



Panduan Pengguna

Amazon Inspector Klasik



Versi Latest

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon Inspector Klasik: Panduan Pengguna

Copyright © 2025 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 tidak terafiliasi, terkait dengan, atau disponsori oleh Amazon.

Table of Contents

.....	viii
Apa itu Amazon Inspector?	1
Manfaat Amazon Inspector	2
Fitur Amazon Inspector	3
Mengakses Amazon Inspector	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
Akhir dukungan Amazon Inspector Classic	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	14
Memulai	15
Pengaturan dalam satu klik	15
Pengaturan lanjutan	16
Tutorial	18
Tutorial Amazon Inspector Klasik - Red Hat Enterprise Linux	18
Langkah 1: Siapkan EC2 instans Amazon untuk digunakan dengan Amazon Inspector Classic	19
Langkah 2: Ubah EC2 instans Amazon Anda	19
Langkah 3: Buat target penilaian dan instal agen pada EC2 instance	19
Langkah 4: Membuat dan menjalankan templat penilaian Anda	20
Langkah 5: Mencari dan menganalisis temuan Anda	21
Langkah 6: Menerapkan perbaikan yang direkomendasikan ke target penilaian Anda	22
Tutorial Amazon Inspector Klasik - Server Ubuntu	23
Langkah 1: Siapkan EC2 instans Amazon untuk digunakan dengan Amazon Inspector Classic	23
Langkah 2: Buat target penilaian dan instal agen pada EC2 instance	24

Langkah 3: Membuat dan menjalankan templat penilaian Anda	25
Langkah 4: Mencari dan menganalisis temuan yang dihasilkan	25
Langkah 5: Menerapkan perbaikan yang direkomendasikan ke target penilaian Anda	27
Keamanan	28
Perlindungan data	29
Enkripsi diam	30
Enkripsi bergerak	30
Identity and Access Management	31
Audiens	32
Mengautentikasi dengan identitas	32
Mengelola akses menggunakan kebijakan	36
Bagaimana Amazon Inspector Classic bekerja dengan IAM	39
Contoh 2: Memungkinkan pengguna untuk melakukan setiap penjelasan dan daftar operasi hanya pada temuan Amazon Inspector	42
Sumber daya kebijakan	43
Kunci kondisi kebijakan	43
ACLs	44
ABAC	44
Kredensial sementara	45
Izin principal	46
Peran layanan	46
Peran terkait layanan	46
Contoh kebijakan berbasis identitas	47
Menggunakan peran terkait layanan	50
Pemecahan Masalah	53
Pencatatan log dan pemantauan	55
Respons insiden	55
Validasi kepatuhan	56
Ketahanan	56
Keamanan infrastruktur	57
Konfigurasi dan analisis kerentanan	58
Praktik terbaik keamanan	58
Agen Amazon Inspector Classic	59
Hak istimewa agen Amazon Inspector Classic	60
Keamanan agen Jaringan dan Amazon Inspector Classic	60
Pembaruan agen Amazon Inspector Classic	61

Siklus hidup data telemetri	61
Kontrol akses dari Amazon Inspector Classic ke dalam akun AWS	62
Batas agen Amazon Inspector Classic	62
Menginstal agen Amazon Inspector Classic	62
Menginstal agen pada beberapa EC2 instance menggunakan Systems Manager Run Command	63
Menginstal agen pada instance berbasis Linux EC2	64
Menginstal agen pada instance berbasis Windows EC2	66
Bekerja dengan agen Amazon Inspector Classic pada sistem operasi berbasis Linux	67
Memverifikasi bahwa agen Amazon Inspector Classic sedang berjalan	68
Menghentikan agen Amazon Inspector Classic	68
Memulai agen Amazon Inspector Classic	68
Memodifikasi pengaturan agen Amazon Inspector Classic	68
Mengkonfigurasi dukungan proxy untuk agen Amazon Inspector Classic	69
Menghapus instalasi agen Amazon Inspector Classic	70
Bekerja dengan agen Amazon Inspector Classic pada sistem operasi berbasis Windows	71
Memulai atau menghentikan agen Amazon Inspector Classic atau memverifikasi bahwa agen tersebut sedang berjalan	71
Memodifikasi pengaturan agen Amazon Inspector Classic	72
Mengkonfigurasi dukungan proxy untuk agen Amazon Inspector Classic	72
Menghapus instalasi agen Amazon Inspector Classic	74
(Opsional) Verifikasi tanda tangan skrip instalasi agen Amazon Inspector pada sistem operasi berbasis Linux	74
Menginstal alat GPG	75
Mengautentikasi dan mengimpor kunci publik	75
Memverifikasi tanda tangan paket	77
(Opsional) Verifikasi tanda tangan skrip instalasi agen Amazon Inspector Classic pada sistem operasi berbasis Windows	79
Target penilaian Amazon Inspector Classic	80
Menandai sumber daya untuk membuat target penilaian	80
Batas target penilaian Amazon Inspector Classic	81
Membuat target penilaian	81
Menghapus target penilaian	83
Aturan dan paket aturan Amazon Inspector	84
Tingkat kepelikan untuk aturan di Amazon Inspector	84
Paket aturan di Amazon Inspector	85

Keterjangkauan Jaringan	85
Konfigurasi yang dianalisis	86
Rute keterjangkauan	87
Jenis temuan	87
Kelemahan dan eksposur umum	89
Patokan Pusat Keamanan Internet (CIS)	91
Praktik terbaik keamanan untuk Amazon Inspector Classic	94
Menonaktifkan login root melalui SSH	95
Mendukung SSH versi 2 saja	95
Menonaktifkan autentikasi kata sandi Melalui SSH	96
Mengonfigurasi usia maksimum kata sandi	97
Mengonfigurasi panjang minimum kata sandi	97
Mengonfigurasi kompleksitas kata sandi	98
Mengaktifkan ASLR	99
Mengaktifkan DEP	99
Mengonfigurasi izin untuk direktori sistem	100
Templat penilaian dan penilaian berjalan Amazon Inspector Classic	101
Templat penilaian Amazon Inspector Classic	101
Batas templat penilaian Amazon Inspector Classic	102
Membuat templat penilaian	102
Menghapus templat penilaian	104
Penilaian berjalan	105
Menghapus penilaian berjalan	105
Batas penilaian Amazon Inspector Classic berjalan Amazon Inspector	106
Mengatur penilaian berjalan otomatis melalui fungsi Lambda	106
Mengatur topik SNS untuk pemberitahuan Amazon Inspector Classic	108
Temuan Amazon Inspector Classic	111
Bekerja dengan temuan	111
Laporan penilaian	114
Pengecualian di Amazon Inspector	116
Jenis pengecualian	116
Pratinjau pengecualian	130
Melihat pengecualian pasca-penilaian	131
Paket aturan Amazon Inspector Classic untuk sistem operasi yang didukung	132
Mencatat panggilan API Amazon Inspector Classic dengan AWS CloudTrail	137
Informasi Amazon Inspector Classic di CloudTrail	137

Memahami entri file log Amazon Inspector Classic	138
Memantau Amazon Inspector Classic menggunakan Amazon CloudWatch	141
Metrik Amazon Inspector Classic CloudWatch	141
Mengkonfigurasi Amazon Inspector Classic menggunakan AWS CloudFormation	143
Integrasi Security Hub	144
Bagaimana Amazon Inspector mengirimkan temuan ke Security Hub	144
Jenis temuan yang dikirimkan Amazon Inspector	145
Latensi untuk mengirim temuan	145
Mencoba kembali saat Security Hub tidak tersedia	145
Memperbarui temuan yang ada di Security Hub	145
Temuan umum dari Amazon Inspector	146
Mengaktifkan dan mengonfigurasi integrasi	148
Bagaimana cara menghentikan pengiriman temuan	148
Amazon Inspector Klasik ARNs	149
ARNs untuk sumber daya Amazon Inspector Classic	149
Amazon Inspector Classic ARNS untuk paket aturan	150
AS Timur (Ohio)	151
AS Timur (Virginia Utara)	151
AS Barat (California Utara)	152
AS Barat (Oregon)	153
Asia Pasifik (Mumbai)	154
Asia Pasifik (Seoul)	154
Asia Pasifik (Sydney)	155
Asia Pasifik (Tokyo)	156
Eropa (Frankfurt)	156
Eropa (Irlandia)	157
Eropa (London)	158
Eropa (Stockholm)	159
AWS GovCloud (AS-Timur)	159
AWS GovCloud (AS-Barat)	160
Riwayat dokumen	161
AWS Glosarium	168

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?

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 (). CVEs Kami mendorong Anda untuk mengeksplorasi dan menggunakan fitur baru dan yang sudah ditingkatkan lainnya, serta manfaat dari nilai keamanan yang ditingkatkan secara signifikan. Untuk mempelajari tentang fitur dan harga Amazon Inspector, lihat Amazon [Inspector](#). Untuk mempelajari cara pindah ke Amazon Inspector baru, lihat. [Akhir dukungan Amazon Inspector Classic](#)

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

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

Amazon Inspector juga menawarkan perangkat lunak standar yang disebut agen yang dapat Anda instal secara opsional dalam sistem operasi EC2 instans yang ingin Anda nilai. Agen memonitor perilaku EC2 instans, 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 potensi masalah keamanan. Temuan yang dihasilkan Amazon Inspector tergantung

pada pilihan paket aturan Anda termasuk dalam setiap templat penilaian, keberadaan AWS non-komponen dalam sistem Anda, dan faktor lainnya. Anda bertanggung jawab untuk keamanan aplikasi, proses, dan alat-alat yang berjalan pada AWS layanan. Untuk informasi lebih lanjut, 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 atas perangkat keras, perangkat lunak, jaringan, dan fasilitas yang menjalankan AWS layanan. AWS Memberikan beberapa laporan dari auditor pihak ketiga yang telah memverifikasi kepatuhan kami dengan berbagai standar keamanan komputer dan peraturan. Untuk informasi lebih lanjut, lihat [Kepatuhan AWS Cloud](#).

Untuk informasi tentang terminologi Amazon Inspector, lihat. [Terminologi dan konsep Amazon Inspector Classic](#)

Manfaat Amazon Inspector

Berikut adalah beberapa manfaat utama Amazon Inspector:

- Mengintegrasikan pemeriksaan keamanan otomatis ke dalam proses deployment dan produksi reguler — Menilai keamanan AWS sumber daya Anda untuk forensik, pemecahan masalah, atau tujuan 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.
- Mendapatkan pemahaman yang lebih mendalam tentang AWS sumber daya Anda — Tetap mendapatkan informasi tentang aktivitas dan konfigurasi data AWS sumber daya Anda dengan meninjau temuan yang dihasilkan Amazon Inspector.

Fitur Amazon Inspector

Berikut adalah beberapa fitur utama Amazon Inspector:

- Mesin pemindaian konfigurasi dan pemantauan aktivitas — Amazon Inspector 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 isi bawaan — Amazon Inspector Classic mencakup 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 dapat diotomatiskan sepenuhnya 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

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

Konsol Classic Amazon Inspector

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

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

AWS SDKs

AWS menyediakan kit pengembangan perangkat lunak (SDKs) yang terdiri atas pustaka dan kode sampel untuk berbagai bahasa dan platform pemrograman. Hal ini termasuk Java, Python, Ruby, .NET, iOS, Android, dan banyak lagi. Ini SDKs menyediakan cara yang nyaman untuk membuat akses terprogram ke layanan Amazon Inspector. Untuk informasi tentang AWS SDKs, termasuk cara mengunduh dan menginstalnya, lihat [Alat untuk Amazon Web Services](#).

API HTTPS Amazon Inspector

Anda dapat mengakses Amazon Inspector dan AWS secara terprogram dengan menggunakan API HTTPS Amazon Inspector, yang memungkinkan Anda menerbitkan permintaan HTTPS secara langsung ke layanan. Untuk informasi lebih lanjut, lihat [Referensi Amazon Inspector](#).

AWS Alat Baris Perintah

Anda dapat menggunakan alat baris AWS perintah untuk menjalankan perintah pada baris perintah sistem Anda guna menjalankan tugas Amazon Inspector. Alat baris perintah juga berguna jika Anda ingin membangun skrip yang melakukan AWS tugas. Untuk informasi lebih lanjut, lihat Antarmuka [Baris AWS Perintah Classic Amazon Inspector](#).

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 dan penilaian berjalan Amazon Inspector Classic](#).

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, silakan 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 [Aturan dan paket aturan Amazon Inspector](#).

Telemetry

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 proses penilaian yang terjadi pada saat yang sama selama target penilaian

Sumber Daya	Batas Default	Komentar
		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

Harga Amazon Inspector didasarkan pada jumlah EC2 instans yang termasuk 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 instance. EC2 Anda dapat menjalankan penilaian tanpa agen dengan paket aturan [Network Reachability](#) pada EC2 instans apa pun terlepas dari 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 instance 64-bit x86 dan Arm.](#) EC2

Agan tersebut kompatibel dengan 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 EC2 instans 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).

Akhir dukungan Amazon Inspector Classic

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 bisa 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 yang 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 dan EventBridge Amazon untuk mengotomatiskan alur kerja, seperti tiket. Temuan terkait gambar kontainer juga didorong ke Amazon ECR.

Untuk mempelajari tentang semua fitur dan harga untuk Amazon Inspector, 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](#)

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 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 menjadi tersedia.

3. Di kotak dialog Laporan penilaian, pilih jenis laporan yang ingin Anda lihat (baik laporan Temuan ataupun laporan Penuh) 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

Anda dapat mengaktifkan Amazon Inspector baru menggunakan Amazon Inspector AWS Management Console 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 AWS Management Console dan buka konsol Amazon Inspector Classic di <https://console.aws.amazon.com/inspector/>
2. Pada halaman Selamat Datang, pilih jenis penilaian yang ingin Anda jalankan. Penilaian Jaringan menganalisis konfigurasi 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 EC2 instance menggunakan Systems Manager Run Command](#).

- c. Menambahkan instans tersebut ke [target penilaian](#).
 - d. Memasukkan target tersebut dalam [templat penilaian](#) dengan seperangkat standar paket aturan.
 - e. Menjalankan penilaian mingguan atau hanya sekali, tergantung pada apakah Anda memilih Jalankan mingguan (disarankan) atau Jalankan sekali.
3. Di kotak dialog Konfirmasi, pilih OK. Amazon Inspector Classic secara otomatis menjalankan penilaian Anda.

Pengaturan lanjutan

Prosedur berikut menunjukkan cara 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 EC2 instance 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 EC2 instance 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 menyiapkan EC2 instans Amazon, menjalankan templat penilaian, dan melakukan perbaikan keamanan yang disarankan 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 EC2 instans Amazon untuk digunakan dengan Amazon Inspector Classic](#)
- [Langkah 2: Ubah EC2 instans Amazon Anda](#)
- [Langkah 3: Buat target penilaian dan instal agen pada EC2 instance](#)
- [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 EC2 instans Amazon untuk digunakan dengan Amazon Inspector Classic

Untuk tutorial ini, buat satu EC2 contoh yang menjalankan Red Hat Enterprise Linux 7.5, dan beri tag menggunakan kunci Nama dan nilai **InspectorEC2InstanceLinux**.

Note

Untuk informasi selengkapnya tentang menandai EC2 instance, lihat [Sumber Daya dan Tag](#).

Langkah 2: Ubah EC2 instans Amazon Anda

Untuk tutorial ini, Anda memodifikasi EC2 instance target Anda untuk mengeksposnya ke masalah keamanan potensial 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.e17
```

Untuk petunjuk tentang cara menyambung ke EC2 instans, lihat [Connect to Your Instance](#) di Panduan EC2 Pengguna Amazon.

Langkah 3: Buat target penilaian dan instal agen pada EC2 instance

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

Untuk membuat target penilaian dan menginstal agen pada sebuah EC2 instance

1. Masuk ke AWS Management Console 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 Menggunakan Tag, pilih EC2 instance yang ingin Anda sertakan dalam target penilaian ini dengan memasukkan nilai untuk bidang Kunci dan Nilai.

Untuk tutorial ini, pilih EC2 contoh yang Anda buat pada langkah sebelumnya dengan memasukkan **Name** di bidang Key dan **InspectorEC2InstanceLinux** di bidang Value.

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

- c. Pilih Simpan.
- d. Instal agen Amazon Inspector Classic pada instans yang diberi tag EC2 . Untuk menginstal agen pada semua EC2 instance yang disertakan 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 pada EC2 instans 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 MyFirstTemplateLinux perubahan 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 EC2 instance 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 EC2 instans Amazon untuk digunakan dengan Amazon Inspector Classic](#)
- [Langkah 2: Buat target penilaian dan instal agen pada EC2 instance](#)
- [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 EC2 instans Amazon untuk digunakan dengan Amazon Inspector Classic

Untuk mengatur sebuah EC2 instance

- Untuk tutorial ini, buat satu EC2 instance yang menjalankan Ubuntu Server 16.04 LTS dan beri tag menggunakan kunci Name dan nilai. **InspectorEC2InstanceUbuntu**

Note

Untuk informasi selengkapnya tentang menandai EC2 instance, lihat [Sumber Daya dan Tag](#).

Langkah 2: Buat target penilaian dan instal agen pada EC2 instance

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

Untuk membuat target penilaian dan menginstal agen pada EC2 instance

1. Masuk ke AWS Management Console 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 Menggunakan Tag, pilih EC2 instance yang ingin Anda sertakan dalam target penilaian ini dengan memasukkan nilai untuk bidang Kunci dan Nilai.

Untuk tutorial ini, pilih EC2 contoh yang Anda buat pada langkah sebelumnya dengan memasukkan **Name** di bidang Key dan **InspectorEC2InstanceUbuntu** di bidang Value.

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

5. Instal Amazon Inspector Classic Agent pada instans yang diberi tag EC2 . Untuk menginstal agen pada semua EC2 instance yang disertakan 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 Amazon Inspector Agent pada EC2 instans 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 ini.

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.

Selain itu, permintaan harus ditandatangani menggunakan ID kunci akses dan kunci akses rahasia yang terkait dengan prinsipal IAM. Atau Anda dapat menggunakan [AWS Security Token Service](#) (AWS STS) untuk menghasilkan kredensial keamanan sementara untuk menandatangani permintaan.

Identity and Access Management untuk Amazon Inspector Classic

AWS Identity and Access Management (IAM) adalah Layanan AWS yang membantu administrator mengontrol akses ke AWS sumber daya dengan aman. 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, tergantung pada pekerjaan yang Anda lakukan di Amazon Inspector.

Pengguna layanan – Jika Anda menggunakan layanan Amazon Inspector untuk melakukan tugas, administrator Anda akan memberikan kredensial dan izin yang dibutuhkan. Saat Anda menggunakan lebih banyak fitur Amazon Inspector untuk melakukan pekerjaan, Anda mungkin memerlukan izin tambahan. Memahami cara akses dikelola dapat membantu Anda meminta izin yang tepat dari administrator Anda. Jika Anda tidak dapat mengakses fitur di Amazon Inspector, lihat [Memecahkan masalah identitas dan akses Amazon Inspector Classic](#).

Administrator layanan – Jika Anda bertanggung jawab atas sumber daya Amazon Inspector di perusahaan Anda, Anda mungkin memiliki akses penuh ke Amazon Inspector. Tugas Anda adalah menentukan fitur dan sumber daya Amazon Inspector mana yang harus diakses pengguna layanan Anda. Kemudian, Anda harus mengirimkan permintaan kepada administrator IAM untuk mengubah izin pengguna layanan Anda. Tinjau informasi di halaman ini untuk memahami konsep dasar IAM. Untuk mempelajari selengkapnya tentang bagaimana perusahaan Anda dapat menggunakan IAM dengan Amazon Inspector, lihat [Bagaimana Amazon Inspector Classic bekerja dengan IAM](#).

Administrator IAM – Jika Anda adalah administrator IAM, Anda mungkin ingin belajar dengan lebih detail tentang cara Anda menulis kebijakan untuk mengelola akses Amazon Inspector. Untuk melihat contoh kebijakan berbasis identitas Amazon Inspector yang dapat Anda gunakan di IAM, lihat [Contoh kebijakan berbasis identitas untuk Amazon Inspector Classic](#).

Mengautentikasi dengan identitas

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

Anda dapat masuk AWS sebagai identitas federasi dengan menggunakan kredensial yang disediakan melalui sumber identitas. AWS IAM Identity Center Pengguna (IAM Identity Center), autentikasi masuk tunggal perusahaan Anda, dan kredensial Google atau Facebook Anda adalah contoh identitas federasi. Saat Anda masuk sebagai identitas terfederasi, administrator Anda sebelumnya menyiapkan federasi identitas menggunakan peran IAM. Ketika Anda mengakses AWS dengan menggunakan federasi, Anda secara tidak langsung mengambil peran.

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

Jika Anda mengakses AWS secara terprogram, AWS sediakan kit pengembangan perangkat lunak (SDK) dan antarmuka baris perintah (CLI) untuk menandatangani permintaan Anda secara kriptografis dengan menggunakan kredensial Anda. Jika Anda tidak menggunakan AWS alat, Anda harus menandatangani permintaan sendiri. Guna mengetahui informasi selengkapnya tentang penggunaan metode yang disarankan untuk menandatangani permintaan sendiri, lihat [AWS Signature Version 4 untuk permintaan API](#) dalam Panduan Pengguna IAM.

Apa pun metode autentikasi yang digunakan, Anda mungkin diminta untuk menyediakan informasi keamanan tambahan. Misalnya, AWS merekomendasikan agar Anda menggunakan otentikasi multi-faktor (MFA) untuk meningkatkan keamanan akun Anda. Untuk mempelajari selengkapnya, lihat [Autentikasi multi-faktor](#) dalam Panduan Pengguna AWS IAM Identity Center dan [Autentikasi multi-faktor AWS di IAM](#) dalam Panduan Pengguna IAM.

Akun AWS pengguna root

Saat Anda membuat Akun AWS, Anda mulai dengan satu identitas masuk yang memiliki akses lengkap ke semua Layanan AWS dan sumber daya di akun. Identitas ini disebut pengguna Akun AWS root dan diakses dengan masuk dengan alamat email dan kata sandi yang Anda gunakan untuk membuat akun. Kami sangat menyarankan agar Anda tidak menggunakan pengguna root untuk tugas sehari-hari. Lindungi kredensial pengguna root Anda dan gunakan kredensial tersebut untuk melakukan tugas yang hanya dapat dilakukan pengguna root. Untuk daftar lengkap tugas yang mengharuskan Anda masuk sebagai pengguna root, lihat [Tugas yang memerlukan kredensial pengguna root](#) dalam Panduan Pengguna IAM.

Identitas gabungan

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

Identitas federasi adalah pengguna dari direktori pengguna perusahaan Anda, penyedia identitas web, direktori Pusat Identitas AWS Directory Service, atau pengguna mana pun yang mengakses Layanan AWS dengan menggunakan kredensi yang disediakan melalui sumber identitas. Ketika identitas federasi mengakses Akun AWS, mereka mengambil peran, dan peran memberikan kredensi sementara.

Untuk manajemen akses terpusat, kami sarankan Anda menggunakan AWS IAM Identity Center. Anda dapat membuat pengguna dan grup di Pusat Identitas IAM, atau Anda dapat menghubungkan dan menyinkronkan ke sekumpulan pengguna dan grup di sumber identitas Anda sendiri untuk digunakan di semua aplikasi Akun AWS dan aplikasi Anda. Untuk informasi tentang Pusat Identitas IAM, lihat [Apakah itu Pusat Identitas IAM?](#) dalam Panduan Pengguna AWS IAM Identity Center .

Pengguna dan grup IAM

[Pengguna IAM](#) adalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus untuk satu orang atau aplikasi. Jika memungkinkan, kami merekomendasikan untuk mengandalkan kredensial sementara, bukan membuat pengguna IAM yang memiliki kredensial jangka panjang seperti kata sandi dan kunci akses. Namun, jika Anda memiliki kasus penggunaan tertentu yang memerlukan kredensial jangka panjang dengan pengguna IAM, kami merekomendasikan Anda merotasi kunci akses. Untuk informasi selengkapnya, lihat [Merotasi kunci akses secara teratur untuk kasus penggunaan yang memerlukan kredensial jangka panjang](#) dalam Panduan Pengguna IAM.

[Grup IAM](#) adalah identitas yang menentukan sekumpulan pengguna IAM. Anda tidak dapat masuk sebagai grup. Anda dapat menggunakan grup untuk menentukan izin bagi beberapa pengguna sekaligus. Grup mempermudah manajemen izin untuk sejumlah besar pengguna sekaligus. Misalnya, Anda dapat meminta kelompok untuk menyebutkan IAMAdmins dan memberikan izin kepada grup tersebut untuk mengelola sumber daya IAM.

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

Peran IAM

[Peran IAM](#) adalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus. Peran ini mirip dengan pengguna IAM, tetapi tidak terkait dengan orang tertentu. Untuk mengambil peran IAM sementara AWS Management Console, Anda dapat [beralih dari pengguna ke peran IAM \(konsol\)](#). Anda dapat mengambil peran dengan memanggil operasi AWS CLI atau AWS API atau dengan menggunakan URL kustom. Untuk informasi selengkapnya tentang cara menggunakan peran, lihat [Metode untuk mengambil peran](#) dalam Panduan Pengguna IAM.

Peran IAM dengan kredensial sementara berguna dalam situasi berikut:

- Akses pengguna terfederasi – Untuk menetapkan izin ke identitas terfederasi, Anda membuat peran dan menentukan izin untuk peran tersebut. Ketika identitas terfederasi mengautentikasi, identitas tersebut terhubung dengan peran dan diberi izin yang ditentukan oleh peran. Untuk informasi tentang peran untuk federasi, lihat [Buat peran untuk penyedia identitas pihak ketiga](#) dalam Panduan Pengguna IAM. Jika menggunakan Pusat Identitas IAM, Anda harus mengonfigurasi set izin. Untuk mengontrol apa yang dapat diakses identitas Anda setelah identitas tersebut diautentikasi, Pusat Identitas IAM akan mengorelasikan set izin ke peran dalam IAM. Untuk informasi tentang set izin, lihat [Set izin](#) dalam Panduan Pengguna AWS IAM Identity Center .
- Izin pengguna IAM sementara – Pengguna atau peran IAM dapat mengambil peran IAM guna mendapatkan berbagai izin secara sementara untuk tugas tertentu.
- Akses lintas akun – Anda dapat menggunakan peran IAM untuk mengizinkan seseorang (prinsipal tepercaya) di akun lain untuk mengakses sumber daya di akun Anda. Peran adalah cara utama untuk memberikan akses lintas akun. Namun, dengan beberapa Layanan AWS, Anda dapat melampirkan kebijakan secara langsung ke sumber daya (alih-alih menggunakan peran sebagai proxy). Untuk mempelajari perbedaan antara peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat [Akses sumber daya lintas akun di IAM](#) dalam Panduan Pengguna IAM.
- Akses lintas layanan — Beberapa Layanan AWS menggunakan fitur lain Layanan AWS. Misalnya, saat Anda melakukan panggilan dalam suatu layanan, biasanya layanan tersebut menjalankan aplikasi di Amazon EC2 atau menyimpan objek di Amazon S3. Sebuah layanan mungkin melakukannya menggunakan izin prinsipal yang memanggil, menggunakan peran layanan, atau peran terkait layanan.
 - Sesi akses teruskan (FAS) — Saat Anda menggunakan pengguna atau peran IAM untuk melakukan tindakan AWS, Anda dianggap sebagai prinsipal. Ketika Anda menggunakan beberapa layanan, Anda mungkin melakukan sebuah tindakan yang kemudian menginisiasi tindakan lain di layanan yang berbeda. FAS menggunakan izin dari pemanggilan utama Layanan AWS, dikombinasikan dengan permintaan Layanan AWS untuk membuat permintaan ke layanan hilir. Permintaan FAS hanya dibuat ketika layanan menerima permintaan yang memerlukan interaksi dengan orang lain Layanan AWS atau sumber daya untuk menyelesaikannya. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan ketika mengajukan permintaan FAS, lihat [Sesi akses maju](#).
- Peran layanan – Peran layanan adalah [peran IAM](#) yang dijalankan oleh 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.

- Peran terkait layanan — 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.
- Aplikasi yang berjalan di Amazon EC2 — Anda dapat menggunakan peran IAM untuk mengelola kredensi sementara untuk aplikasi yang berjalan pada EC2 instance dan membuat AWS CLI atau AWS permintaan API. Ini lebih baik untuk menyimpan kunci akses dalam EC2 instance. Untuk menetapkan AWS peran ke EC2 instance dan membuatnya tersedia untuk semua aplikasinya, Anda membuat profil instance yang dilampirkan ke instance. Profil instance berisi peran dan memungkinkan program yang berjalan pada EC2 instance untuk mendapatkan kredensi sementara. Untuk informasi selengkapnya, lihat [Menggunakan peran IAM untuk memberikan izin ke aplikasi yang berjalan di EC2 instans Amazon di Panduan Pengguna IAM](#).

Mengelola akses menggunakan kebijakan

Anda mengontrol akses AWS dengan membuat kebijakan dan melampirkannya ke AWS identitas atau sumber daya. Kebijakan adalah objek AWS yang, ketika dikaitkan dengan identitas atau sumber daya, menentukan izinnya. AWS mengevaluasi kebijakan ini ketika prinsipal (pengguna, pengguna root, atau sesi peran) membuat permintaan. Izin dalam kebijakan menentukan apakah permintaan diizinkan atau ditolak. Sebagian besar kebijakan disimpan AWS sebagai dokumen JSON. Untuk informasi selengkapnya tentang struktur dan isi dokumen kebijakan JSON, lihat [Gambaran umum kebijakan JSON](#) dalam Panduan Pengguna IAM.

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Artinya, prinsipal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan kondisi apa.

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

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

Kebijakan berbasis identitas

Kebijakan berbasis identitas adalah dokumen kebijakan izin JSON yang dapat Anda lampirkan ke sebuah identitas, seperti pengguna IAM, grup pengguna IAM, atau peran IAM. Kebijakan ini mengontrol jenis tindakan yang dapat dilakukan 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.

Kebijakan berbasis identitas dapat dikategorikan lebih lanjut sebagai kebijakan inline atau kebijakan yang dikelola. Kebijakan inline disematkan langsung ke satu pengguna, grup, atau peran. Kebijakan terkelola adalah kebijakan mandiri yang dapat dilampirkan ke beberapa pengguna, grup, dan peran dalam akun AWS. Kebijakan AWS terkelola mencakup kebijakan terkelola dan kebijakan yang dikelola pelanggan. Untuk mempelajari cara memilih antara kebijakan yang dikelola atau kebijakan inline, lihat [Pilih antara kebijakan yang dikelola dan kebijakan inline](#) dalam Panduan Pengguna IAM.

Kebijakan berbasis sumber daya

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

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

Daftar kontrol akses (ACLs)

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

Amazon S3, AWS WAF, dan Amazon VPC adalah contoh layanan yang mendukung ACLs. Untuk mempelajari selengkapnya ACLs, lihat [Ringkasan daftar kontrol akses \(ACL\)](#) di Panduan Pengembang Layanan Penyimpanan Sederhana Amazon.

Jenis-jenis kebijakan lain

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

- **Batasan izin** – Batasan izin adalah fitur lanjutan tempat Anda mengatur izin maksimum yang dapat diberikan oleh kebijakan berbasis identitas ke entitas IAM (pengguna IAM atau peran IAM). Anda dapat menetapkan batasan izin untuk suatu entitas. Izin yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas milik entitas dan batasan izinnya. Kebijakan berbasis sumber daya yang menentukan pengguna atau peran dalam bidang `Principal` tidak dibatasi oleh batasan izin. Penolakan eksplisit dalam salah satu kebijakan ini akan menggantikan pemberian izin. Untuk informasi selengkapnya tentang batasan izin, lihat [Batasan izin untuk entitas IAM](#) dalam Panduan Pengguna IAM.
- **Kebijakan kontrol layanan (SCPs)** — SCPs adalah kebijakan JSON yang menentukan izin maksimum untuk organisasi atau unit organisasi (OU) di AWS Organizations. AWS Organizations adalah layanan untuk mengelompokkan dan mengelola secara terpusat beberapa Akun AWS yang dimiliki bisnis Anda. Jika Anda mengaktifkan semua fitur dalam organisasi, Anda dapat menerapkan kebijakan kontrol layanan (SCPs) ke salah satu atau semua akun Anda. SCP membatasi izin untuk entitas di akun anggota, termasuk masing-masing. Pengguna root akun AWS. Untuk informasi selengkapnya tentang Organizations dan SCPs, lihat [Kebijakan kontrol layanan](#) di Panduan AWS Organizations Pengguna.
- **Kebijakan kontrol sumber daya (RCPs)** — RCPs adalah kebijakan JSON yang dapat Anda gunakan untuk menetapkan izin maksimum yang tersedia untuk sumber daya di akun Anda tanpa memperbarui kebijakan IAM yang dilampirkan ke setiap sumber daya yang Anda miliki. RCP membatasi izin untuk sumber daya di akun anggota dan dapat memengaruhi izin efektif untuk identitas, termasuk Pengguna root akun AWS, terlepas dari apakah itu milik organisasi Anda. Untuk informasi selengkapnya tentang Organizations dan RCPs, termasuk daftar dukungan Layanan AWS tersebut RCPs, lihat [Kebijakan kontrol sumber daya \(RCPs\)](#) di Panduan AWS Organizations Pengguna.
- **Kebijakan sesi** – Kebijakan sesi adalah kebijakan lanjutan yang Anda berikan sebagai parameter ketika Anda membuat sesi sementara secara programatis untuk peran atau pengguna terfederasi. Izin sesi yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas pengguna atau peran dan kebijakan sesi. Izin juga bisa datang dari kebijakan berbasis sumber daya. Penolakan eksplisit dalam salah satu kebijakan ini akan menggantikan pemberian izin. 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 yang tersedia untuk digunakan dengan Amazon Inspector.

Fitur IAM yang dapat Anda gunakan dengan Amazon Inspector Classic

Fitur IAM	Dukungan Amazon Inspector
Kebijakan berbasis identitas	Ya
Kebijakan berbasis sumber daya	Tidak
Tindakan kebijakan	Ya
Sumber daya kebijakan	Ya
kunci-kunci persyaratan kebijakan (spesifik layanan)	Ya
ACLs	Tidak
ABAC (tanda dalam kebijakan)	Parsial
Kredensial sementara	Ya
Izin principal	Ya
Peran layanan	Tidak
Peran terkait layanan	Ya

Untuk mendapatkan tampilan tingkat tinggi tentang cara kerja Amazon Inspector dan layanan AWS lainnya dengan 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 dikabulkannya atau ditolakannya tindakan tersebut. Anda tidak dapat menentukan secara spesifik prinsipal dalam sebuah kebijakan berbasis identitas karena prinsipal berlaku bagi pengguna atau peran yang melekat kepadanya. Untuk mempelajari semua elemen yang dapat Anda gunakan dalam 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 prinsipal tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus [menentukan prinsipal](#) dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau. Layanan AWS

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

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

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

Untuk melihat daftar tindakan Amazon Inspector, lihat [Tindakan yang ditentukan oleh Amazon Inspector Classic di Referensi](#) Otorisasi Layanan.

Tindakan kebijakan di Amazon Inspector menggunakan awalan berikut sebelum tindakan:

```
inspector
```

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

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

```
]
```

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

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

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

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

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

```

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

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

Sumber daya kebijakan untuk Amazon Inspector

Mendukung sumber daya kebijakan: Ya

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Artinya, prinsipal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan kondisi apa.

Elemen kebijakan JSON `Resource` menentukan objek yang menjadi target penerapan tindakan. Pernyataan harus menyertakan elemen `Resource` atau `NotResource`. Praktik terbaiknya, tentukan sumber daya menggunakan [Amazon Resource Name \(ARN\)](#). Anda dapat melakukan ini untuk tindakan yang mendukung jenis sumber daya tertentu, yang dikenal sebagai izin tingkat sumber daya.

Untuk tindakan yang tidak mendukung izin di tingkat sumber daya, misalnya operasi pencantuman, gunakan wildcard (*) untuk 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](#) dalam 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. Artinya, prinsipal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan kondisi apa.

Elemen `Condition` (atau blok `Condition`) akan memungkinkan Anda menentukan kondisi yang menjadi dasar suatu pernyataan berlaku. Elemen `Condition` bersifat opsional. Anda dapat membuat ekspresi bersyarat yang menggunakan [operator kondisi](#), misalnya sama dengan atau kurang dari, untuk mencocokkan kondisi dalam kebijakan dengan nilai-nilai yang diminta.

Jika Anda menentukan beberapa elemen `Condition` dalam sebuah pernyataan, atau beberapa kunci dalam elemen `Condition` tunggal, maka AWS akan mengevaluasinya menggunakan operasi AND logis. Jika Anda menentukan beberapa nilai untuk satu kunci kondisi, AWS mengevaluasi kondisi menggunakan OR operasi logis. Semua kondisi harus dipenuhi sebelum izin pernyataan diberikan.

Anda juga dapat menggunakan variabel placeholder saat menentukan kondisi. Sebagai contoh, Anda dapat memberikan izin kepada pengguna IAM untuk mengakses sumber daya hanya jika izin tersebut mempunyai tanda yang sesuai dengan nama pengguna IAM mereka. Untuk informasi selengkapnya, lihat [Elemen kebijakan IAM: variabel dan tanda](#) dalam Panduan Pengguna IAM.

AWS mendukung kunci kondisi global dan kunci kondisi khusus layanan. Untuk melihat semua kunci kondisi AWS global, lihat [kunci konteks kondisi AWS global](#) di Panduan Pengguna IAM.

Untuk melihat daftar kunci kondisi Amazon Inspector, lihat Kunci kondisi [untuk Amazon Inspector 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. Dalam AWS, atribut ini disebut tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke banyak AWS sumber daya. Penandaan ke entitas dan sumber daya adalah langkah pertama dari ABAC. Kemudian rancanglah kebijakan ABAC untuk mengizinkan operasi ketika tanda milik prinsipal cocok dengan tanda yang ada di sumber daya yang ingin diakses.

ABAC sangat berguna di lingkungan yang berkembang dengan cepat dan berguna di situasi saat manajemen kebijakan menjadi rumit.

Untuk mengendalikan akses berdasarkan tanda, berikan informasi tentang tanda di [elemen kondisi](#) dari kebijakan menggunakan kunci kondisi `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`, atau `aws:TagKeys`.

Jika sebuah layanan mendukung ketiga kunci kondisi untuk setiap jenis sumber daya, nilainya adalah Ya untuk layanan tersebut. Jika suatu layanan mendukung ketiga kunci kondisi untuk hanya beberapa jenis sumber daya, nilainya adalah Parsial.

Untuk informasi 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

Beberapa Layanan AWS tidak berfungsi saat Anda masuk menggunakan kredensial sementara. Untuk informasi tambahan, termasuk yang Layanan AWS bekerja dengan kredensial sementara, lihat [Layanan AWS yang bekerja dengan IAM di Panduan Pengguna IAM](#).

Anda menggunakan kredensial sementara jika Anda masuk AWS Management Console menggunakan metode apa pun kecuali nama pengguna dan kata sandi. Misalnya, ketika Anda mengakses AWS menggunakan tautan masuk tunggal (SSO) perusahaan Anda, proses tersebut secara otomatis membuat kredensial sementara. Anda juga akan secara otomatis membuat kredensial sementara ketika Anda masuk ke konsol sebagai seorang pengguna lalu beralih peran. Untuk informasi selengkapnya tentang peralihan peran, lihat [Beralih dari pengguna ke peran IAM \(konsol\)](#) dalam Panduan Pengguna IAM.

Anda dapat membuat kredensial sementara secara manual menggunakan API AWS CLI atau AWS . Anda kemudian dapat menggunakan kredensial sementara tersebut untuk mengakses AWS. AWS merekomendasikan agar Anda secara dinamis menghasilkan kredensial sementara alih-

alih menggunakan kunci akses jangka panjang. Untuk informasi selengkapnya, lihat [Kredensial keamanan sementara di IAM](#).

Izin utama lintas layanan untuk Amazon Inspector

Mendukung sesi akses maju (FAS): Ya

Saat Anda menggunakan pengguna atau peran IAM untuk melakukan tindakan AWS, Anda dianggap sebagai prinsipal. Ketika Anda menggunakan beberapa layanan, Anda mungkin melakukan sebuah tindakan yang kemudian menginisiasi tindakan lain di layanan yang berbeda. FAS menggunakan izin dari pemanggilan utama Layanan AWS, dikombinasikan dengan permintaan Layanan AWS untuk membuat permintaan ke layanan hilir. Permintaan FAS hanya dibuat ketika layanan menerima permintaan yang memerlukan interaksi dengan orang lain Layanan AWS atau sumber daya untuk menyelesaikannya. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan ketika mengajukan permintaan FAS, lihat [Sesi akses maju](#).

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 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 tertaut layanan Amazon Inspector, lihat [Menggunakan peran terkait layanan untuk Amazon Inspector Classic](#).

Contoh kebijakan berbasis identitas untuk Amazon Inspector Classic

Secara default, pengguna dan peran tidak memiliki izin untuk membuat atau memodifikasi sumber daya Amazon Inspector. Mereka juga tidak dapat melakukan tugas dengan menggunakan AWS Management Console, AWS Command Line Interface (AWS CLI), atau AWS API. Untuk memberikan izin kepada pengguna untuk melakukan tindakan di sumber daya yang mereka perlukan, administrator IAM dapat membuat kebijakan IAM. Administrator kemudian dapat menambahkan kebijakan IAM ke peran, dan pengguna dapat mengambil peran.

Untuk mempelajari cara membuat kebijakan berbasis identitas IAM dengan menggunakan contoh dokumen kebijakan JSON ini, lihat [Membuat kebijakan IAM \(konsol\) 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 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 AWS 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.

```

{
  "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 AWS Management Console, 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 AWS Health Dashboard. Untuk informasi tentang cara menggunakan AWS Health Dashboard, lihat [Panduan AWS Health Pengguna](#).

Validasi kepatuhan untuk Amazon Inspector Classic

Auditor pihak ketiga menilai keamanan dan kepatuhan Amazon Inspector Classic sebagai bagian dari AWS beberapa program kepatuhan. 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](#)— 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.

Selain itu, permintaan harus ditandatangani menggunakan ID kunci akses dan kunci akses rahasia yang terkait dengan prinsipal IAM. Atau Anda dapat menggunakan [AWS Security Token Service](#) (AWS STS) untuk menghasilkan kredensial keamanan sementara untuk menandatangani permintaan.

Untuk informasi selengkapnya tentang jaringan Amazon Inspector Classic dan keamanan agen, lihat [the section called “Keamanan agen Jaringan dan Amazon Inspector Classic”](#)

Analisis konfigurasi dan kerentanan di Amazon Inspector Classic

Amazon Inspector Classic menawarkan perangkat lunak standar yang disebut agen yang dapat Anda instal secara opsional di sistem operasi EC2 instance yang ingin Anda nilai. Agen mengumpulkan seperangkat data konfigurasi yang dikenal sebagai telemetry. 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 EC2 instans Amazon target Anda untuk menilai keamanan mereka 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 EC2 instans Amazon agar berfungsi dengan benar. Ini mengakses metadata instance menggunakan versi 1 atau versi 2 dari Layanan Metadata Instance (atau). IMDSv1 IMDSv2 Lihat [Metadata Instance dan Data Pengguna](#) untuk mempelajari metadata EC2 instans dan metode akses selengkapnya.

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 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 instance, atau, jika tidak ada peran yang ditetapkan, dengan dokumen metadata instans. AWS EC2 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 bagi Anda untuk melacak dan secara manual mempertahankan versi agen yang telah Anda instal pada instans Anda. EC2 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 dikirimkan near-real-time melalui TLS ke Amazon Inspector Classic, di mana file tersebut dienkrpsi dengan kunci turunan KMS per-assessment-run sesaat. File disimpan dengan aman di bucket Amazon S3 yang didedikasikan untuk Amazon Inspector Classic. Mesin aturan Amazon Inspector Classic mengakses data telemetri terenkripsi di bucket S3, mendekripsi dalam memori, dan memproses data berdasarkan aturan penilaian yang dikonfigurasi untuk menghasilkan temuan. Data telemetri yang disimpan di S3 dipertahankan hanya untuk memungkinkan bantuan dengan permintaan dukungan. Hal ini tidak digunakan atau dikumpulkan oleh Amazon untuk tujuan lain. Setelah 30 hari, data telemetri dihapus secara permanen sesuai dengan kebijakan siklus hidup bucket S3 standar untuk data Amazon Inspector Classic. Saat ini,

Amazon Inspector Classic tidak menyediakan API atau mekanisme akses bucket S3 ke telemetri yang dikumpulkan.

Kontrol akses dari Amazon Inspector Classic ke dalam akun AWS

Sebagai layanan keamanan, Amazon Inspector Classic mengakses AWS akun dan sumber daya Anda hanya jika perlu menemukan EC2 instance 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 EC2 pada instans. Objek layanan Amazon Inspector Classic yang dibuat, seperti target penilaian, templat penilaian, dan temuan yang dihasilkan oleh layanan, disimpan dalam database yang dikelola oleh dan hanya dapat diakses oleh Amazon Inspector Classic.

Batas agen Amazon Inspector Classic

Untuk informasi tentang batas agen Amazon Inspector Classic, lihat. [Batas layanan Amazon Inspector Classic](#)

Menginstal agen Amazon Inspector Classic

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

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

Topik

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

 Note

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

Menginstal agen pada beberapa EC2 instance menggunakan Systems Manager Run Command

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

 Important

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

 Important

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

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

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

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

Note

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

Menginstal agen pada instance berbasis Linux EC2

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

Untuk menginstal agen pada instance berbasis Linux EC2

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

Note

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

2. Unduh skrip instalasi agen dengan menjalankan salah satu dari perintah berikut ini:
 - `wget https://inspector-agent.amazonaws.com/linux/latest/install`
 - `curl -O https://inspector-agent.amazonaws.com/linux/latest/install`

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

 Note

Jika Anda menginstal agen di SELinux lingkungan, Amazon Inspector Classic dapat dideteksi sebagai daemon yang tidak terbatas. Anda dapat menghindari hal ini dengan mengubah domain proses agen dari default `initrc_t` ke `bin_t`. Gunakan perintah berikut untuk menetapkan `bin_t` konteks ke skrip run Amazon Inspector Classic sebelum menginstal agen untuk: SELinux

```
sudo semanage fcontext -a -t bin_t /etc/rc\.d/init\.d/awsagent
sudo semanage fcontext -a -t bin_t /etc/init\.d/awsagent
```

 Note

Ketika pembaruan untuk agen tersedia, mereka secara otomatis diunduh dari Amazon S3 dan diterapkan. Untuk informasi selengkapnya, lihat [Pembaruan agen Amazon Inspector Classic](#).

Jika Anda ingin melewati proses pembaruan otomatis ini, jalankan perintah berikut ketika Anda menginstal agen:

```
sudo bash install -u false
```

 Note

(Opsional) Untuk menghapus skrip instalasi agen, jalankan `rm install`.

5. Verifikasi bahwa file-file yang diperlukan agar agen berhasil diinstal dan berfungsi dengan benar berikut ini telah diinstal:
 - `libcurl4` (diperlukan untuk menginstal agen di Ubuntu 18.04)
 - `libcurl3`
 - `libgcc1`

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

Menginstal agen pada instance berbasis Windows EC2

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

Untuk menginstal agen pada instance berbasis Windows EC2

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

Note

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

2. Unduh file `.exe` berikut ini:

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

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

Note

Ketika pembaruan untuk agen tersedia, mereka secara otomatis diunduh dari Amazon S3 dan diterapkan. Untuk informasi selengkapnya, lihat [Pembaruan agen Amazon Inspector Classic](#).

Jika Anda ingin melewati proses pembaruan otomatis ini, jalankan perintah berikut ketika Anda menginstal agen:

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

Bekerja dengan agen Amazon Inspector Classic pada sistem operasi berbasis Linux

Anda dapat menginstal, menghapus, memverifikasi, dan memodifikasi perilaku agen Amazon Inspector Classic. Masuk ke EC2 instans Amazon 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 EC2 instans Amazon agar berfungsi dengan benar. Ini mengakses metadata instance menggunakan versi 1 atau versi 2 dari Layanan Metadata Instance (atau). IMDSv1 IMDSv2 Lihat [Metadata Instance dan Data Pengguna](#) untuk mempelajari metadata EC2 instans dan metode akses selengkapnya.

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 dijalankan, masuk ke EC2 instance 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 EC2 instans Anda, 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.

Lengkapi salah satu prosedur berikut:

Untuk menginstal agen pada EC2 instance yang menggunakan server proxy

1. Buat file bernama `awsagent.env` dan simpan di direktori `/etc/init.d/`.
2. Edit `awsagent.env` untuk memasukkan variabel lingkungan ini dalam format berikut:
 - `export https_proxy=hostname:port`
 - `export http_proxy=hostname:port`
 - `export no_proxy=169.254.169.254`

Note

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

3. Instal agen Amazon Inspector Classic dengan menyelesaikan langkah-langkah dalam prosedur. [Menginstal agen pada instance berbasis Linux EC2](#)

Untuk mengonfigurasi dukungan proxy pada EC2 instance dengan agen yang sedang berjalan

1. Untuk mengonfigurasi dukungan proxy, versi agen yang berjalan pada EC2 instans 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 agen pada EC2 instance ini lagi dengan mengikuti [Menginstal agen pada instance berbasis Linux EC2](#) prosedur.
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 EC2 instans Anda yang menjalankan sistem operasi berbasis Linux tempat 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 EC2 instans Anda yang menjalankan sistem operasi berbasis Windows dan lakukan prosedur apa pun di 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 EC2 instans Amazon agar berfungsi dengan benar. Ini mengakses metadata instance menggunakan versi 1 atau versi 2 dari Layanan Metadata Instance (). IMDSv1 or IMDSv2 Lihat [Metadata Instance dan Data Pengguna](#) untuk mempelajari metadata EC2 instans dan metode akses selengkapnya.

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 EC2 contoh 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 dijalankan, masuk ke EC2 instans Anda, dan buka prompt 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 EC2 instans Anda, 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 EC2 instance yang menggunakan server proxy

1. Unduh file .exe berikut: <https://d1wk0tztpsntt1.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 proxy pada EC2 instance dengan agen yang sedang berjalan

1. Untuk mengonfigurasi dukungan proxy, versi agen Amazon Inspector Classic yang berjalan di EC2 instans 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 agen pada EC2 instance ini lagi dengan mengikuti [Menginstal agen pada instance berbasis Windows EC2](#) prosedur.
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 EC2 instans Anda 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 EC2 contoh Anda, navigasikan ke Control Panel, Tambah/Hapus Program.
3. Dalam daftar program yang terinstal, pilih agen AWS, lalu pilih Hapus instalasi.

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

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

Saat Anda mengunduh aplikasi dari internet, kami merekomendasikan Anda untuk mengautentikasi identitas penerbit perangkat lunak dan memeriksa apakah aplikasi tersebut belum diubah atau rusak setelah diterbitkan. 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 menganggap bahwa perangkat lunak untuk agen Amazon Inspector Classic telah diubah atau rusak, JANGAN menjalankan file instalasi. Alih-alih, hubungi AWS Support.

File agen Amazon Inspector untuk sistem operasi berbasis Linux ditandatangani menggunakan GnuPG implementasi sumber terbuka dari standar Pretty Good Privacy (OpenPGP) untuk tanda tangan digital yang aman. GnuPG(juga dikenal sebagaiGPG) menyediakan pemeriksaan autentikasi dan integritas melalui tanda tangan digital. Amazon EC2 menerbitkan kunci publik dan tanda tangan

yang dapat Anda gunakan untuk memverifikasi alat Amazon CLI EC2 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 berikutnya dalam proses ini adalah mengautentikasi kunci publik Amazon Inspector dan menambahkannya sebagai kunci tepercaya di dalam 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
tCdBbWF6b24gSW5zcGVjdG9yIDxpbnNwZWNo3JAYW1hem9uLmNvbT6JAJgEEwEC
ACIFAlYDlFEcGwMGCwkIBwMCBhUIAgkKCwQWAgMBAh4BAheAAoJECR0CWBYNgQY
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 jendela perintah di direktori tempat Anda menyimpan `inspector.gpg`, gunakan perintah berikut untuk mengimpor kunci publik Amazon Inspector Classic ke dalam keyring Anda:

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

Perintah tersebut mengembalikan hasil yang serupa dengan berikut ini:

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

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

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

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

Perintah ini mengembalikan hasil yang serupa dengan berikut ini:

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

Selain itu, string sidik jari harus identik dengan DDA0 D4C5 10AE 3C20 6F46 6DC0 2474 0960 5836 0418, seperti yang ditunjukkan dalam contoh sebelumnya. Bandingkan sidik jari kunci yang dikembalikan dengan yang dipublikasikan di halaman ini. Mereka harus cocok. Jika mereka tidak cocok, jangan instal skrip instalasi agen Amazon Inspector 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 tersebut dapat 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 jendela 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 dalam keyakinan bahwa Anda memiliki kunci publik yang autentik 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 ditemukan kunci yang benar-benar tepercaya. Hal ini berarti Anda (atau orang lain yang Anda percaya) tidak "benar-benar memercayai" kunci tersebut.

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

(Opsional) Verifikasi tanda tangan skrip instalasi agen Amazon Inspector 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 EC2 instance 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 peluncuran EC2 instans, lihat dokumentasi [Amazon Elastic Compute Cloud](#).

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 dinilai, Anda mulai dengan menandai EC2 instance 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 EC2 instance untuk membangun target penilaian, Anda dapat membuat kunci tag kustom sendiri atau menggunakan kunci tag yang dibuat oleh orang lain di AWS akun yang sama. Anda juga dapat menggunakan tombol tag yang dibuat AWS secara otomatis. Misalnya, AWS secara otomatis membuat kunci tag Nama untuk EC2 instance yang Anda luncurkan.

Anda dapat menambahkan tag ke EC2 instance saat membuatnya, atau Anda dapat menambahkan, mengubah, atau menghapus tag tersebut satu per satu di halaman konsol untuk setiap EC2 instance. Anda juga dapat menambahkan tag ke beberapa EC2 instance sekaligus menggunakan Editor Tag.

Untuk informasi lebih lanjut, lihat [Editor Tanda](#). Untuk informasi selengkapnya tentang menandai EC2 instance, lihat [Sumber Daya dan Tag](#).

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 AWS Management Console 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 hal berikut ini:
 - Untuk menyertakan semua EC2 instance di AWS akun ini dan Wilayah dalam target penilaian ini, pilih kotak centang Semua instance.

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 EC2 instance yang ingin Anda sertakan dalam target penilaian ini, untuk Gunakan Tag, masukkan nama kunci tag dan pasangan nilai kunci.
5. (Opsional) Saat membuat target, Anda dapat memilih kotak centang Instal Agen untuk menginstal agen pada semua EC2 instance dalam target ini. Untuk menggunakan opsi ini, EC2 instance Anda harus menginstal Agen SSM dan peran IAM yang memungkinkan Run Command. Agen SSM diinstal, secara default, pada instans Amazon EC2 Windows dan instans Amazon Linux. Amazon EC2 Systems Manager memerlukan peran IAM untuk EC2 instance yang memproses perintah dan peran terpisah untuk pengguna yang menjalankan perintah. Untuk informasi lebih lanjut, lihat [Menginstal dan Mengonfigurasi SSM Agent](#) dan [Mengonfigurasi Peran Keamanan untuk System Manager](#).

Important

Jika sebuah EC2 instance sudah memiliki agen yang berjalan di atasnya, menggunakan opsi ini menggantikan agen yang saat ini berjalan pada instance dengan versi agen terbaru.

Note

Untuk target penilaian yang ada, Anda dapat memilih tombol Install Agents with Run Command untuk menginstal agen pada semua EC2 instance dalam target ini.

Note

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

[Menginstal Agen Amazon Inspector di Beberapa EC2 Instans Menggunakan Perintah Jalankan Systems Manager.](#)

6. Pilih Simpan.

Note

Anda dapat menggunakan tombol Pratinjau Target pada halaman Target Penilaian untuk meninjau semua EC2 instance yang disertakan dalam target penilaian. Untuk setiap EC2 instance, 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 EC2 instance.

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](#).

Aturan dan paket aturan Amazon Inspector

Anda dapat menggunakan Amazon Inspector untuk menilai target penilaian Anda (koleksi sumber daya AWS) untuk potensi masalah keamanan dan kelemahan. Amazon Inspector membandingkan perilaku dan konfigurasi keamanan target penilaian untuk paket aturan keamanan yang dipilih. Dalam konteks Amazon Inspector, aturan adalah pemeriksaan keamanan yang dilakukan Amazon Inspector selama menjalankan penilaian.

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

- [Tingkat kepelikan untuk aturan di Amazon Inspector](#)
- [Paket aturan di Amazon Inspector](#)

Tingkat kepelikan untuk aturan di Amazon Inspector

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

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

Tingkat Informasi hanya menyoroti detail konfigurasi keamanan target penilaian Anda.

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

- Tinggi – Masalah dengan tingkat kepelikan tinggi bersifat sangat mendesak. Amazon Inspector merekomendasikan bahwa Anda memperlakukan masalah keamanan ini sebagai keadaan darurat dan menerapkan perbaikan segera.

- **Medium** – Masalah dengan tingkat kepelikan medium bersifat agak mendesak. Amazon Inspector merekomendasikan bahwa Anda memperbaiki masalah ini pada kemungkinan kesempatan berikutnya, misalnya, selama pembaruan layanan berikutnya.
- **Rendah** – Masalah dengan tingkat kepelikan rendah bersifat kurang mendesak. Amazon Inspector merekomendasikan bahwa Anda memperbaiki masalah ini sebagai bagian dari salah satu pembaruan layanan masa depan 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.

Paket aturan di Amazon Inspector

Penilaian Amazon Inspector dapat menggunakan kombinasi dari paket aturan berikut:

Penilaian jaringan:

- [Keterjangkauan Jaringan](#)

Penilaian host:

- [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 Anda. EC2 Temuan yang dihasilkan Amazon Inspector juga memberikan panduan tentang membatasi akses yang tidak aman.

Paket aturan Keterjangkauan Jaringan menggunakan teknologi terbaru dari inisiatif Keamanan yang AWS [dapat dibuktikan](#).

Temuan yang dihasilkan oleh aturan ini menunjukkan apakah port Anda dapat dijangkau dari internet melalui gateway internet (termasuk instans di balik Application Load Balancer atau Classic Load Balancer), koneksi peering VPC, atau VPN melalui gateway virtual. Temuan ini juga menyoroti

konfigurasi jaringan yang memungkinkan akses yang berpotensi berbahaya, seperti grup keamanan yang salah dikelola, ACLs IGWs, dan sebagainya.

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

Important

Agan Amazon Inspector Classic tidak diperlukan untuk menilai EC2 instans 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:

- [EC2 Contoh Amazon](#)
- [Application Load Balancer](#)
- [Direct Connect](#)
- [Elastic Load Balancer](#)
- [Antarmuka Jaringan Elastis](#)
- [Gateway Internet \(\) IGWs](#)
- [Daftar Kontrol Akses \(ACLs\) Jaringan](#)
- [Tabel Rute](#)
- [Grup Keamanan \(SGs\)](#)

- [Subnet](#)
- [Virtual Private Cloud \(VPCs\)](#)
- [Virtual Private Gateway \(\) 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 EC2 instans 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 target EC2 . Temuan jenis ini diberi kepelikan Rendah.

NetworkExposure

Temuan jenis ini menunjukkan informasi agregat pada port yang dapat dijangkau pada instans Anda. EC2 Untuk setiap kombinasi dari antarmuka jaringan elastis dan grup keamanan pada EC2 instans, 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	≥ 5	Kritis atau Penting
Sedang	< 5 and $\geq 2,1$	Sedang
Rendah	< 2.1 and ≥ 0.8	Rendah
Informasi	$< 0,8$	N/A

Aturan yang disertakan dalam paket ini membantu Anda menilai apakah 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.

Untuk informasi selengkapnya, lihat [Paket aturan Amazon Inspector Classic untuk sistem operasi yang didukung](#).

Patokan Pusat Keamanan Internet (CIS)

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

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

Amazon Linux

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

CentOS Linux

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

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

Perusahaan Topi Merah Linux

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

Ubuntu

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

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

Windows

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

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

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

Untuk informasi selengkapnya, lihat [Paket aturan Amazon Inspector Classic untuk sistem operasi yang didukung](#).

Praktik terbaik keamanan untuk Amazon Inspector Classic

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

Important

Saat ini, Anda dapat menyertakan EC2 instans target penilaian yang menjalankan sistem operasi berbasis Linux atau berbasis Windows.

Selama penilaian dijalankan, aturan yang dijelaskan dalam bagian ini menghasilkan temuan hanya untuk EC2 instance yang menjalankan sistem operasi berbasis Linux. Aturan tidak menghasilkan temuan untuk EC2 instance 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 EC2 instance Anda sebagai root.](#)

Keparahan

[Sedang](#)

Menemukan

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

Resolusi

Kami menyarankan Anda mengonfigurasi EC2 instans 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 EC2 instance Anda dikonfigurasi untuk mendukung protokol SSH versi 1.

Keparahan

[Sedang](#)

Menemukan

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

Resolusi

Kami menyarankan Anda mengonfigurasi EC2 instans 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 EC2 instance Anda dikonfigurasi untuk mendukung otentikasi kata sandi melalui protokol SSH.

Keparahan

[Sedang](#)

Menemukan

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

Resolusi

Kami menyarankan Anda menonaktifkan otentikasi kata sandi melalui SSH pada EC2 instans Anda dan mengaktifkan dukungan untuk otentikasi 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 EC2 instance Anda.

Keparahan

[Sedang](#)

Menemukan

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

Resolusi

Jika Anda menggunakan kata sandi, kami sarankan Anda mengonfigurasi usia maksimum untuk kata sandi pada semua EC2 instance dalam 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 EC2 instance Anda.

Keparahan

[Sedang](#)

Menemukan

EC2 Instance dalam target penilaian Anda tidak dikonfigurasi untuk durasi minimum untuk kata sandi.

Resolusi

Jika Anda menggunakan kata sandi, kami sarankan Anda mengonfigurasi panjang minimum untuk kata sandi pada semua EC2 instance dalam 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 EC2 instance Anda.

Keparahan

[Sedang](#)

Menemukan

Tidak ada mekanisme atau batasan kompleksitas kata sandi yang dikonfigurasi pada EC2 instance dalam 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, sebaiknya Anda mengonfigurasi semua EC2 instance dalam target penilaian agar memerlukan tingkat kompleksitas kata 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 EC2 instance dalam target penilaian Anda.

Keparahan

[Sedang](#)

Menemukan

EC2 Instance dalam target penilaian Anda tidak mengaktifkan ASLR.

Resolusi

Untuk meningkatkan keamanan target penilaian Anda, kami sarankan Anda mengaktifkan ASLR pada sistem operasi semua EC2 instans dalam 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 EC2 instans dalam target penilaian Anda.

Note

Aturan ini tidak didukung untuk EC2 instance dengan prosesor ARM.

Keparahan

[Sedang](#)

Menemukan

EC2 Instance dalam target penilaian Anda tidak mengaktifkan DEP.

Resolusi

Kami menyarankan Anda mengaktifkan DEP pada sistem operasi semua EC2 instans 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

EC2 Instance 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 yang jahat, konfigurasi semua direktori sistem pada semua EC2 instance di target Anda agar dapat ditulis hanya oleh pengguna yang masuk dengan menggunakan kredensi akun root.

Templat penilaian dan penilaian berjalan Amazon Inspector Classic

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

Untuk memulai, Anda membuat target penilaian (kumpulan AWS sumber daya yang Anda inginkan Amazon Inspector Classic untuk menganalisis). 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](#)
- [Batas penilaian Amazon Inspector Classic berjalan Amazon Inspector](#)
- [Mengatur penilaian berjalan otomatis melalui fungsi Lambda](#)
- [Mengatur topik SNS untuk pemberitahuan 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 menjadi tujuan Amazon SNS mengirimkan pemberitahuan tentang temuan dan keadaan penilaian berjalan Amazon SNS
- Atribut Amazon Inspector Classic (pasangan nilai-kunci) yang dapat Anda tetapkan ke temuan yang dihasilkan oleh penilaian berjalan yang menggunakan templat penilaian ini

Setelah Amazon Inspector Classic membuat templat penilaian, Anda dapat menandainya seperti sumber daya yang lain 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 menawarkan sejumlah besar aturan yang dapat Anda gunakan untuk menilai target penilaian Anda. Anda mungkin ingin menyertakan berbagai subset dari aturan yang tersedia dalam templat penilaian Anda untuk menargetkan area tertentu yang menjadi perhatian atau untuk mengungkap masalah keamanan tertentu. Menandai templat penilaian memungkinkan Anda untuk menemukan dan menjalankannya dengan cepat setiap saat sesuai dengan strategi dan tujuan keamanan Anda.

Important

Setelah membuat templat penilaian, Anda tidak dapat memodifikasinya.

Batas templat penilaian Amazon Inspector Classic

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

Untuk informasi selengkapnya, lihat [Batas layanan Amazon Inspector Classic](#).

Membuat templat penilaian

Untuk membuat templat penilaian

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

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

 Note

Ketika Anda membuat templat penilaian, Anda dapat menggunakan tombol Pratinjau Target pada halaman Templat Penilaian untuk meninjau semua EC2 instans yang termasuk dalam target penilaian. Untuk setiap EC2 instans, 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 TIDAK DIKETAHUI 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 EC2 instans 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 untuk menjadi tujuan Amazon Inspector Classic mengirimkan pemberitahuan tentang temuan dan keadaan penilaian berjalan. Amazon Inspector Classic dapat mengirimkan pemberitahuan SNS tentang kejadian 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 [Mengatur topik SNS untuk pemberitahuan 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 untuk semua temuan yang dihasilkan oleh templat 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

Ketika Anda menggunakan kotak centang ini, Amazon Inspector Classic secara otomatis membuat aturan Amazon CloudWatch Events untuk jadwal penilaian berjalan yang Anda atur. Amazon Inspector Classic kemudian secara otomatis juga membuat IAM role bernama `AWS_InspectorEvents_Invoke_Assessment_Template`. Peran ini memungkinkan CloudWatch Events membuat panggilan API terhadap sumber daya Amazon Inspector Classic. Untuk informasi selengkapnya, lihat [Apa yang dimaksud dengan Amazon CloudWatch Events?](#) 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 penilaian berjalan menggunakan templat yang sama selama Anda masih berada dalam batasan untuk setiap AWS akun. Untuk informasi selengkapnya, lihat [Batas penilaian Amazon Inspector Classic berjalan Amazon Inspector](#).

Jika Anda menggunakan konsol Amazon Inspector Classic, Anda harus memulai proses pertama templat penilaian baru Anda dari halaman Templat penilaian baru. 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](#).

Batas penilaian Amazon Inspector Classic berjalan Amazon Inspector

Anda dapat membuat hingga 50.000 penilaian berjalan 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 yang tumpang tindih EC2 .

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 berjalan otomatis menggunakan AWS Lambda konsol, lakukan prosedur berikut.

Untuk mengatur proses otomatis melalui fungsi Lambda

1. Masuk ke AWS Management Console, dan buka [AWS Lambda konsol](#).
2. Di panel navigasi, pilih Dasbor atau Fungsi, lalu pilih Buat Fungsi Lambda.
3. Pada halaman Buat fungsi, pilih Jelajahi repositori aplikasi tanpa server, lalu masukkan **inspector** di bidang pencarian.
4. Pilih inspector-scheduled-runcetak biru.
5. Pada halaman Meninjau, mengonfigurasi, dan men-deploy, siapkan jadwal berulang untuk proses otomatis dengan menentukan CloudWatch kejadian 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 kejadian dan konsep, lihat [Apa yang dimaksud dengan Amazon CloudWatch Events?](#)

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

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

7. Tinjau pilihan Anda, lalu pilih Buat fungsi.

Mengatur topik SNS untuk pemberitahuan 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 pemberitahuan 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 memublikasikan 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 Menentukan 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 Lanjutkan. Ini akan mengarahkan Anda ke editor JSON.
 - ii. Tambahkan kondisi berikut:

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

- e. (Opsional) Untuk informasi tambahan tentang aws: SourceAccount dan aws:SourceArn, lihat [Kunci konteks kondisi global](#) di Panduan Pengguna IAM.
 - f. Perbarui pengaturan lain untuk topik yang diperlukan, lalu pilih Buat topik.
2. (Opsional) Untuk membuat topik SNS terenkripsi, lihat [Enkripsi saat istirahat di Panduan Pengembang SNS](#).
 3. Untuk melindungi diri Anda dari Inspector yang digunakan sebagai wakil bingung untuk kunci KMS Anda, ikuti langkah-langkah tambahan di bawah ini:
 - a. Buka CMK Anda di konsol KMS.
 - b. Pilih Edit.
 - c. Tambahkan kondisi berikut:

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

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

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

Temuan Amazon Inspector Classic

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

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

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

Bekerja dengan temuan

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

Untuk menemukan, menganalisis, dan menetapkan atribut untuk temuan

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

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

Note

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

3. Untuk melihat detail temuan tertentu, pilih widget Perluas di samping temuan tersebut. Detail temuan tersebut mencakup hal-hal berikut:
 - Nama target penilaian yang mencakup 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 dan penilaian berjalan Amazon Inspector Classic](#).

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

Note

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

Anda dapat melihat jenis laporan penilaian berikut:

- Laporan temuan – laporan ini berisi informasi berikut:
 - Ringkasan penilaian
 - EC2 Instans yang dievaluasi selama penilaian berjalan
 - Paket aturan yang termasuk dalam penilaian berjalan
 - Informasi detail tentang setiap temuan, termasuk semua EC2 instans 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, Anda tidak dapat menghapus laporan individu. Ketika Anda menghapus penilaian berjalan, semua versi laporan dari proses tersebut dan semua temuan juga dihapus.

Anda juga dapat menghapus penilaian berjalan dengan menggunakan API [DeleteAssessmentRun](#).

Pengecualian di Amazon Inspector

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

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

Untuk menghindari timbulnya AWS biaya yang tidak perlu, Amazon Inspector memungkinkan Anda untuk melakukan pratinjau pengecualian sebelum menjalankan penilaian. Anda dapat menemukan pratinjau di halaman Templat penilaian di konsol. Untuk informasi selengkapnya, lihat [Pratinjau pengecualian](#).

Note

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

Topik

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

Jenis pengecualian

Amazon Inspector dapat menghasilkan jenis pengecualian berikut.

Jenis Pengecualian	Deskripsi	Rekomendasi									
Tidak ada	Tidak ada EC2	Periksa bahwa									

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

Jenis Pengecualian	Deskripsi	Rekomendasi								
Agen tidak ditemukan	Agen Amazon Inspector tidak ditemukan pada instans target EC2 .	Menginstall atau menginstall ulang agen Amazon Inspector pada instans target. EC2 Untuk informasi selengkapnya, lihat Menginstall agen Amazon Inspector Classic.								

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

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

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 instans target tidak didukung oleh paket aturan yang disertakan dalam templat penilaian.	<p>Buat templat penilaian tanpa paket aturan yang bertentangan atau hapus EC2 instans target dari templat penilaian.</p> <p>Untuk daftar paket aturan yang didukung oleh sistem operasi, lihat Ketersediaan Paket Aturan yang Tersedia di Seluruh Sistem Operasi</p>									

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

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

Jenis Pengecualian	Deskripsi	Rekomendasi									
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 support jika pengecualian tetap ada saat Anda menjalankan kembali penilaian.									

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

Jenis Pengecualian	Deskripsi	Rekomendasi									
Kesalahan Keterjangkauan Jaringan – 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 support jika pengecualian tetap ada saat Anda menjalankan kembali penilaian.									

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

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

Jenis Pengecualian	Deskripsi	Rekomendasi								
Kesalahan 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 support jika pengecualian tetap ada saat Anda menjalankan kembali penilaian.								

Pratinjau pengecualian

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

Untuk melakukan pratinjau pengecualian penilaian

1. Masuk ke AWS Management Console dan buka konsol Amazon Inspector 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 AWS Management Console dan buka konsol Amazon Inspector 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 EC2 instans 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 [Network Reachability](#) pada EC2 instance apa pun terlepas dari 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	Dihentikan
Amazon Linux 2018,	Didukung	Didukung	Didukung	Didukung	Dihentikan
Amazon Linux 2017,	Didukung	Didukung	Didukung	Didukung	Dihentikan

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	Dihentikan
Amazon Linux 2016,	Didukung	Didukung	Didukung	Didukung	Dihentikan
Amazon Linux 2016,	Didukung	Didukung	Didukung	Didukung	Dihentikan
Amazon Linux 2015,	Didukung	Didukung	Didukung	Didukung	Dihentikan
Amazon Linux 2015,	Didukung	Didukung	Didukung	Didukung	Dihentikan
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	Dihentikan
Ubuntu 16.04 LTS	Didukung	Didukung	Didukung	Didukung	Dihentikan
Ubuntu 14.04 LTS	Didukung	Didukung	Didukung	Didukung	Dihentikan

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	Dihentikan
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	Dihentikan
Windows Server 2019 Base	Didukung		Didukung		
Windows Server 2016 Base	Didukung	Didukung	Didukung		Dihentikan
Windows Server 2012 R2	Didukung	Didukung	Didukung		Dihentikan
Windows Server 2012	Didukung	Didukung	Didukung		Dihentikan
Windows Server 2008 R2	Didukung	Didukung	Didukung		Dihentikan

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 siapa yang membuat permintaan tersebut. Informasi identitas membantu Anda menentukan 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 AWS Management Console 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.

AssessmentTargetARNmetrik:

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

AssessmentTemplateARNmetrik:

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

[AWS Security Hub](#) memberi Anda pandangan komprehensif tentang keadaan keamanan Anda AWS dan membantu Anda memeriksa lingkungan Anda terhadap standar industri keamanan dan praktik terbaik. Security Hub 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 memungkinkan Anda untuk mengirimkan temuan dari Amazon Inspector ke Security Hub. Security Hub kemudian dapat menyertakan temuan tersebut dalam analisis postur keamanan Anda.

Daftar Isi

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

Bagaimana Amazon Inspector mengirimkan temuan ke Security Hub

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

Security Hub menyediakan alat untuk mengelola temuan dari seluruh sumber tersebut. Anda dapat melihat dan memfilter daftar temuan dan melihat detail untuk temuan. Lihat [Melihat temuan](#) di Panduan Pengguna AWS Security Hub . Anda juga dapat melacak status penyelidikan ke temuan. Lihat [Mengambil tindakan pada temuan](#) di Panduan Pengguna AWS Security Hub .

Semua temuan di Security Hub menggunakan format JSON standar yang disebut 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.

Jenis temuan yang dikirimkan Amazon Inspector

Amazon Inspector mengirimkan semua temuan yang dihasilkannya ke Security Hub.

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

- Perangkat Lunak dan Konfigurasi Checks/Vulnerabilities/CVE
- Keterjangkauan Perangkat Lunak dan Konfigurasi Checks/AWS Security Best Practices/Network
- Tolok Ukur Pengerasan Checks/Industry and Regulatory Standards/CIS Host Perangkat Lunak dan Konfigurasi

Latensi untuk mengirim temuan

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

Mencoba kembali saat Security Hub tidak tersedia

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

Memperbarui temuan yang ada di Security Hub

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

Temuan umum dari Amazon Inspector

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

Berikut adalah contoh temuan umum dari Amazon Inspector.

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

```

    "serviceAttributes/schemaVersion": "1",
    "aws/inspector/arn": "arn:aws:inspector:us-east-1:111122223333:target/0-8zh1cWkg/
template/0-rqtRV0u0/run/0-Ck2F6tY9/finding/0-B458MQWe",
    "attributes/ACL": "acl-154b8273",
    "serviceAttributes/assessmentRunArn": "arn:aws:inspector:us-
east-1:111122223333:target/0-8zh1cWkg/template/0-rqtRV0u0/run/0-Ck2F6tY9",
    "attributes/PROTOCOL": "TCP",
    "attributes/RULE_TYPE": "RecognizedPortNoAgent",
    "aws/inspector/RulesPackageName": "Network Reachability",
    "attributes/INSTANCE_ID": "i-0c10c2c7863d1a356",
    "attributes/PORT_GROUP_NAME": "SSH",
    "attributes/IGW": "igw-e209d785",
    "serviceAttributes/rulesPackageArn": "arn:aws:inspector:us-
east-1:111122223333:rulespackage/0-PmNV0Tcd",
    "attributes/SECURITY_GROUP": "sg-0af64c8a5eb30ca75",
    "attributes/ENI": "eni-078eac9d6ad9b20d1",
    "attributes/REACHABILITY_TYPE": "Internet",
    "attributes/PORT": "22",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/inspector/
inspector/us-east-1/111122223333/629ff13fbbb44c872f7bba3e7f79f60cb6d443d8",
    "aws/securityhub/ProductName": "Inspector",
    "aws/securityhub/CompanyName": "Amazon"
  },
  "Resources": [
    {
      "Type": "AwsEc2Instance",
      "Id": "arn:aws:ec2:us-east-1:193043430472:instance/i-0c10c2c7863d1a356",
      "Partition": "aws",
      "Region": "us-east-1",
      "Tags": {
        "Name": "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, Anda harus mengaktifkan Security Hub. Untuk informasi tentang cara mengaktifkan Security Hub, lihat [Menyiapkan Security Hub](#) di Panduan Pengguna AWS Security Hub .

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

Bagaimana cara menghentikan pengiriman temuan

Untuk berhenti mengirim temuan ke Security Hub, Anda dapat menggunakan konsol Security Hub atau API.

Lihat [Menonaktifkan dan mengaktifkan aliran temuan dari integrasi \(konsol\)](#) atau [Menonaktifkan aliran temuan dari integrasi \(Security Hub API, AWS CLI\)](#) di Panduan Pengguna AWS Security Hub .

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 menguraikan riwayat rilis dokumentasi Amazon Inspector setelah Mei 2018.

Perubahan	Deskripsi	Tanggal
Akhir dari pemberitahuan dukungan	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 lebih lanjut, lihat Akhir dari dukungan Amazon Inspector .	20 Mei 2025
Praktik terbaik keamanan diperbarui untuk kata sandi	Persyaratan praktik terbaik keamanan Amazon Inspector untuk panjang kata sandi dan kompleksitas kata sandi EC2 misalnya telah diperbarui. Lihat Mengonfigurasi panjang minimum kata sandi dan Mengonfigurasi kompleksitas kata sandi	Selasa, 08 Maret 2021
Dukungan ditambahkan untuk versi sistem operasi yang lebih baru	Amazon Inspector sekarang mendukung versi sistem operasi berikut: Ubuntu 20.4 LTS, Debian 10.x, RHEL 8.x, dan Windows Server 2019 Base.	15 Oktober 2020

Informasi keamanan terkonsolidasi ke dalam babak keamanan baru	Informasi keamanan untuk Amazon Inspector, termasuk informasi tentang mengelola identity and access management, dikonsolidasikan ke dalam babak keamanan. Lihat Keamanan di Amazon Inspector Classic .	7 April 2020
Dokumentasi diperbarui untuk menghapus dukungan untuk paket aturan Analisis Perilaku Waktu Aktif.	Beberapa topik diperbarui untuk menghapus informasi tentang paket aturan Analisis Perilaku Waktu Aktif, yang tidak lagi didukung.	Selasa, 05 September 2019
Dukungan OS ditambahkan	Dukungan Amazon Inspector ditambahkan untuk CentOS 7.6. Untuk informasi lebih lanjut, lihat Sistem Operasi dan Wilayah yang Didukung Amazon Inspector dan Ketersediaan Paket Aturan di Seluruh Sistem Operasi yang Didukung .	Selasa, 03 Desember 2018
Konten baru	Ditambahkan paket aturan Keterjangkauan Jaringan Amazon Inspector, yang memungkinkan pengguna untuk menjalankan penilaian tanpa agen yang menganalisis konfigurasi jaringan untuk kelemahan keamanan. Untuk informasi lebih lanjut, lihat Keterjangkauan Jaringan .	9 November 2018

Dukungan OS ditambahkan	Dukungan Amazon Inspector ditambahkan untuk RHEL 7.6. Untuk informasi lebih lanjut, lihat Sistem Operasi dan Wilayah yang Didukung Amazon Inspector dan Ketersediaan Paket Aturan di Seluruh Sistem Operasi yang Didukung .	30 Oktober 2018
Dukungan OS ditambahkan	Dukungan ditambahkan untuk berbagai sistem operasi ke paket aturan Patokan CIS. Untuk informasi lebih lanjut, lihat Patokan Pusat Keamanan Internet (CIS) dan Ketersediaan Paket Aturan di Seluruh Sistem Operasi yang Didukung .	13 Agustus 2018
Menambahkan dukungan Wilayah	Dukungan Wilayah ditambahkan untuk AWS GovCloud (US).	13 Juni 2018

Tabel berikut menguraikan riwayat rilis dokumentasi Amazon Inspector sebelum Mei 2018.

Perubahan	Deskripsi	Tanggal
Konten baru	Ditambahkan kemampuan untuk menargetkan semua EC2 instans Amazon di suatu akun. Untuk informasi selengkapnya, lihat Target penilaian Amazon Inspector Classic .	24 Mei 2018

Perubahan	Deskripsi	Tanggal
Dukungan OS ditambahkan	Dukungan Amazon Inspector ditambahkan untuk Amazon Linux 2018.03 dan Ubuntu 18.04.	15 Mei 2018
Konten baru	Ditambahkan kemampuan untuk mengatur penilaian Amazon Inspector berulang.	30 April 2018
Konten baru	Ditambahkan kemampuan untuk menginstal agen Amazon Inspector melalui konsol.	30 April 2018
Dukungan OS ditambahkan	Dukungan Amazon Inspector ditambahkan untuk Amazon Linux 2.	13 Maret 2018
Dukungan OS ditambahkan	Dukungan penilaian Amazon Inspector ditambahkan 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 sekarang dapat berjalan ketika modul kernel tidak tersedia.	11 Januari 2018
Dukungan Wilayah ditambahkan	Menambahkan dukungan Amazon Inspector Classic untuk Wilayah. EU (Frankfurt)	19 Desember 2017

Perubahan	Deskripsi	Tanggal
Konten baru	Ditambahkan kemampuan untuk memeriksa kesehatan agen Amazon Inspector dengan konsol dan API Amazon Inspector.	15 Desember 2017
Konten baru	Ditambahkan fitur berikut: <ul style="list-style-type: none">• Penggunaan peran tertaut layanan• AMI agen Amazon Inspector tersedia di Marketplace AWS• Templat Amazon Inspector Classic AWS CloudFormation	Selasa, 05 Desember 2017
Dukungan OS ditambahkan	Dukungan penilaian Amazon Inspector ditambahkan untuk CentOS 7.4.	9 November 2017
Dukungan OS ditambahkan	Dukungan penilaian Amazon Inspector ditambahkan untuk Amazon Linux 2017.09.	11 Oktober 2017
Dukungan OS ditambahkan	Dukungan penilaian Amazon Inspector ditambahkan untuk RHEL 7.4.	20 Februari 2018
Kelayakan HIPAA ditambahkan	Amazon Inspector sekarang memenuhi syarat HIPAA.	31 Juli 2017

Perubahan	Deskripsi	Tanggal
Konten baru	Ditambahkan kemampuan untuk secara otomatis memicu penilaian keamanan Amazon Inspector 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	Dukungan penilaian Amazon Inspector ditambahkan 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	Dukungan penilaian Amazon Inspector ditambahkan untuk Amazon Linux 2017.03.	25 April 2017
Konten baru dan dukungan OS ditambahkan	Ditambahkan: <ul style="list-style-type: none">• Dukungan Amazon Inspector Classic untuk Ubuntu 16.04.• Ketersediaan cetak biru Lambda untuk mengotomatiskan operasi Amazon Inspector.	Selasa, 05 Januari 2017
Dukungan OS baru	Dukungan Amazon Inspector ditambahkan untuk Microsoft Windows.	26 Agustus 2016

Perubahan	Deskripsi	Tanggal
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	Layanan Amazon Inspector diluncurkan.	7 Okt 2015

AWS Glosarium

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