginstal agen | 30 April 2018 |

| Perubahan | Deskripsi | Tanggal |
| --- | --- | --- |
| | Amazon Inspector Classic melalui konsol. | |
| Dukungan OS ditambahkan | Menambahkan dukungan Amazon Inspector Classic untuk Amazon Linux 2. | 13 Maret 2018 |
| Dukungan OS ditambahkan | Menambahkan dukungan penilaian Amazon Inspector Classic untuk Windows Server 2016 Base. | 20 Februari 2018 |
| Dukungan Wilayah ditambahkan | Menambahkan dukungan Amazon Inspector Classic untuk Wilayah. `US East (Ohio)` | Selasa, 07 Februari 2018 |
| Konten baru | Penilaian Amazon Inspector Classic sekarang dapat berjalan ketika modul kernel tidak tersedia. | 11 Januari 2018 |
| Dukungan Wilayah ditambahkan | Menambahkan dukungan Amazon Inspector Classic untuk Wilayah. `EU (Frankfurt)` | 19 Desember 2017 |
| Konten baru | Menambahkan kemampuan untuk memeriksa kesehatan agen Amazon Inspector Classic dengan Amazon Inspector Classic API dan konsol. | 15 Desember 2017 |

| Perubahan | Deskripsi | Tanggal |
| --- | --- | --- |
| Konten baru | Ditambahkan fitur berikut:<br>• Penggunaan peran tertaut layanan<br>• Agen Amazon Inspector Classic AMI tersedia di Marketplace AWS<br>• Templat Amazon Inspector Classic AWS CloudFormation | Selasa, 05 Desember 2017 |
| Dukungan OS ditambahkan | Menambahkan dukungan penilaian Amazon Inspector Classic untuk CentOS 7.4. | 9 November 2017 |
| Dukungan OS ditambahkan | Menambahkan dukungan penilaian Amazon Inspector Classic untuk Amazon Linux 2017.09. | 11 Oktober 2017 |
| Dukungan OS ditambahkan | Menambahkan dukungan penilaian Amazon Inspector Classic untuk RHEL 7.4. | 20 Februari 2018 |
| Kelayakan HIPAA ditambahkan | Amazon Inspector Classic sekarang memenuhi syarat HIPAA. | 31 Juli 2017 |
| Konten baru | Menambahkan kemampuan untuk secara otomatis memicu penilaian keamanan Amazon Inspector Classic dengan Amazon CloudWatch Events. | 27 Juli 2017 |

| Perubahan | Deskripsi | Tanggal |
| --- | --- | --- |
| Dukungan Wilayah ditambahkan | Menambahkan dukungan Amazon Inspector Classic untuk Wilayah. `US West (N. California)` | Selasa, 06 Juni 2018 |
| Dukungan OS ditambahkan | Menambahkan dukungan penilaian Amazon Inspector Classic untuk RHEL 6.2-6.9, RHEL 7.2-7.3, CentOS 6.9, dan CentOS 7.2-7.3. | 23 Mei 2017 |
| Dukungan OS ditambahkan | Menambahkan dukungan penilaian Amazon Inspector Classic untuk Amazon Linux 2017.03. | 25 April 2017 |
| Konten baru dan dukungan OS ditambahkan | Ditambahkan:<br>• Dukungan Amazon Inspector Classic untuk Ubuntu 16.04.<br>• Ketersediaan cetak biru Lambda untuk mengotomatiskan operasi Amazon Inspector Classic. | Selasa, 05 Januari 2017 |
| Dukungan OS baru | Menambahkan dukungan Amazon Inspector Classic untuk Microsoft Windows. | 26 Agustus 2016 |
| Dukungan Wilayah ditambahkan | Menambahkan dukungan Amazon Inspector Classic untuk Wilayah. `Asia Pacific (Seoul)` | 26 Agustus 2016 |

| Perubahan | Deskripsi | Tanggal |
| --- | --- | --- |
| Dukungan Wilayah ditambahkan | Menambahkan dukungan Amazon Inspector Classic untuk Wilayah. `Asia Pacific (Mumbai)` | 25 April 2016 |
| Dukungan Wilayah ditambahkan | Menambahkan dukungan Amazon Inspector Classic untuk Wilayah. `Asia Pacific (Sydney)` | 25 April 2016 |
| Peluncuran layanan | Amazon Inspector Classic dilayani diluncurkan. | 7 Okt 2015 |

# AWSGlosarium

Untuk AWS terminologi terbaru, lihat AWSglosarium di Referensi. Glosarium AWS