



Panduan Pengguna

# Amazon Inspector Klasik



Versi Latest

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

# Amazon Inspector Klasik: Panduan Pengguna

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Merek dagang dan tampilan dagang Amazon tidak boleh digunakan sehubungan dengan produk atau layanan apa pun yang bukan milik Amazon, dengan cara apa pun yang dapat menyebabkan kebingungan di antara pelanggan, atau dengan cara apa pun yang merendahkan atau mendiskreditkan Amazon. Semua merek dagang lain yang tidak dimiliki oleh Amazon merupakan hak milik masing-masing pemiliknya, yang mungkin atau mungkin tidak terafiliasi, terkait dengan, atau disponsori oleh Amazon.

---

# Table of Contents

.....	viii
Apa itu Amazon Inspector Classic? .....	1
Manfaat Amazon Inspector Classic .....	2
Fitur Amazon Inspector Classic .....	3
Mengakses Amazon Inspector Classic .....	3
Terminologi dan konsep .....	4
Batas layanan .....	6
Harga .....	7
Harga untuk paket aturan jangkauan jaringan .....	7
Harga untuk paket aturan penilaian tuan rumah .....	8
Sistem operasi dan Wilayah yang didukung .....	9
Sistem operasi berbasis Linux yang didukung untuk agen Amazon Inspector Classic .....	10
Sistem operasi berbasis Windows yang didukung untuk agen Amazon Inspector Classic .....	10
Wilayah AWS yang Didukung .....	11
Amazon Inspector Classic akhir dukungan .....	12
Langkah 1: (Opsional) Laporan dan temuan penilaian ekspor .....	13
Langkah 2: Hapus semua penilaian terjadwal yang berjalan di Amazon Inspector Classic .....	14
Langkah 3: Aktifkan Amazon Inspector baru .....	14
Mulai menggunakan .....	15
Pengaturan dalam satu klik .....	15
Pengaturan lanjutan .....	16
Tutorial .....	18
Tutorial Amazon Inspector Klasik - Red Hat Enterprise Linux .....	18
Langkah 1: Siapkan instans Amazon EC2 untuk digunakan dengan Amazon Inspector Classic .....	19
Langkah 2: Memodifikasi instans Amazon EC2 Anda .....	19
Langkah 3: Membuat target penilaian dan menginstal agen pada instans EC2 .....	19
Langkah 4: Membuat dan menjalankan templat penilaian Anda .....	21
Langkah 5: Mencari dan menganalisis temuan Anda .....	21
Langkah 6: Menerapkan perbaikan yang direkomendasikan ke target penilaian Anda .....	23
Tutorial Amazon Inspector Klasik - Server Ubuntu .....	23
Langkah 1: Siapkan instans Amazon EC2 untuk digunakan dengan Amazon Inspector Classic .....	24
Langkah 2: Membuat target penilaian dan menginstal agen pada instans EC2 .....	24

Langkah 3: Membuat dan menjalankan templat penilaian Anda .....	25
Langkah 4: Mencari dan menganalisis temuan yang dihasilkan .....	26
Langkah 5: Menerapkan perbaikan yang direkomendasikan ke target penilaian Anda .....	27
Keamanan .....	28
Perlindungan data .....	29
Enkripsi saat diam .....	30
Enkripsi saat bergerak .....	30
Identity and Access Management .....	31
Audiens .....	31
Mengautentikasi dengan identitas .....	32
Mengelola akses menggunakan kebijakan .....	33
Bagaimana Amazon Inspector Classic bekerja dengan IAM .....	35
Contoh 2: Memungkinkan pengguna untuk melakukan setiap penjelasan dan daftar operasi hanya pada temuan Amazon Inspector .....	38
Sumber daya kebijakan .....	39
Kunci kondisi kebijakan .....	39
ACLs .....	40
ABAC .....	40
Kredensial sementara .....	41
Izin principal .....	41
Peran layanan .....	41
Peran terkait layanan .....	41
Contoh kebijakan berbasis identitas .....	42
Menggunakan Peran Terkait Layanan .....	45
Pemecahan masalah .....	48
Pencatatan log dan pemantauan .....	50
Respons insiden .....	50
Validasi kepatuhan .....	51
Ketahanan .....	51
Keamanan infrastruktur .....	52
Konfigurasi dan analisis kerentanan .....	53
Praktik terbaik keamanan .....	53
Agen Amazon Inspector Classic .....	54
Hak istimewa agen Amazon Inspector Classic .....	55
Keamanan agen Jaringan dan Amazon Inspector Classic .....	55
Pembaruan agen Amazon Inspector Classic .....	56

Siklus hidup data telemetri .....	56
Kontrol akses dari Amazon Inspector Classic ke dalam akun AWS .....	57
Batas agen Amazon Inspector Classic .....	57
Menginstal agen Amazon Inspector Classic .....	57
Menginstal agen pada beberapa instans EC2 menggunakan Systems Manager Run Command .....	58
Menginstal agen pada instans EC2 berbasis Linux .....	59
Menginstal agen pada instans EC2 berbasis Windows .....	61
Bekerja dengan agen Amazon Inspector Classic pada sistem operasi berbasis Linux .....	62
Memverifikasi bahwa agen Amazon Inspector Classic sedang berjalan .....	63
Menghentikan agen Amazon Inspector Classic .....	63
Memulai agen Amazon Inspector Classic .....	63
Memodifikasi pengaturan agen Amazon Inspector Classic .....	63
Mengkonfigurasi dukungan proxy untuk agen Amazon Inspector Classic .....	64
Menghapus instalasi agen Amazon Inspector Classic .....	65
Bekerja dengan agen Amazon Inspector Classic pada sistem operasi berbasis Windows .....	66
Memulai atau menghentikan agen Amazon Inspector Classic atau memverifikasi bahwa agen tersebut sedang berjalan .....	66
Memodifikasi pengaturan agen Amazon Inspector Classic .....	67
Mengkonfigurasi dukungan proxy untuk agen Amazon Inspector Classic .....	67
Menghapus instalasi agen Amazon Inspector Classic .....	69
(Opsional) Verifikasi tanda tangan skrip instalasi agen Amazon Inspector Classic pada sistem operasi berbasis Linux .....	69
Menginstal alat GPG .....	70
Mengautentikasi dan mengimpor kunci publik .....	70
Memverifikasi tanda tangan paket .....	72
(Opsional) Verifikasi tanda tangan skrip instalasi agen Amazon Inspector Classic pada sistem operasi berbasis Windows .....	74
Target penilaian Amazon Inspector Classic .....	75
Menandai sumber daya untuk membuat target penilaian .....	75
Batas target penilaian Amazon Inspector Classic .....	76
Membuat target penilaian .....	76
Menghapus target penilaian .....	78
Amazon Inspector Classic mengatur paket dan aturan .....	79
Tingkat keparahan untuk aturan di Amazon Inspector Classic .....	79
Aturan paket di Amazon Inspector Classic .....	80

Keterjangkauan Jaringan .....	80
Konfigurasi yang dianalisis .....	81
Rute keterjangkauan .....	82
Jenis temuan .....	82
Kelemahan dan eksposur umum .....	84
Patokan Pusat Keamanan Internet (CIS) .....	86
Praktik terbaik keamanan untuk Amazon Inspector Classic .....	89
Menonaktifkan login root melalui SSH .....	90
Mendukung SSH versi 2 saja .....	90
Menonaktifkan autentikasi kata sandi Melalui SSH .....	91
Mengonfigurasi usia maksimum kata sandi .....	92
Mengonfigurasi panjang minimum kata sandi .....	92
Mengonfigurasi kompleksitas kata sandi .....	93
Mengaktifkan ASLR .....	94
Mengaktifkan DEP .....	94
Mengonfigurasi izin untuk direktori sistem .....	95
Templat penilaian Amazon Inspector Classic dan penilaian berjalan .....	96
Templat penilaian Amazon Inspector Classic .....	96
Batas templat penilaian Amazon Inspector Classic .....	97
Membuat templat penilaian .....	97
Menghapus templat penilaian .....	99
Penilaian berjalan .....	100
Menghapus penilaian berjalan .....	100
Penilaian Amazon Inspector Classic menjalankan batas .....	101
Mengatur penilaian berjalan otomatis melalui fungsi Lambda .....	101
Menyiapkan topik SNS untuk notifikasi Amazon Inspector Classic .....	103
Temuan Amazon Inspector Classic .....	106
Bekerja dengan temuan .....	106
Laporan penilaian .....	109
Pengecualian di Amazon Inspector Classic .....	111
Jenis pengecualian .....	111
Pratinjau pengecualian .....	125
Melihat pengecualian pasca-penilaian .....	126
Paket aturan Amazon Inspector Classic untuk sistem operasi yang didukung .....	127
Mencatat panggilan API Amazon Inspector Classic dengan AWS CloudTrail .....	132
Informasi Amazon Inspector Classic di CloudTrail .....	132

Memahami entri file log Amazon Inspector Classic .....	133
Memantau Amazon Inspector Classic menggunakan Amazon CloudWatch .....	136
Metrik Amazon Inspector Classic CloudWatch .....	136
Mengkonfigurasi Amazon Inspector Classic menggunakan AWS CloudFormation .....	138
Integrasi CSPM Security Hub .....	139
Bagaimana Amazon Inspector mengirimkan temuan ke Security Hub CSPM .....	139
Jenis temuan yang dikirimkan Amazon Inspector .....	140
Latensi untuk mengirim temuan .....	140
Mencoba lagi saat Security Hub CSPM tidak tersedia .....	140
Memperbarui temuan yang ada di Security Hub CSPM .....	140
Temuan umum dari Amazon Inspector .....	141
Mengaktifkan dan mengonfigurasi integrasi .....	143
Bagaimana cara menghentikan pengiriman temuan .....	143
Amazon Inspector Klasik ARNs .....	144
ARNs untuk sumber daya Amazon Inspector Classic .....	144
Amazon Inspector Classic ARNS untuk paket aturan .....	145
AS Timur (Ohio) .....	146
AS Timur (Virginia Utara) .....	146
AS Barat (California Utara) .....	147
AS Barat (Oregon) .....	148
Asia Pasifik (Mumbai) .....	149
Asia Pasifik (Seoul) .....	149
Asia Pasifik (Sydney) .....	150
Asia Pasifik (Tokyo) .....	151
Eropa (Frankfurt) .....	151
Eropa (Irlandia) .....	152
Eropa (London) .....	153
Eropa (Stockholm) .....	154
AWS GovCloud (AS-Timur) .....	154
AWS GovCloud (AS-Barat) .....	155
Riwayat dokumen .....	156
AWS Glosarium .....	163

Pemberitahuan akhir dukungan: Pada 20 Mei 2026, AWS akan mengakhiri dukungan untuk Amazon Inspector Classic. Setelah 20 Mei 2026, Anda tidak akan lagi dapat mengakses konsol Amazon Inspector Classic atau sumber daya Amazon Inspector Classic. Amazon Inspector Classic tidak lagi tersedia untuk akun dan akun baru yang belum menyelesaikan penilaian dalam 6 bulan terakhir. Untuk semua akun lain, akses akan tetap berlaku hingga 20 Mei 2026, setelah itu Anda tidak lagi dapat mengakses konsol Amazon Inspector Classic atau sumber daya Amazon Inspector Classic. Untuk informasi selengkapnya, lihat [bagian akhir dukungan Amazon Inspector Classic](#).

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 instance. EC2 Amazon Inspector yang baru menawarkan dukungan multi-akun melalui integrasi dengan AWS Organizations, dan kerentanan perangkat lunak berkelanjutan dan pemindaian jangkauan jaringan berdasarkan kerentanan dan eksposur umum (CWEs). 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 [Amazon Inspector Classic akhir dukungan](#).

Amazon Inspector Classic menguji aksesibilitas jaringan EC2 instans Amazon 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 yang telah ditentukan sebelumnya yang disebut agen yang dapat Anda instal secara opsional di sistem operasi EC2 instance yang ingin Anda nilai. Agen memantau perilaku EC2 instance, 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 Classic](#)

## 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 Klasik

Masuk ke Konsol Manajemen AWS 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 SDKs

AWS menyediakan kit pengembangan perangkat lunak (SDKs) 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. SDKs Menyediakan cara mudah untuk membuat

akses terprogram ke layanan Amazon Inspector Classic. Untuk informasi tentang AWS SDKs, 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 Classic

Saat Anda memulai dengan Amazon Inspector Classic, Anda bisa mendapatkan keuntungan dari mempelajari konsep-konsep utamanya.

## Agen Amazon Inspector Classic

Agen perangkat lunak yang dapat Anda instal pada EC2 instance 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 Classic, kumpulan sumber daya AWS yang bekerja sama sebagai satu unit untuk membantu Anda mencapai tujuan bisnis Anda. Amazon Inspector Classic mengevaluasi status keamanan sumber daya yang merupakan target penilaian.

### Important

Saat ini, target penilaian Amazon Inspector Classic Anda hanya dapat terdiri dari instance EC2 Untuk informasi selengkapnya, lihat [Batas layanan Amazon Inspector Classic](#)

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

## Templat penilaian

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

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

## Temuan

Masalah keamanan potensial yang ditemukan Amazon Inspector Classic selama penilaian target yang ditentukan. Temuan ditampilkan di konsol Amazon Inspector Classic atau diambil melalui API. Mereka berisi uraian detail tentang masalah keamanan dan rekomendasi tentang cara memperbaikinya. Untuk informasi selengkapnya, lihat [Temuan Amazon Inspector Classic](#).

## Aturan

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

## Paket aturan

Dalam konteks Amazon Inspector Classic, kumpulan aturan. Paket aturan sesuai dengan tujuan keamanan yang mungkin Anda miliki. Anda dapat menentukan sasaran keamanan dengan memilih paket aturan yang sesuai saat membuat templat penilaian Amazon Inspector Classic. Untuk informasi selengkapnya, lihat [Amazon Inspector Classic mengatur paket dan aturan](#).

## Telemetri

Menginstal informasi paket dan konfigurasi perangkat lunak untuk sebuah EC2 contoh. Amazon Inspector Classic mengumpulkan data selama penilaian dijalankan.

## 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 EC2 instance.

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

Sumber daya	Batas Default	Komentar
Instans dalam menjalankan penilaian	500	Jumlah maksimum EC2 instans yang dapat disertakan di semua penilaian yang berjalan per akun per wilayah.
Penilaian berjalan	50000	Jumlah maksimum penilaian berjalan yang dapat Anda buat per akun per wilayah. Anda dapat memiliki beberapa

Sumber daya	Batas Default	Komentar
		proses penilaian yang terjadi pada saat yang sama selama target penilaian yang digunakan untuk proses ini tidak mengandung instance yang tumpang tindih EC2 .
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 EC2 instans 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
Berikutnya 4.000 instance-assessment	\$0,10
Berikutnya 45.000 instance-assessment	\$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 EC2 Instans Amazon yang menjalankan aplikasi yang ingin Anda nilai. Penilaian dengan paket aturan tuan rumah diberi harga per agen per penilaian (agent-assessment) 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](#)
- [Sistem operasi berbasis Windows yang didukung untuk agen Amazon Inspector Classic](#)
- [Wilayah AWS yang Didukung](#)

## 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, 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).

# Amazon Inspector Classic akhir dukungan

Setelah mempertimbangkan dengan cermat, kami memutuskan untuk mengakhiri dukungan untuk Amazon Inspector Classic, efektif 20 Mei 2026. Amazon Inspector Classic tidak akan lagi menerima pelanggan baru mulai 20 Mei 2025. Sebagai pelanggan lama dengan akun yang mendaftar untuk layanan sebelum 20 Mei 2025, Anda dapat terus menggunakan fitur Amazon Inspector Classic. Setelah 20 Mei 2026, Anda tidak akan lagi dapat menggunakan Amazon Inspector Classic.

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 mengkonsolidasikan 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 Anda. EC2 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 EC2 instans 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 EC2 instance baru yang diluncurkan, gambar kontainer didorong ke Amazon ECR, pemasangan paket baru dalam sebuah EC2 instance, 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 dikalkulasi 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 CSPM 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](#)
- [Langkah 2: Hapus semua penilaian terjadwal yang berjalan di Amazon Inspector Classic](#)
- [Langkah 3: Aktifkan Amazon Inspector baru](#)

## 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 Konsol Manajemen AWS atau Amazon Inspector baru. APIs Untuk memulai dengan Amazon Inspector baru, lihat [Memulai di Panduan Pengguna](#) Amazon Inspector.

# Memulai dengan Amazon Inspector Classic

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

## Pengaturan dalam satu klik

Prosedur berikut menunjukkan kepada Anda cara membuat dan menjalankan penilaian otomatis menggunakan templat bawaan dan parameter penjadwalan yang telah ditentukan sebelumnya (seminggu sekali atau hanya satu kali) di semua instans Amazon Elastic Compute Cloud (Amazon EC2) yang tersedia saat ini dan. Akun AWS Wilayah AWS

1. Masuk ke Konsol Manajemen AWS 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 jaringan AWS lingkungan Anda untuk kerentanan, dan tidak memerlukan agen Amazon Inspector Classic. Penilaian Host menganalisis perangkat lunak on-host dan konfigurasi EC2 instans Anda untuk kerentanan, dan mengharuskan agen 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 EC2 instans yang ditentukan dalam target penilaian, Amazon Inspector Classic perlu menghitung EC2 instans dan tag Anda. Amazon Inspector Classic mendapatkan akses ke sumber daya ini di Anda Akun AWS melalui peran terkait layanan yang disebut `AWSServiceRoleForAmazonInspector` 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](#) di semua instans yang EC2 tersedia di Wilayah dan Anda. Akun AWS

**Note**

Layanan ini menginstal agen Amazon Inspector Classic hanya pada instans EC2 yang AWS Systems Manager mengizinkan Run Command. Untuk menggunakan opsi ini, pastikan bahwa semua EC2 instance Anda saat ini Akun AWS dan Wilayah AWS memiliki Agen SSM diinstal dan memiliki peran IAM yang memungkinkan Run Command. Untuk informasi selengkapnya, lihat [Menginstal agen pada beberapa instans EC2 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 memilih EC2 instans Amazon tertentu, paket aturan, dan parameter penjadwalan untuk disertakan dalam target dan templat penilaian.

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 menyertakan semua EC2 instance di wilayah Anda Akun AWS dan wilayah dalam target penilaian. Jika Anda ingin memilih EC2 instance mana yang akan disertakan, kosongkan kotak centang Semua Instans, dan masukkan tag Kunci dan Nilai yang terkait dengan instance target EC2 . Untuk informasi selengkapnya tentang menandai EC2 instans Anda, lihat [Menandai Sumber Daya Amazon Anda](#). EC2
4. Untuk Install Agents, Anda dapat menyimpan kotak centang yang dipilih secara default jika instance Anda mengizinkan [System Manager Run Command](#). Layanan ini menginstal agen Amazon Inspector Classic pada EC2 semua instans dalam target penilaian yang memungkinkan. AWS Systems Manager Untuk menggunakan opsi ini, pastikan bahwa semua EC2 instance Anda saat ini Akun AWS dan Wilayah AWS memiliki Agen SSM diinstal dan memiliki peran

IAM yang memungkinkan Run Command. Untuk informasi selengkapnya, lihat [Menginstal agen pada beberapa instans EC2 menggunakan Systems Manager Run Command](#). Jika Anda ingin menginstal agen secara manual, lihat [Menginstal Agen Amazon Inspector](#).

5. Pilih Berikutnya.
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, tetapkan jadwal untuk menjalankan penilaian berulang.
10. Pilih Berikutnya.
11. Pada halaman Tinjauan, tinjau pilihan Anda untuk target dan templat penilaian. Jika Anda puas dengan konfigurasi, pilih Buat. Jika Anda menetapkan jadwal penilaian untuk templat penilaian Anda, penilaian berjalan secara otomatis setelah Anda memilih Buat.

#### Note

Untuk mengidentifikasi EC2 instans yang ditentukan dalam target penilaian, Amazon Inspector Classic perlu menghitung EC2 instans dan tag Anda. Amazon Inspector Classic mendapatkan akses ke sumber daya ini di Anda Akun AWS melalui peran terkait layanan yang disebut. `AWSServiceRoleForAmazonInspector` Untuk informasi selengkapnya tentang penggunaan peran terkait layanan di Amazon Inspector Classic, lihat [Menggunakan peran terkait layanan untuk Amazon Inspector Classic](#) Untuk informasi mendetail tentang penggunaan peran terkait layanan, lihat [Menggunakan peran terkait layanan](#) di Panduan Pengguna.AWS Identity and Access Management

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 kepada Anda bagaimana melakukan penilaian Amazon Inspector Classic 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 Klasik - Red Hat Enterprise Linux

Sebelum Anda mengikuti petunjuk di tutorial ini, kami merekomendasikan agar Anda terbiasa dengan [Terminologi dan konsep Amazon Inspector Classic](#).

Tutorial ini menunjukkan cara menggunakan Amazon Inspector Classic untuk menganalisis perilaku instans EC2 yang menjalankan sistem operasi Red Hat Enterprise Linux 7.5. Ini memberikan step-by-step instruksi 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 menyiapkan dan menjalankan penilaian Amazon Inspector Classic dengan satu klik, [lihat Membuat](#) Penilaian Dasar.

## Topik

- [Langkah 1: Siapkan instans Amazon EC2 untuk digunakan dengan Amazon Inspector Classic](#)
- [Langkah 2: Memodifikasi instans Amazon EC2 Anda](#)
- [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: Siapkan 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: Memodifikasi instans Amazon EC2 Anda

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 ke Konsol Manajemen AWS dan buka konsol Amazon Inspector Classic di <https://console.aws.amazon.com/inspector/>
2. Di panel navigasi, pilih Target penilaian, lalu pilih Buat.

Lakukan hal-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 Simpan.
- d. Instal agen Amazon Inspector Classic pada instans EC2 Anda yang diberi tag. 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 Classic menggunakan [AWS Systems Manager Run Command](#). 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 Classic di instans EC2 Anda secara manual. Untuk informasi selengkapnya, lihat [Menginstal agen Amazon Inspector Classic](#).

- e. Pilih Simpan.

 Note

Pada titik ini, Amazon Inspector Classic membuat peran terkait layanan yang disebut `AWSServiceRoleForAmazonInspector`. Peran tersebut memberi Amazon Inspector Classic akses yang diperlukan ke 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

Proses penilaian yang lengkap 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 run untuk template penilaian yang dipanggil 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 MyFirstTemplateLinuxperubahan pertama menjadi Berhenti, kemudian dalam beberapa menit untuk Menganalisis, dan akhirnya Analisis selesai. Untuk melihat perubahan status ini, pilih ikon Segarkan.

3. Di panel navigasi, pilih Temuan.

Anda dapat melihat temuan baru tingkat keparahan Tinggi yang disebut Instance Inspector rentan terhadap EC2 InstanceLinux 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 Classic
- 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.e17
```

2. Pada halaman Templat penilaian, pilih MyFirstTemplateLinux, lalu pilih Jalankan untuk memulai proses penilaian baru menggunakan templat ini.
3. Ikuti langkah-langkah [Langkah 5: Mencari dan menganalisis temuan Anda](#) untuk melihat temuan yang dihasilkan dari proses MyFirstTemplateLinuxtemplate berikutnya ini.

Karena Anda menyelesaikan masalah keamanan CVE-2018-1111, Anda seharusnya tidak lagi melihat temuan untuk itu.

## Tutorial Amazon Inspector Klasik - Server Ubuntu

Sebelum Anda mengikuti petunjuk di tutorial ini, kami merekomendasikan agar Anda terbiasa dengan [Terminologi dan konsep Amazon Inspector Classic](#).

Tutorial ini menunjukkan cara menggunakan Amazon Inspector Classic untuk menganalisis perilaku instans EC2 yang menjalankan sistem operasi Ubuntu Server 16.04 LTS. Ini memberikan step-by-step instruksi tentang cara menavigasi alur kerja Amazon Inspector Classic.

Jika Anda adalah pengguna pertama kali dan ingin menyiapkan dan menjalankan penilaian Amazon Inspector Classic dengan satu klik, [lihat Membuat](#) Penilaian Dasar.

Topik

- [Langkah 1: Siapkan 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: Siapkan 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 Classic menggunakan target penilaian untuk menunjuk sumber daya AWS untuk dievaluasi.

Untuk membuat target penilaian dan menginstal agen pada instans EC2

1. Masuk ke Konsol Manajemen AWS dan buka konsol Amazon Inspector Classic di <https://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 Amazon Inspector Classic Agent pada instans EC2 yang diberi tag. 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 selengkapnya, lihat [Menginstal agen Amazon Inspector Classic](#).

6. Pilih Simpan.

 Note

Pada titik ini, peran terkait layanan yang `AWSServiceRoleForAmazonInspector` disebut dibuat untuk memberikan Amazon Inspector Classic 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

Proses penilaian yang lengkap 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.

1. Navigasikan ke halaman Penilaian Berjalan. Verifikasi bahwa status run untuk template penilaian MyFirstTemplateUbuntuyang disebut yang Anda buat pada langkah sebelumnya 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 MyFirstTemplateUbuntuperubahan pertama menjadi Berhenti, kemudian dalam beberapa menit untuk Menganalisis, dan akhirnya 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 Classic
- 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, pilih MyFirstTemplateUbuntu, lalu pilih Jalankan untuk memulai proses baru menggunakan templat ini.
3. Ikuti langkah-langkah [Langkah 4: Mencari dan menganalisis temuan yang dihasilkan](#) untuk melihat temuan yang dihasilkan dari proses MyFirstTemplateUbuntutemplate 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 dari cloud dan keamanan dalam cloud:

- Keamanan cloud — AWS bertanggung jawab untuk melindungi infrastruktur yang menjalankan AWS layanan di AWS Cloud. AWS juga memberi Anda layanan yang dapat Anda gunakan dengan aman. Auditor pihak ketiga secara teratur menguji dan memverifikasi efektivitas keamanan kami sebagai bagian dari [Program AWS Kepatuhan Program AWS Kepatuhan](#) . Untuk mempelajari tentang program kepatuhan yang berlaku untuk Amazon Inspector Classic, lihat AWS [Services in Scope by Compliance Program AWS](#) 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 layanan AWS lain yang membantu Anda memantau dan mengamankan sumber daya Amazon Inspector Classic Anda.

## Topik

- [Perlindungan data di Amazon Inspector Classic](#)
- [Identity and Access Management untuk Amazon Inspector Classic](#)
- [Pencatatan dan pemantauan di Amazon Inspector Classic](#)
- [Tanggapan insiden di Amazon Inspector Classic](#)
- [Validasi kepatuhan untuk Amazon Inspector Classic](#)
- [Ketahanan di Amazon Inspector Classic](#)
- [Keamanan infrastruktur di Amazon Inspector Classic](#)
- [Analisis konfigurasi dan kerentanan di Amazon Inspector Classic](#)
- [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. Lihat informasi yang lebih lengkap tentang privasi data dalam [Pertanyaan Umum Privasi Data](#). Lihat informasi tentang perlindungan data di Eropa di pos blog [Model Tanggung Jawab Bersama dan GDPR AWS](#) di Blog Keamanan AWS .

Untuk tujuan perlindungan data, kami menyarankan Anda melindungi Akun AWS kredensial dan mengatur pengguna individu dengan AWS IAM Identity Center atau AWS Identity and Access Management (IAM). Dengan cara itu, setiap pengguna hanya diberi izin yang diperlukan untuk memenuhi tanggung jawab tugasnya. Kami juga menyarankan supaya Anda mengamankan data dengan cara-cara berikut:

- Gunakan autentikasi multi-faktor (MFA) pada setiap akun.
- Gunakan SSL/TLS untuk berkomunikasi dengan AWS sumber daya. Kami mensyaratkan TLS 1.2 dan menganjurkan 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 modul kriptografi tervalidasi FIPS 140-3 saat mengakses AWS melalui antarmuka baris perintah atau API, gunakan titik akhir FIPS. Lihat informasi selengkapnya tentang titik akhir FIPS yang tersedia di [Standar Pemrosesan Informasi Federal \(FIPS\) 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. Saat Anda memberikan URL ke server eksternal, kami sangat menganjurkan supaya Anda tidak menyertakan informasi kredensial di dalam URL untuk memvalidasi permintaan Anda ke server itu.

## Topik

- [Enkripsi data saat tidak digunakan](#)
- [Mengenkripsi data saat transit](#)

## 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 melalui TLS ke Amazon Inspector Classic, di mana mereka dienkripsi dengan per-assessment-run kunci turunan fana. 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 panggilan API yang AWS dipublikasikan untuk mengakses Amazon Inspector Classic melalui jaringan. Klien harus mendukung hal-hal berikut:

- Keamanan Lapisan Pengangkutan (TLS). Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Sandi cocok dengan sistem kerahasiaan maju sempurna (perfect forward secrecy, PFS) seperti DHE (Ephemeral Diffie-Hellman) atau ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Sebagian besar sistem modern seperti Java 7 dan versi lebih baru mendukung mode-mode ini.

# 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. Administrator IAM mengontrol siapa yang dapat terautentikasi (masuk) dan berwenang (memiliki izin) untuk menggunakan sumber daya Amazon Inspector. IAM adalah Layanan AWS yang dapat Anda gunakan tanpa biaya tambahan.

## Topik

- [Audiens](#)
- [Mengautentikasi dengan identitas](#)
- [Mengelola akses menggunakan kebijakan](#)
- [Bagaimana Amazon Inspector Classic bekerja dengan IAM](#)
- [Contoh 2: Memungkinkan pengguna untuk melakukan setiap penjelasan dan daftar operasi hanya pada temuan Amazon Inspector](#)
- [Sumber daya kebijakan untuk Amazon Inspector](#)
- [Kunci kondisi kebijakan untuk Amazon Inspector](#)
- [ACLs di Amazon Inspector](#)
- [ABAC dengan Amazon Inspector](#)
- [Menggunakan kredensial sementara dengan Amazon Inspector](#)
- [Izin utama lintas layanan untuk Amazon Inspector](#)
- [Peran layanan untuk Amazon Inspector](#)
- [Peran terkait layanan untuk Amazon Inspector](#)
- [Contoh kebijakan berbasis identitas untuk Amazon Inspector Classic](#)
- [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 berdasarkan peran Anda:

- Pengguna layanan - minta izin dari administrator Anda jika Anda tidak dapat mengakses fitur (lihat [Memecahkan masalah identitas dan akses Amazon Inspector Classic](#))

- Administrator layanan - tentukan akses pengguna dan mengirimkan permintaan izin (lihat [Bagaimana Amazon Inspector Classic bekerja dengan IAM](#))
- Administrator IAM - tulis kebijakan untuk mengelola akses (lihat [Contoh kebijakan berbasis identitas untuk Amazon Inspector Classic](#))

## Mengautentikasi dengan identitas

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

Anda dapat masuk sebagai identitas federasi menggunakan kredensial dari sumber identitas seperti AWS IAM Identity Center (Pusat Identitas IAM), autentikasi masuk tunggal, atau kredensial. Google/Facebook Untuk informasi selengkapnya tentang cara masuk, lihat [Cara masuk ke Akun AWS Anda](#) dalam Panduan Pengguna AWS Sign-In .

Untuk akses terprogram, AWS sediakan SDK dan CLI untuk menandatangani permintaan secara kriptografis. Untuk informasi selengkapnya, lihat [AWS Signature Version 4 untuk permintaan API](#) dalam Panduan Pengguna IAM.

### Akun AWS pengguna root

Saat Anda membuat Akun AWS, Anda mulai dengan satu identitas masuk yang disebut pengguna Akun AWS root yang memiliki akses lengkap ke semua Layanan AWS dan sumber daya. Kami sangat menyarankan agar Anda tidak menggunakan pengguna root untuk tugas sehari-hari. Untuk tugas yang memerlukan kredensial pengguna root, lihat [Tugas yang memerlukan kredensial pengguna root](#) dalam Panduan Pengguna IAM.

### Identitas terfederasi

Sebagai praktik terbaik, mewajibkan pengguna manusia untuk menggunakan federasi dengan penyedia identitas untuk mengakses Layanan AWS menggunakan kredensial sementara.

Identitas federasi adalah pengguna dari direktori perusahaan Anda, penyedia identitas web, atau Directory Service yang mengakses Layanan AWS menggunakan kredensial dari sumber identitas. Identitas terfederasi mengambil peran yang memberikan kredensial sementara.

Untuk manajemen akses terpusat, kami menyarankan AWS IAM Identity Center. Untuk informasi selengkapnya, lihat [Apa itu Pusat Identitas IAM?](#) dalam Panduan Pengguna AWS IAM Identity Center

## Pengguna dan grup IAM

[Pengguna IAM](#) adalah identitas dengan izin khusus untuk satu orang atau aplikasi. Sebaiknya gunakan kredensial sementara alih-alih pengguna IAM dengan kredensial jangka panjang. Untuk informasi selengkapnya, lihat [Mewajibkan pengguna manusia untuk menggunakan federasi dengan penyedia identitas untuk mengakses AWS menggunakan kredensial sementara](#) di Panduan Pengguna IAM.

[Grup IAM](#) menentukan kumpulan pengguna IAM dan mempermudah pengelolaan izin untuk pengguna dalam jumlah besar. Untuk mempelajari selengkapnya, lihat [Kasus penggunaan untuk pengguna IAM](#) dalam Panduan Pengguna IAM.

## Peran IAM

[Peran IAM](#) adalah identitas dengan izin khusus yang menyediakan kredensial sementara. Anda dapat mengambil peran dengan [beralih dari pengguna ke peran IAM \(konsol\)](#) atau dengan memanggil operasi AWS CLI atau AWS API. Untuk informasi selengkapnya, lihat [Metode untuk mengambil peran](#) dalam Panduan Pengguna IAM.

Peran IAM berguna untuk akses pengguna terfederasi, izin pengguna IAM sementara, akses lintas akun, akses lintas layanan, dan aplikasi yang berjalan di Amazon EC2. Untuk informasi selengkapnya, lihat [Akses sumber daya lintas akun di IAM](#) dalam Panduan Pengguna IAM.

## Mengelola akses menggunakan kebijakan

Anda mengontrol akses AWS dengan membuat kebijakan dan melampirkannya ke AWS identitas atau sumber daya. Kebijakan menentukan izin saat dikaitkan dengan identitas atau sumber daya. AWS mengevaluasi kebijakan ini ketika kepala sekolah membuat permintaan. Sebagian besar kebijakan disimpan AWS sebagai dokumen JSON. Untuk informasi selengkapnya tentang dokumen kebijakan JSON, lihat [Gambaran umum kebijakan JSON](#) dalam Panduan Pengguna IAM.

Menggunakan kebijakan, administrator menentukan siapa yang memiliki akses ke apa dengan mendefinisikan principal mana yang dapat melakukan tindakan pada sumber daya apa, dan dalam kondisi apa.

Secara default, pengguna dan peran tidak memiliki izin. Administrator IAM membuat kebijakan IAM dan menambahkannya ke peran, yang kemudian dapat diambil oleh pengguna. Kebijakan IAM mendefinisikan izin terlepas dari metode yang Anda gunakan untuk melakukannya.

## Kebijakan berbasis identitas

Kebijakan berbasis identitas adalah dokumen kebijakan izin JSON yang Anda lampirkan ke identitas (pengguna, grup, atau peran). Kebijakan ini mengontrol tindakan apa yang bisa dilakukan oleh identitas tersebut, terhadap sumber daya yang mana, dan dalam kondisi apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat [Tentukan izin IAM kustom dengan kebijakan yang dikelola pelanggan](#) dalam Panduan Pengguna IAM.

Kebijakan berbasis identitas dapat berupa kebijakan inline (disematkan langsung ke dalam satu identitas) atau kebijakan terkelola (kebijakan mandiri yang dilampirkan pada banyak identitas). Untuk mempelajari cara memilih antara kebijakan terkelola dan kebijakan inline, lihat [Pilih antara kebijakan terkelola dan kebijakan inline](#) dalam Panduan Pengguna IAM.

## Kebijakan berbasis sumber daya

Kebijakan berbasis sumber daya adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contohnya termasuk kebijakan kepercayaan peran IAM dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Anda harus [menentukan principal](#) dalam kebijakan berbasis sumber daya.

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

## Jenis-jenis kebijakan lain

AWS mendukung jenis kebijakan tambahan yang dapat menetapkan izin maksimum yang diberikan oleh jenis kebijakan yang lebih umum:

- Batasan izin – Menetapkan izin maksimum yang dapat diberikan oleh kebijakan berbasis identitas kepada entitas IAM. Untuk informasi selengkapnya, lihat [Batasan izin untuk entitas IAM](#) dalam Panduan Pengguna IAM.
- Kebijakan kontrol layanan (SCPs) — Tentukan izin maksimum untuk organisasi atau unit organisasi di AWS Organizations. Untuk informasi selengkapnya, lihat [Kebijakan kontrol layanan](#) dalam Panduan Pengguna AWS Organizations .
- Kebijakan kontrol sumber daya (RCPs) — Tetapkan izin maksimum yang tersedia untuk sumber daya di akun Anda. Untuk informasi selengkapnya, lihat [Kebijakan kontrol sumber daya \(RCPs\)](#) di Panduan AWS Organizations Pengguna.

- Kebijakan sesi – Kebijakan lanjutan yang diteruskan sebagai parameter saat membuat sesi sementara untuk peran atau pengguna terfederasi. Untuk informasi selengkapnya, lihat [Kebijakan sesi](#) dalam Panduan Pengguna IAM.

## Berbagai jenis kebijakan

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

## Bagaimana Amazon Inspector Classic bekerja dengan IAM

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

Fitur IAM yang dapat Anda gunakan dengan Amazon Inspector Classic

Fitur IAM	Dukungan Amazon Inspector
<a href="#">Kebijakan berbasis identitas</a>	Ya
<a href="#">Kebijakan berbasis sumber daya</a>	Tidak
<a href="#">Tindakan kebijakan</a>	Ya
<a href="#">Sumber daya kebijakan</a>	Ya
<a href="#">kunci-kunci persyaratan kebijakan (spesifik layanan)</a>	Ya
<a href="#">ACLs</a>	Tidak
<a href="#">ABAC (tanda dalam kebijakan)</a>	Parsial
<a href="#">Kredensial sementara</a>	Ya
<a href="#">Izin principal</a>	Ya
<a href="#">Peran layanan</a>	Tidak

Fitur IAM	Dukungan Amazon Inspector
<a href="#">Peran terkait layanan</a>	Ya

Untuk mendapatkan tampilan tingkat tinggi tentang cara kerja Amazon Inspector dan layanan AWS lainnya dengan sebagian besar fitur IAM, [AWS lihat layanan yang bekerja dengan IAM di Panduan Pengguna IAM](#).

## Kebijakan berbasis identitas untuk Amazon Inspector

Mendukung kebijakan berbasis identitas: Ya

Kebijakan berbasis identitas adalah dokumen kebijakan izin JSON yang dapat Anda lampirkan ke sebuah identitas, seperti pengguna IAM, grup pengguna IAM, atau peran IAM. Kebijakan ini mengontrol jenis tindakan yang dapat dilakukan oleh pengguna dan peran, di sumber daya mana, dan berdasarkan kondisi seperti apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat [Tentukan izin IAM kustom dengan kebijakan terkelola pelanggan](#) dalam Panduan Pengguna IAM.

Dengan kebijakan berbasis identitas IAM, Anda dapat menentukan secara spesifik apakah tindakan dan sumber daya diizinkan atau ditolak, serta kondisi yang menjadi dasar dikabulkan atau ditolaknya tindakan tersebut. Untuk mempelajari semua elemen yang dapat Anda gunakan dalam kebijakan JSON, lihat [Referensi elemen kebijakan JSON IAM](#) dalam Panduan Pengguna IAM.

Contoh kebijakan berbasis identitas untuk Amazon Inspector

Untuk melihat contoh kebijakan berbasis identitas Amazon Inspector, lihat [Contoh kebijakan berbasis identitas untuk Amazon Inspector Classic](#).

## Kebijakan berbasis sumber daya dalam Amazon Inspector

Mendukung kebijakan berbasis sumber daya: Tidak

Kebijakan berbasis sumber daya adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah kebijakan kepercayaan peran IAM dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Untuk sumber daya tempat kebijakan dilampirkan, kebijakan menentukan tindakan apa yang dapat

dilakukan oleh principal tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus [menentukan principal](#) dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau Layanan AWS

Untuk mengaktifkan akses lintas akun, Anda dapat menentukan secara spesifik seluruh akun atau entitas IAM di akun lain sebagai principal dalam kebijakan berbasis sumber daya. Untuk informasi selengkapnya, lihat [Akses sumber daya lintas akun di IAM](#) dalam Panduan Pengguna IAM.

## Tindakan kebijakan untuk Amazon Inspector

Mendukung tindakan kebijakan: Ya

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

Elemen `Action` dari kebijakan JSON menjelaskan tindakan yang dapat Anda gunakan untuk mengizinkan atau menolak akses dalam sebuah kebijakan. 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:

JSON

```
{
  "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.

JSON

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

Elemen kebijakan JSON `Resource` menentukan objek yang menjadi target penerapan tindakan. Praktik terbaiknya, tentukan sumber daya menggunakan [Amazon Resource Name \(ARN\)](#). Untuk tindakan yang tidak mendukung izin di tingkat sumber daya, gunakan wildcard (\*) untuk menunjukkan bahwa pernyataan tersebut berlaku untuk semua sumber daya.

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

Untuk melihat daftar jenis sumber daya Amazon Inspector dan jenisnya ARNs, lihat Sumber daya yang [ditentukan oleh Amazon Inspector Classic](#) di Referensi Otorisasi Layanan. Untuk mempelajari tindakan mana 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 kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Yaitu, principal dapat melakukan tindakan pada suatu sumber daya, dan dalam suatu syarat.

Elemen `Condition` menentukan ketika pernyataan dieksekusi berdasarkan kriteria yang ditetapkan. 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. Untuk melihat semua kunci kondisi AWS global, lihat [kunci konteks kondisi AWS global](#) di Panduan Pengguna IAM.

Untuk melihat daftar kunci kondisi Amazon Inspector, lihat Kunci kondisi [untuk Amazon Inspector 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](#).

## ACLs di Amazon Inspector

Mendukung ACLs: Tidak

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

## ABAC dengan Amazon Inspector

Mendukung ABAC (tag dalam kebijakan): Sebagian

Kontrol akses berbasis atribut (ABAC) adalah strategi otorisasi yang menentukan izin berdasarkan atribut tanda. Anda dapat melampirkan tag ke entitas dan AWS sumber daya IAM, lalu merancang kebijakan ABAC untuk mengizinkan operasi saat tag prinsipal cocok dengan tag pada sumber daya.

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 selengkapnya tentang ABAC, lihat [Tentukan izin dengan otorisasi ABAC](#) dalam Panduan Pengguna IAM. Untuk melihat tutorial yang menguraikan langkah-langkah pengaturan ABAC, lihat [Menggunakan kontrol akses berbasis atribut \(ABAC\)](#) dalam Panduan Pengguna IAM.

## Menggunakan kredensial sementara dengan Amazon Inspector

Mendukung kredensial sementara: Ya

Kredensial sementara menyediakan akses jangka pendek ke AWS sumber daya dan secara otomatis dibuat saat Anda menggunakan federasi atau beralih peran. AWS merekomendasikan agar Anda secara dinamis menghasilkan kredensi sementara alih-alih menggunakan kunci akses jangka panjang. Untuk informasi selengkapnya, lihat [Kredensial keamanan sementara di IAM](#) dan [Layanan AWS yang berfungsi dengan IAM](#) dalam Panduan Pengguna IAM.

## Izin utama lintas layanan untuk Amazon Inspector

Mendukung sesi akses terusan (FAS): Ya

Sesi akses terusan (FAS) menggunakan izin dari pemanggilan utama Layanan AWS, dikombinasikan dengan permintaan Layanan AWS untuk membuat permintaan ke layanan hilir. Untuk detail kebijakan ketika mengajukan permintaan FAS, lihat [Sesi akses terusan](#).

## Peran layanan untuk Amazon Inspector

Mendukung peran layanan: Tidak

Peran layanan adalah [peran IAM](#) yang diambil oleh sebuah layanan untuk melakukan tindakan atas nama Anda. Administrator IAM dapat membuat, mengubah, dan menghapus peran layanan dari dalam IAM. Untuk informasi selengkapnya, lihat [Buat sebuah peran untuk mendelegasikan izin ke Layanan AWS](#) dalam Panduan pengguna IAM.

### Warning

Mengubah izin untuk peran layanan dapat merusak fungsionalitas Amazon Inspector. Edit peran layanan hanya jika Amazon Inspector memberikan panduan untuk melakukannya.

## Peran terkait layanan untuk Amazon Inspector

Mendukung peran 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. Administrator IAM dapat melihat, tetapi tidak dapat mengedit izin untuk peran terkait layanan.

Untuk detail tentang cara membuat atau mengelola peran terkait 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. Untuk memberikan izin kepada pengguna untuk melakukan tindakan di sumber daya yang mereka perlukan, administrator IAM dapat membuat kebijakan IAM.

Untuk mempelajari cara membuat kebijakan berbasis identitas IAM dengan menggunakan contoh dokumen kebijakan JSON ini, lihat [Membuat kebijakan IAM \(konsol\) 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 yang dikelola AWS](#) atau [Kebijakan yang dikelola AWS untuk fungsi tugas](#) dalam Panduan Pengguna IAM.

- Menerapkan izin dengan hak akses paling rendah – Ketika Anda menetapkan izin dengan kebijakan IAM, hanya berikan izin yang diperlukan untuk melakukan tugas. Anda 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 cara menggunakan IAM untuk mengajukan izin, lihat [Kebijakan dan izin dalam IAM](#) dalam Panduan Pengguna IAM.
- Gunakan kondisi dalam kebijakan IAM untuk membatasi akses lebih lanjut – Anda dapat menambahkan suatu kondisi ke kebijakan Anda untuk membatasi akses ke tindakan dan sumber daya. Sebagai contoh, Anda dapat menulis kondisi kebijakan untuk menentukan bahwa semua permintaan harus dikirim menggunakan SSL. Anda juga dapat menggunakan ketentuan untuk memberikan akses ke tindakan layanan jika digunakan melalui yang spesifik Layanan AWS, seperti CloudFormation. Untuk informasi selengkapnya, lihat [Elemen kebijakan JSON IAM: Kondisi](#) dalam Panduan Pengguna IAM.
- Gunakan IAM Access Analyzer untuk memvalidasi kebijakan IAM Anda untuk memastikan izin yang aman dan fungsional – IAM Access Analyzer memvalidasi kebijakan baru dan yang sudah ada sehingga kebijakan tersebut mematuhi bahasa kebijakan IAM (JSON) dan praktik terbaik IAM. IAM Access Analyzer menyediakan lebih dari 100 pemeriksaan kebijakan dan rekomendasi yang dapat ditindaklanjuti untuk membantu Anda membuat kebijakan yang aman dan fungsional. Untuk informasi selengkapnya, lihat [Validasi kebijakan dengan IAM Access Analyzer](#) dalam Panduan Pengguna IAM.
- Memerlukan otentikasi multi-faktor (MFA) - Jika Anda memiliki skenario yang mengharuskan pengguna IAM atau pengguna root di Anda, Akun AWS aktifkan MFA untuk keamanan tambahan. Untuk meminta MFA ketika operasi API dipanggil, tambahkan kondisi MFA pada kebijakan Anda. Untuk informasi selengkapnya, lihat [Amankan akses API dengan MFA](#) dalam Panduan Pengguna IAM.

Untuk informasi selengkapnya tentang praktik terbaik dalam IAM, lihat [Praktik terbaik keamanan di IAM](#) dalam Panduan Pengguna IAM.

## 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 sesuai dengan operasi API yang coba mereka 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 [Menambah izin untuk pengguna](#) dalam Panduan Pengguna IAM.

## Mengizinkan pengguna melihat izin mereka sendiri

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

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
        "iam:GetUserPolicy",
        "iam:ListGroupsWithUser",
        "iam:ListAttachedUserPolicies",
        "iam:ListUserPolicies",
        "iam:GetUser"
      ],
      "Resource": ["arn:aws:iam::*:user/${aws:username}"]
    },
    {
      "Sid": "NavigateInConsole",
      "Effect": "Allow",
      "Action": [
        "iam:GetGroupPolicy",
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam:ListAttachedGroupPolicies",

```

```
        "iam:ListGroupPolicies",
        "iam:ListPolicyVersions",
        "iam:ListPolicies",
        "iam:ListUsers"
    ],
    "Resource": "*"
}
]
```

## 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.

### JSON

```
{
  "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 peran terkait AWS Identity and Access Management layanan \(IAM\)](#). Peran terkait layanan adalah jenis peran IAM unik yang ditautkan langsung ke

Amazon Inspector Classic. 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-izin yang ditentukan mencakup kebijakan kepercayaan dan kebijakan izin, serta bahwa kebijakan izin tidak dapat dilampirkan ke entitas 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 [Layanan AWS yang Bekerja bersama IAM](#) dan mencari layanan yang memiliki Ya dalam Peran Terkait Layanan. Pilih Ya dengan sebuah tautan untuk melihat dokumentasi peran terkait layanan untuk layanan tersebut.

## Izin peran terkait layanan untuk Amazon Inspector Classic

Amazon Inspector Classic menggunakan peran terkait layanan bernama —  
AWSServiceRoleForAmazonInspector ServiceLinkedRoleDescription

Peran AWSService RoleForAmazonInspector 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 entitas IAM (seperti pengguna, grup, atau peran IAM) untuk membuat, mengedit, atau menghapus peran terkait layanan. Untuk informasi selengkapnya, lihat [Izin peran terkait layanan](#) dalam Panduan Pengguna IAM.

## Membuat peran terkait layanan untuk Amazon Inspector Classic

Anda tidak perlu membuat peran terkait layanan secara manual. Saat Anda `CompleteThisCreateActionInThisService` berada di Konsol Manajemen AWS, API AWS CLI, atau AWS API, 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 terkait layanan, Anda tidak dapat mengubah nama peran karena berbagai entitas mungkin merujuk peran tersebut. Namun, Anda dapat mengedit penjelasan peran menggunakan IAM. Untuk informasi selengkapnya, lihat [Mengedit peran terkait layanan](#) dalam Panduan Pengguna IAM.

## Menghapus peran terkait layanan untuk Amazon Inspector Classic

Jika Anda tidak perlu lagi menggunakan fitur atau layanan yang memerlukan peran terkait layanan, sebaiknya hapus 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 Classic](#).

Untuk menghapus peran tertaut layanan secara manual menggunakan IAM

Gunakan konsol IAM, the AWS CLI, atau AWS API untuk menghapus peran AWSService RoleForAmazonInspector terkait layanan. Untuk informasi selengkapnya, lihat [Menghapus peran terkait layanan](#) dalam 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 mengatasi masalah umum yang mungkin Anda temui saat bekerja menggunakan Amazon Inspector dan IAM.

### Topik

- [Saya tidak berwenang untuk melakukan tindakan di Amazon Inspector](#)
- [Saya tidak berwenang untuk melakukan iam: PassRole](#)
- [Saya ingin mengizinkan orang di luar saya Akun AWS untuk mengakses sumber daya Amazon Inspector saya](#)

## Saya tidak berwenang untuk melakukan tindakan di Amazon Inspector

Jika Anda menerima pesan kesalahan bahwa Anda tidak memiliki otorisasi untuk melakukan tindakan, kebijakan Anda harus diperbarui agar Anda dapat melakukan tindakan tersebut.

Contoh kesalahan berikut terjadi ketika pengguna IAM mateojackson mencoba menggunakan konsol untuk melihat detail tentang suatu sumber daya *my-example-widget* rekaan, tetapi tidak memiliki izin `inspector:GetWidget` rekaan.

```
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 saat pengguna IAM bernama `marymajor` mencoba menggunakan konsol tersebut untuk melakukan tindakan di Amazon Inspector. Namun, tindakan tersebut memerlukan layanan untuk mendapatkan izin yang diberikan oleh peran layanan. Mary tidak memiliki izin untuk meneruskan peran tersebut pada layanan.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
iam:PassRole
```

Dalam kasus ini, kebijakan Mary harus diperbarui agar dia mendapatkan izin untuk melakukan tindakan `iam:PassRole` tersebut.

Jika Anda memerlukan bantuan, hubungi AWS administrator Anda. Administrator Anda adalah orang yang memberi Anda kredensial masuk.

## Saya ingin mengizinkan orang di luar saya Akun AWS untuk mengakses sumber daya Amazon Inspector saya

Anda dapat membuat peran yang dapat digunakan pengguna di akun lain atau 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 pengguna IAM di pengguna lain Akun AWS yang Anda miliki](#) di Panduan Pengguna IAM.

- Untuk mempelajari cara menyediakan akses ke sumber daya Anda kepada pihak ketiga Akun AWS, lihat [Menyediakan akses yang Akun AWS dimiliki oleh pihak ketiga](#) dalam Panduan Pengguna IAM.
- Untuk mempelajari cara memberikan akses melalui federasi identitas, lihat [Menyediakan akses ke pengguna terautentikasi eksternal \(federasi identitas\)](#) dalam Panduan Pengguna IAM.
- Untuk mempelajari perbedaan antara menggunakan peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat [Akses sumber daya lintas akun di IAM di 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 panggilan API untuk Amazon Inspector Classic sebagai peristiwa, 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 Classic dengan AWS 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 Dasbor AWS Health. Untuk informasi tentang cara menggunakan Dasbor Health, 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. Program ini mencakup SOC, PCI, FedRAMP, HIPAA, dan lainnya.

Untuk daftar AWS layanan dalam lingkup program kepatuhan tertentu, lihat [AWS Services in Scope by Compliance Program](#) . Untuk informasi umum, lihat [Program AWS Kepatuhan Program AWS](#) .

Anda dapat mengunduh laporan audit pihak ketiga menggunakan AWS Artifact. Untuk informasi selengkapnya, lihat [Pengunduhan Laporan dalam 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 Keamanan dan Kepatuhan HIPAA di Amazon Web Services](#) — Whitepaper ini menjelaskan bagaimana perusahaan dapat menggunakan AWS untuk membuat aplikasi yang sesuai dengan HIPAA.
- [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 CSPM](#)— 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 panggilan API yang AWS dipublikasikan untuk mengakses Amazon Inspector Classic melalui jaringan. Klien harus mendukung hal-hal berikut:

- Keamanan Lapisan Pengangkutan (TLS). Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Sandi cocok dengan sistem kerahasiaan maju sempurna (perfect forward secrecy, PFS) seperti DHE (Ephemeral Diffie-Hellman) atau ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Sebagian besar sistem modern seperti Java 7 dan versi lebih baru mendukung mode-mode ini.

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 instans EC2 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 Classic 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. Ini mengakses metadata instance menggunakan versi 1 atau versi 2 dari Layanan Metadata Instance (atau). IMDSv1 IMDSv2 Lihat [Metadata Instans dan Data Pengguna](#) untuk mempelajari lebih lanjut tentang metadata instans EC2 dan metode akses.

## Topik

- [Hak istimewa agen Amazon Inspector Classic](#)
- [Keamanan agen Jaringan dan Amazon Inspector Classic](#)
- [Pembaruan agen Amazon Inspector Classic](#)
- [Siklus hidup data telemetri](#)
- [Kontrol akses dari Amazon Inspector Classic ke dalam akun AWS](#)
- [Batas agen Amazon Inspector Classic](#)
- [Menginstal agen Amazon Inspector Classic](#)
- [Bekerja dengan agen Amazon Inspector Classic pada sistem operasi berbasis Linux](#)

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

Agan 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.

Agan 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

tempatnyanya 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. Tidak ada 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 dikirim near-real-time melalui TLS ke Amazon Inspector Classic, di mana mereka dienkrpsi dengan per-assessment-run kunci turunan KMS sementara. 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). Selain itu, Anda dapat menginstal agen secara individual dengan masuk ke setiap instans EC2. Prosedur dalam bab ini memberikan instruksi untuk kedua metode.

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

### Topik

- [Menginstal agen pada beberapa instans EC2 menggunakan Systems Manager Run Command](#)
- [Menginstal agen pada instans EC2 berbasis Linux](#)
- [Menginstal agen pada instans EC2 berbasis Windows](#)

**Note**

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

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

Anda dapat menginstal agen Amazon Inspector Classic pada instans EC2 menggunakan perintah [Systems Manager Run Command](#). 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 bahwa instans EC2 Anda memiliki SSM Agent terinstal dan memiliki 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 selengkapnya, lihat [Menginstal dan mengonfigurasi Agen SSM](#) dan [Mengonfigurasi peran keamanan untuk SSM](#).

Untuk menginstal agen pada beberapa instans EC2 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-Manage AWSSAgent yang dimiliki oleh Amazon. Dokumen ini berisi skrip untuk menginstal agen Amazon Inspector Classic pada instans EC2.
5. Untuk Target, Anda dapat memilih instans EC2 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 instans EC2 (berbasis Linux dan berbasis Windows) ketika Anda membuat target penilaian, atau Anda dapat menggunakan tombol Menginstal Agen dengan Run Command untuk target yang ada. Untuk informasi selengkapnya, lihat [Membuat target penilaian](#).

## Menginstal agen pada instans EC2 berbasis Linux

Lakukan prosedur berikut untuk menginstal agen Amazon Inspector Classic pada instans EC2 berbasis Linux.

Untuk menginstal agen pada instans EC2 berbasis Linux


1. Masuk ke instans EC2 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 Classic 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 instans EC2 berbasis Windows

Lakukan prosedur berikut untuk menginstal agen Amazon Inspector Classic pada instans EC2 berbasis Windows.

Untuk menginstal agen pada instans EC2 berbasis Windows

1. Masuk ke instans EC2 Anda yang menjalankan sistem operasi berbasis Windows di mana 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

Agan Amazon Inspector Classic mengandalkan metadata instans Amazon EC2 agar berfungsi dengan benar. Ini mengakses metadata instance menggunakan versi 1 atau versi 2 dari Layanan Metadata Instance (atau). IMDSv1 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](#)
- [Menghentikan agen Amazon Inspector Classic](#)
- [Memulai agen Amazon Inspector Classic](#)
- [Memodifikasi pengaturan agen Amazon Inspector Classic](#)
- [Mengkonfigurasi dukungan proxy untuk agen Amazon Inspector Classic](#)
- [Menghapus instalasi agen Amazon Inspector Classic](#)

## 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\\_pengaturan](https://wiki.archlinux.org/index.php/proxy_pengaturan).

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 instans EC2 berbasis Linux](#)

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 instans EC2 berbasis Linux](#).
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 Classic pada sistem operasi berbasis Windows

Anda dapat memulai, menghentikan, dan memodifikasi perilaku agen Amazon Inspector Classic. Masuk ke instans EC2 Anda yang menjalankan sistem operasi berbasis Windows dan lakukan salah satu prosedur dalam bab ini. Untuk informasi selengkapnya tentang sistem operasi yang didukung Amazon Inspector Classic, lihat. [Amazon Inspector Classic mendukung sistem operasi dan Wilayah](#)

## Important

Agan Amazon Inspector Classic mengandalkan metadata instans Amazon EC2 agar berfungsi dengan benar. Ini mengakses metadata instance menggunakan versi 1 atau versi 2 dari Layanan Metadata Instance (). IMDSv1 or IMDSv2 Lihat [Metadata Instans dan Data Pengguna](#) untuk mempelajari lebih lanjut tentang metadata instans EC2 dan metode akses.

## Note

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

## Topik

- [Memulai atau menghentikan agen Amazon Inspector Classic atau memverifikasi bahwa agen tersebut sedang berjalan](#)
- [Memodifikasi pengaturan agen Amazon Inspector Classic](#)
- [Mengkonfigurasi dukungan proxy untuk agen Amazon Inspector Classic](#)
- [Menghapus instalasi agen Amazon Inspector Classic](#)

## Memulai atau menghentikan agen Amazon Inspector Classic atau memverifikasi bahwa agen tersebut sedang 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 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 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.

## Mengkonfigurasi dukungan proxy untuk agen Amazon Inspector Classic

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://d1wk0tztptsntt1.cloudfront.net/windows/installer/latest/AWSAgentInstall.exe>
2. Buka jendela atau PowerShell jendela prompt 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 proxy, versi agen Amazon Inspector Classic 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 Classic atau memverifikasi bahwa agen tersebut 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 instans EC2 berbasis Windows](#).
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 Classic atau memverifikasi bahwa agen tersebut sedang berjalan](#)). Melihat status agen Anda dan memverifikasi bahwa statusnya menggunakan proksi dikonfigurasi.

## Menghapus instalasi agen Amazon Inspector Classic

Untuk menghapus instalasi agen

1. Masuk ke instans EC2 Anda yang menjalankan sistem operasi berbasis Windows tempat Anda ingin menghapus instalasi agen Amazon Inspector Classic.

### Note

Untuk informasi selengkapnya tentang sistem operasi yang didukung Amazon Inspector Classic, lihat. [Amazon Inspector Classic mendukung sistem operasi dan Wilayah](#)

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 Classic pada sistem operasi berbasis Linux

Topik ini menjelaskan proses yang direkomendasikan untuk memverifikasi validitas skrip instalasi agen Amazon Inspector Classic 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. Hal 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 menentukan bahwa perangkat lunak untuk agen Amazon Inspector Classic diubah atau rusak, **JANGAN** jalankan file instalasi. Alih-alih, hubungi AWS Support.

File agen Amazon Inspector Classic untuk sistem operasi berbasis Linux ditandatangani menggunakan GnuPG, implementasi open source dari standar Pretty Good Privacy (OpenPGP) untuk tanda tangan digital yang aman. GnuPG (juga dikenal sebagai GPG) menyediakan otentikasi dan pemeriksaan 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](#)
- [Mengautentikasi dan mengimpor kunci publik](#)
- [Memverifikasi tanda tangan paket](#)

## 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 terinstal, Anda akan melihat prompt perintah 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 selanjutnya dalam proses ini adalah mengautentikasi kunci publik Amazon Inspector Classic dan menambahkannya sebagai kunci tepercaya di GPG keyring Anda.

Untuk mengautentikasi dan mengimpor kunci publik Amazon Inspector Classic

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+PfHY9bdXAD68yhp2m9NyH3B0zle/MXI
8siNfoRgzDwuWnIaezHwwLWkDw2paRxp1NMQ9qRe8Phq0ewheLrQu95dwDgMcw90
gf9m1iKVHjdVQ9qNH1B20FknPDxMDRHcrlJYDKYCX3+MODEHn1K25tIH2KWezXP
FPSU+TkwjLRzSMYH1L8IwjFUIIi78jQS9a31R/c014zuC5f0VghY1SomLI8irfoD
JSa3csVRujSm0Af9o3beiMR/kNDMpgD0xgiQTu/Kh39c16o8AKe+QKK48kq07hra
h1dpzLbfeZEVU6dWMZt1UksG/zKxuzD6d8vXYH7Z+x09P0PFALQCQMC3WisIKgj
zJEFhXMCCQ3NLC3CeyMq3vP7MbVRBYE7t3d2uDREkZBgIf+mbUYfYPhrzy0qT9Tr
PgwcUvDZuazxuuPzucZG0J5kbptat3DcUpstjdmGAId3JawBbps77qRzda+swr
o9o3jbowgmf0y5ZS6KwvZnC6XyTAKXy2io7mSrAIRECrANrzYzfp5v7uD7w8Dk0X
10rf0m1VufMzAyTu0YQGBWaqKzSB8tCkvFw54PrRuUTcV826XU7SIJNzmNQo58uL
bKyLVBSCVabfs01kECIESq8PT9xMYfQJ421uATHyYUnFTU2TYrCQEab7oQARAQAB
tCdBbWF6b24gSW5zcGVjdG9yIDxpbmNwZWNo3JAYW1hem9uLmNvbT6JAJgEEwEC
ACIFALYDlFEcGwMGCwkIBwMCBhUIAgkKCwQWAgMBAh4BAheAAAoJECR0CWBYNgQY
8yUP/2GpI140f3mKBUISTe0XQLvwiBCHmY+V9f0uKqDTinxssjEMCnz0vsKeCZF/
L35pwNa/ow00Ja8D7sCkKG+8LuyMpcPDyqptLrYPprUWtz2+qLCHgpWsrku7ateF
x4hWS0jUVEHPaBzI9V1NTHsCx9+nbpWQ5Fk+7VJI8hbMDY7NQx6fcse8WT1P/0r/
HIkKzzqQ0aa0f5t9zc5DKwi+dFmJbRUyaq22xs8C81U0DjHunhjHdZ21cnsGk91S
fvuaum9aR4/uVIY0TVWnjC5J3+VlczuYt5FaYrrQ5ov0dm+biTUXwve3X8Q85Nu
DPn0/+zxb7Jz3QCHXnuTbxZTjvvl600i8//uRTnPXjz4wZLwQfibgHmk1++hzND7
w0YA02Js6v5FZQ1LQAod7q2wuA1pq4MroLXzziDfy/9ea8B+tzyxlmNVRpVZY4L1
DOHyqGQhpkyV3drjjNZ1Eofwbfu7m60DwsgM15ynzhKk1JzwPJFFB3mMc7qLi+qX
MJtEX8KJ/iVUQStHHAG7daL1bXPWSI3BRuaHsWbBGQ/mcHBgUU0QJyEp5LADg9Fs
VP55gWtF7pIqifiqlcfcgG00v+A3NmVbmiGKSZvfrc5KsF/k43rCGqDx1RV6gZvyI
Lf09+3sEi1NrsMib0KRLDeBt3EuDsaBZg0kqjDhgJUesqiCy
=iEhB
-----END PGP PUBLIC KEY BLOCK-----
```

2. Pada prompt perintah di direktori tempat Anda menyimpan `inspector.gpg`, gunakan perintah berikut untuk mengimpor kunci publik Amazon Inspector Classic ke 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 tidak cocok, jangan instal skrip instalasi agen Amazon Inspector Classic, dan hubungi AWS Support.

## Memverifikasi tanda tangan paket

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

Untuk memverifikasi tanda tangan skrip instalasi

1. Pada prompt perintah, 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 prompt perintah di direktori tempat Anda menyimpan `install.sig` dan file instalasi Amazon Inspector Classic. Kedua file tersebut harus ada.

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

Output-nya 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 tanda tangan telah berhasil diverifikasi, dan Anda dapat melanjutkan untuk menjalankan skrip instalasi Amazon Inspector Classic.

Jika output berisi 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 pada keyakinan Anda bahwa Anda memiliki kunci publik otentik untuk Amazon Inspector Classic. 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 ada kunci tepercaya yang ditemukan. 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 Classic pada sistem operasi berbasis Windows

Topik ini menjelaskan proses yang disarankan untuk memverifikasi validitas skrip instalasi agen Amazon Inspector Classic 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. Hal 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 menentukan bahwa perangkat lunak untuk agen Amazon Inspector Classic diubah atau rusak, JANGAN jalankan 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 Classic

Anda dapat menggunakan Amazon Inspector Classic untuk mengevaluasi apakah target AWS penilaian Anda (kumpulan AWS sumber daya Anda) 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](#)
- [Batas target penilaian Amazon Inspector Classic](#)
- [Membuat target penilaian](#)
- [Menghapus target penilaian](#)

## Menandai sumber daya untuk membuat target penilaian

Untuk membuat target penilaian Amazon Inspector Classic untuk menilai, Anda mulai dengan menandai instans EC2 yang ingin Anda sertakan dalam target Anda. Tag adalah kata atau frasa yang bertindak sebagai metadata untuk mengidentifikasi dan mengatur instance Anda dan sumber daya lainnya. AWS Amazon Inspector Classic menggunakan tag yang Anda buat untuk mengidentifikasi instance milik target Anda.

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

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

Saat menandai instans EC2 untuk membangun target penilaian, Anda dapat membuat kunci tag kustom sendiri atau menggunakan kunci tag yang dibuat oleh orang lain di akun yang sama AWS . Anda juga dapat menggunakan tombol tag yang dibuat AWS secara otomatis. Misalnya, AWS secara otomatis membuat kunci tag 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 Classic


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

## Membuat target penilaian

Anda dapat menggunakan konsol Amazon Inspector Classic untuk membuat target penilaian.


Untuk membuat target penilaian

1. Masuk ke Konsol Manajemen AWS dan buka konsol Amazon Inspector Classic di. <https://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 tindakan berikut:
  - Untuk menyertakan semua instans EC2 di AWS akun 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 tombol Install Agents with Run Command untuk menginstal agen pada semua instans EC2 di 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 di Beberapa Instans EC2 Menggunakan Perintah Jalankan Systems Manager.](#)

### 6. Pilih 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-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.

## 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 keparahan Tinggi.

- [Tingkat keparahan untuk aturan di Amazon Inspector Classic](#)
- [Aturan paket di Amazon Inspector Classic](#)

## 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 keparahannya:

- 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 kelola, ACLs IGWs, 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 menyertakan paket ini dalam proses penilaian Anda, Anda dapat menerapkan pemeriksaan keamanan jaringan terperinci tanpa harus menginstal pemindai dan mengirim paket, yang rumit dan mahal untuk dirawat, terutama di seluruh koneksi peering VPC dan VPNs

#### Important

Agan 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](#)
- [Gateway Internet \(\) IGWs](#)
- [Daftar Kontrol Akses Jaringan \(ACLs\)](#)
- [Tabel Rute](#)

- [Grup Keamanan \(SGs\)](#)
- [Subnet](#)
- [Awan Pribadi Virtual \(VPCs\)](#)
- [Gateway Pribadi Virtual \(\) VGWs](#)
- [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

## UnrecognizedPortWithListener

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 EC2 instance dalam target penilaian Anda terkena kerentanan dan eksposur umum (). CVEs 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 mengurangnya.

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	$\geq 5$	Kritis atau Penting
Sedang	$< 5$ and $\geq 2,1$	Sedang
Rendah	$< 2.1$ and $\geq 0.8$	Rendah
Informasi	$< 0,8$	N/A

Aturan yang disertakan dalam paket ini membantu Anda menilai apakah EC2 instans Anda terpapar CVEs dalam daftar regional berikut:

- [AS Timur \(Virginia N.\)](#)
- [AS Timur \(Ohio\)](#)
- [AS Barat \(California N.\)](#)
- [AS Barat \(Oregon\)](#)
- [UE \(Irlandia\)](#)
- [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 CVEs yang disertakan dalam penilaian berjalan yang terjadi pada saat yang sama ketika daftar ini diambil.

Lihat informasi yang lebih lengkap di [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/](https://benchmarks.cisecurity.org/) (pendaftaran gratis diperlukan). Dokumen patokan menyediakan informasi detail tentang patokan CIS ini, tingkat kepelikan, dan cara menguranginya.

Lihat informasi yang lebih lengkap di [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](#)
- [Mendukung SSH versi 2 saja](#)
- [Menonaktifkan autentikasi kata sandi Melalui SSH](#)
- [Mengonfigurasi usia maksimum kata sandi](#)
- [Mengonfigurasi panjang minimum kata sandi](#)
- [Mengonfigurasi kompleksitas kata sandi](#)
- [Mengaktifkan ASLR](#)
- [Mengaktifkan DEP](#)
- [Mengonfigurasi izin untuk direktori sistem](#)

## Menonaktifkan login root melalui SSH

Aturan ini membantu menentukan apakah daemon SSH dikonfigurasi untuk mengizinkan masuk ke instans EC2 Anda sebagai [root](#).

### Keparahan

[Sedang](#)

### Menemukan

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.

## Keparahan

[Sedang](#)

## Menemukan

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.

## Keparahan

[Sedang](#)

## Menemukan

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 lebih lanjut, lihat <https://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.

Keparahan

[Sedang](#)

Menemukan

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.

Keparahan

[Sedang](#)

Menemukan

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 di file `pwquality.conf`: `minlen`. 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 `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.

Keparahan

[Sedang](#)

Menemukan

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.

Keparahan

[Sedang](#)

Menemukan

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.

Keparahan

[Sedang](#)

Menemukan

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.

### Keparahan

[Tinggi](#)

### Menemukan

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, konfigurasi 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 sedang 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](#)
- [Batas templat penilaian Amazon Inspector Classic](#)
- [Membuat templat penilaian](#)
- [Menghapus templat penilaian](#)
- [Penilaian berjalan](#)
- [Penilaian Amazon Inspector Classic menjalankan batas](#)
- [Mengatur penilaian berjalan otomatis melalui fungsi Lambda](#)
- [Menyiapkan topik SNS untuk notifikasi Amazon Inspector Classic](#)

## 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 nilai 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 Konsol Manajemen AWS 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 Konsol Manajemen AWS, dan buka [AWS Lambda konsol](#).
2. Di panel navigasi, pilih Dasbor atau Fungsi, lalu pilih Buat Fungsi Lambda.
3. Pada halaman Buat fungsi, pilih Jelajahi repositori aplikasi tanpa server, lalu masukkan **inspector** di bidang pencarian.
4. Pilih inspector-scheduled-runcetak biru.
5. Pada halaman Tinjau, konfigurasi, 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:

JSON

```
{
  "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 Konsol Manajemen AWS 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 EC2 contoh di mana 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 berjalan dengan menggunakan API [DeleteAssessmentRun](#).

# Laporan penilaian

Laporan penilaian Amazon Inspector Classic adalah dokumen yang merinci apa yang diuji dalam proses penilaian 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 proses penilaian yang terjadi setelah 25 April 2017, yaitu saat laporan penilaian di Amazon Inspector Classic tersedia.

Anda dapat melihat jenis laporan penilaian berikut:

- Laporan temuan – laporan ini berisi informasi berikut:
  - Ringkasan penilaian
  - EC2 contoh yang dievaluasi selama penilaian dijalankan
  - Paket aturan yang termasuk dalam penilaian berjalan
  - Informasi terperinci tentang setiap temuan, termasuk semua EC2 contoh 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

Mulai 24 Maret 2025, laporan penilaian tidak akan lagi menyertakan informasi tingkat keparahan untuk temuan jangkauan jaringan. Informasi ini tersedia di konsol Amazon Inspector.


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 individual. 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 Classic

Pengecualian adalah hasil dari penilaian Amazon Inspector Classic. Pengecualian menunjukkan pemeriksaan keamanan mana yang tidak dapat diselesaikan dan cara menyelesaikan masalah. Misalnya, masalah dapat disebabkan oleh tidak adanya agen pada EC2 instance target yang ditentukan, penggunaan sistem operasi yang tidak didukung, atau kesalahan yang tidak terduga.

Anda dapat melihat pengecualian di halaman Penilaian berjalan di konsol. Untuk informasi selengkapnya, lihat [Melihat pengecualian pasca-penilaian](#).

Untuk menghindari AWS biaya yang tidak perlu, Amazon Inspector Classic memungkinkan Anda untuk melihat 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 Classic tersedia. Namun, pratinjau pengecualian tersedia untuk semua templat penilaian pada tanggal berapa pun.

## Topik

- [Jenis pengecualian](#)
- [Pratinjau pengecualian](#)
- [Melihat pengecualian pasca-penilaian](#)

## Jenis pengecualian

Amazon Inspector Classic dapat menghasilkan jenis pengecualian berikut.

Jenis Pengecualian	Deskripsi	Rekomendasi									
Tidak ada	Tidak ada EC2	Periksa apakah tag									

Jenis Pengecualian	Deskripsi	Rekomendasi									
instan dalam target	contoh dengan tag yang ditentukan dalam target penilaian.	di target penilaian Anda cocok dengan tag EC2 instance target Anda.									
Agen sudah berjalan	Jalankan penilaian sudah berlangsung pada EC2 instance target.	Tunggu hingga penilaian saat ini berjalan pada EC2 instance target selesai.									

Jenis Pengecualian	Deskripsi	Rekomendasi									
Agen tidak ditemukan	Agen Amazon Inspector Classic tidak ditemukan pada instance target EC2 .	Instal atau instal ulang agen Amazon Inspector Classic pada instance target. EC2 Untuk informasi selengkapnya, lihat <a href="#">Menginstal agen Amazon Inspector Classic.</a>									

Jenis Pengecualian	Deskripsi	Rekomendasi									
Agen tidak sehat	Agen Amazon Inspector Classic pada EC2 instance target berada dalam keadaan tidak sehat.	Periksa status agen Amazon Inspector Classic pada instance ini dan ambil tindakan yang diperlukan. Untuk informasi lebih lanjut, lihat <a href="#">Agen Inspector</a> .									

Jenis Pengecualian	Deskripsi	Rekomendasi								
Versi OS yang tidak didukung	Sistem operasi EC2 instans target tidak didukung untuk penilaian Amazon Inspector Classic.	Hapus EC2 instance target dari target penilaian, atau buat target yang tidak menyertakan instance ini. Untuk mengetahui daftar sistem operasi yang didukung, lihat Sistem Operasi <a href="#">dan Wilayah yang Didukung Amazon Inspector Classic.</a>								

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 aturar yang tidak didukung oleh OS	Sistem operasi EC2 instance target tidak didukung oleh paket aturan yang disertakan dalam template penilaian.	<p>Buat template penilaian tanpa paket aturan yang bertentangan atau hapus EC2 instance target dari template penilaian.</p> <p>Untuk daftar paket aturan yang didukung oleh sistem operasi, lihat <a href="#">Ketersediaan Paket Aturan yang Tersedia di Seluruh Sistem Operasi</a></p>									

Jenis Pengecualian	Deskripsi	Rekomendasi									
		<a href="#">yang Didukung.</a>									
Kesalahan evaluasi aturan untuk instansi tungg	Kesalahan internal telah menyebabkan kegagalan evaluasi aturan untuk instans ini.	Cobalah untuk menjalankan penilaian Anda lagi. Hubungi <a href="#">support</a> 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 <a href="#">support</a> jika pengecualian tetap ada saat Anda menjalankan kembali penilaian.									

Jenis Pengecualian	Deskripsi	Rekomendasi									
Kesalahan Keterjangkauan Jaringan – 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 <a href="#">support</a> jika pengecualian tetap ada saat Anda menjalankan kembali penilaian.									

Jenis Pengecualian	Deskripsi	Rekomendasi									
Kesalahan Keterjaringan – Jaringan intern melalu Applicon Load Balan	Kesalahan internal telah menyebabkan kegagalan evaluasi Keterjaringan Jaringan pemeriksa port yang dapat dijangkau dari internet melalui Applicati on Load Balancer. Anda mungkin mendapatk an temuan untuk jenis Keterjang kauan Jaringan lainnya.	Cobalah untuk menjalank an penilaian lagi. Hubungi <a href="#">support</a> jika pengecualian tetap ada saat Anda menjalank an kembali penilaian.									

Jenis Pengecualian	Deskripsi	Rekomendasi									
Kesalahan Keterjangkauan Jaringan – intern melalu penye bebar Elastic Load Balan	Kesalahan internal telah menyebabkan kegagalan evaluasi Keterjangkauan Jaringan pada pemeriksa port yang dapat dijangkau dari internet melalui penyeimbangan beban Elastic Load Balancing. Anda mungkin mendapatkan temuan untuk jenis Keterjangkauan	Cobalah untuk menjalankan penilaian lagi. Hubungi <a href="#">support</a> 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 <a href="#">support</a> jika pengecualian tetap ada saat Anda menjalankan kembali penilaian.									

Jenis Pengecualian	Deskripsi	Rekomendasi								
Kesalahan Jaringan - AWS Direct Connect	Kesalahan internal telah menyebabkan an evaluasi Network Reachability gagal pada pemeriksaan port yang dapat dijangkau . AWS Direct Connect Anda mungkin mendapatkan temuan untuk jenis Keterjangkauan Jaringan lainnya.	Cobalah untuk menjalankan penilaian lagi. Hubungi <a href="#">support</a> jika pengecualian tetap ada saat Anda menjalankan kembali penilaian.								

Jenis Pengecualian	Deskripsi	Rekomendasi									
Kesalahan Keterjaringan – peerir 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 <a href="#">support</a> jika pengecualian tetap ada saat Anda menjalankan kembali penilaian.									

## Pratinjau pengecualian

Amazon Inspector Classic memungkinkan Anda melihat pratinjau kemungkinan pengecualian sebelum menjalankan penilaian.

Untuk melakukan pratinjau pengecualian penilaian

1. Masuk ke Konsol Manajemen AWS dan buka konsol Amazon Inspector Classic di. <https://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 ke Konsol Manajemen AWS dan buka konsol Amazon Inspector Classic di. <https://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 disertakan 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	Usang
Amazon Linux 2018,	Didukung	Didukung	Didukung	Didukung	Usang
Amazon Linux 2017,	Didukung	Didukung	Didukung	Didukung	Usang

Sistem Operasi yang Didukung	Kelemahan dan Eksposur Umum	Patokan CIS	Keterjangkauan Jaringan	Praktik Terbaik Keamanan	Analisis Perilaku Waktu Aktif
Amazon Linux 2017,	Didukung	Didukung	Didukung	Didukung	Usang
Amazon Linux 2016,	Didukung	Didukung	Didukung	Didukung	Usang
Amazon Linux 2016,	Didukung	Didukung	Didukung	Didukung	Usang
Amazon Linux 2015,	Didukung	Didukung	Didukung	Didukung	Usang
Amazon Linux 2015,	Didukung	Didukung	Didukung	Didukung	Usang
Amazon Linux 2014,	Didukung		Didukung	Didukung	
Amazon Linux 2014,	Didukung		Didukung	Didukung	
Amazon Linux 2013,	Didukung		Didukung	Didukung	

Sistem Operasi yang Didukung	Kelemahan dan Eksposur Umum	Patokan CIS	Keterjangkauan Jaringan	Praktik Terbaik Keamanan	Analisis Perilaku Waktu Aktif
Amazon Linux 2013,	Didukung		Didukung	Didukung	
Amazon Linux 2012,	Didukung		Didukung	Didukung	
Amazon Linux 2012,	Didukung		Didukung	Didukung	
Amazon Linux 2012,	Didukung		Didukung	Didukung	
Ubuntu 20.04 LTS	Didukung		Didukung	Didukung	
Ubuntu 18.04 LTS	Didukung	Didukung	Didukung	Didukung	Usang
Ubuntu 16.04 LTS	Didukung	Didukung	Didukung	Didukung	Usang
Ubuntu 14.04 LTS	Didukung	Didukung	Didukung	Didukung	Usang

Sistem Operasi yang Didukung	Kelemahan dan Eksposur Umum	Patokan CIS	Keterjangkauan Jaringan	Praktik Terbaik Keamanan	Analisis Perilaku Waktu Aktif
Debian 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	Usang
CentOS 7.6 - 7.X	Didukung	Didukung	Didukung	Didukung	

Sistem Operasi yang Didukung	Kelemahan dan Eksposur Umum	Patokan CIS	Keterjangkauan Jaringan	Praktik Terbaik Keamanan	Analisis Perilaku Waktu Aktif
CentOS 6.2 - 6.9, 7.2 - 7.5	Didukung	Didukung	Didukung	Didukung	Usang
Windows Server 2019 Base	Didukung		Didukung		
Windows Server 2016 Base	Didukung	Didukung	Didukung		Usang
Windows Server 2012 R2	Didukung	Didukung	Didukung		Usang
Windows Server 2012	Didukung	Didukung	Didukung		Usang
Windows Server 2008 R2	Didukung	Didukung	Didukung		Usang

# Mencatat panggilan API Amazon Inspector Classic dengan AWS CloudTrail

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 panggilan API untuk Amazon Inspector Classic sebagai peristiwa, termasuk panggilan dari konsol Amazon Inspector Classic dan panggilan kode ke operasi Amazon Inspector Classic API. Jika Anda membuat jejak, Anda dapat mengaktifkan pengiriman CloudTrail acara secara terus menerus ke bucket Amazon S3, termasuk acara untuk Amazon Inspector Classic. Jika Anda tidak mengonfigurasi jejak, Anda masih dapat melihat peristiwa terbaru di CloudTrail konsol dalam Riwayat acara. Dengan menggunakan informasi yang dikumpulkan oleh CloudTrail, Anda dapat menentukan permintaan yang dibuat ke Amazon Inspector Classic, alamat IP tempat permintaan dibuat, siapa yang membuat permintaan, kapan dibuat, dan banyak lagi.

Untuk mempelajari selengkapnya CloudTrail, lihat [Panduan AWS CloudTrail Pengguna](#). Untuk daftar lengkap operasi Amazon Inspector Classic API, lihat [Tindakan](#) di Referensi API Amazon Inspector Classic.

## Informasi Amazon Inspector Classic di CloudTrail

CloudTrail diaktifkan di AWS akun Anda saat Anda membuat akun. Ketika aktivitas terjadi di Amazon Inspector Classic, aktivitas tersebut direkam dalam suatu CloudTrail peristiwa bersama dengan peristiwa AWS layanan lainnya dalam riwayat Acara. Anda dapat melihat, mencari, dan mengunduh peristiwa terbaru di akun AWS. Untuk informasi selengkapnya, lihat [Melihat Acara dengan Riwayat CloudTrail Acara](#).

Untuk catatan peristiwa yang sedang berlangsung di AWS akun Anda, termasuk acara untuk Amazon Inspector Classic, buat jejak. Jejak memungkinkan CloudTrail untuk mengirimkan 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 AWS partisi dan mengirimkan file log ke bucket Amazon S3 yang Anda tentukan. Selain itu, Anda dapat mengonfigurasi AWS layanan lain untuk menganalisis lebih lanjut dan menindaklanjuti data peristiwa yang dikumpulkan dalam CloudTrail log. Untuk informasi selengkapnya, lihat berikut:

- [Gambaran Umum untuk Membuat Jejak](#)
- [CloudTrail Layanan dan Integrasi yang Didukung](#)

- [Mengkonfigurasi Notifikasi Amazon SNS untuk CloudTrail](#)
- [Menerima File CloudTrail Log dari Beberapa Wilayah](#) dan [Menerima File CloudTrail Log dari Beberapa Akun](#)

CloudTrail mencatat semua operasi Amazon Inspector Classic, termasuk operasi hanya-baca, seperti `ListAssessmentRuns` dan, dan operasi manajemen `DescribeAssessmentTargets`, seperti dan `AddAttributesToFindings` `CreateAssessmentTemplate`

#### Note

CloudTrail hanya mencatat informasi permintaan operasi hanya-baca Amazon Inspector Classic. Informasi permintaan dan respons dicatat untuk semua operasi Amazon Inspector Classic lainnya.

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

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

Untuk informasi selengkapnya, lihat Elemen [CloudTrail UserIdentity](#).

## Memahami entri file log Amazon Inspector Classic

Trail adalah konfigurasi yang memungkinkan pengiriman peristiwa sebagai file log ke bucket Amazon S3 yang Anda tentukan. CloudTrail file log berisi satu atau lebih entri log. Peristiwa mewakili permintaan tunggal dari sumber manapun dan mencakup informasi tentang tindakan yang diminta, tanggal dan waktu tindakan, dan parameter permintaan lainnya. CloudTrail file log bukanlah jejak tumpukan yang diurutkan dari panggilan API publik, jadi file tersebut tidak muncul dalam urutan tertentu.

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan operasi Amazon Inspector `CreateResourceGroup` Classic:

```
{
  "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-oc1RMp8B"
  },
  "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 Amazon CloudWatch, yang mengumpulkan dan memproses data mentah menjadi metrik hampir real-time yang dapat dibaca. Secara default, Amazon Inspector Classic mengirimkan data metrik ke CloudWatch dalam periode 5 menit. Anda dapat menggunakan, API Konsol Manajemen AWS AWS CLI, atau API untuk melihat metrik yang dikirimkan Amazon Inspector Classic. CloudWatch

Untuk informasi selengkapnya tentang Amazon CloudWatch, lihat [Panduan CloudWatch Pengguna Amazon](#).

## 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
TotalAssessmentRun Findings	Jumlah temuan untuk templat ini

### Metrik agregat

Metrik	Deskripsi
TotalAssessmentRuns	Jumlah penilaian berjalan di AWS akun ini

# Mengkonfigurasi Amazon Inspector Classic menggunakan AWS CloudFormation

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

- [AWS::Inspector::AssessmentTarget](#)
- [AWS::Inspector::AssessmentTemplate](#)
- [AWS::Inspector::ResourceGroup](#)

## Important

Untuk daftar paket aturan Amazon Inspector Classic di AWS Wilayah yang didukung, lihat ARNs [Amazon Inspector Classic ARNS untuk paket aturan](#)

# Integrasi dengan AWS Security Hub CSPM

[AWS Security Hub CSPM](#) memberi Anda pandangan komprehensif tentang keadaan keamanan Anda AWS dan membantu Anda memeriksa lingkungan Anda terhadap standar industri keamanan dan praktik terbaik. Security Hub CSPM mengumpulkan data keamanan dari berbagai AWS akun, 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 CSPM memungkinkan Anda mengirim temuan dari Amazon Inspector ke Security Hub CSPM. Security Hub CSPM kemudian dapat memasukkan temuan-temuan tersebut dalam analisisnya tentang postur keamanan Anda.

## Daftar Isi

- [Bagaimana Amazon Inspector mengirimkan temuan ke Security Hub CSPM](#)
  - [Jenis temuan yang dikirimkan Amazon Inspector](#)
  - [Latensi untuk mengirim temuan](#)
  - [Mencoba lagi saat Security Hub CSPM tidak tersedia](#)
  - [Memperbarui temuan yang ada di Security Hub CSPM](#)
- [Temuan umum dari Amazon Inspector](#)
- [Mengaktifkan dan mengonfigurasi integrasi](#)
- [Bagaimana cara menghentikan pengiriman temuan](#)

## Bagaimana Amazon Inspector mengirimkan temuan ke Security Hub CSPM

Di Security Hub CSPM, masalah keamanan dilacak sebagai temuan. Beberapa temuan berasal dari masalah yang terdeteksi oleh AWS layanan lain atau oleh mitra pihak ketiga. Security Hub CSPM juga memiliki seperangkat aturan yang digunakan untuk mendeteksi masalah keamanan dan menghasilkan temuan.

Security Hub CSPM menyediakan alat untuk mengelola temuan dari seluruh sumber ini. 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 CSPM menggunakan format JSON standar yang disebut AWS Security Finding Format (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 AWS layanan yang mengirimkan temuan ke Security Hub CSPM.

## Jenis temuan yang dikirimkan Amazon Inspector

Amazon Inspector mengirimkan semua temuan yang dihasilkannya ke Security Hub CSPM.

Amazon Inspector mengirimkan temuan ke Security Hub CSPM menggunakan Security [Finding Format \(AWS ASFF\)](#). Dalam ASFF, bidang Types menyediakan jenis temuan. Temuan dari Amazon Inspector dapat memiliki nilai berikut untuk Types.

- Perangkat Lunak dan Konfigurasi Checks/Vulnerabilities/CVE
- Perangkat Lunak dan Konfigurasi Checks/AWS Keamanan Jangkauan Terbaik Practices/Network
- Perangkat Lunak dan Konfigurasi Checks/Industry dan Tolok Ukur Pengerasan Standards/CIS Host Regulatory

## Latensi untuk mengirim temuan

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

## Mencoba lagi saat Security Hub CSPM tidak tersedia

Jika Security Hub CSPM tidak tersedia, Amazon Inspector mencoba mengirim ulang temuan sampai diterima.

## Memperbarui temuan yang ada di Security Hub CSPM

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

## Temuan umum dari Amazon Inspector

Amazon Inspector mengirimkan temuan ke Security Hub CSPM menggunakan [AWS Security Finding Format](#) (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": "kubect1"
      },
      "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 CSPM, Anda harus mengaktifkan Security Hub CSPM. Untuk informasi tentang cara mengaktifkan CSPM Security Hub, lihat [Menyiapkan Security Hub](#) di AWS Security Hub Panduan Pengguna.

Saat Anda mengaktifkan Amazon Inspector dan Security Hub CSPM, integrasi diaktifkan secara otomatis. Amazon Inspector mulai mengirimkan temuan ke Security Hub CSPM.

## Bagaimana cara menghentikan pengiriman temuan

Untuk menghentikan pengiriman temuan ke Security Hub CSPM, Anda dapat menggunakan konsol CSPM 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 .

# Amazon Inspector Klasik ARNs

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

## Daftar Isi

- [ARNs untuk sumber daya Amazon Inspector Classic](#)
- [Amazon Inspector Classic ARNs untuk paket aturan](#)
  - [AS Timur \(Ohio\)](#)
  - [AS Timur \(Virginia Utara\)](#)
  - [AS Barat \(California Utara\)](#)
  - [AS Barat \(Oregon\)](#)
  - [Asia Pasifik \(Mumbai\)](#)
  - [Asia Pasifik \(Seoul\)](#)
  - [Asia Pasifik \(Sydney\)](#)
  - [Asia Pasifik \(Tokyo\)](#)
  - [Eropa \(Frankfurt\)](#)
  - [Eropa \(Irlandia\)](#)
  - [Eropa \(London\)](#)
  - [Eropa \(Stockholm\)](#)
  - [AWS GovCloud \(AS-Timur\)](#)
  - [AWS GovCloud \(AS-Barat\)](#)

## ARNs untuk sumber daya Amazon Inspector Classic

Di Amazon Inspector Classic, sumber daya utama adalah grup sumber daya, target penilaian, templat penilaian, proses penilaian, dan temuan. Sumber daya ini memiliki Nama Sumber Daya Amazon (ARNs) unik yang terkait dengannya, seperti yang ditunjukkan pada tabel berikut.

Jenis Sumber Daya	Format ARN
Grup sumber daya	arn:aws:inspector: <i>region:account-id</i> :resource group/ <i>ID</i>
Target penilaian	arn:aws:inspector: <i>region:account-id</i> :target/ <i>ID</i>
Templat penilaian	arn:aws:inspector: <i>region:account-id</i> :target/ <i>ID</i> :template: <i>ID</i>
Penilaian berjalan	arn:aws:inspector: <i>region:account-id</i> :target/ <i>ID</i> /template/ <i>ID</i> /run/ <i>ID</i>
Temuan	arn:aws:inspector: <i>region:account-id</i> :target/ <i>ID</i> /template/ <i>ID</i> /run/ <i>ID</i> /finding/ <i>ID</i>

## Amazon Inspector Classic ARNS untuk paket aturan

Tabel berikut menunjukkan paket aturan ARNs Amazon Inspector Classic di semua Wilayah yang didukung.

### Topik

- [AS Timur \(Ohio\)](#)
- [AS Timur \(Virginia Utara\)](#)
- [AS Barat \(California Utara\)](#)
- [AS Barat \(Oregon\)](#)
- [Asia Pasifik \(Mumbai\)](#)
- [Asia Pasifik \(Seoul\)](#)
- [Asia Pasifik \(Sydney\)](#)
- [Asia Pasifik \(Tokyo\)](#)
- [Eropa \(Frankfurt\)](#)
- [Eropa \(Irlandia\)](#)
- [Eropa \(London\)](#)
- [Eropa \(Stockholm\)](#)

- [AWS GovCloud \(AS-Timur\)](#)
- [AWS GovCloud \(AS-Barat\)](#)

## AS Timur (Ohio)

Nama Paket Aturan	ARN
Kelemahan dan Eksposur Umum	<code>arn:aws:inspector:us-east-2:64665939:0643:rulespackage/0-JnA8Zp85</code>
Patokan Konfigurasi Keamanan Sistem Operasi CIS	<code>arn:aws:inspector:us-east-2:64665939:0643:rulespackage/0-m8r61nnh</code>
Keterjangkauan Jaringan	<code>arn:aws:inspector:us-east-2:64665939:0643:rulespackage/0-cE4kTR30</code>
Praktik Terbaik Keamanan	<code>arn:aws:inspector:us-east-2:64665939:0643:rulespackage/0-AxKmMHPX</code>

## AS Timur (Virginia Utara)

Nama Paket Aturan	ARN
Kelemahan dan Eksposur Umum	<code>arn:aws:inspector:us-east-1:31611246:3485:rulespackage/0-gEjTy7T7</code>

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

## AS Barat (California Utara)

Nama Paket Aturan	ARN
Kelemahan dan Eksposur Umum	arn:aws:inspector:us-west-1:166987590008:rulespackage/0-TKgzoV0a
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-1:16698759 0008:rulespackage/ 0-byoQRFYm

## AS Barat (Oregon)

Nama Paket Aturan	ARN
Kelemahan dan Eksposur Umum	arn:aws:inspector: us-west-2:75805808 6616:rulespackage/ 0-9hgA516p
Patokan Konfigurasi Keamanan Sistem Operasi CIS	arn:aws:inspector: us-west-2:75805808 6616:rulespackage/ 0-H5hpSawc
Keterjangkauan Jaringan	arn:aws:inspector: us-west-2:75805808 6616:rulespackage/ 0-rD1z6dp1
Praktik Terbaik Keamanan	arn:aws:inspector: us-west-2:75805808 6616:rulespackage/ 0-JJ0tZiqQ

## Asia Pasifik (Mumbai)

Nama Paket Aturan	ARN
Kelemahan dan Eksposur Umum	<code>arn:aws:inspector:ap-south-1:162588757376:rulespackage/0-LqnJE9d0</code>
Patokan Konfigurasi Keamanan Sistem Operasi CIS	<code>arn:aws:inspector:ap-south-1:162588757376:rulespackage/0-PSU1X14m</code>
Keterjangkauan Jaringan	<code>arn:aws:inspector:ap-south-1:162588757376:rulespackage/0-YxKfjFu1</code>
Praktik Terbaik Keamanan	<code>arn:aws:inspector:ap-south-1:162588757376:rulespackage/0-fs0IZZBj</code>

## Asia Pasifik (Seoul)

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

Nama Paket Aturan	ARN
	946625049:rulespac kage/0-T9srhg1z
Keterjangkauan Jaringan	arn:aws:inspector: ap-northeast-2:526 946625049:rulespac kage/0-s30mLzhL
Praktik Terbaik Keamanan	arn:aws:inspector: ap-northeast-2:526 946625049:rulespac kage/0-2WRpmi4n

## Asia Pasifik (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 Pasifik (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

## Eropa (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

## Eropa (Irlandia)

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-1:35755712 9151:rulespackage/ 0-SnojL3Z6

## Eropa (London)

Nama Paket Aturan	ARN
Kelemahan dan Eksposur Umum	arn:aws:inspector: eu-west-2:14683893 6955:rulespackage/ 0-kZGCqcE1
Patokan Konfigurasi Keamanan Sistem Operasi CIS	arn:aws:inspector: eu-west-2:14683893 6955:rulespackage/ 0-IeCjwf1W
Keterjangkauan Jaringan	arn:aws:inspector: eu-west-2:14683893 6955:rulespackage/ 0-AizSYyNq
Praktik Terbaik Keamanan	arn:aws:inspector: eu-west-2:14683893 6955:rulespackage/ 0-XApUiSaP

## Eropa (Stockholm)

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

## AWS GovCloud (AS-Timur)

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

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 (AS-Barat)

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-Ac4CF0uc
Praktik Terbaik Keamanan	arn:aws-us-gov:inspector:us-gov-west-1:850862329162:rulespackage/0-r0TGqe5G

# Riwayat dokumen

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

Perubahan	Deskripsi	Tanggal
<a href="#">Pemberitahuan akhir dukungan</a>	Pemberitahuan akhir dukungan: Pada 20 Mei 2026, AWS akan mengakhiri dukungan untuk Amazon Inspector Classic. Setelah 20 Mei 2026, Anda tidak akan lagi dapat mengakses konsol Amazon Inspector Classic atau sumber daya Amazon Inspector Classic. Untuk informasi selengkapnya, lihat <a href="#">bagian akhir dukungan Amazon Inspector Classic</a> .	Mei 20, 2025
<a href="#">Praktik terbaik keamanan yang diperbarui untuk kata sandi</a>	Persyaratan praktik terbaik keamanan Amazon Inspector Classic untuk panjang kata sandi instans EC2 dan kompleksitas kata sandi telah diperbarui. Lihat <a href="#">Mengonfigurasi panjang minimum kata sandi</a> dan <a href="#">Mengonfigurasi kompleksitas kata sandi</a>	Selasa, 08 Maret 2021
<a href="#">Menambahkan dukungan untuk versi sistem operasi yang lebih baru</a>	Amazon Inspector Classic sekarang mendukung versi sistem operasi berikut: Ubuntu 20.4 LTS, Debian 10.x, RHEL 8.x, dan Windows Server 2019 Base.	15 Oktober 2020

<a href="#">Informasi keamanan dikonsolidasikan ke dalam babak keamanan baru</a>	Informasi keamanan untuk Amazon Inspector Classic, termasuk informasi tentang pengelolaan identitas dan manajemen akses, dikonsolidasikan ke dalam bagian keamanan. Lihat <a href="#">Keamanan di Amazon Inspector Classic</a> .	7 April 2020
<a href="#">Dokumentasi yang diperbarui untuk menghapus dukungan untuk paket aturan Analisis Perilaku Runtime.</a>	Beberapa topik diperbarui untuk menghapus informasi tentang paket aturan Analisis Perilaku Waktu Aktif, yang tidak lagi didukung.	Selasa, 05 September 2019
<a href="#">Ditambahkan OS Support</a>	Menambahkan dukungan Amazon Inspector Classic untuk CentOS 7.6. Untuk informasi selengkapnya, lihat <a href="#">Amazon Inspector Classic Supported Operating Systems and Regions and Rules Packages Availability Across Supported Operating Systems</a> .	Selasa, 03 Desember 2018
<a href="#">Konten baru</a>	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 <a href="#">Keterjangkauan Jaringan</a> .	9 November 2018

<a href="#">Ditambahkan OS Support</a>	Menambahkan dukungan Amazon Inspector Classic untuk RHEL 7.6. Untuk informasi selengkapnya, lihat <a href="#">Amazon Inspector Classic Supported Operating Systems and Regions and Rules Packages Availability Across Supported Operating Systems</a> .	30 Oktober 2018
<a href="#">Menambahkan dukungan OS</a>	Dukungan ditambahkan untuk berbagai sistem operasi ke paket aturan Patokan CIS. Untuk informasi lebih lanjut, lihat <a href="#">Patokan Pusat Keamanan Internet (CIS)</a> dan <a href="#">Ketersediaan Paket Aturan di Seluruh Sistem Operasi yang Didukung</a> .	13 Agustus 2018
<a href="#">Ditambahkan dukungan Wilayah</a>	Dukungan Wilayah ditambahkan untuk AWS GovCloud (US).	13 Juni 2018

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

Ubah	Deskripsi	Tanggal
Konten baru	Ditambahkan kemampuan untuk menargetkan semua instans Amazon EC2 di suatu akun. Untuk informasi selengkapnya, lihat <a href="#">Target penilaian Amazon Inspector Classic</a> .	24 Mei 2018

Ubah	Deskripsi	Tanggal
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 Amazon Inspector Classic melalui konsol.	30 April 2018
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

Ubah	Deskripsi	Tanggal
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
Konten baru	Ditambahkan fitur berikut: <ul style="list-style-type: none"><li>• Penggunaan peran tertaut layanan</li><li>• Agen Amazon Inspector Classic AMI tersedia di Marketplace AWS</li><li>• Templat Amazon Inspector Classic CloudFormation</li></ul>	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

Ubah	Deskripsi	Tanggal
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
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: <ul style="list-style-type: none"><li>• Dukungan Amazon Inspector Classic untuk Ubuntu 16.04.</li><li>• Ketersediaan cetak biru Lambda untuk mengotomatiskan operasi Amazon Inspector Classic.</li></ul>	Selasa, 05 Januari 2017

Ubah	Deskripsi	Tanggal
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
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

# AWS Glosarium

Untuk AWS terminologi terbaru, lihat [AWS glosarium di Referensi](#).Glosarium AWS