Panduan Pengguna

Incident Manager

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

Incident Manager: 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

Apa itu Manajer Insiden AWS Systems Manager? ... 1
Komponen dan fitur utama ... 1
Manfaat menggunakan Manajer Insiden ... 3
Layanan terkait ... 5
Mengakses Manajer Insiden ... 5
Wilayah Manajer Insiden dan kuota ... 5
Harga untuk Manajer Insiden ... 6
Siklus hidup insiden ... 6
Peringatan dan keterlibatan ... 7
Triase ... 8
Investigasi dan mitigasi ... 9
Analisis pasca-insiden ... 10
Pengaturan ... 12
Mendaftar untuk Akun AWS ... 12
Buat pengguna dengan akses administratif ... 13
Memberikan akses programatis ... 14
Peran yang diperlukan untuk pengaturan Manajer Insiden ... 15
Memulai ... 16
Prasyarat ... 16
Siapkan penyihir ... 16
Mengelola insiden di seluruh Akun AWS dan Wilayah ... 23
Manajemen insiden lintas wilayah ... 23
Manajemen insiden lintas akun ... 24
Praktik terbaik ... 24
Siapkan dan konfigurasikan manajemen insiden lintas akun ... 24
Batasan ... 26
Mempersiapkan insiden ... 28
Pemantauan ... 30
Mengkonfigurasi set replikasi dan Temuan ... 30
Set replikasi ... 31
Mengelola tag untuk set replikasi ... 32
Mengelola fitur Temuan ... 33
Membuat dan mengonfigurasi kontak ... 34
Saluran kontak ... 34

Rencana keterlibatan ... 35
Buat kontak ... 36
Impor detail kontak ke buku alamat Anda ... 37
Mengelola rotasi responden dengan jadwal panggilan ... 37
Membuat jadwal panggilan dan rotasi ... 38
Mengelola jadwal panggilan yang ada ... 43
Membuat rencana eskalasi untuk keterlibatan responden ... 49
Tahapan ... 49
Buat rencana eskalasi ... 50
Membuat dan mengintegrasikan saluran obrolan untuk responden ... 50
Tugas 1: Membuat atau memperbarui topik Amazon SNS untuk saluran obrolan Anda ... 51
Tugas 2: Buat saluran obrolan di Amazon Q Developer di aplikasi obrolan ... 53
Tugas 3: Tambahkan saluran obrolan ke rencana respons di Manajer Insiden ... 56
Berinteraksi melalui saluran obrolan ... 56
Mengintegrasikan runbook Automation Systems Manager untuk remediasi insiden ... 57
Izin IAM diperlukan untuk memulai dan menjalankan alur kerja runbook ... 58
Bekerja dengan parameter runbook ... 61
Tentukan runbook ... 63
Templat runbook Manajer Insiden ... 64
Membuat dan mengonfigurasi rencana respons ... 65
Membuat rencana respons ... 66
Mengidentifikasi potensi penyebab insiden dari layanan lain ... 73
Mengaktifkan dan membuat peran layanan untuk temuan ... 74
Konfigurasikan izin untuk dukungan temuan lintas akun ... 75
Membuat insiden secara otomatis atau manual ... 76
Membuat insiden secara otomatis dengan alarm CloudWatch ... 77
Membuat insiden secara otomatis dengan acara EventBridge ... 78
Membuat insiden menggunakan acara mitra SaaS ... 78
Membuat insiden menggunakan acara AWS layanan ... 80
Membuat insiden secara manual ... 81
Izin IAM yang diperlukan untuk memulai insiden secara manual ... 81
Melihat detail insiden di konsol ... 84
Melihat daftar insiden di konsol ... 84
Melihat detail insiden di konsol ... 84
Spanduk teratas ... 85
Catatan insiden ... 86

Tab ... 86
Gambaran Umum ... 86
Diagnosis ... 87
Garis Waktu ... 89
Runbook ... 89
Keterlibatan ... 90
Item terkait ... 91
Properti ... 91
Melakukan analisis pasca-insiden ... 93
Rincian analisis ... 93
Gambaran Umum ... 93
Metrik ... 94
Garis Waktu ... 94
Pertanyaan ... 95
Tindakan ... 95
Daftar periksa ... 95
Template analisis ... 96
AWS Template standar ... 96
Buat template analisis ... 96
Buat analisis ... 96
Cetak analisis insiden yang diformat ... 97
Tutorial ... 98
Menggunakan runbook dengan Manajer Insiden ... 98
Tugas 1: Membuat runbook ... 99
Tugas 2: Membuat peran IAM ... 102
Tugas 3: Menghubungkan runbook ke rencana respons Anda ... 104
Tugas 4: Menetapkan CloudWatch alarm ke rencana respons Anda ... 105
Tugas 5: Memverifikasi hasil ... 105
Mengelola insiden keamanan ... 107
Pemberian tag pada sumber daya ... 109
Keamanan ... 111
Perlindungan data ... 112
Enkripsi data ... 113
Identity and Access Management ... 115
Audiens ... 116
Mengautentikasi dengan identitas ... 116

Mengelola akses menggunakan kebijakan 120
Bagaimana Manajer Insiden AWS Systems Manager bekerja dengan IAM 123
Contoh kebijakan berbasis identitas 131
Contoh kebijakan berbasis sumber daya 135
Pencegahan "confused deputy" lintas layanan 137
Menggunakan peran terkait layanan 138
AWS kebijakan terkelola untuk Manajer Insiden 141
Pemecahan Masalah 149
Bekerja dengan kontak bersama dan rencana respons di Manajer Insiden 151
Prasyarat untuk berbagi kontak dan rencana respons 152
Layanan terkait 152
Berbagi rencana kontak atau respons 153
Berhenti berbagi kontak bersama atau rencana tanggapan 153
Mengidentifikasi kontak bersama atau rencana tanggapan 154
Izin rencana kontak dan respons bersama 155
Tagihan dan pengukuran 155
Batas instans 155
Validasi kepatuhan 155
Ketahanan 156
Keamanan infrastruktur 157
Bekerja dengan titik akhir VPC ()AWS PrivateLink 158
Pertimbangan untuk titik akhir VPC Manajer Insiden 158
Membuat titik akhir VPC antarmuka untuk Manajer Insiden 158
Membuat kebijakan titik akhir VPC untuk Manajer Insiden 159
Konfigurasi dan analisis kerentanan 160
Praktik terbaik keamanan 160
Praktik terbaik keamanan preventif untuk Manajer Insiden 160
Praktik terbaik keamanan Detektif untuk Manajer Insiden 162
Pemantauan 164
Memantau metrik dengan Amazon CloudWatch 164
Melihat metrik Manajer Insiden di konsol CloudWatch 166
Dimensi untuk Metrik 167
Logging panggilan API menggunakan AWS CloudTrail 168
Acara manajemen Manajer Insiden di CloudTrail 169
Contoh acara Manajer Insiden 170
Integrasi produk dan layanan 172

Integrasi dengan Layanan AWS 172
Integrasi dengan produk dan layanan lainnya 178
Menyimpan kredensyal PagerDuty akses secara rahasia AWS Secrets Manager 184
Pemecahan Masalah 190
Pesan galat: `ValidationException – We were unable to validate the AWS Secrets Manager secret` 190
Masalah pemecahan masalah lainnya 192
Riwayat dokumen 193
..... ccxii

Apa itu Manajer Insiden AWS Systems Manager?

Incident Manager, alat di AWS Systems Manager, dirancang untuk membantu Anda mengurangi dan memulihkan dari insiden yang memengaruhi aplikasi Anda yang di-host. AWS

Dalam konteks AWS, insiden adalah gangguan yang tidak direncanakan atau penurunan kualitas layanan yang dapat berdampak signifikan pada operasi bisnis. Oleh karena itu, sangat penting bagi organisasi untuk menetapkan strategi respons untuk mengurangi dan memulihkan secara efisien dari insiden, dan menerapkan tindakan untuk mencegah insiden di masa depan.

Manajer Insiden membantu mengurangi waktu untuk menyelesaikan insiden dengan:

- Menyediakan rencana otomatis untuk melibatkan orang-orang yang bertanggung jawab untuk menanggapi insiden secara efisien.
- Menyediakan data pemecahan masalah yang relevan.
- Mengaktifkan tindakan respons otomatis dengan menggunakan runbook Otomasi yang telah ditentukan sebelumnya.
- Menyediakan metode untuk berkolaborasi dan berkomunikasi dengan semua pemangku kepentingan.

Fitur dan alur kerja yang dibangun ke dalam Manajer Insiden didasarkan pada praktik terbaik untuk respons insiden yang telah dikembangkan Amazon hampir sejak awal. Incident Manager terintegrasi dengan Layanan AWS seperti Amazon CloudWatch,, AWS CloudTrail AWS Systems Manager, dan Amazon EventBridge.

Komponen dan fitur utama

Bagian ini menjelaskan fitur di Manajer Insiden yang Anda gunakan untuk menyiapkan rencana respons insiden.

Rencana respons

Rencana respons berfungsi sebagai templat yang mendefinisikan apa yang harus ada ketika suatu insiden terjadi. Ini termasuk informasi seperti:

- Siapa yang diminta untuk merespons ketika suatu insiden terjadi.

- Respon otomatis yang mapan untuk mengurangi insiden tersebut.
- Alat kolaborasi yang harus digunakan responden untuk berkomunikasi dan menerima pemberitahuan otomatis tentang insiden tersebut.

Deteksi insiden

Anda dapat mengonfigurasi CloudWatch alarm Amazon dan EventBridge peristiwa Amazon untuk membuat insiden saat kondisi atau perubahan yang memengaruhi AWS sumber daya Anda terdeteksi.

Dukungan otomatisasi Runbook

Anda dapat memulai runbook Otomasi dari dalam Manajer Insiden untuk mengotomatiskan respons kritis Anda terhadap insiden dan memberikan langkah-langkah terperinci kepada responden pertama.

Keterlibatan dan eskalasi

Rencana keterlibatan menentukan setiap orang untuk memberi tahu setiap insiden unik. Anda dapat menentukan kontak individual yang telah ditambahkan ke Manajer Insiden atau menentukan jadwal panggilan yang Anda buat di Manajer Insiden. Rencana keterlibatan juga menentukan jalur eskalasi untuk membantu memastikan visibilitas di antara para pemangku kepentingan dan partisipasi aktif selama proses respons insiden.

Jadwal panggilan

Jadwal panggilan di Manajer Insiden terdiri dari satu atau lebih rotasi yang Anda buat untuk jadwal tersebut. Untuk setiap rotasi, Anda dapat menyertakan hingga 30 kontak. Ketika ditambahkan ke rencana eskalasi atau rencana respons, jadwal panggilan menentukan siapa yang diberitahu ketika insiden terjadi yang memerlukan intervensi responden. Jadwal panggilan membantu memastikan bahwa Anda memiliki cakupan penuh, berlebihan, 24/7 sesuai kebutuhan untuk respons insiden Anda.

Kolaborasi aktif

Responden insiden secara aktif menanggapi insiden melalui integrasi dengan Pengembang Amazon Q di klien aplikasi obrolan. Pengembang Amazon Q dalam aplikasi obrolan mendukung pembuatan saluran obrolan untuk Manajer Insiden yang menggunakan Slack, Microsoft Teams, atau Amazon Chime. Responden dapat berkomunikasi langsung satu sama lain, menerima pemberitahuan otomatis tentang insiden, dan—di Slack and Microsoft Teams—langsung menjalankan beberapa operasi antarmuka baris perintah Manajer Insiden (CLI).

Diagnosis insiden

Responden dapat melihat up-to-date informasi di konsol Manajer Insiden selama insiden terjadi. Berdasarkan perubahan informasi, responden kemudian dapat membuat item tindak lanjut dan memperbaikinya dengan menggunakan runbook Otomasi.

Temuan dari layanan lain

Untuk mendukung diagnosis insiden responden, Anda dapat mengaktifkan fitur Temuan di Manajer Insiden. Temuan adalah informasi tentang AWS CodeDeploy penyebaran dan pembaruan AWS CloudFormation tumpukan yang terjadi sekitar waktu insiden, dan yang melibatkan satu atau lebih sumber daya yang kemungkinan terkait dengan insiden tersebut. Memiliki informasi ini mengurangi waktu yang dibutuhkan untuk mengevaluasi penyebab potensial, yang dapat mengurangi mean time to recover (MTTR) dari suatu insiden.

Analisis pasca-insiden

Setelah insiden diselesaikan, Anda menggunakan analisis pasca-insiden untuk mengidentifikasi peningkatan respons insiden Anda, termasuk waktu untuk deteksi dan mitigasi. Analisis juga dapat membantu Anda memahami akar penyebab insiden tersebut. Manajer Insiden membuat item tindakan tindak lanjut yang direkomendasikan yang dapat Anda gunakan untuk meningkatkan respons insiden Anda.

Manfaat menggunakan Manajer Insiden

Pelajari tentang manfaat menggunakan Manajer Insiden dalam operasi deteksi dan respons insiden Anda.

Bagian ini menjelaskan keuntungan yang dapat diperoleh organisasi Anda saat Anda menerapkan rencana respons Manajer Insiden.

Mendiagnosis masalah secara efisien dan segera

CloudWatch Alarm Amazon dan EventBridge peristiwa Amazon yang Anda konfigurasikan dapat membuat insiden secara otomatis ketika ada gangguan yang tidak direncanakan atau pengurangan kualitas layanan Anda.

CloudWatch alarm mendeteksi dan melaporkan ketika ada perubahan pada nilai metrik atau ekspresi yang relatif terhadap ambang batas selama beberapa periode waktu. EventBridge peristiwa dibuat sebagai hasil dari perubahan lingkungan, aplikasi, atau layanan yang telah Anda tentukan dalam EventBridge aturan. Saat Anda membuat alarm atau acara, Anda dapat menentukan tindakan untuk

insiden yang akan dibuat di Manajer Insiden dan rencana respons yang sesuai untuk memfasilitasi keterlibatan, eskalasi, dan mitigasi insiden tersebut.

Manajer Insiden menyediakan kemampuan untuk secara otomatis mengumpulkan dan melacak metrik yang terkait dengan suatu insiden, melalui penggunaan CloudWatch metrik. Selain metrik otomatis yang dihasilkan untuk insiden saat dibuat melalui CloudWatch alarm, Anda dapat menambahkan metrik secara manual secara real time, untuk memberikan konteks dan data tambahan kepada responden dalam suatu insiden.

Gunakan timeline insiden Manajer Insiden untuk menampilkan tempat menarik dalam urutan kronologis. Responden juga dapat menggunakan timeline untuk menambahkan peristiwa khusus untuk menggambarkan apa yang mereka lakukan atau apa yang terjadi. Tempat menarik otomatis meliputi:

- CloudWatch Alarm atau EventBridge aturan menciptakan insiden.
- Metrik insiden dilaporkan ke Manajer Insiden.
- Responden terlibat.
- Langkah-langkah buku runbook berhasil diselesaikan.

Terlibat secara efektif

Manajer Insiden menyatukan responden insiden melalui penggunaan kontak, jadwal panggilan, rencana eskalasi, dan saluran obrolan. Anda menentukan kontak individu secara langsung di Manajer Insiden dan menentukan preferensi kontak (email, SMS, atau suara). Anda menambahkan kontak ke rotasi jadwal panggilan untuk menentukan siapa yang terlibat untuk menangani insiden selama periode tertentu. Dengan menggunakan kontak dan jadwal panggilan yang ditentukan, Anda membuat rencana eskalasi untuk melibatkan responden yang diperlukan pada waktu yang tepat selama insiden.

Berkolaborasi secara real time

Komunikasi selama insiden adalah kunci untuk resolusi yang lebih cepat. Menggunakan Pengembang Amazon Q di aplikasi obrolan yang disiapkan klien untuk digunakan Slack, Microsoft Teams, atau Amazon Chime, Anda dapat mempertemukan responden di saluran obrolan terhubung pilihan mereka di mana mereka berinteraksi langsung dengan insiden tersebut dan satu sama lain. Manajer Insiden juga menampilkan tindakan real-time dari responden insiden di saluran obrolan, memberikan konteks kepada orang lain.

Mengotomatiskan restorasi layanan

Manajer Insiden memungkinkan responden Anda untuk fokus pada tugas-tugas utama yang diperlukan untuk menyelesaikan insiden melalui penggunaan runbook Otomasi. Di Manajer Insiden, runbook adalah serangkaian tindakan yang telah ditentukan sebelumnya yang diambil untuk menyelesaikan suatu insiden. Mereka menggabungkan kekuatan tugas otomatis dengan langkah-langkah manual sesuai kebutuhan, membuat responden lebih tersedia untuk menganalisis dan menanggapi dampak.

Mencegah insiden future

Dengan menggunakan analisis pasca insiden Manajer Insiden, tim Anda dapat mengembangkan rencana respons yang lebih kuat dan perubahan efek di seluruh aplikasi Anda untuk mencegah insiden dan waktu henti di masa depan. Analisis pasca-insiden juga menyediakan pembelajaran berulang dan peningkatan runbook, rencana respons, dan metrik.

Layanan terkait

Incident Manager terintegrasi dengan beberapa layanan Layanan AWS dan alat pihak ketiga lainnya untuk membantu Anda mendeteksi dan menyelesaikan insiden, dan berinteraksi dengan operasi API-nya secara tidak langsung dan mengelola infrastruktur. Untuk informasi, lihat Integrasi produk dan layanan dengan Manajer Insiden.

Mengakses Manajer Insiden

Anda dapat mengakses Manajer Insiden dengan salah satu cara berikut:

- Konsol Manajer Insiden
- AWS CLI— Untuk informasi umum, lihat Memulai dengan AWS CLI di Panduan AWS Command Line Interface Pengguna. Untuk informasi tentang perintah CLI untuk Manajer Insiden, lihat ssm-incidents dan ssm-contactsdalam AWS CLI Command Reference.
- API Manajer Insiden — Untuk informasi selengkapnya, lihat Referensi Manajer Insiden AWS Systems Manager API.
- AWS SDKs— Untuk informasi selengkapnya, lihat Alat untuk Dibangun AWS.

Wilayah Manajer Insiden dan kuota

Incident Manager tidak didukung di semua yang Wilayah AWS didukung oleh Systems Manager.

Untuk melihat informasi tentang Wilayah Manajer Insiden dan kuota, lihat Manajer Insiden AWS Systems Manager titik akhir dan kuota di. Referensi Umum Amazon Web

Harga untuk Manajer Insiden

Ada biaya untuk menggunakan Manajer Insiden. Untuk informasi selengkapnya, lihat harga AWS Systems Manager.

> **Note**
>
> Konten lain Layanan AWS, AWS konten, dan konten pihak ketiga yang tersedia sehubungan dengan layanan ini dapat dikenakan biaya terpisah dan diatur oleh ketentuan tambahan.

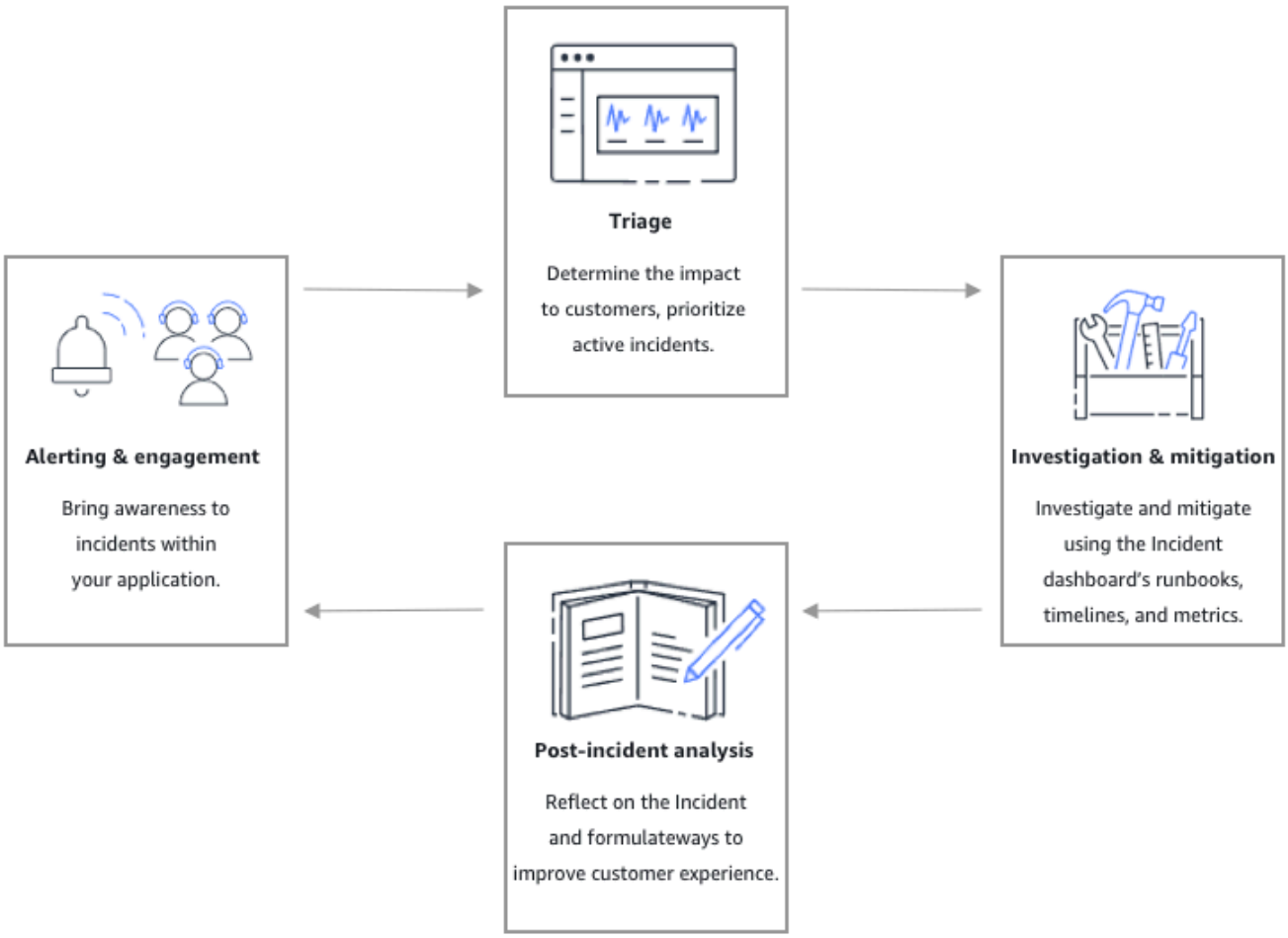
Untuk gambaran umum Trusted Advisor, layanan yang membantu Anda mengoptimalkan biaya, keamanan, dan kinerja AWS lingkungan Anda, lihat AWS Trusted Advisordi Panduan AWS Dukungan Pengguna.

Siklus hidup insiden di Manajer Insiden

Manajer Insiden AWS Systems Manager menyediakan step-by-step kerangka kerja berdasarkan praktik terbaik untuk mengidentifikasi dan bereaksi terhadap insiden, seperti pemadaman layanan atau ancaman keamanan. Fokus utama Manajer Insiden adalah membantu memulihkan layanan atau aplikasi yang terpengaruh ke normal secepat mungkin melalui solusi manajemen siklus hidup insiden yang lengkap.

Seperti yang digambarkan dalam ilustrasi berikut, Manajer Insiden menyediakan alat dan praktik terbaik untuk setiap fase siklus hidup insiden:

- Peringatan dan keterlibatan
- Triase
- Investigasi dan mitigasi
- Analisis pasca-insiden



Peringatan dan keterlibatan

Fase peringatan dan keterlibatan dari siklus hidup insiden berfokus pada kesadaran akan insiden dalam aplikasi dan layanan Anda. Fase ini dimulai sebelum insiden terdeteksi dan membutuhkan pemahaman mendalam tentang aplikasi Anda. Anda dapat menggunakan CloudWatchmetrik Amazon untuk memantau data tentang kinerja aplikasi Anda, atau menggunakan Amazon EventBridge untuk mengumpulkan peringatan dari berbagai sumber, aplikasi, dan layanan. Setelah menyiapkan pemantauan untuk aplikasi Anda, Anda dapat mulai memberi tahu metrik yang menyimpang di luar norma historis. Untuk mempelajari lebih lanjut tentang memantau praktik terbaik, lihatPemantauan.

Untuk mendukung diagnosis insiden responden, Anda dapat mengaktifkan fitur Temuan di Manajer Insiden. Temuan adalah informasi tentang AWS CodeDeploy penyebaran dan pembaruan AWS CloudFormation tumpukan yang terjadi sekitar waktu insiden. Memiliki informasi ini mengurangi waktu

yang dibutuhkan untuk mengevaluasi penyebab potensial, yang dapat mengurangi mean time to recover (MTTR) dari suatu insiden.

Sekarang setelah Anda memantau insiden dalam aplikasi Anda, Anda dapat menentukan rencana respons insiden yang akan digunakan selama insiden. Untuk mempelajari lebih lanjut tentang membuat rencana respons, lihatMembuat dan mengonfigurasi rencana respons di Manajer Insiden. EventBridge Acara Amazon atau CloudWatch Alarm dapat secara otomatis membuat insiden menggunakan paket respons sebagai templat. Untuk mempelajari lebih lanjut tentang penciptaan insiden, lihatMembuat insiden secara otomatis atau manual di Manajer Insiden.

Rencana respons meluncurkan rencana eskalasi terkait dan rencana keterlibatan untuk membawa responden pertama ke dalam insiden tersebut. Untuk informasi selengkapnya tentang menyiapkan rencana eskalasi, lihatBuat rencana eskalasi. Secara bersamaan, Pengembang Amazon Q dalam aplikasi obrolan memberi tahu responden menggunakan saluran obrolan yang mengarahkan mereka ke halaman detail insiden. Dengan menggunakan saluran obrolan dan detail insiden, tim dapat berkomunikasi dan melakukan triase insiden. Untuk informasi selengkapnya tentang menyiapkan saluran obrolan di Manajer Insiden, lihatTugas 2: Buat saluran obrolan di Amazon Q Developer di aplikasi obrolan.

Triase

Triase adalah ketika responden pertama mencoba untuk menentukan dampaknya terhadap pelanggan. Tampilan detail insiden di konsol Manajer Insiden memberi responden jadwal dan metrik untuk membantu mereka menilai insiden tersebut. Menilai dampak dari suatu insiden juga meletakkan dasar untuk waktu respons, resolusi, dan komunikasi untuk insiden tersebut. Responden memprioritaskan insiden dengan menggunakan peringkat dampak dari 1 (Kritis) hingga 5 (Tanpa Dampak).

Organisasi Anda dapat menentukan cakupan yang tepat dari setiap peringkat dampak sesuai pilihan Anda. Tabel berikut memberikan contoh bagaimana setiap tingkat dampak biasanya dapat didefinisikan.

Kode dampak	Nama dampak	Sampel ruang lingkup yang ditentukan
1	`Critical`	Kegagalan aplikasi penuh yang berdampak pada sebagian besar pelanggan.

Kode dampak	Nama dampak	Sampel ruang lingkup yang ditentukan
2	`High`	Kegagalan aplikasi penuh yang berdampak pada sebagian pelanggan.
3	`Medium`	Kegagalan aplikasi sebagian yang berdampak pada pelanggan.
4	`Low`	Kegagalan intermiten yang berdampak terbatas pada pelanggan.
5	`No Impact`	Pelanggan saat ini tidak terpengaruh tetapi tindakan mendesak diperlukan untuk menghindari dampak.

Investigasi dan mitigasi

Tampilan detail insiden memberi tim Anda runbook, garis waktu, dan metrik. Untuk melihat bagaimana Anda dapat bekerja dengan suatu insiden, lihatMelihat detail insiden di konsol.

Runbook biasanya menyediakan langkah-langkah investigasi dan dapat secara otomatis menarik data atau mencoba solusi yang umum digunakan. Runbook juga memberikan langkah-langkah yang jelas dan berulang yang menurut tim Anda berguna dalam mengurangi insiden. Tab runbook berfokus pada langkah runbook saat ini dan menunjukkan langkah masa lalu dan masa depan.

Incident Manager terintegrasi dengan Systems Manager Automation untuk membangun runbook. Gunakan runbook untuk melakukan salah satu hal berikut:

- Mengelola contoh dan sumber daya AWS
- Jalankan skrip secara otomatis
- Kelola AWS CloudFormation sumber daya

Untuk informasi selengkapnya tentang jenis tindakan yang didukung, lihat referensi tindakan Otomasi Systems Manager di Panduan AWS Systems Manager Pengguna.

Tab Timeline menunjukkan tindakan apa yang telah diambil. Timeline mencatat masing-masing dengan stempel waktu dan detail yang dibuat secara otomatis. Untuk menambahkan peristiwa khusus ke timeline, lihat Garis Waktu bagian di halaman Detail insiden di panduan pengguna ini.

Tab Diagnosis menampilkan metrik yang diisi secara otomatis dan metrik yang ditambahkan secara manual. Pandangan ini memberikan informasi berharga tentang aktivitas aplikasi Anda selama insiden.

Tab Keterlibatan memungkinkan Anda menambahkan kontak tambahan ke insiden tersebut dan membantu menyediakan sumber daya bagi kontak yang terlibat untuk mempercepat dengan cepat setelah terlibat dalam insiden tersebut. Kontak terlibat melalui rencana eskalasi yang ditentukan atau rencana keterlibatan pribadi.

Menggunakan saluran obrolan, Anda dapat langsung berinteraksi dengan insiden Anda dan responden lain di tim Anda. Menggunakan Amazon Q Developer dalam aplikasi obrolan, Anda dapat mengonfigurasi saluran obrolan di. Slack, Microsoft Teams, dan Amazon Chime. Masuk Slack and Microsoft Teams saluran, responden dapat berinteraksi dengan insiden langsung dari saluran obrolan menggunakan sejumlah perintah. `ssm-incidents` Untuk informasi selengkapnya, lihat Berinteraksi melalui saluran obrolan.

Analisis pasca-insiden

Incident Manager menyediakan kerangka kerja untuk merefleksikan insiden, mengambil langkah-langkah yang diperlukan untuk mencegah insiden terjadi lagi di masa depan, dan untuk meningkatkan aktivitas respons insiden secara keseluruhan. Perbaikan dapat mencakup:

- Perubahan pada aplikasi yang terlibat dalam suatu insiden. Tim Anda dapat menggunakan waktu ini untuk meningkatkan sistem dan membuatnya lebih toleran terhadap kesalahan.
- Perubahan pada rencana respons insiden. Luangkan waktu untuk memasukkan pelajaran yang dipelajari.
- Perubahan pada runbook. Tim Anda dapat menyelam jauh ke dalam langkah-langkah yang diperlukan untuk resolusi dan langkah-langkah yang dapat Anda otomatiskan.
- Perubahan pada peringatan. Setelah insiden, tim Anda mungkin telah memperhatikan titik-titik penting dalam metrik yang dapat Anda gunakan untuk mengingatkan tim lebih cepat tentang suatu insiden.

Manajer Insiden memfasilitasi peningkatan potensial ini dengan menggunakan serangkaian pertanyaan analisis pasca-insiden dan item tindakan di samping garis waktu insiden. Untuk mempelajari lebih lanjut tentang peningkatan melalui analisis, lihatMenjalankan analisis pasca-insiden di Incident Manager.

Menyiapkan Manajer Insiden AWS Systems Manager

Sebaiknya siapkan Manajer Insiden AWS Systems Manager di akun yang Anda gunakan untuk mengelola operasi Anda. Sebelum Anda menggunakan Manajer Insiden untuk pertama kalinya, selesaikan tugas-tugas berikut:

Topik

- Mendaftar untuk Akun AWS
- Buat pengguna dengan akses administratif
- Memberikan akses programatis
- Peran yang diperlukan untuk pengaturan Manajer Insiden

Mendaftar untuk Akun AWS

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

Untuk mendaftar untuk Akun AWS

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

   Bagian dari prosedur pendaftaran melibatkan menerima panggilan telepon atau pesan teks dan memasukkan kode verifikasi pada keypad telepon.

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

AWS mengirimkan email konfirmasi setelah proses pendaftaran selesai. Kapan saja, Anda dapat melihat aktivitas akun Anda saat ini dan mengelola akun Anda dengan masuk https://aws.amazon.comke/ dan memilih Akun Saya.

Buat pengguna dengan akses administratif

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

Amankan Anda Pengguna root akun AWS

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

   Untuk bantuan masuk dengan menggunakan pengguna root, lihat Masuk sebagai pengguna root di AWS Sign-In Panduan Pengguna.

2. Mengaktifkan autentikasi multi-faktor (MFA) untuk pengguna root Anda.

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

Buat pengguna dengan akses administratif

1. Aktifkan Pusat Identitas IAM.

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

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

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

Masuk sebagai pengguna dengan akses administratif

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

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

Tetapkan akses ke pengguna tambahan

1. Di Pusat Identitas IAM, buat set izin yang mengikuti praktik terbaik menerapkan izin hak istimewa paling sedikit.

   Untuk petunjuk, lihat Membuat set izin di Panduan AWS IAM Identity Center Pengguna.
2. Tetapkan pengguna ke grup, lalu tetapkan akses masuk tunggal ke grup.

   Untuk petunjuk, lihat Menambahkan grup di Panduan AWS IAM Identity Center Pengguna.

Memberikan akses programatis

Pengguna membutuhkan akses terprogram jika mereka ingin berinteraksi dengan AWS luar. AWS Management Console Cara untuk memberikan akses terprogram tergantung pada jenis pengguna yang mengakses AWS.

Untuk memberi pengguna akses programatis, pilih salah satu opsi berikut.

Pengguna mana yang membutuhkan akses programatis?	Untuk	Oleh
Identitas tenaga kerja (Pengguna yang dikelola di Pusat Identitas IAM)	Gunakan kredensi sementara untuk menandatangani permintaan terprogram ke AWS CLI,, AWS SDKs atau. AWS APIs	Mengikuti petunjuk untuk antarmuka yang ingin Anda gunakan. • Untuk AWS CLI, lihat Mengkonfigurasi yang akan AWS CLI digunakan AWS IAM Identity Center dalam Panduan AWS Command Line Interface Pengguna. • Untuk AWS SDKs, alat, dan AWS APIs, lihat Autentika si Pusat Identitas IAM di Panduan Referensi Alat AWS SDKs dan Alat.

Pengguna mana yang membutuhkan akses programatis?	Untuk	Oleh
IAM	Gunakan kredensi sementara untuk menandatangani permintaan terprogram ke AWS CLI,, AWS SDKs atau. AWS APIs	Mengikuti petunjuk dalam Menggunakan kredensil sementara dengan AWS sumber daya di Panduan Pengguna IAM.
IAM	(Tidak direkomendasikan) Gunakan kredensi jangka panjang untuk menandata ngani permintaan terprogra m ke AWS CLI,, AWS SDKs atau. AWS APIs	Mengikuti petunjuk untuk antarmuka yang ingin Anda gunakan. • Untuk mengetahui AWS CLI, lihat Mengautentikasi menggunakan kredensil pengguna IAM di Panduan Pengguna.AWS Command Line Interface • Untuk AWS SDKs dan alat, lihat Mengautentikasi menggunakan kredensil jangka panjang di Panduan Referensi Alat AWS SDKs dan Alat. • Untuk AWS APIs, lihat Mengelola kunci akses untuk pengguna IAM di Panduan Pengguna IAM.

Peran yang diperlukan untuk pengaturan Manajer Insiden

Sebelum memulai, akun Anda harus memiliki izin `iam:CreateServiceLinkedRole` IAM. Manajer Insiden menggunakan izin ini untuk membuat akun Anda. `AWSServiceRoleforIncidentManager` Lihat informasi yang lebih lengkap di Menggunakan peran terkait layanan untuk Manajer Insiden.

Memulai dengan Manajer Insiden

Bagian ini berjalan melalui Bersiaplah di konsol Manajer Insiden. Anda harus menyelesaikan Bersiaplah di konsol sebelum Anda dapat menggunakannya untuk manajemen insiden. Wizard memandu Anda melalui pengaturan set replikasi Anda, setidaknya satu kontak dan satu rencana eskalasi, dan rencana respons pertama Anda. Panduan berikut akan membantu Anda memahami Manajer Insiden dan siklus hidup insiden:

- Apa itu Manajer Insiden AWS Systems Manager?
- Siklus hidup insiden di Manajer Insiden

Prasyarat

Jika Anda menggunakan Manajer Insiden untuk pertama kalinya, lihatMenyiapkan Manajer Insiden AWS Systems Manager. Sebaiknya siapkan Manajer Insiden di akun yang Anda gunakan untuk mengelola operasi Anda.

Kami menyarankan Anda menyelesaikan pengaturan cepat Systems Manager sebelum memulai panduan Incident Manager Get prepared. Gunakan Pengaturan Cepat Systems Manager untuk mengonfigurasi AWS layanan dan fitur yang sering digunakan dengan praktik terbaik yang direkomendasikan. Incident Manager menggunakan fitur Systems Manager untuk mengelola insiden yang terkait dengan Anda Akun AWS dan manfaat dari konfigurasi Systems Manager terlebih dahulu.

Siapkan penyihir

Saat pertama kali Anda menggunakan Manajer Insiden, Anda dapat mengakses panduan Bersiaplah dari beranda layanan Manajer Insiden. Untuk mengakses panduan Bersiaplah setelah Anda pertama kali menyelesaikan penyiapan, pilih Siapkan pada halaman daftar Insiden.

1. Buka konsol Manajer Insiden.
2. Di beranda layanan Manajer Insiden, pilih Bersiaplah.

Pengaturan umum

1. Di bawah Pengaturan umum, pilih Mengatur.

2. Baca syarat dan ketentuan. Jika Anda menyetujui syarat dan ketentuan Manajer Insiden, pilih Saya telah membaca dan menyetujui syarat dan ketentuan Manajer Insiden, lalu pilih Berikutnya.
3. Di area Regions, Anda saat ini Wilayah AWS muncul sebagai Region pertama di set replikasi Anda. Untuk menambahkan lebih banyak Wilayah ke set replikasi Anda, pilih dari daftar Wilayah.

   Kami merekomendasikan untuk menyertakan setidaknya dua Wilayah. Jika satu Wilayah tidak tersedia sementara, kegiatan terkait insiden masih dapat dialihkan ke Wilayah lain.

   > **Note**
   >
   > Membuat set replikasi akan menciptakan peran `AWSServiceRoleforIncidentManager` terkait layanan di akun Anda. Untuk mempelajari selengkapnya tentang peran ini, lihat Menggunakan peran terkait layanan untuk Manajer Insiden.

4. Untuk menyiapkan enkripsi untuk set replikasi Anda, lakukan salah satu hal berikut:

   > **Note**
   >
   > Semua sumber daya Manajer Insiden dienkripsi. Untuk mempelajari lebih lanjut tentang cara data Anda dienkripsi, lihat. Perlindungan data di Manajer Insiden Untuk informasi selengkapnya tentang set replikasi Manajer Insiden Anda, lihatMengkonfigurasi set replikasi Manajer Insiden.

   - Untuk menggunakan kunci yang AWS dimiliki, pilih Gunakan kunci AWS yang dimiliki.
   - Untuk menggunakan AWS KMS kunci Anda sendiri, pilih Pilih yang sudah ada AWS KMS key. Untuk setiap Wilayah yang Anda pilih pada langkah 3, pilih AWS KMS kunci, atau masukkan Nama Sumber Daya AWS KMS Amazon (ARN).

     > **Tip**
     >
     > Jika Anda tidak memiliki yang tersedia AWS KMS key, pilih Buat AWS KMS key.

5. (Opsional) Di area Tag, tambahkan satu atau lebih tag ke set replikasi. Tag menyertakan kunci dan, secara opsional, nilai.

Tanda adalah metadata opsional yang Anda tetapkan ke sumber daya. Tag memungkinkan Anda untuk mengkategorikan sumber daya dengan berbagai cara, seperti berdasarkan tujuan, pemilik, atau lingkungan. Untuk informasi selengkapnya, lihat Menandai sumber daya di Manajer Insiden.

6. (Opsional) Di area akses Layanan, untuk mengaktifkan fitur Temuan, pilih kotak centang Buat peran layanan untuk temuan di akun ini.

   Temuan adalah informasi tentang penyebaran kode atau perubahan infrastruktur yang terjadi sekitar waktu yang sama ketika sebuah insiden dibuat. Sebuah temuan dapat diperiksa sebagai penyebab potensial dari insiden tersebut. Informasi tentang penyebab potensial ini ditambahkan ke halaman Detail insiden untuk insiden tersebut. Dengan informasi tentang penerapan dan perubahan ini, responden tidak perlu mencari informasi ini secara manual.

   > **Tip**
   >
   > Untuk melihat informasi tentang peran yang akan dibuat, pilih Lihat detail izin.

7. Pilih Buat.

   Untuk mempelajari lebih lanjut tentang set replikasi dan ketahanan, lihat. Ketahanan di Manajer Insiden AWS Systems Manager

Kontak (Opsional selama Bersiaplah)

Manajer Insiden melibatkan kontak selama insiden. Untuk informasi selengkapnya tentang kontak, lihatMembuat dan mengonfigurasi kontak di Manajer Insiden.

1. Pilih Buat kontak.
2. Untuk Nama, masukkan nama kontak.
3. Untuk alias Unik, masukkan alias untuk mengidentifikasi kontak ini.
4. Di bagian Saluran kontak., lakukan hal berikut untuk menentukan bagaimana kontak terlibat selama insiden:

   a. Untuk Jenis, pilih Email, SMS, atau Suara.

   b. Untuk nama Saluran, masukkan nama unik untuk membantu Anda mengidentifikasi saluran.

   c. Untuk Detail, masukkan alamat email atau nomor telepon untuk kontak tersebut.

Nomor telepon harus memiliki 9-15 karakter dan mulai dengan + diikuti dengan kode negara dan nomor pelanggan.

d. Untuk membuat saluran kontak lain, pilih Tambahkan saluran kontak. Kami merekomendasikan untuk mendefinisikan setidaknya dua saluran untuk setiap kontak.

5. Di area Rencana Keterlibatan, lakukan hal berikut untuk menentukan saluran mana yang akan diberi tahu kontak, dan berapa lama menunggu pengakuan melalui setiap saluran.

> **Note**
>
> Kami merekomendasikan untuk mendefinisikan setidaknya dua saluran dalam rencana keterlibatan.

a. Untuk nama saluran Kontak, pilih saluran yang Anda tentukan di area Saluran kontak.

b. Untuk waktu Engagement (min), masukkan jumlah menit untuk menunggu sebelum melibatkan saluran kontak.

   Kami menyarankan Anda memilih setidaknya satu perangkat untuk terlibat di awal keterlibatan, dengan menentukan waktu tunggu **0** (nol) menit.

c. Untuk menambahkan lebih banyak saluran kontak ke paket keterlibatan, pilih Tambahkan keterlibatan.

6. (Opsional) Di area Tag, tambahkan satu atau lebih tag ke kontak. Tag menyertakan kunci dan, secara opsional, nilai.

   Tanda adalah metadata opsional yang Anda tetapkan ke sumber daya. Tag memungkinkan Anda untuk mengkategorikan sumber daya dengan berbagai cara, seperti berdasarkan tujuan, pemilik, atau lingkungan. Untuk informasi selengkapnya, lihat Menandai sumber daya di Manajer Insiden.

7. Untuk membuat catatan kontak dan mengirim kode aktivasi ke saluran kontak yang ditentukan, pilih Buat.

8. (Opsional) Di halaman Aktivasi saluran kontak, masukkan kode aktivasi yang dikirim ke setiap saluran.

   Anda dapat membuat kode aktivasi baru nanti jika Anda tidak dapat memasukkan kode sekarang.

9. Untuk menambahkan kontak tambahan, pilih Buat kontak dan ulangi langkah sebelumnya.

(Opsional selama Bersiaplah) Rencana eskalasi

1. Pilih Buat rencana eskalasi.

   Rencana eskalasi meningkat melalui kontak Anda selama insiden, memastikan bahwa Manajer Insiden melibatkan responden yang benar selama insiden. Untuk informasi lebih lanjut tentang rencana eskalasi, lihatMembuat rencana eskalasi untuk keterlibatan responden di Manajer Insiden.
2. Untuk Nama, masukkan nama unik untuk rencana eskalasi.
3. Untuk Alias, masukkan alias unik untuk membantu Anda mengidentifikasi rencana eskalasi.
4. Di area Tahap 1, lakukan hal berikut:

   a. Untuk saluran Eskalasi, pilih saluran kontak untuk terlibat.

   b. Jika Anda ingin kontak dapat menghentikan perkembangan tahapan rencana eskalasi, pilih Pengakuan menghentikan perkembangan rencana.

   c. Untuk menambahkan lebih banyak saluran ke panggung, pilih Tambahkan saluran eskalasi.
5. Untuk membuat tahap baru dalam rencana eskalasi, pilih Tambahkan tahap dan tambahkan detail tahapnya.
6. (Opsional) Di area Tag, tambahkan satu atau beberapa tag ke rencana eskalasi. Tag menyertakan kunci dan, secara opsional, nilai.

   Tanda adalah metadata opsional yang Anda tetapkan ke sumber daya. Tag memungkinkan Anda untuk mengkategorikan sumber daya dengan berbagai cara, seperti berdasarkan tujuan, pemilik, atau lingkungan. Untuk informasi selengkapnya, lihat Menandai sumber daya di Manajer Insiden.
7. Pilih Buat rencana eskalasi.

Rencana respons

> **Note**
>
> Anda mungkin perlu kembali ke halaman awal Manajer Insiden dan memilih Siapkan untuk melanjutkan.

1. Pilih Buat rencana respons.

Gunakan rencana respons untuk mengumpulkan kontak dan rencana eskalasi yang Anda buat.

Selama panduan Memulai ini, bagian berikut bersifat opsional, terutama jika ini adalah pertama kalinya Anda menyiapkan rencana respons:

- Saluran obrolan
- Runbook
- Keterlibatan
- Integrasi pihak ketiga

Untuk informasi tentang menambahkan elemen-elemen ini ke rencana respons nanti, lihatMempersiapkan Insiden di Manajer Insiden.

2. Untuk Nama, masukkan nama unik yang dapat diidentifikasi untuk paket respons. Nama ini digunakan untuk membuat rencana respons ARN atau dalam rencana respons tanpa nama tampilan.
3. (Opsional) Untuk Nama tampilan, masukkan nama untuk membantu Anda mengidentifikasi rencana respons ini saat membuat insiden.
4. Untuk Judul, masukkan judul untuk membantu mengidentifikasi jenis insiden yang terkait dengan rencana respons ini.

   Nilai yang Anda tentukan disertakan dalam judul setiap insiden. Alarm atau peristiwa yang memulai insiden juga ditambahkan ke judul.
5. Untuk Dampak, pilih tingkat dampak yang Anda harapkan untuk insiden yang terkait dengan rencana respons ini, seperti **`Critical`** atau**`Low`**.
6. (Opsional) Untuk Ringkasan, masukkan deskripsi singkat yang digunakan untuk memberikan gambaran umum tentang insiden tersebut. Manajer Insiden secara otomatis mengisi informasi yang relevan ke dalam ringkasan selama insiden.
7. (Opsional) Untuk string Dedupe, masukkan string dedupe. Incident Manager menggunakan string ini untuk mencegah akar penyebab yang sama membuat beberapa insiden di akun yang sama.

   String deduplikasi adalah istilah atau frasa yang digunakan sistem untuk memeriksa insiden duplikat. Jika Anda menentukan string deduplikasi, Manajer Insiden akan mencari insiden terbuka yang berisi string yang sama di `dedupeString` bidang saat membuat insiden. Jika

duplikat terdeteksi, Manajer Insiden menghapus duplikasi insiden yang lebih baru ke dalam insiden yang ada.

> **Note**
>
> Secara default, Manajer Insiden secara otomatis menghapus duplikasi beberapa insiden yang dibuat oleh alarm Amazon CloudWatch atau peristiwa Amazon yang sama. EventBridge Anda tidak perlu memasukkan string deduplikasi Anda sendiri untuk mencegah duplikasi untuk jenis sumber daya ini.

8. (Opsional) Di area Tag Insiden, tambahkan satu atau beberapa tag ke paket respons. Tag menyertakan kunci dan, secara opsional, nilai.

   Tanda adalah metadata opsional yang Anda tetapkan ke sumber daya. Tag memungkinkan Anda untuk mengkategorikan sumber daya dengan berbagai cara, seperti berdasarkan tujuan, pemilik, atau lingkungan. Untuk informasi selengkapnya, lihat Menandai sumber daya di Manajer Insiden.
9. Pilih kontak dan rencana eskalasi untuk diterapkan pada insiden dari dropdown Engagements.
10. Pilih Buat rencana respons.

Setelah membuat paket respons, Anda dapat mengaitkan CloudWatch alarm Amazon atau EventBridge peristiwa Amazon dengan paket respons. Ini akan secara otomatis membuat insiden berdasarkan alarm atau peristiwa. Lihat informasi yang lebih lengkap di Membuat insiden secara otomatis atau manual di Manajer Insiden.

Mengelola insiden di seluruh Akun AWS dan Wilayah di Manajer Insiden

Anda dapat mengonfigurasi Manajer Insiden, alat di AWS Systems Manager, untuk bekerja dengan banyak Wilayah AWS dan akun. Bagian ini menjelaskan praktik terbaik lintas wilayah dan lintas akun, langkah-langkah pengaturan, dan batasan yang diketahui.

Topik

- Manajemen insiden lintas wilayah
- Manajemen insiden lintas akun

Manajemen insiden lintas wilayah

Manajer Insiden mendukung pembuatan insiden otomatis dan manual di beberapa Wilayah AWS. Saat Anda pertama kali bergabung dengan Manajer Insiden dengan menggunakan wizard Get prepared, Anda dapat menentukan hingga tiga Wilayah AWS untuk set replikasi Anda. Untuk insiden yang dibuat secara otomatis oleh CloudWatch alarm Amazon atau EventBridge peristiwa Amazon, Manajer Insiden mencoba membuat insiden yang Wilayah AWS sama dengan aturan acara atau alarm. Jika Manajer Insiden mengalami pemadaman di Wilayah tersebut, maka CloudWatch atau EventBridge secara otomatis membuat insiden di Wilayah lain tempat data Anda direplikasi.

> **Important**
>
> Perhatikan detail penting berikut.
>
> - Kami menyarankan Anda menentukan setidaknya dua Wilayah AWS di set replikasi Anda. Jika Anda tidak menentukan setidaknya dua Wilayah, sistem akan gagal membuat insiden selama periode ketika Manajer Insiden tidak tersedia.
> - Insiden yang dibuat oleh failover lintas wilayah tidak memanggil runbook yang ditentukan dalam paket respons.

Untuk informasi lebih lanjut tentang on-boarding dengan Manajer Insiden dan menentukan Wilayah tambahan, lihat. Memulai dengan Manajer Insiden

Manajemen insiden lintas akun

Manajer Insiden menggunakan AWS Resource Access Manager (AWS RAM) untuk berbagi sumber daya Manajer Insiden di seluruh akun manajemen dan aplikasi. Bagian ini menjelaskan praktik terbaik lintas akun, cara mengatur fungsionalitas lintas akun untuk Manajer Insiden, dan batasan fungsionalitas lintas akun yang diketahui di Manajer Insiden.

Akun manajemen adalah akun tempat Anda melakukan manajemen operasi. Dalam pengaturan organisasi, akun manajemen memiliki rencana respons, kontak, rencana eskalasi, runbook, dan sumber daya lainnya. AWS Systems Manager

Akun aplikasi adalah akun yang memiliki sumber daya yang membentuk aplikasi Anda. Sumber daya ini dapat berupa EC2 instans Amazon, tabel Amazon DynamoDB, atau sumber daya lain yang Anda gunakan untuk membangun aplikasi di file. AWS Cloud Akun aplikasi juga memiliki CloudWatch alarm Amazon dan EventBridge peristiwa Amazon yang membuat insiden di Manajer Insiden.

AWS RAM menggunakan pembagian sumber daya untuk berbagi sumber daya antar akun. Anda dapat membagikan paket respons dan sumber daya kontak antar akun di AWS RAM. Dengan berbagi sumber daya ini, akun aplikasi dan akun manajemen dapat berinteraksi dengan keterlibatan dan insiden. Berbagi rencana respons membagikan semua insiden masa lalu dan masa depan yang dibuat menggunakan rencana respons tersebut. Berbagi kontak membagikan semua keterlibatan masa lalu dan masa depan dari rencana kontak atau respons.

Praktik terbaik

Ikuti praktik terbaik ini saat membagikan sumber daya Manajer Insiden Anda di seluruh akun:

- Perbarui pembagian sumber daya secara teratur dengan rencana respons dan kontak.
- Tinjau prinsip berbagi sumber daya secara teratur.
- Siapkan Manajer Insiden, runbook, dan saluran obrolan di akun manajemen Anda.

Siapkan dan konfigurasikan manajemen insiden lintas akun

Langkah-langkah berikut menjelaskan cara mengatur dan mengonfigurasi sumber daya Manajer Insiden dan menggunakannya untuk fungsionalitas lintas akun. Anda mungkin telah mengonfigurasi beberapa layanan dan sumber daya untuk fungsionalitas lintas akun di masa lalu. Gunakan langkah-langkah ini sebagai daftar persyaratan sebelum memulai insiden pertama Anda menggunakan sumber daya lintas akun.

1. (Opsional) Buat organisasi dan unit organisasi menggunakan AWS Organizations. Ikuti langkah-langkah dalam Tutorial: Membuat dan mengkonfigurasi organisasi di Panduan AWS Organizations Pengguna.
2. (Opsional) Gunakan Quick Setup, alat di AWS Systems Manager, untuk mengatur AWS Identity and Access Management peran yang benar untuk Anda gunakan saat mengonfigurasi runbook lintas akun Anda. Untuk informasi selengkapnya, lihat Pengaturan Cepat di Panduan AWS Systems Manager Pengguna.
3. Ikuti langkah-langkah yang tercantum dalam Menjalankan otomatisasi di beberapa Wilayah AWS dan akun di Panduan AWS Systems Manager Pengguna untuk membuat runbook di dokumen otomatisasi Systems Manager Anda. Runbook dapat dijalankan oleh akun manajemen, atau oleh salah satu akun aplikasi Anda. Tergantung pada kasus penggunaan Anda, Anda perlu menginstal AWS CloudFormation template yang sesuai untuk peran yang diperlukan untuk membuat dan melihat runbook selama insiden.
   - Menjalankan runbook di akun manajemen. Akun manajemen harus mengunduh dan menginstal AWS-SystemsManager-AutomationReadOnlyRole CloudFormation templat. Saat memasang AWS-SystemsManager-AutomationReadOnlyRole, tentukan akun IDs semua akun aplikasi. Peran ini akan memungkinkan akun aplikasi Anda membaca status runbook dari halaman detail insiden. Akun aplikasi harus menginstal AWS-SystemsManager-AutomationAdministrationReadOnlyRole CloudFormation templat. Halaman detail insiden menggunakan peran ini untuk mendapatkan status otomatisasi dari akun manajemen.
   - Menjalankan runbook di akun aplikasi. Akun manajemen harus mengunduh dan menginstal AWS-SystemsManager-AutomationAdministrationReadOnlyRole CloudFormation templat. Peran ini memungkinkan akun manajemen untuk membaca status runbook di akun aplikasi. Akun aplikasi harus mengunduh dan menginstal AWS-SystemsManager-AutomationReadOnlyRole CloudFormation templat. Saat menginstal`AWS-SystemsManager-AutomationReadOnlyRole`, tentukan ID akun akun manajemen dan akun aplikasi lainnya. Akun manajemen dan akun aplikasi lainnya mengambil peran ini untuk membaca status runbook.
4. (Opsional) Di setiap akun aplikasi di organisasi, unduh dan instal AWS-SystemsManager-IncidentManagerIncidentAccessServiceRole CloudFormation templat. Saat memasang AWS-SystemsManager-IncidentManagerIncidentAccessServiceRole, tentukan ID akun akun manajemen. Peran ini memberikan izin yang dibutuhkan Manajer Insiden untuk mengakses informasi tentang AWS CodeDeploy penerapan dan AWS CloudFormation pembaruan tumpukan. Informasi ini dilaporkan sebagai temuan untuk suatu insiden jika fitur Temuan

diaktifkan. Untuk informasi selengkapnya, lihat Mengidentifikasi potensi penyebab insiden dari layanan lain sebagai “temuan” di Manajer Insiden.

5. Untuk menyiapkan dan membuat kontak, rencana eskalasi, saluran obrolan, dan rencana respons, ikuti langkah-langkah yang dijelaskan di dalamnyaMempersiapkan Insiden di Manajer Insiden.
6. Tambahkan sumber daya kontak dan rencana respons ke pembagian sumber daya yang ada atau pembagian sumber daya baru AWS RAM. Untuk informasi selengkapnya, lihat Memulai dengan AWS RAM dalam Panduan Pengguna AWS RAM . Menambahkan rencana respons untuk AWS RAM memungkinkan akun aplikasi mengakses insiden dan dasbor insiden yang dibuat menggunakan rencana respons. Akun aplikasi juga mendapatkan kemampuan untuk mengaitkan CloudWatch alarm dan EventBridge peristiwa ke rencana respons. Menambahkan kontak dan rencana eskalasi untuk AWS RAM memungkinkan akun aplikasi melihat keterlibatan dan melibatkan kontak dari dasbor insiden.
7. Tambahkan fungsionalitas lintas wilayah lintas akun ke konsol Anda CloudWatch . Untuk langkah dan informasi, lihat CloudWatch Konsol lintas wilayah lintas akun di CloudWatch Panduan Pengguna Amazon. Menambahkan fungsi ini memastikan bahwa akun aplikasi dan akun manajemen yang Anda buat dapat melihat dan mengedit metrik dari dasbor insiden dan analisis.
8. Buat bus EventBridge acara Amazon lintas akun. Untuk langkah dan informasi, lihat Mengirim dan menerima EventBridge peristiwa Amazon antar AWS akun. Anda kemudian dapat menggunakan bus acara ini untuk membuat aturan acara yang mendeteksi insiden di akun aplikasi dan membuat insiden di akun manajemen.

Batasan

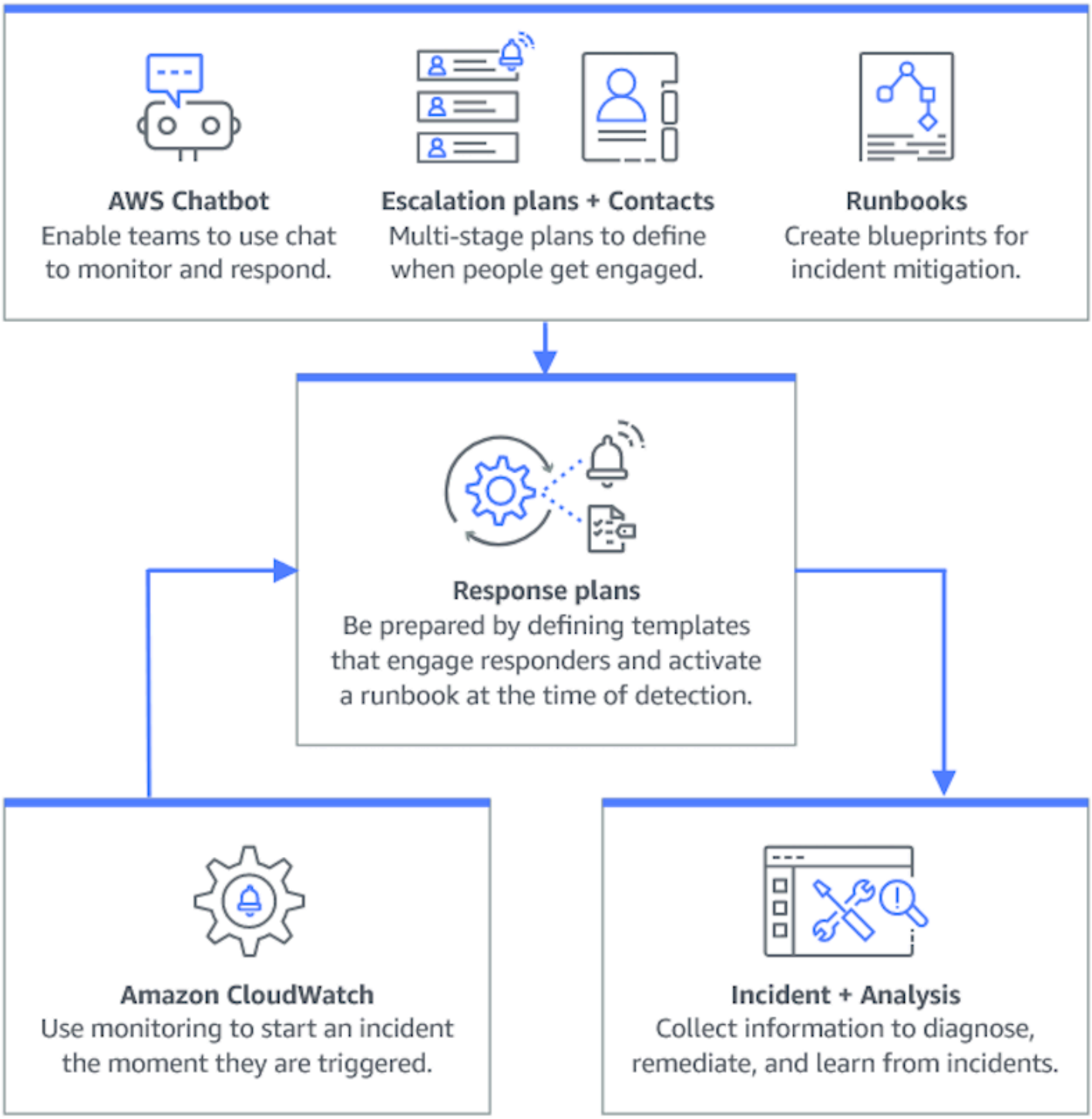
Berikut ini adalah batasan yang diketahui dari fungsionalitas lintas akun Manajer Insiden:

- Akun yang membuat analisis pasca-insiden adalah satu-satunya akun yang dapat melihat dan mengubahnya. Jika Anda menggunakan akun aplikasi untuk membuat analisis pasca-insiden, hanya anggota akun tersebut yang dapat melihat dan mengubahnya. Hal yang sama berlaku jika Anda menggunakan akun manajemen untuk membuat analisis pasca-insiden.
- Peristiwa timeline tidak diisi untuk dokumen otomatisasi yang dijalankan di akun aplikasi. Pembaruan dokumen otomatisasi yang dijalankan di akun aplikasi terlihat di tab Runbook insiden tersebut.

- Topik Layanan Pemberitahuan Sederhana Amazon tidak dapat digunakan lintas akun. Topik Amazon SNS harus dibuat di Wilayah dan akun yang sama dengan paket respons yang digunakan. Sebaiknya gunakan akun manajemen untuk membuat semua topik SNS dan rencana respons.
- Paket eskalasi hanya dapat dibuat menggunakan kontak di akun yang sama. Kontak yang telah dibagikan dengan Anda tidak dapat ditambahkan ke paket eskalasi di akun Anda.
- Tag yang diterapkan pada rencana respons, catatan insiden, dan kontak hanya dapat dilihat dan dimodifikasi dari akun pemilik sumber daya.

Mempersiapkan Insiden di Manajer Insiden

Perencanaan untuk insiden dimulai jauh sebelum siklus hidup insiden. Seperti yang ditunjukkan ilustrasi berikut, sebelum mulai menanggapi insiden, Anda bersiap-siap dengan menyiapkan saluran obrolan, membuat rencana eskalasi, menentukan kontak, dan menentukan runbook Otomasi yang akan digunakan dalam respons insiden. Kemudian, gunakan rencana respons yang menentukan bagaimana pemantauan terjadi dan apakah respons otomatis. Setelah remediasi selesai, Anda dapat menganalisis insiden dan respons insiden untuk lebih menyempurnakan rencana respons Anda untuk insiden masa depan.



Topik

- Pemantauan
- Mengkonfigurasi set replikasi dan Temuan di Manajer Insiden
- Membuat dan mengonfigurasi kontak di Manajer Insiden

- Mengelola rotasi responden dengan jadwal panggilan di Manajer Insiden
- Membuat rencana eskalasi untuk keterlibatan responden di Manajer Insiden
- Membuat dan mengintegrasikan saluran obrolan untuk responden di Manajer Insiden
- Mengintegrasikan runbook Otomasi Systems Manager di Incident Manager untuk remediasi insiden
- Membuat dan mengonfigurasi rencana respons di Manajer Insiden
- Mengidentifikasi potensi penyebab insiden dari layanan lain sebagai “temuan” di Manajer Insiden

Pemantauan

Memantau kesehatan aplikasi yang Anda AWS host adalah kunci untuk memastikan waktu dan kinerja aplikasi. Saat menentukan solusi pemantauan, pertimbangkan hal berikut:

- Kekritisan fitur — Jika sistem gagal, seberapa kritis dampaknya bagi pengguna hilir.
- Kesamaan kegagalan — Seberapa sering suatu sistem gagal; sistem yang membutuhkan intervensi sering harus dipantau secara ketat.
- Peningkatan latensi — Berapa banyak waktu untuk menyelesaikan tugas telah meningkat atau menurun.
- Metrik sisi klien versus sisi server — Jika ada perbedaan antara metrik terkait pada klien dan server.
- Kegagalan ketergantungan — Kegagalan yang dapat dan harus disiapkan oleh tim Anda.

Setelah membuat rencana respons, Anda dapat menggunakan solusi pemantauan untuk melacak insiden secara otomatis saat terjadi di lingkungan Anda. Untuk informasi selengkapnya tentang pelacakan dan pembuatan insiden, lihatMelihat detail insiden di konsol Manajer Insiden.

Untuk informasi lebih lanjut tentang merancang aplikasi dan beban kerja infrastruktur yang aman, berkinerja tinggi, tangguh, dan efisien, lihat Well-Architected.AWS

Mengkonfigurasi set replikasi dan Temuan di Manajer Insiden

Setelah Anda menyelesaikan wizard Incident Manager Get prepared, Anda dapat mengelola opsi tertentu di halaman Pengaturan. Opsi ini termasuk set replikasi Anda, tag yang diterapkan ke set replikasi, dan fitur Temuan.

Topik

- Mengkonfigurasi set replikasi Manajer Insiden
- Mengelola tag untuk set replikasi
- Mengelola fitur Temuan

Mengkonfigurasi set replikasi Manajer Insiden

Kumpulan replikasi Manajer Insiden mereplikasi data Anda ke banyak Wilayah AWS untuk melakukan hal berikut:

- Meningkatkan redundansi lintas wilayah
- Izinkan Manajer Insiden mengakses sumber daya di Wilayah yang berbeda dan mengurangi latensi bagi pengguna Anda.
- Enkripsi data Anda dengan kunci yang dikelola pelanggan Kunci yang dikelola AWS atau Anda sendiri.

  Semua sumber daya Manajer Insiden dienkripsi secara default. Untuk mempelajari lebih lanjut tentang cara sumber daya Anda dienkripsi, lihat. Perlindungan data di Manajer Insiden

Untuk memulai dengan Incident Manager, pertama buat set replikasi Anda menggunakan wizard Get prepared. Untuk mempelajari lebih lanjut tentang persiapan di Manajer Insiden, lihatSiapkan penyihir.

Mengedit set replikasi Anda

Dengan menggunakan halaman Pengaturan Manajer Insiden, Anda dapat mengedit set replikasi Anda. Anda dapat menambahkan Wilayah, menghapus Wilayah, dan mengaktifkan atau menonaktifkan perlindungan penghapusan set replikasi. Anda tidak dapat mengedit kunci yang digunakan untuk mengenkripsi data Anda. Untuk mengubah kunci, hapus dan buat ulang set replikasi.

Tambahkan Region.

1. Buka konsol Manajer Insiden, lalu pilih Pengaturan di panel navigasi kiri.
2. Pilih Tambah Wilayah.
3. Pilih Wilayah.
4. Pilih Tambahkan.

Menghapus Wilayah

1. Buka konsol Manajer Insiden, lalu pilih Pengaturan di panel navigasi kiri.
2. Pilih Wilayah yang ingin Anda hapus.
3. Pilih Hapus.
4. Masukkan hapus ke dalam kotak teks, dan pilih Hapus.

Menghapus set replikasi Anda

Menghapus Wilayah terakhir di set replikasi Anda akan menghapus seluruh rangkaian replikasi. Sebelum Anda dapat menghapus Wilayah terakhir, nonaktifkan perlindungan penghapusan dengan mematikan Perlindungan penghapusan pada halaman Pengaturan. Setelah Anda menghapus set replikasi Anda, Anda dapat membuat set replikasi baru dengan menggunakan wizard Get prepared.

Untuk menghapus Region dari set replikasi Anda, tunggu 24 jam setelah membuatnya. Mencoba menghapus Wilayah dari set replikasi Anda lebih cepat dari 24 jam setelah pembuatan menyebabkan penghapusan gagal.

Menghapus set replikasi Anda akan menghapus semua data Manajer Insiden.

Hapus set replikasi

1. Buka konsol Manajer Insiden, lalu pilih Pengaturan di panel navigasi kiri.
2. Pilih Wilayah terakhir di set replikasi Anda.
3. Pilih Hapus.
4. Masukkan hapus ke dalam kotak teks, dan pilih Hapus.

Mengelola tag untuk set replikasi

Tag adalah metadata opsional yang Anda tetapkan ke sumber daya. Gunakan tag untuk mengkategorikan sumber daya dengan cara yang berbeda, seperti berdasarkan tujuan, pemilik, atau lingkungan.

Untuk mengelola tag untuk set replikasi

1. Buka konsol Manajer Insiden, lalu pilih Pengaturan di panel navigasi kiri.
2. Di area Tag, pilih Edit.

3. Untuk menambahkan tanda, lakukan hal berikut:
   a. Pilih Tambahkan tag baru.
   b. Masukkan kunci dan nilai opsional untuk tag.
   c. Pilih Simpan.
4. Untuk menghapus tag, lakukan hal berikut:
   a. Di bawah tag yang ingin Anda hapus, pilih Hapus.
   b. Pilih Simpan.

Mengelola fitur Temuan

Fitur Temuan membantu responden di organisasi Anda mengidentifikasi potensi akar penyebab insiden segera setelah insiden dimulai. Saat ini, Manajer Insiden menyediakan temuan untuk AWS CodeDeploy penerapan dan pembaruan AWS CloudFormation tumpukan.

Untuk dukungan lintas akun untuk temuan, setelah Anda mengaktifkan fitur, Anda harus menyelesaikan langkah penyiapan tambahan di setiap akun aplikasi di organisasi.

Untuk menggunakan fitur ini, Anda mengizinkan Manajer Insiden membuat peran layanan yang menyertakan izin yang diperlukan untuk mengakses data atas nama Anda.

Untuk mengaktifkan fitur Temuan

1. Buka konsol Manajer Insiden, lalu pilih Pengaturan di panel navigasi kiri.
2. Di area Temuan, pilih Buat peran layanan.
3. Tinjau informasi tentang peran layanan yang akan dibuat, lalu pilih Buat.

Untuk menonaktifkan fitur Temuan

Untuk berhenti menggunakan fitur Temuan, hapus `IncidentManagerIncidentAccessServiceRole` peran dari setiap akun yang telah dibuat.

1. Buka konsol IAM di https://console.aws.amazon.com/iam/.
2. Di panel navigasi sebelah kiri, pilih Peran.
3. Dalam kotak pencarian, masukkan **`IncidentManagerIncidentAccessServiceRole`**.
4. Pilih nama peran, lalu pilih Hapus.

5. Masukkan nama peran di kotak dialog untuk mengonfirmasi bahwa Anda ingin menghapus peran, lalu pilih Hapus.

Membuat dan mengonfigurasi kontak di Manajer Insiden

Manajer Insiden AWS Systems Manager kontak adalah responden terhadap insiden. Kontak dapat memiliki beberapa saluran yang dapat dilibatkan oleh Manajer Insiden selama insiden. Anda dapat menentukan rencana keterlibatan kontak untuk menjelaskan bagaimana dan kapan Manajer Insiden melibatkan kontak tersebut.

Topik

- Saluran kontak
- Rencana keterlibatan
- Buat kontak
- Impor detail kontak ke buku alamat Anda

Saluran kontak

Saluran kontak adalah berbagai metode yang digunakan Manajer Insiden untuk melibatkan kontak.

Manajer Insiden mendukung saluran kontak berikut:

- Email
- Layanan Pesan Singkat (SMS)
- Suara

Aktivasi saluran kontak

Untuk melindungi privasi dan keamanan Anda, Manajer Insiden mengirimkan kode aktivasi perangkat kepada Anda saat Anda membuat kontak. Untuk menggunakan perangkat Anda selama insiden, Anda harus mengaktifkannya terlebih dahulu. Untuk melakukannya, masukkan kode aktivasi perangkat pada halaman buat kontak.

Fitur tertentu dari Manajer Insiden mencakup fungsionalitas yang mengirim pemberitahuan ke saluran kontak. Dengan menggunakan fitur-fitur ini, Anda menyetujui layanan ini untuk mengirimkan pemberitahuan tentang gangguan layanan atau peristiwa lain ke saluran kontak yang disertakan

dalam alur kerja yang ditentukan. Ini termasuk pemberitahuan yang dikirim ke kontak sebagai bagian dari rotasi jadwal panggilan. Pemberitahuan dapat dikirim melalui email, pesan SMS, atau panggilan suara sebagaimana ditentukan dalam detail kontak. Anda mengonfirmasi dengan menggunakan fitur-fitur ini bahwa Anda berwenang untuk menambahkan saluran kontak yang Anda berikan ke Manajer Insiden.

Memilih keluar

Anda dapat membatalkan pemberitahuan ini kapan saja dengan menghapus perangkat seluler sebagai saluran kontak. Penerima pemberitahuan individu juga dapat membatalkan pemberitahuan kapan saja dengan menghapus perangkat dari kontak mereka.

Untuk menghapus saluran kontak dari kontak

1. Arahkan ke konsol Manajer Insiden dan pilih Kontak dari navigasi kiri.
2. Pilih kontak dengan saluran kontak yang Anda hapus dan pilih Edit.
3. Pilih Hapus di sebelah saluran kontak yang ingin Anda hapus.
4. Pilih Perbarui.

Penonaktifan saluran kontak

Untuk menonaktifkan perangkat, balas BERHENTI BERLANGGANAN. Membalas BERHENTI BERLANGGANAN menghentikan Pengelola Insiden untuk melibatkan perangkat Anda.

Reaktivasi saluran kontak

1. Balas MULAI ke pesan dari Manajer Insiden.
2. Arahkan ke konsol Manajer Insiden dan pilih Kontak dari navigasi kiri.
3. Pilih kontak dengan saluran kontak yang Anda hapus dan pilih Edit.
4. Pilih Aktifkan perangkat.
5. Masukkan kode Aktivasi yang dikirim ke perangkat oleh Manajer Insiden.
6. Pilih Aktifkan.

Rencana keterlibatan

Rencana keterlibatan menentukan kapan Manajer Insiden melibatkan saluran kontak. Anda dapat melibatkan saluran kontak beberapa kali pada tahap yang berbeda sejak awal keterlibatan. Anda

dapat menggunakan rencana keterlibatan dalam rencana eskalasi atau rencana respons. Untuk mempelajari lebih lanjut tentang rencana eskalasi, lihatMembuat rencana eskalasi untuk keterlibatan responden di Manajer Insiden.

Buat kontak

Untuk membuat kontak, gunakan langkah-langkah berikut.

1. Buka konsol Manajer Insiden dan pilih Kontak dari navigasi kiri.
2. Pilih Buat kontak.
3. Ketik nama lengkap kontak dan berikan alias yang unik dan dapat diidentifikasi.
4. Tentukan saluran Kontak. Kami merekomendasikan memiliki dua atau lebih jenis saluran kontak yang berbeda.
   a. Pilih jenis: email, SMS, atau suara.
   b. Masukkan nama yang dapat diidentifikasi untuk saluran kontak.
   c. Berikan rincian saluran kontak, seperti email: arosalez@example.com
5. Untuk menentukan lebih dari satu saluran kontak, pilih Tambahkan saluran kontak. Ulangi langkah 4 untuk setiap saluran kontak baru yang ditambahkan.
6. Tentukan rencana keterlibatan.

   > **Important**
   > Untuk melibatkan kontak, Anda harus menentukan rencana keterlibatan.

   a. Pilih nama saluran Kontak.
   b. Tentukan berapa menit dari awal keterlibatan untuk menunggu hingga Manajer Insiden melibatkan saluran kontak ini.
   c. Untuk menambahkan saluran kontak lain, pilih Tambahkan keterlibatan.
7. Setelah menentukan rencana keterlibatan Anda, pilih Buat. Manajer Insiden mengirimkan kode aktivasi ke masing-masing saluran kontak yang ditentukan.
8. (Opsional) Untuk mengaktifkan saluran kontak, masukkan kode aktivasi yang dikirim Manajer Insiden ke setiap saluran kontak yang ditentukan.
9. (Opsional) Untuk mengirim kode aktivasi baru, pilih Kirim kode baru.

10. Pilih Selesai.

Setelah Anda menentukan kontak dan mengaktifkan saluran kontaknya, Anda dapat menambahkan kontak ke rencana eskalasi untuk membentuk rantai eskalasi. Untuk mempelajari lebih lanjut tentang rencana eskalasi, lihatMembuat rencana eskalasi untuk keterlibatan responden di Manajer Insiden. Anda dapat menambahkan kontak ke rencana respons untuk keterlibatan langsung. Untuk mempelajari lebih lanjut tentang membuat rencana respons, lihatMembuat dan mengonfigurasi rencana respons di Manajer Insiden.

Impor detail kontak ke buku alamat Anda

Ketika insiden dibuat, Manajer Insiden dapat memberi tahu responden dengan menggunakan pemberitahuan suara atau SMS. Untuk memastikan bahwa responden melihat bahwa pemberitahuan panggilan atau SMS berasal dari Manajer Insiden, kami menyarankan agar semua responden mengunduh file format kartu virtual Manajer Insiden (.vcf) ke buku alamat di perangkat seluler mereka. File ini di-host di Amazon CloudFront dan tersedia di partisi AWS komersial.

Untuk mengunduh file.vcf Manajer Insiden

1. Di perangkat seluler Anda, pilih atau masukkan URL berikut: https://d26vhuvd5b89k2.cloudfront.net/ aws-incident-manager .vcf.
2. Simpan atau impor file ke buku alamat di perangkat seluler Anda.

Mengelola rotasi responden dengan jadwal panggilan di Manajer Insiden

Jadwal panggilan di Manajer Insiden menentukan siapa yang diberi tahu ketika insiden terjadi yang memerlukan intervensi operator. Jadwal panggilan terdiri dari satu atau lebih rotasi yang Anda buat untuk jadwal tersebut. Setiap rotasi dapat mencakup hingga 30 kontak.

Setelah Anda membuat jadwal panggilan, Anda dapat memasukkannya sebagai eskalasi dalam rencana eskalasi Anda. Ketika insiden yang terkait dengan rencana eskalasi itu terjadi, Manajer Insiden memberi tahu operator (atau operator) yang sedang menelepon sesuai dengan jadwal. Kontak ini kemudian dapat mengakui keterlibatan. Dalam rencana eskalasi Anda, Anda dapat menetapkan satu atau lebih jadwal panggilan, serta satu atau lebih kontak individu, di beberapa tahap eskalasi. Untuk informasi selengkapnya, lihat Membuat rencana eskalasi untuk keterlibatan responden di Manajer Insiden.

> **Tip**
>
> Sebagai praktik terbaik, kami merekomendasikan menambahkan kontak dan jadwal panggilan sebagai saluran eskalasi dalam rencana eskalasi. Anda kemudian harus memilih rencana eskalasi sebagai keterlibatan dalam rencana respons. Pendekatan ini memberikan cakupan penuh untuk respons insiden di organisasi Anda.

Setiap jadwal panggilan mendukung hingga delapan rotasi. Rotasi dapat tumpang tindih atau berjalan secara bersamaan. Ini meningkatkan jumlah operator yang diberitahu untuk merespons ketika insiden terjadi. Anda juga dapat membuat rotasi yang berjalan berurutan. Ini mendukung skenario seperti manajemen insiden “ikuti matahari” di mana Anda memiliki grup di seluruh dunia yang mendukung layanan yang sama.

Gunakan topik di bagian ini untuk membantu Anda membuat dan mengelola jadwal panggilan untuk operasi respons insiden Anda.

Topik

- Membuat jadwal panggilan dan rotasi di Manajer Insiden
- Mengelola jadwal panggilan yang ada di Manajer Insiden

Membuat jadwal panggilan dan rotasi di Manajer Insiden

Buat jadwal panggilan dengan satu atau lebih rotasi kontak untuk terlibat dalam menanggapi insiden selama shift mereka.

Sebelum Anda mulai

Sebelum Anda membuat jadwal panggilan, pastikan bahwa Anda sebelumnya membuat kontak yang ingin Anda tambahkan ke rotasi dalam jadwal. Untuk informasi, lihatMembuat dan mengonfigurasi kontak di Manajer Insiden.

Perubahan Akuntansi Daylight Savings Time (DST)

Saat Anda membuat rotasi, Anda menentukan zona waktu global yang berfungsi sebagai dasar untuk waktu cakupan shift dan tanggal yang Anda tentukan untuk rotasi ini. Anda dapat menggunakan zona waktu apa pun yang ditentukan oleh Internet Assigned Numbers Authority (IANA). Misalnya:`America/Los_Angeles`,`UTC`, dan`Asia/Seoul`. Anda dapat menambahkan lebih dari satu rotasi ke jadwal panggilan. Namun, ketika responden untuk setiap rotasi secara geografis

terletak di zona waktu yang berbeda, perlu diingat setiap perubahan DST yang mungkin dikenakan setiap rotasi.

Misalnya, `America/Los_Angeles` dan `Europe/Dublin` amati jadwal DST yang berbeda. Akibatnya, perbedaan waktu antara kedua zona dapat bervariasi dari 6 hingga 8 jam, tergantung pada waktu dalam setahun. Misalnya, jadwal follow-the-sun panggilan memiliki satu rotasi di zona `America/Los_Angeles` waktu dan satu rotasi masuk`Europe/Dublin`. Dalam contoh ini, jadwal dapat berisi celah shift satu jam atau shift satu jam tumpang tindih karena perubahan DST.

Untuk menghindari situasi ini, kami merekomendasikan pendekatan berikut:

1. Gunakan satu zona waktu untuk semua rotasi dalam jadwal panggilan.
2. Hitung waktu lokal saat Anda menetapkan responden di luar zona waktu tertentu.

Jika Anda memutuskan untuk menetapkan setiap rotasi ke zona waktu lokalnya, tinjau jadwal sebelum DST apa pun. Kemudian, sesuaikan waktu pergeseran rotasi sesuai kebutuhan untuk memastikan bahwa Anda menghindari celah atau tumpang tindih yang tidak diinginkan dalam cakupan panggilan Anda sebelum perubahan DST berlaku.

Untuk membuat sesuai jadwal panggilan

1. Buka konsol Manajer Insiden.
2. Di navigasi kiri, pilih Jadwal panggilan.
3. Pilih Buat jadwal panggilan.
4. Untuk nama Jadwal, masukkan nama untuk membantu Anda mengidentifikasi jadwal, seperti**`MyApp Primary On-call Schedule`**.
5. Untuk alias Jadwal, masukkan alias untuk jadwal ini yang unik di saat ini Wilayah AWS, seperti. **`my-app-primary-on-call-schedule`**
6. (Opsional) Di area Tag, terapkan satu atau beberapa nama kunci tag dan pasangan nilai ke jadwal panggilan.

   Tanda adalah metadata opsional yang Anda tetapkan ke sumber daya. Tag memungkinkan Anda untuk mengkategorikan sumber daya dengan berbagai cara, seperti berdasarkan tujuan, pemilik, atau lingkungan. Misalnya, Anda dapat menandai jadwal untuk mengidentifikasi periode waktu di mana ia berjalan, jenis operator yang dikandungnya, atau rencana eskalasi yang didukungnya. Untuk informasi selengkapnya tentang menandai sumber daya Manajer Insiden, lihatMenandai sumber daya di Manajer Insiden.

7. Lanjutkan dengan menambahkan satu atau lebih rotasi ke jadwal panggilan.

Membuat rotasi untuk jadwal panggilan di Manajer Insiden

Rotasi dalam jadwal panggilan menentukan kapan shift berlaku. Ini juga menentukan kontak yang bergeser memutar. Anda dapat menyertakan hingga delapan rotasi dalam satu jadwal panggilan.

Anda dapat menambahkan individu yang Anda buat sebagai kontak di Manajer Insiden ke rotasi. Untuk informasi tentang mengelola kontak, lihatMembuat dan mengonfigurasi kontak di Manajer Insiden.

Saat Anda mengonfigurasi rotasi, Anda dapat melihat bagaimana jadwal keseluruhan terlihat di kalender Pratinjau di sisi kanan halaman.

Untuk membuat rotasi untuk jadwal panggilan

1. Di bagian Rotasi 1 dari halaman Buat jadwal panggilan, untuk nama Rotasi, masukkan nama yang mengidentifikasi rotasi, seperti**`00:00 - 7:59 Support`**, atau. **`Dublin Support Group`**
2. Untuk Tanggal mulai, masukkan tanggal ketika rotasi ini menjadi aktif dalam `YYYY/MM/DD` format, seperti`2023/07/14`.
3. Untuk zona waktu, pilih zona waktu global yang berfungsi sebagai dasar untuk waktu cakupan shift dan tanggal yang Anda tentukan untuk rotasi ini.

   Anda dapat menggunakan zona waktu apa pun yang ditentukan oleh Internet Assigned Numbers Authority (IANA). Misalnya: "America/Los_Angeles", "UTC", "Asia/Seoul”. Untuk informasi selengkapnya, lihat Database Zona Waktu di situs web IANA.

   > **Warning**
   >
   > Anda dapat mendasarkan setiap rotasi pada zona waktunya sendiri. Namun, setiap perubahan Daylight Savings Time di zona waktu yang Anda pilih dapat memengaruhi jendela cakupan yang Anda inginkan. Untuk informasi selengkapnya, lihat Perubahan Akuntansi untuk Daylight Savings Time (DST) sebelumnya dalam topik ini.

4. Untuk waktu mulai Rotasi, masukkan waktu ketika pergeseran rotasi ini dimulai dalam `hh:mm` format 24 jam, seperti`16:00`.

   Perhatikan perbedaan waktu lokal untuk kontak di zona waktu yang berbeda dari yang Anda tentukan. Misalnya, jika Anda memilih `America/Los_Angeles` sebagai zona waktu dan `00:00`

sebagai waktu mulai rotasi, ini sama dengan 08:00 di Dublin, Irlandia, dan 13:30 di Mumbai, India.

5. Untuk waktu akhir Rotasi, masukkan waktu ketika pergeseran rotasi ini berakhir dalam `hh:mm` format 24 jam, seperti`23:59`.

> **Note**
>
> Lamanya waktu antara awal dan akhir rotasi harus minimal 30 menit.

6. (Opsional) Untuk mengatur panjang rotasi menjadi 24 jam, pilih cakupan 24 jam dan masukkan waktu mulai untuk rotasi ini di bidang Waktu mulai rotasi. Nilai waktu akhir Rotasi diperbarui secara otomatis.

   Misalnya, jika Anda ingin panggilan Anda memiliki cakupan 24 jam dengan perubahan shift pada pukul 11 pagi, pilih cakupan 24 jam dan masukkan **`11:00`** sebagai waktu mulai.

7. Untuk hari Aktif, pilih hari dalam seminggu saat rotasi ini aktif. Jika paket panggilan Anda tidak termasuk cakupan akhir pekan misalnya, pilih semua hari kecuali hari Minggu dan Sabtu.
8. Lanjutkan dengan menambahkan kontak ke rotasi.

Menambahkan kontak ke rotasi dalam jadwal panggilan di Manajer Insiden

Untuk setiap rotasi dalam jadwal panggilan Anda, Anda dapat menambahkan satu atau lebih kontak, hingga total 30. Anda memilih dari kontak yang diatur dalam konfigurasi Manajer Insiden Anda.

Saat Anda menambahkan kontak ke rotasi, kontak tersebut dapat menerima pemberitahuan sebagai bagian dari tugas panggilan mereka. Pemberitahuan dapat dikirim melalui email, SMS, atau panggilan suara sebagaimana ditentukan dalam detail kontak.

Untuk informasi tentang mengelola kontak dan opsi pemberitahuan kontak, lihatMembuat dan mengonfigurasi kontak di Manajer Insiden.

Untuk menambahkan kontak ke rotasi dalam jadwal panggilan

1. Pada halaman Buat jadwal panggilan, di bagian Kontak untuk rotasi, pilih Tambah atau hapus kontak.
2. Dalam kotak dialog Tambah atau hapus kontak, pilih alias kontak yang akan disertakan dalam rotasi.

Urutan yang Anda pilih kontak adalah urutan yang pertama kali tercantum dalam jadwal rotasi. Anda dapat mengubah pesanan setelah menambahkan kontak.

3. Pilih Konfirmasi.
4. Untuk mengubah posisi kontak dalam urutan, pilih tombol radio untuk pengguna tersebut dan gunakan tombol Up
   ( )
   dan Down
   ( )
   untuk memperbarui pesanan kontak.
5. Lanjutkan dengan menentukan kekambuhan pergeseran individu dan panjang untuk rotasi.

Menentukan pengulangan dan panjang shift dan menambahkan tag ke rotasi di Manajer Insiden

Shift recurrence menentukan seberapa sering kontak dalam rotasi berputar masuk dan keluar dari panggilan. Panjang kekambuhan dapat ditentukan dalam beberapa hari, minggu, atau bulan.

Untuk menentukan pengulangan dan panjang shift dan menambahkan tag ke rotasi

1. Pada halaman Buat jadwal panggilan, di bagian Pengaturan berulang untuk rotasi, lakukan hal berikut:
   - Untuk jenis pengulangan Shift, tentukan apakah setiap shift saat panggilan berlangsung beberapa hari, minggu, atau bulan dengan memilih dari`Daily`,`Weekly`, dan. `Monthly`
   - Untuk panjang Shift, masukkan berapa hari, minggu, atau bulan shift berlangsung.

     Misalnya, jika Anda memilih `Daily` dan masuk**`1`**, shift panggilan setiap kontak berlangsung satu hari. Jika Anda memilih `Weekly` dan masuk**`3`**, shift panggilan setiap kontak berlangsung selama tiga minggu.
2. (Opsional) Di area Tag, terapkan satu atau lebih nama kunci tag dan pasangan nilai ke rotasi.

   Tanda adalah metadata opsional yang Anda tetapkan ke sumber daya. Tag memungkinkan Anda untuk mengkategorikan sumber daya dengan berbagai cara, seperti berdasarkan tujuan, pemilik, atau lingkungan. Misalnya, Anda dapat menandai rotasi untuk mengidentifikasi lokasi kontak yang ditetapkan padanya, jenis cakupan yang dimaksudkan untuk disediakan, atau

rencana eskalasi yang akan didukungnya. Untuk informasi selengkapnya tentang menandai sumber daya Manajer Insiden, lihatMenandai sumber daya di Manajer Insiden.

3. (Disarankan) Gunakan pratinjau kalender untuk memastikan tidak ada celah yang tidak diinginkan dalam cakupan untuk jadwal panggilan Anda.
4. Pilih Buat.

Anda sekarang dapat menambahkan jadwal panggilan sebagai saluran eskalasi dalam rencana eskalasi. Untuk informasi, lihat Buat rencana eskalasi.

Mengelola jadwal panggilan yang ada di Manajer Insiden

Gunakan konten di bagian ini untuk membantu Anda bekerja dengan jadwal panggilan yang telah Anda buat.

Topik

- Melihat detail jadwal panggilan
- Mengedit jadwal panggilan
- Menyalin jadwal panggilan
- Membuat penggantian untuk rotasi jadwal panggilan
- Menghapus jadwal panggilan

Melihat detail jadwal panggilan

Anda dapat mengakses at-a-glance ringkasan jadwal panggilan di halaman Lihat detail jadwal panggilan. Halaman ini juga berisi informasi tentang siapa yang sedang menelepon dan siapa yang sedang menelepon berikutnya. Halaman ini menyertakan tampilan kalender yang menunjukkan kontak mana yang sedang dipanggil pada waktu tertentu.

Untuk melihat detail jadwal panggilan

1. Buka konsol Manajer Insiden.
2. Di navigasi kiri, pilih Jadwal panggilan.
3. Di baris agar jadwal panggilan dapat dilihat, lakukan salah satu hal berikut:

   - Untuk membuka tampilan ringkasan kalender, pilih alias jadwal.

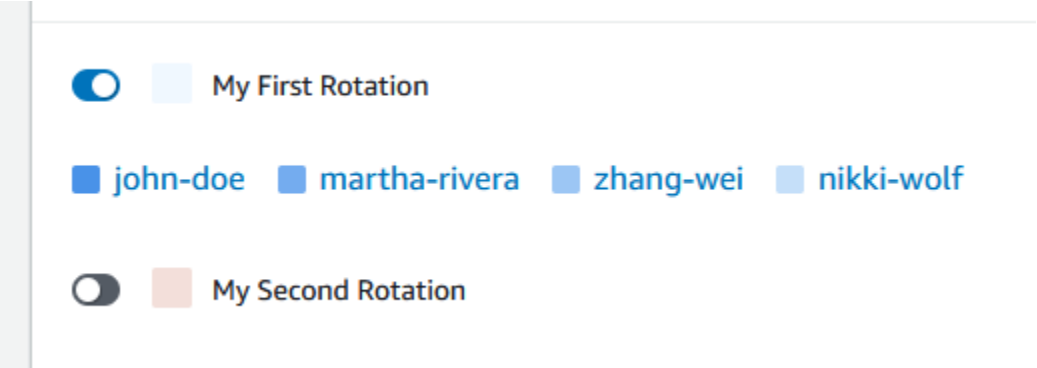
     -atau-

Pilih tombol radio untuk baris, lalu pilih Lihat.

- Untuk membuka tampilan kalender jadwal, pilih Lihat kalender

  Dalam tampilan kalender, pilih nama kontak pada tanggal tertentu dalam jadwal untuk melihat detail tentang shift yang ditetapkan atau membuat penggantian,.

- Untuk mengaktifkan atau mematikan tampilan rotasi tertentu di kalender, pilih sakelar di sebelah nama rotasi.



Mengedit jadwal panggilan

Anda dapat memperbarui konfigurasi untuk jadwal panggilan dan rotasinya, kecuali detail berikut:

- Jadwal alias
- Nama rotasi
- Tanggal mulai rotasi

Untuk menggunakan kalender yang ada sebagai dasar kalender baru dengan kemampuan untuk mengubah nilai-nilai ini, Anda dapat menyalin kalender sebagai gantinya. Untuk informasi, lihat Menyalin jadwal panggilan.

Untuk mengedit jadwal panggilan

1. Buka konsol Manajer Insiden.
2. Di navigasi kiri, pilih Jadwal panggilan.
3. Lakukan salah satu hal berikut ini:
   - Pilih tombol radio di baris untuk jadwal panggilan untuk mengedit, lalu pilih Edit.

- Pilih alias jadwal untuk jadwal panggilan untuk membuka halaman Lihat detail jadwal panggilan, lalu pilih Edit.

4. Lakukan modifikasi apa pun yang diperlukan pada jadwal panggilan dan rotasinya. Anda dapat mengubah opsi konfigurasi rotasi seperti waktu mulai dan akhir, kontak, dan pengulangan. Anda dapat menambah atau menghapus rotasi dari jadwal sesuai kebutuhan. Pratinjau kalender mencerminkan perubahan saat Anda membuatnya.

   Untuk informasi tentang bekerja dengan opsi pada halaman, lihatMembuat jadwal panggilan dan rotasi di Manajer Insiden.

5. Pilih Perbarui.

> **Important**
>
> Jika Anda mengedit jadwal yang berisi penggantian, perubahan Anda dapat memengaruhi penggantian. Untuk memastikan bahwa penggantian Anda tetap dikonfigurasi seperti yang diharapkan, kami sarankan untuk meninjau penggantian shift Anda dengan cermat setelah Anda memperbarui jadwal.

Menyalin jadwal panggilan

Untuk menggunakan konfigurasi jadwal panggilan yang ada sebagai titik awal untuk jadwal baru, Anda dapat membuat salinan kalender dan memodifikasinya sesuai kebutuhan.

Untuk menyalin jadwal panggilan

1. Buka konsol Manajer Insiden.
2. Di navigasi kiri, pilih Jadwal panggilan.
3. Pilih tombol radio di baris untuk jadwal panggilan untuk disalin.
4. Pilih Salin.
5. Buat modifikasi apa pun yang Anda butuhkan pada kalender dan rotasinya. Anda dapat mengubah, menambah, atau menghapus rotasi sesuai kebutuhan.

> **Note**
>
> Saat Anda menyalin jadwal yang ada, Anda harus menentukan tanggal mulai baru untuk setiap rotasi. Jadwal yang disalin tidak mendukung rotasi dengan tanggal mulai di masa lalu.

Untuk informasi tentang bekerja dengan opsi pada halaman, lihat[Membuat jadwal panggilan dan rotasi di Manajer Insiden](#).

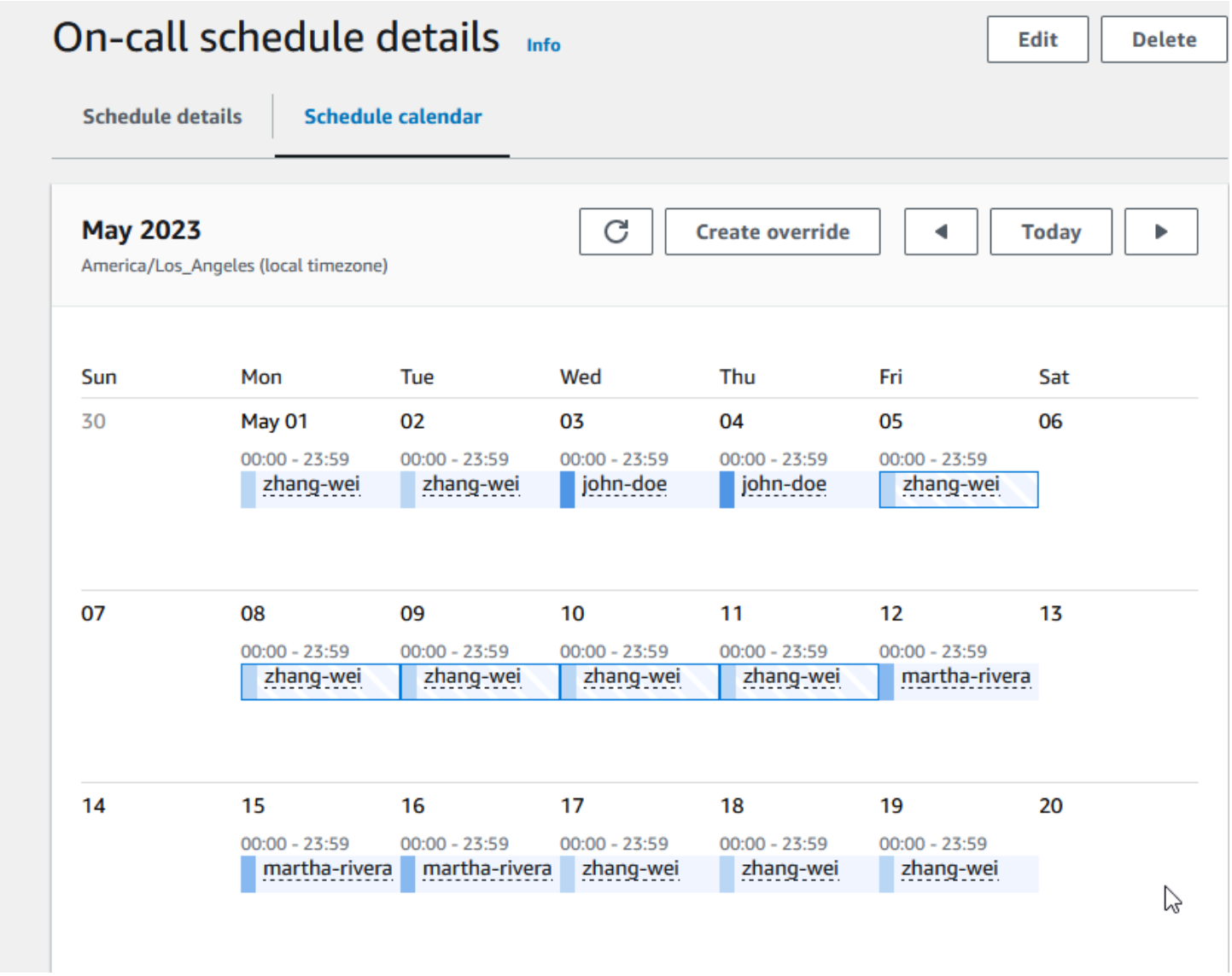
6. Pilih Buat salinan.

Membuat penggantian untuk rotasi jadwal panggilan

Jika Anda perlu membuat perubahan satu kali pada jadwal rotasi yang ada, Anda dapat membuat penggantian. Override memungkinkan Anda mengganti semua atau sebagian shift kontak dengan kontak lain. Anda juga dapat membuat override yang mencakup beberapa shift.

Anda hanya dapat menetapkan kontak ke penggantian yang sudah ditetapkan ke rotasi.

Dalam pratinjau kalender, shift yang diganti ditampilkan dengan latar belakang bergaris, bukan latar belakang yang solid. Gambar berikut menunjukkan bahwa kontak bernama Zhang Wei sedang dipanggil dalam penggantian. Pengesampingan termasuk bagian dari shift untuk John Doe dan Martha Rivera, mulai 5 Mei dan berakhir 11 Mei.



Untuk membuat penggantian untuk jadwal panggilan

1. Buka konsol Manajer Insiden.
2. Di navigasi kiri, pilih Jadwal panggilan.
3. Di baris agar jadwal panggilan dapat dilihat, lakukan salah satu hal berikut:
   - Pilih alias jadwal, lalu pilih tab Jadwal kalender.
   - Pilih Lihat kalender
4. Lakukan salah satu hal berikut ini:
   - Pilih Buat penggantian.
   - Pilih nama kontak di pratinjau kalender, lalu pilih Ganti shift.

5. Dalam kotak dialog Create shift override, lakukan hal berikut:

> **Note**
>
> Penggantian harus berdurasi minimal 30 menit. Anda hanya dapat menentukan penggantian untuk shift yang terjadi tidak lebih dari enam bulan di masa depan.

   a. Untuk Pilih rotasi, pilih nama rotasi untuk membuat penggantian.
   b. Untuk Tanggal mulai, pilih atau masukkan tanggal ketika penggantian dimulai.
   c. Untuk Waktu mulai, masukkan waktu ketika penggantian dimulai dalam `hh:mm` format.
   d. Untuk Tanggal akhir, pilih atau masukkan tanggal ketika penggantian berakhir.
   e. Untuk Waktu akhir, masukkan waktu ketika penggantian berakhir, dalam `hh:mm` format.
   f. Untuk Pilih kontak ganti, pilih nama kontak rotasi yang sedang dipanggil selama periode penggantian.
6. Pilih Buat penggantian.

Setelah Anda membuat override, Anda dapat mengidentifikasinya dengan latar belakangnya yang bergaris. Saat Anda memilih nama kontak untuk shift yang diganti, kotak informasi mengidentifikasinya sebagai shift yang diganti. Anda dapat memilih Delete override untuk menghapusnya dan mengembalikan penetapan panggilan asli.

Menghapus jadwal panggilan

Ketika Anda tidak lagi memerlukan jadwal panggilan tertentu, Anda dapat menghapusnya dari Manajer Insiden.

Jika ada rencana eskalasi atau rencana respons yang saat ini menggunakan jadwal panggilan sebagai saluran eskalasi, Anda harus menghapusnya dari paket tersebut sebelum menghapus jadwal.

Untuk menghapus jadwal panggilan

1. Buka konsol Manajer Insiden.
2. Di navigasi kiri, pilih Jadwal panggilan.
3. Pilih tombol radio di baris untuk menghapus jadwal panggilan.
4. Pilih Hapus.

5. Dalam jadwal Hapus panggilan? kotak dialog, masukkan **`confirm`** di kotak teks.
6. Pilih Hapus.

Membuat rencana eskalasi untuk keterlibatan responden di Manajer Insiden

Manajer Insiden AWS Systems Manager menyediakan jalur eskalasi melalui kontak yang ditentukan atau jadwal panggilan Anda, yang secara kolektif dikenal sebagai saluran eskalasi. Anda dapat menarik beberapa saluran eskalasi ke dalam insiden pada saat yang bersamaan. Jika kontak yang ditunjuk di saluran eskalasi tidak merespons, Manajer Insiden akan meningkat ke rangkaian kontak berikutnya. Anda juga dapat memilih apakah rencana berhenti meningkat setelah pengguna mengakui keterlibatan. Anda dapat menambahkan rencana eskalasi ke rencana respons sehingga eskalasi secara otomatis dimulai pada awal insiden. Anda juga dapat menambahkan rencana eskalasi ke insiden aktif.

Topik

- Tahapan
- Buat rencana eskalasi

Tahapan

Rencana eskalasi menggunakan tahapan di mana setiap tahap berlangsung dalam jumlah menit yang ditentukan. Setiap tahap memiliki informasi berikut:

- Durasi — Jumlah waktu rencana menunggu sampai memulai tahap berikutnya. Tahap pertama dari rencana eskalasi dimulai setelah pertunangan dimulai.
- Saluran eskalasi — Saluran eskalasi adalah satu kontak atau jadwal panggilan yang terdiri dari beberapa kontak yang memutar tanggung jawab pada jadwal yang ditentukan. Rencana eskalasi melibatkan setiap saluran menggunakan rencana keterlibatan yang ditentukan. Anda dapat mengatur setiap saluran eskalasi untuk menghentikan perkembangan rencana eskalasi sebelum melanjutkan ke tahap berikutnya. Setiap tahap dapat memiliki beberapa saluran eskalasi.

  Untuk informasi tentang pengaturan kontak individual, lihatMembuat dan mengonfigurasi kontak di Manajer Insiden. Untuk informasi tentang membuat jadwal panggilan, lihat. Mengelola rotasi responden dengan jadwal panggilan di Manajer Insiden

Buat rencana eskalasi

1. Buka konsol Manajer Insiden dan pilih Paket eskalasi dari navigasi kiri.
2. Pilih Buat rencana eskalasi.
3. Untuk Nama, masukkan nama unik untuk rencana eskalasi, seperti**`My Escalation Plan`**.
4. Untuk Alias, masukkan alias untuk membantu Anda mengidentifikasi rencana, seperti. **`my-escalation-plan`**
5. Untuk durasi Stage, masukkan jumlah menit bagi Manajer Insiden untuk menunggu hingga berlanjut ke tahap berikutnya.
6. Untuk saluran Escalation, pilih satu atau beberapa kontak atau jadwal panggilan untuk terlibat selama tahap ini.
7. (Opsional) Untuk membiarkan kontak menghentikan rencana eskalasi setelah mereka mengakui keterlibatan, pilih Pengakuan menghentikan perkembangan rencana.
8. Untuk menambahkan saluran lain ke tahap ini, pilih Tambahkan saluran eskalasi.
9. Untuk menambahkan tahap lain ke rencana eskalasi, pilih Tambahkan tahap.
10. Ulangi langkah 5 hingga 9 sampai Anda selesai menambahkan saluran eskalasi dan tahapan yang Anda inginkan untuk rencana eskalasi ini.
11. (Opsional) Di area Tag, terapkan satu atau beberapa nama kunci tag dan pasangan nilai ke rencana eskalasi.

    Tanda adalah metadata opsional yang Anda tetapkan ke sumber daya. Tag memungkinkan Anda untuk mengkategorikan sumber daya dengan berbagai cara, seperti berdasarkan tujuan, pemilik, atau lingkungan. Misalnya, Anda dapat menandai rencana eskalasi untuk mengidentifikasi jenis insiden yang akan digunakan, jenis saluran eskalasi yang dikandungnya, atau rencana eskalasi yang didukungnya. Untuk informasi selengkapnya tentang menandai sumber daya Manajer Insiden, lihatMenandai sumber daya di Manajer Insiden.
12. Pilih Buat rencana eskalasi.

Membuat dan mengintegrasikan saluran obrolan untuk responden di Manajer Insiden

Manajer Insiden, alat dalam AWS Systems Manager, memberikan responden insiden kemampuan untuk berkomunikasi langsung melalui saluran obrolan selama insiden. Saluran obrolan adalah ruang

obrolan yang Anda atur di Amazon Q Developer di aplikasi obrolan. Anda kemudian menghubungkan saluran ini ke rencana respons di Manajer Insiden.

Selama insiden, responden menggunakan saluran obrolan untuk berkomunikasi satu sama lain tentang insiden tersebut. Manajer Insiden juga mendorong pembaruan dan pemberitahuan tentang insiden tersebut langsung ke saluran obrolan. Ini mengirimkan notifikasi ini menggunakan satu atau beberapa topik Amazon Simple Notification Service (Amazon SNS) yang Anda tentukan dalam konfigurasi ruang obrolan Anda.

Pengembang Amazon Q dalam aplikasi obrolan dan Manajer Insiden mendukung saluran obrolan dalam aplikasi berikut:

- Slack
- Microsoft Teams
- Amazon Chime

Proses untuk menyiapkan saluran obrolan untuk digunakan dalam insiden Anda terdiri dari tugas di tiga layanan Amazon Web Services yang berbeda.

Tugas

- Tugas 1: Membuat atau memperbarui topik Amazon SNS untuk saluran obrolan Anda
- Tugas 2: Buat saluran obrolan di Amazon Q Developer di aplikasi obrolan
- Tugas 3: Tambahkan saluran obrolan ke rencana respons di Manajer Insiden
- Berinteraksi melalui saluran obrolan

Tugas 1: Membuat atau memperbarui topik Amazon SNS untuk saluran obrolan Anda

Amazon SNS adalah layanan terkelola yang menyediakan pengiriman pesan dari penerbit ke pelanggan (juga dikenal sebagai produsen dan konsumen). Penerbit berkomunikasi secara asinkron dengan pelanggan dengan mengirim pesan ke topik, yang merupakan titik akses logis dan saluran komunikasi. Manajer Insiden menggunakan satu atau beberapa topik yang Anda kaitkan dengan rencana respons untuk mengirim pemberitahuan tentang insiden kepada responden insiden.

Dalam paket respons, Anda dapat menyertakan satu atau beberapa topik Amazon SNS ke pemberitahuan insiden. Sebagai praktik terbaik, Anda harus membuat topik SNS di setiap yang telah Wilayah AWS Anda tambahkan ke set replikasi Anda.

> **Tip**
>
> Untuk alur kerja penyiapan yang lebih linier, kami sarankan Anda mengonfigurasi topik Amazon SNS Anda untuk digunakan dengan Manajer Insiden terlebih dahulu. Setelah dikonfigurasi, Anda dapat membuat saluran obrolan.

Untuk membuat atau memperbarui topik Amazon SNS untuk saluran obrolan Anda

1. Ikuti langkah-langkah dalam topik Membuat Amazon SNS di Panduan Pengembang Layanan Pemberitahuan Sederhana Amazon.

   > **Note**
   >
   > Setelah membuat topik, Anda mengeditnya untuk memperbarui kebijakan aksesnya.

2. Pilih topik yang Anda buat, dan catat atau salin Nama Sumber Daya Amazon (ARN) topik, dalam format seperti. `arn:aws:sns:us-east-2:111122223333:My_SNS_topic`
3. Pilih Edit, lalu perluas bagian Kebijakan akses untuk mengonfigurasi izin akses tambahan di luar default.
4. Tambahkan pernyataan berikut ke array Pernyataan kebijakan:

```
{
    "Sid": "IncidentManagerSNSPublishingPermissions",
    "Effect": "Allow",
    "Principal": {
        "Service": "ssm-incidents.amazonaws.com"
    },
    "Action": "SNS:Publish",
    "Resource": "sns-topic-arn",
    "Condition": {
        "StringEqualsIfExists": {
            "AWS:SourceAccount": "account-id"
        }
    }
```

```
}
```

Ganti *placeholder values* sebagai berikut:

- *sns-topic-arn*adalah Nama Sumber Daya Amazon (ARN) dari topik yang Anda buat untuk Wilayah ini, dalam format. `arn:aws:sns:us-east-2:111122223333:My_SNS_topic`
- *account-id*adalah ID tempat Akun AWS Anda bekerja, seperti`111122223333`.

5. Pilih Simpan perubahan.
6. Ulangi proses di setiap Wilayah yang disertakan dalam set replikasi Anda.

Tugas 2: Buat saluran obrolan di Amazon Q Developer di aplikasi obrolan

Anda dapat membuat saluran obrolan di Slack, Microsoft Teams, atau Amazon Chime. Anda hanya perlu satu saluran obrolan untuk setiap paket respons.

Untuk saluran obrolan Anda, sebaiknya ikuti prinsip hak istimewa paling sedikit (tidak memberi pengguna izin lebih dari yang diperlukan untuk menyelesaikan tugas mereka). Anda juga harus secara teratur meninjau keanggotaan Pengembang Amazon Q Anda di saluran obrolan aplikasi obrolan. Ulasan membantu memeriksa bahwa hanya responden yang sesuai dan pemangku kepentingan lainnya yang memiliki akses ke saluran obrolan Anda.

Masuk Slack saluran dan Microsoft Teams saluran yang dibuat di Amazon Q Developer dalam aplikasi obrolan, responden insiden dapat menjalankan sejumlah perintah CLI Manajer Insiden langsung dari Slack atau Microsoft Teams aplikasi. Untuk informasi selengkapnya, lihat Berinteraksi melalui saluran obrolan.

> **Important**
>
> Pengguna yang Anda tambahkan ke saluran obrolan Anda harus memiliki kontak yang sama yang tercantum pada rencana eskalasi atau respons Anda. Anda juga dapat menambahkan pengguna tambahan ke saluran obrolan, seperti pemangku kepentingan dan pengamat insiden.

Untuk informasi umum tentang Pengembang Amazon Q dalam aplikasi obrolan, lihat Apa itu Pengembang Amazon Q dalam aplikasi obrolan di Panduan Administrator Pengembang Amazon Q dalam aplikasi obrolan.

Pilih dari aplikasi berikut untuk membuat saluran Anda di:

Slack

Langkah-langkah dalam prosedur ini memberikan pengaturan izin yang disarankan untuk memungkinkan semua pengguna saluran menggunakan perintah obrolan dengan Manajer Insiden. Menggunakan perintah obrolan yang didukung, responden insiden Anda dapat memperbarui dan berinteraksi dengan insiden langsung dari Slack saluran obrolan. Untuk informasi, lihat Berinteraksi melalui saluran obrolan.

Untuk membuat saluran obrolan di Slack

- Ikuti langkah-langkah dalam Tutorial: Memulai dengan Slackdi Pengembang Amazon Q dalam aplikasi obrolan Panduan Administrator dan sertakan yang berikut ini dalam konfigurasi Anda.
  - Pada langkah 10, untuk Pengaturan peran, pilih Peran saluran.
  - Pada langkah 10d, untuk templat Kebijakan, pilih izin Manajer Insiden.
  - Pada langkah 11, untuk kebijakan pagar pembatas Saluran, untuk nama Kebijakan, pilih. `AWSIncidentManagerResolverAccess`
  - Pada langkah 12, di bagian topik SNS, lakukan hal berikut:
    - Untuk Wilayah 1, pilih Wilayah AWS yang disertakan dalam set replikasi Anda.
    - Untuk Topik 1, pilih topik SNS yang Anda buat di Wilayah tersebut untuk digunakan untuk mengirim pemberitahuan insiden ke saluran obrolan.
    - Untuk setiap Wilayah tambahan dalam kumpulan replikasi Anda, pilih Tambahkan Wilayah lain dan tambahkan topik Wilayah dan SNS tambahan.

Microsoft Teams

Langkah-langkah dalam prosedur ini memberikan pengaturan izin yang disarankan untuk memungkinkan semua pengguna saluran menggunakan perintah obrolan dengan Manajer Insiden. Menggunakan perintah obrolan yang didukung, responden insiden Anda dapat memperbarui dan berinteraksi dengan insiden langsung dari Microsoft Teams saluran obrolan. Untuk informasi, lihat Berinteraksi melalui saluran obrolan.

Untuk membuat saluran obrolan di Microsoft Teams

- Ikuti langkah-langkah dalam Tutorial: Memulai dengan Microsoft Teamsdi Pengembang Amazon Q dalam aplikasi obrolan Panduan Administrator dan sertakan yang berikut ini dalam konfigurasi Anda:
  - Pada langkah 10, untuk Pengaturan peran, pilih Peran saluran.
  - Pada langkah 10d, untuk templat Kebijakan, pilih izin Manajer Insiden.
  - Pada langkah 11, untuk kebijakan pagar pembatas Saluran, untuk nama Kebijakan, pilih. `AWSIncidentManagerResolverAccess`
  - Pada langkah 12, di bagian topik SNS, lakukan hal berikut:
    - Untuk Wilayah 1, pilih Wilayah AWS yang disertakan dalam set replikasi Anda.
    - Untuk Topik 1, pilih topik SNS yang Anda buat di Wilayah tersebut untuk digunakan untuk mengirim pemberitahuan insiden ke saluran obrolan.
    - Untuk setiap Wilayah tambahan dalam kumpulan replikasi Anda, pilih Tambahkan Wilayah lain dan tambahkan topik Wilayah dan SNS tambahan.

Amazon Chime

Untuk membuat saluran obrolan di Amazon Chime

- Ikuti langkah-langkah dalam Tutorial: Mulai dengan Amazon Chime di Pengembang Amazon Q dalam aplikasi obrolan Panduan Administrator dan sertakan yang berikut ini dalam konfigurasi Anda:
  - Pada langkah 11, untuk templat Kebijakan, pilih Izin Manajer Insiden.
  - Pada langkah 12, di bagian topik SNS, pilih topik SNS yang akan mengirim pemberitahuan ke webhook Amazon Chime:
    - Untuk Wilayah 1, pilih Wilayah AWS yang disertakan dalam set replikasi Anda.
    - Untuk Topik 1, pilih topik SNS yang Anda buat di Wilayah tersebut untuk digunakan untuk mengirim pemberitahuan insiden ke saluran obrolan.
    - Untuk setiap Wilayah tambahan dalam kumpulan replikasi Anda, pilih Tambahkan Wilayah lain dan tambahkan topik Wilayah dan SNS tambahan.

> **Note**
>
> Perintah obrolan, yang dapat digunakan oleh responden insiden Slack and Microsoft Teams saluran obrolan, tidak didukung di Amazon Chime.

Tugas 3: Tambahkan saluran obrolan ke rencana respons di Manajer Insiden

Saat membuat atau memperbarui rencana respons, Anda dapat menambahkan saluran obrolan agar responden dapat berkomunikasi dan menerima pembaruan.

Saat mengikuti langkah-langkah diMembuat rencana respons, untuk bagian tersebut (Opsional) Menentukan saluran obrolan respons insiden, pilih saluran yang ingin Anda gunakan untuk insiden yang terkait dengan rencana respons ini.

Berinteraksi melalui saluran obrolan

Untuk saluran di Slack and Microsoft Teams, Manajer Insiden memungkinkan responden untuk berinteraksi dengan insiden langsung dari saluran obrolan menggunakan perintah berikut: `ssm-incidents`

- insiden awal
- list-response-plan
- get-response-plan
- create-timeline-event
- delete-timeline-event
- get-incident-record
- get-timeline-event
- list-incident-records
- list-timeline-events
- list-related-items
- update-related-items
- update-incident-record

- update-timeline-event

Untuk menjalankan perintah di saluran obrolan insiden aktif, gunakan format berikut. Ganti *cli-options* dengan opsi apa pun yang akan disertakan untuk perintah.

```
@aws ssm-incidents cli-options
```

Sebagai contoh:

```
@aws ssm-incidents start-incident --response-plan-arn arn:aws:ssm-
incidents::111122223333:response-plan/test-response-plan-chat --region us-east-2
```

```
@aws ssm-incidents create-timeline-event --event-data "\"example timeline event"\" --
event-time 2023-03-31 T20:30:00.000  --event-type Custom Event --incident-record-arn
 arn:aws:ssm-incidents::111122223333:incident-record/MyResponsePlanChat/98c397e6-7c10-
aa10-9b86-f199aEXAMPLE
```

```
@aws ssm-incidents list-incident-records
```

Mengintegrasikan runbook Otomasi Systems Manager di Incident Manager untuk remediasi insiden

Anda dapat menggunakan runbook dari AWS Systems Manager Automation, alat di AWS Systems Manager, untuk mengotomatiskan tugas aplikasi dan infrastruktur umum di lingkungan Anda AWS Cloud .

Setiap runbook mendefinisikan alur kerja runbook, yang terdiri dari tindakan yang dilakukan Systems Manager pada node terkelola atau jenis sumber daya lainnya. AWS Anda dapat menggunakan runbook untuk mengotomatiskan pemeliharaan, penyebaran, dan remediasi sumber daya Anda. AWS

Di Manajer Insiden, runbook mendorong respons dan mitigasi insiden, dan Anda menentukan runbook yang akan digunakan sebagai bagian dari rencana respons.

Dalam paket respons Anda, Anda dapat memilih dari lusinan runbook yang telah dikonfigurasi sebelumnya untuk tugas yang biasanya otomatis, atau Anda dapat membuat runbook khusus. Saat

Anda menentukan runbook dalam definisi rencana respons, sistem dapat secara otomatis memulai buku runbook saat insiden dimulai.

> **Important**
>
> Insiden yang dibuat oleh failover lintas wilayah tidak memanggil runbook yang ditentukan dalam paket respons.

Untuk informasi selengkapnya tentang Otomasi Systems Manager, runbook, dan menggunakan runbook dengan Manajer Insiden, lihat topik berikut:

- Untuk menambahkan runbook ke rencana respons, lihatMembuat dan mengonfigurasi rencana respons di Manajer Insiden.
- Untuk mempelajari selengkapnya tentang runbook, lihat AWS Systems Manager Otomatisasi di Panduan AWS Systems Manager Pengguna dan referensi buku runbook AWS Systems Manager Otomasi.
- Untuk informasi tentang biaya penggunaan runbook, lihat harga Systems Manager.
- Untuk informasi tentang menjalankan runbook secara otomatis saat insiden dibuat oleh CloudWatch alarm Amazon atau EventBridge peristiwa Amazon, lihat Tutorial: Menggunakan runbook Otomasi Systems Manager dengan Manajer Insiden.

Topik

- Izin IAM diperlukan untuk memulai dan menjalankan alur kerja runbook
- Bekerja dengan parameter runbook
- Tentukan runbook
- Templat runbook Manajer Insiden

Izin IAM diperlukan untuk memulai dan menjalankan alur kerja runbook

Manajer Insiden memerlukan izin untuk menjalankan runbook sebagai bagian dari respons insiden Anda. Untuk memberikan izin ini, Anda menggunakan peran AWS Identity and Access Management (IAM), peran layanan Runbook, dan Otomasi. `AssumeRole`

Peran layanan Runbook adalah peran layanan yang diperlukan. Peran ini memberi Manajer Insiden izin yang diperlukan untuk mengakses dan memulai alur kerja untuk runbook.

Otomasi `AssumeRole` menyediakan izin yang diperlukan untuk menjalankan perintah individual yang ditentukan dalam runbook.

> **Note**
>
> Jika no `AssumeRole` ditentukan, Systems Manager Automation mencoba menggunakan peran layanan Runbook untuk perintah individual. Jika Anda tidak menentukan`AssumeRole`, Anda harus menambahkan izin yang diperlukan ke peran layanan Runbook. Jika tidak, runbook gagal menjalankan perintah tersebut.
> Namun, sebagai praktik terbaik keamanan, kami sarankan menggunakan yang terpisah`AssumeRole`. Dengan terpisah`AssumeRole`, Anda dapat membatasi izin yang diperlukan yang harus Anda tambahkan ke setiap peran.

Untuk informasi selengkapnya tentang Otomasi`AssumeRole`, lihat Mengonfigurasi akses peran layanan (mengambil peran) untuk otomatisasi 'di AWS Systems Manager Panduan Pengguna.

Anda dapat membuat salah satu jenis peran secara manual sendiri di konsol IAM.- Anda juga dapat membiarkan Manajer Insiden membuat salah satu untuk Anda saat Anda membuat atau memperbarui rencana respons.

Izin peran layanan Runbook

Izin peran layanan Runbook disediakan melalui kebijakan yang serupa dengan berikut ini.

Pernyataan pertama memungkinkan Incident Manager untuk memulai `StartAutomationExecution` operasi Systems Manager. Operasi ini kemudian berjalan pada sumber daya yang diwakili oleh tiga format Amazon Resource Name (ARN).

Pernyataan kedua memungkinkan peran layanan Runbook untuk mengambil peran di akun lain ketika runbook tersebut berjalan di akun yang terkena dampak. Untuk informasi selengkapnya, lihat Menjalankan otomatisasi di beberapa akun Wilayah AWS dan di Panduan AWS Systems Manager Pengguna.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ssm:StartAutomationExecution",
      "Resource": [
```

```
        "arn:aws:ssm:*:{{DocumentAccountId}}:automation-definition/{{DocumentName}}:*",
        "arn:aws:ssm:*:{{DocumentAccountId}}:document/{{DocumentName}}:*",
        "arn:aws:ssm:*::automation-definition/{{DocumentName}}:*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Resource": "arn:aws:iam::*:role/AWS-SystemsManager-AutomationExecutionRole",
      "Condition": {
        "StringEquals": {
          "aws:CalledViaLast": "ssm.amazonaws.com"
        }
      }
    }
  ]
}
```

AssumeRole Izin otomatisasi

Saat membuat atau memperbarui rencana respons, Anda dapat memilih dari beberapa kebijakan AWS terkelola untuk dilampirkan ke Manajer Insiden AssumeRole yang dibuat. Kebijakan ini memberikan izin untuk menjalankan sejumlah operasi umum yang digunakan dalam skenario runbook Manajer Insiden. Anda dapat memilih satu atau beberapa kebijakan terkelola ini untuk memberikan izin bagi `AssumeRole` kebijakan Anda. Tabel berikut menjelaskan kebijakan yang dapat Anda pilih saat membuat dari konsol Manajer Insiden. `AssumeRole`

Nama kebijakan terkelola AWS	Deskripsi kebijakan
`AmazonSSMAutomationRole`	Memberikan izin untuk layanan Otomasi Systems Manager untuk menjalankan aktivitas yang ditentukan dalam runbook. Menetapkan kebijakan ini untuk administrator dan pengguna daya terpercaya.
`AWSIncidentManagerResolverAccess`	Memberikan izin bagi pengguna untuk memulai, melihat, dan memperbarui insiden. Anda juga dapat menggunakannya untuk membuat peristiwa timeline pelanggan dan item terkait di dasbor insiden.

Anda dapat menggunakan kebijakan terkelola ini untuk memberikan izin bagi banyak skenario respons insiden umum. Namun, izin yang diperlukan untuk tugas tertentu yang Anda butuhkan dapat bervariasi. Dalam kasus ini, Anda perlu memberikan izin kebijakan tambahan untuk Anda`AssumeRole`. Untuk selengkapnya, lihat referensi buku runbook AWS Systems Manager Otomasi.

Bekerja dengan parameter runbook

Saat menambahkan runbook ke rencana respons, Anda dapat menentukan parameter yang harus digunakan runbook saat runtime. Rencana respons mendukung parameter dengan nilai statis dan dinamis. Untuk nilai statis, Anda memasukkan nilai saat Anda menentukan parameter dalam rencana respons. Untuk nilai dinamis, sistem menentukan nilai parameter yang benar dengan mengumpulkan informasi dari insiden tersebut. Manajer Insiden mendukung parameter dinamis berikut:

`Incident ARN`

Ketika Manajer Insiden membuat insiden, sistem menangkap Nama Sumber Daya Amazon (ARN) dari catatan insiden yang sesuai dan memasukkannya untuk parameter ini di runbook.

> **Note**
>
> Nilai ini hanya dapat ditetapkan ke parameter tipe`String`. Jika ditetapkan ke parameter jenis lain, runbook gagal dijalankan.

`Involved resources`

Ketika Manajer Insiden menciptakan insiden, sistem menangkap sumber ARNs daya yang terlibat dalam insiden tersebut. Sumber daya ARNs ini kemudian ditetapkan ke parameter ini di runbook.

Tentang sumber daya terkait

Manajer Insiden dapat mengisi nilai parameter runbook dengan AWS sumber daya ARNs yang ditentukan dalam CloudWatch alarm, EventBridge peristiwa, dan insiden yang dibuat secara manual. Bagian ini menjelaskan berbagai jenis sumber daya yang dapat ditangkap oleh Manajer Insiden ARNs saat mengisi parameter ini.

CloudWatch alarm

Ketika insiden dibuat dari tindakan CloudWatch alarm, Manajer Insiden secara otomatis mengekstrak jenis sumber daya berikut dari metrik terkait. Kemudian mengisi parameter yang dipilih dengan sumber daya yang terlibat berikut:

AWS layanan	Jenis sumber daya
Amazon DynamoDB	Indeks sekunder global Pengaliran Tabel
Amazon EC2	Citra Instans
AWS Lambda	Alias fungsi Versi fungsi Fungsi
Amazon Relational Database Service (Amazon RDS)	Klaster Contoh database
Amazon Simple Storage Service (Amazon S3)	Bucket

EventBridge aturan

Ketika sistem membuat insiden dari suatu EventBridge peristiwa, Manajer Insiden mengisi parameter yang dipilih dengan `Resources` properti dalam acara tersebut. Untuk informasi selengkapnya, lihat EventBridgeAcara Amazon di Panduan EventBridge Pengguna Amazon.

Insiden yang dibuat secara manual

Saat Anda membuat insiden menggunakan tindakan StartIncidentAPI, Manajer Insiden mengisi parameter yang dipilih dengan menggunakan informasi dalam panggilan API. Secara khusus, ini mengisi parameter dengan menggunakan item dari jenis `INVOLVED_RESOURCE` yang diteruskan dalam `relatedItems` parameter.

> **Note**
>
> `INVOLVED_RESOURCES`Nilai hanya dapat ditetapkan ke parameter tipe`StringList`. Jika ditetapkan ke parameter jenis lain, runbook gagal dijalankan.

Tentukan runbook

Saat membuat runbook, Anda dapat mengikuti langkah-langkah yang disediakan di sini, atau Anda dapat mengikuti panduan lebih rinci yang disediakan di bagian Bekerja dengan runbook di Panduan Pengguna Systems Manager. Jika Anda membuat runbook multi-akun multi-wilayah, lihat Menjalankan otomatisasi di beberapa akun Wilayah AWS dan akun di Panduan Pengguna Systems Manager.

Tentukan runbook

1. Buka konsol Systems Manager di https://console.aws.amazon.com/systems-manager/.
2. Di panel navigasi, pilih Dokumen.
3. Pilih Buat otomatisasi.
4. Masukkan nama runbook yang unik dan dapat diidentifikasi.
5. Masukkan deskripsi runbook.
6. Berikan peran IAM untuk diasumsikan oleh dokumen otomatisasi. Hal ini memungkinkan runbook untuk menjalankan perintah secara otomatis. Untuk informasi selengkapnya, lihat Mengonfigurasi akses peran layanan untuk alur kerja Otomasi.
7. (Opsional) Tambahkan parameter input apa pun yang dimulai dengan runbook. Anda dapat menggunakan parameter dinamis atau statis saat memulai runbook. Parameter dinamis menggunakan nilai dari insiden tempat runbook dimulai. Parameter statis menggunakan nilai yang Anda berikan.
8. (Opsional) Tambahkan tipe Target.
9. (Opsional) Tambahkan tanda.
10. Isi langkah-langkah yang akan diambil runbook saat berjalan. Setiap langkah membutuhkan:
    - Nama.
    - Deskripsi tujuan langkah.
    - Tindakan untuk dijalankan selama langkah. Runbook menggunakan tipe tindakan Jeda untuk menjelaskan langkah manual.

- (Opsional) Properti perintah.

11. Setelah menambahkan semua langkah runbook yang diperlukan, pilih Buat Otomasi.

Untuk mengaktifkan fungsionalitas lintas akun, bagikan runbook di akun manajemen Anda dengan semua akun aplikasi yang menggunakan runbook selama insiden terjadi.

Bagikan buku runbook

1. Buka konsol Systems Manager di https://console.aws.amazon.com/systems-manager/.
2. Di panel navigasi, pilih Dokumen.
3. Dalam daftar dokumen, pilih dokumen yang ingin Anda bagikan, lalu pilih Lihat detail. Pada tab Izin, verifikasi bahwa Anda adalah pemilik dokumen. Hanya pemilik dokumen yang dapat berbagi dokumen.
4. Pilih Edit.
5. Untuk berbagi perintah secara publik, pilih publik lalu pilih Simpan. Untuk membagikan perintah secara pribadi, pilih Pribadi, masukkan Akun AWS ID, pilih Tambah izin, lalu pilih Simpan.

Templat runbook Manajer Insiden

Incident Manager menyediakan template runbook berikut untuk membantu tim Anda mulai membuat runbook dalam otomatisasi Systems Manager. Anda dapat menggunakan template ini apa adanya, atau mengeditnya untuk menyertakan detail khusus untuk aplikasi dan sumber daya Anda.

Temukan templat runbook Manajer Insiden

1. Buka konsol Systems Manager di https://console.aws.amazon.com/systems-manager/.
2. Di panel navigasi, pilih Dokumen.
3. Di area Dokumen, masukkan **`AWSIncidents-`** di bidang pencarian untuk menampilkan semua runbook Manajer Insiden.

> **Tip**
>
> Masukkan **`AWSIncidents-`** sebagai teks gratis alih-alih menggunakan opsi filter awalan nama Dokumen.

Menggunakan template

1. Buka konsol Systems Manager di https://console.aws.amazon.com/systems-manager/.
2. Di panel navigasi, pilih Dokumen.
3. Pilih template yang ingin Anda perbarui dari daftar dokumen.
4. Pilih tab Konten, lalu salin konten dokumen.
5. Di panel navigasi, pilih Dokumen.
6. Pilih Buat otomatisasi.
7. Masukkan nama yang unik dan dapat diidentifikasi.
8. Pilih tab Editor.
9. Pilih Edit.
10. Tempel atau masukkan detail yang disalin di area editor Dokumen.
11. Pilih Buat otomatisasi.

`AWSIncidents-CriticalIncidentRunbookTemplate`

`AWSIncidents-CriticalIncidentRunbookTemplate`Ini adalah template yang menyediakan siklus hidup insiden Manajer Insiden dalam langkah-langkah manual. Langkah-langkah ini cukup umum untuk digunakan di sebagian besar aplikasi, tetapi cukup rinci bagi responden untuk memulai dengan resolusi insiden.

Membuat dan mengonfigurasi rencana respons di Manajer Insiden

Paket respons memungkinkan Anda merencanakan cara merespons insiden yang berdampak pada pengguna Anda. Rencana respons berfungsi sebagai templat yang mencakup informasi tentang siapa yang harus dilibatkan, tingkat keparahan acara yang diharapkan, runbook otomatis untuk memulai, dan metrik untuk dipantau.

Praktik terbaik

Anda dapat mengurangi dampak pada insiden pada tim Anda ketika Anda merencanakan insiden sebelumnya. Tim harus mempertimbangkan praktik terbaik berikut saat Anda merancang rencana respons.

- Keterlibatan yang efisien — Identifikasi tim yang paling tepat untuk suatu insiden. Jika Anda melibatkan daftar distribusi yang terlalu luas, atau jika Anda melibatkan tim yang salah, Anda dapat menyebabkan kebingungan dan membuang waktu responden selama insiden.
- Eskalasi yang andal — Untuk keterlibatan Anda dalam rencana respons, sebaiknya pilih rencana keterlibatan alih-alih kontak atau jadwal panggilan. Rencana keterlibatan harus menentukan kontak individu atau jadwal panggilan (yang berisi beberapa kontak berputar) untuk terlibat selama insiden. Karena responden yang ditentukan dalam rencana keterlibatan Anda kadang-kadang tidak dapat dijangkau, Anda harus mengonfigurasi responden cadangan dalam rencana respons Anda untuk mencakup skenario ini. Dengan kontak cadangan, jika kontak primer dan sekunder tidak tersedia atau ada celah lain yang tidak direncanakan dalam cakupan, Manajer Insiden masih memberi tahu kontak tentang insiden tersebut.
- Runbook — Gunakan runbook untuk memberikan langkah-langkah yang dapat diulang dan dimengerti yang mengurangi stres yang dialami responden selama insiden.
- Kolaborasi — Gunakan saluran obrolan untuk merampingkan komunikasi selama insiden. Saluran obrolan membantu responden tetap up to date dengan informasi. Mereka juga dapat berbagi informasi dengan responden lain melalui saluran ini.

Membuat rencana respons

Gunakan prosedur berikut untuk membuat rencana respons dan mengotomatiskan respons insiden.

Untuk membuat rencana respons

1. Buka konsol Manajer Insiden, dan di panel navigasi, pilih Paket respons.
2. Pilih Buat rencana respons.
3. Untuk Nama, masukkan nama paket respons yang unik dan dapat diidentifikasi untuk digunakan di Amazon Resource Name (ARN) untuk paket respons.
4. (Opsional) Untuk nama Tampilan, masukkan nama yang lebih mudah dibaca manusia untuk membantu mengidentifikasi rencana respons saat Anda membuat insiden.
5. Lanjutkan dengan menentukan nilai default untuk catatan insiden.

Menentukan nilai default insiden

Untuk membantu Anda mengelola insiden secara lebih efektif, Anda dapat menentukan nilai default. Manajer Insiden menerapkan nilai-nilai ini untuk semua insiden yang terkait dengan rencana respons.

Untuk menentukan nilai default insiden

1. Untuk Judul, masukkan judul untuk insiden ini untuk membantu Anda mengidentifikasinya di halaman beranda Manajer Insiden.
2. Untuk Dampak, pilih tingkat dampak untuk menunjukkan potensi ruang lingkup insiden yang dibuat dari rencana respons ini, seperti Kritis atau Rendah. Untuk informasi tentang peringkat dampak di Manajer Insiden, lihatTriase.
3. (Opsional) Untuk Ringkasan, masukkan ringkasan singkat jenis insiden yang dibuat dari rencana respons ini.
4. (Opsional) Untuk string Dedupe, masukkan string dedupe. Incident Manager menggunakan string ini untuk mencegah akar penyebab yang sama membuat beberapa insiden di akun yang sama.

   String deduplikasi adalah istilah atau frasa yang digunakan sistem untuk memeriksa insiden duplikat. Jika Anda menentukan string deduplikasi, Manajer Insiden akan mencari insiden terbuka yang berisi string yang sama di `dedupeString` bidang saat membuat insiden. Jika duplikat terdeteksi, Manajer Insiden menghapus duplikasi insiden yang lebih baru ke dalam insiden yang ada.

   > **Note**
   >
   > Secara default, Manajer Insiden secara otomatis menghapus duplikasi beberapa insiden yang dibuat oleh alarm Amazon CloudWatch atau peristiwa Amazon yang sama. EventBridge Anda tidak perlu memasukkan string deduplikasi Anda sendiri untuk mencegah duplikasi untuk jenis sumber daya ini.

5. (Opsional) Di bawah Tag Insiden, tambahkan kunci tag dan nilai untuk ditetapkan ke insiden yang dibuat dari rencana respons ini.

   Anda harus memiliki `TagResource` izin untuk sumber catatan insiden untuk menetapkan tag insiden dalam rencana respons.
6. Lanjutkan dengan menentukan saluran obrolan opsional untuk penyelesai untuk berkomunikasi satu sama lain tentang insiden.

(Opsional) Menentukan saluran obrolan respons insiden

Saat Anda menyertakan saluran obrolan dalam rencana respons, responden menerima pembaruan insiden melalui saluran tersebut. Mereka dapat berinteraksi dengan insiden langsung dari saluran obrolan dengan menggunakan perintah obrolan.

Menggunakan Amazon Q Developer dalam aplikasi obrolan, Anda dapat membuat saluran untuk Slack, untuk Microsoft Teams, atau untuk Amazon Chime untuk digunakan dalam paket respons Anda. Untuk informasi tentang membuat saluran obrolan di Amazon Q Developer dalam aplikasi obrolan, lihat Panduan Administrator Amazon Q Developer dalam aplikasi obrolan.

> **Important**
>
> Manajer Insiden harus memiliki izin untuk mempublikasikan ke topik Simple Notification Service Amazon (Amazon SNS) saluran obrolan. Tanpa izin untuk mempublikasikan ke topik SNS itu, Anda tidak dapat menambahkannya ke paket respons. Manajer Insiden menerbitkan pemberitahuan pengujian ke topik SNS untuk memverifikasi izin.

Untuk informasi selengkapnya tentang saluran obrolan, lihatMembuat dan mengintegrasikan saluran obrolan untuk responden di Manajer Insiden.

Untuk menentukan saluran obrolan respons insiden

1. Untuk saluran Obrolan, pilih Pengembang Amazon Q di saluran obrolan aplikasi obrolan tempat responden dapat berkomunikasi selama insiden.

   > **Tip**
   >
   > Untuk membuat saluran obrolan baru di Amazon Q Developer di aplikasi obrolan, pilih Konfigurasi klien Chatbot baru.

2. Untuk topik SNS saluran Obrolan, pilih topik SNS tambahan untuk dipublikasikan selama insiden. Menambahkan topik SNS dalam beberapa Wilayah AWS meningkatkan redundansi jika suatu Wilayah turun pada saat insiden.
3. Lanjutkan dengan memilih kontak, jadwal panggilan, dan rencana eskalasi yang akan dilibatkan selama insiden.

(Opsional) Pilih sumber daya untuk terlibat dalam respons insiden

Penting untuk mengidentifikasi responden yang paling tepat ketika suatu insiden terjadi. Sebagai praktik terbaik, kami menyarankan Anda melakukan hal berikut:

1. Tambahkan kontak dan jadwal panggilan sebagai saluran eskalasi dalam rencana eskalasi.

> **Note**
>
> Saat ini, kemampuan untuk menambahkan kontak yang dibagikan dari akun lain ke paket respons tidak didukung.

2. Pilih rencana eskalasi sebagai keterlibatan dalam rencana respons.

Untuk informasi selengkapnya tentang kontak dan rencana eskalasi, lihat Membuat dan mengonfigurasi kontak di Manajer Insiden danMembuat rencana eskalasi untuk keterlibatan responden di Manajer Insiden.

Untuk memilih sumber daya untuk terlibat dalam respons insiden

1. Untuk Keterlibatan, pilih sejumlah rencana eskalasi, jadwal panggilan, dan kontak individu.
2. Lanjutkan dengan secara opsional menentukan runbook untuk dijalankan sebagai bagian dari mitigasi insiden Anda.

(Opsional) Menentukan runbook untuk mitigasi insiden

Anda dapat menggunakan runbook dari AWS Systems Manager Automation, alat di AWS Systems Manager, untuk mengotomatiskan tugas aplikasi dan infrastruktur umum di lingkungan Anda AWS Cloud .

Setiap runbook mendefinisikan alur kerja runbook. Alur kerja buku runbook mencakup tindakan yang dilakukan Systems Manager pada node terkelola atau jenis AWS sumber daya lainnya. Di Manajer Insiden, sebuah runbook mendorong respons insiden dan mitigasi.

Untuk informasi lebih lanjut tentang menggunakan runbook dalam rencana respons,Mengintegrasikan runbook Otomasi Systems Manager di Incident Manager untuk remediasi insiden.

Untuk menentukan runbook untuk mitigasi insiden:

1. Untuk Runbook, lakukan salah satu hal berikut:

   - Pilih Clone runbook dari template untuk membuat salinan runbook Manajer Insiden default. Untuk nama Runbook, masukkan nama deskriptif untuk runbook baru.
   - Pilih Pilih runbook yang ada. Pilih Pemilik, Runbook, dan Versi yang akan digunakan.

   > **Tip**
   >
   > Untuk membuat runbook dari awal, pilih Configure new runbook.
   > Untuk informasi tentang membuat peran, lihat Mengintegrasikan runbook Otomasi Systems Manager di Incident Manager untuk remediasi insiden.

2. Di area Parameter, berikan parameter apa pun yang diminta untuk runbook yang Anda pilih.

   Parameter yang tersedia adalah yang ditentukan oleh runbook. Satu runbook mungkin memerlukan parameter yang berbeda dari yang lain. Beberapa parameter mungkin diperlukan dan yang lainnya opsional.

   Dalam banyak kasus, Anda dapat memilih untuk memasukkan nilai statis untuk parameter secara manual, seperti daftar EC2 instance Amazon IDs. Anda juga dapat membiarkan Manajer Insiden memberikan nilai parameter yang dihasilkan secara dinamis oleh insiden.

3. (Opsional) Untuk AutomationAssumeRole, tentukan peran AWS Identity and Access Management (IAM) yang akan digunakan. Peran ini harus memiliki izin yang diperlukan untuk menjalankan perintah individual yang ditentukan dalam runbook.

   > **Note**
   >
   > Jika tidak `AssumeRole` ditentukan, Manajer Insiden mencoba menggunakan peran layanan Runbook untuk menjalankan perintah individual yang ditentukan dalam runbook.

   Pilih dari yang berikut ini:

   - Masukkan nilai ARN — Masukkan Nama Sumber Daya Amazon (ARN) secara manual dari AssumeRole, dalam format. `arn:aws:iam::`*`account-id`*`:role/`*`assume-role-name` Misalnya, **`arn:aws:iam::123456789012:role/MyAssumeRole`**.
   - Gunakan peran layanan yang ada — Pilih peran dengan izin yang diperlukan dari daftar peran yang ada di akun Anda.

- Buat peran layanan baru — Pilih dari antara kebijakan AWS terkelola untuk dilampirkan ke Anda AssumeRole. Setelah memilih opsi ini, untuk kebijakan AWS terkelola, pilih satu atau beberapa kebijakan dari daftar.

  Anda dapat menerima nama default yang disarankan untuk peran baru, atau memasukkan nama yang Anda pilih.

  > **Note**
  >
  > Peran layanan Runbook baru ini dikaitkan dengan runbook tertentu yang Anda pilih. Itu tidak dapat digunakan dengan runbook yang berbeda. Ini karena bagian Sumber Daya kebijakan tidak akan mendukung runbook lain.

4. Untuk peran layanan Runbook, tentukan peran IAM yang akan digunakan untuk memberikan izin yang diperlukan untuk mengakses dan memulai alur kerja untuk runbook itu sendiri.

   Minimal, peran harus memungkinkan `ssm:StartAutomationExecution` tindakan untuk runbook spesifik Anda. Agar runbook berfungsi di seluruh akun, peran juga harus mengizinkan `sts:AssumeRole` tindakan untuk `AWS-SystemsManager-AutomationExecutionRole` peran yang Anda buat selama Mengelola insiden di seluruh Akun AWS dan Wilayah di Manajer Insiden ini.

   Pilih dari yang berikut ini:

   - Buat peran layanan baru — Manajer Insiden membuat peran layanan Runbook untuk Anda yang menyertakan izin minimum yang diperlukan untuk memulai alur kerja buku runbook.

     Untuk nama Peran, Anda dapat menerima nama default yang disarankan, atau memasukkan nama yang Anda pilih. Sebaiknya gunakan nama yang disarankan atau menyimpan nama runbook dalam namanya. Ini karena yang baru AssumeRole dikaitkan dengan runbook tertentu yang Anda pilih dan mungkin tidak menyertakan izin yang diperlukan untuk runbook lain.

   - Gunakan peran layanan yang ada — Peran IAM yang Anda atau Manajer Insiden buat sebelumnya memberikan izin yang diperlukan.

     Untuk nama Peran, pilih nama peran yang ada untuk digunakan.

5. Perluas Opsi tambahan dan pilih salah satu dari berikut ini untuk menentukan di Akun AWS mana alur kerja runbook harus dijalankan.

- Akun pemilik paket respons — Mulai alur kerja runbook di Akun AWS yang membuatnya.
- Akun yang terkena dampak — Mulai alur kerja runbook di akun yang memulai atau melaporkan kejadian tersebut.

  Pilih Akun yang Terdampak saat Anda menggunakan Manajer Insiden untuk skenario lintas akun dan buku runbook perlu mengakses sumber daya di akun yang terkena dampak untuk memulihkannya.

6. Lanjutkan dengan mengintegrasikan PagerDuty layanan secara opsional ke dalam rencana respons.

(Opsional) Mengintegrasikan PagerDuty layanan ke dalam rencana respons

Untuk mengintegrasikan PagerDuty layanan ke dalam rencana respons

Saat Anda mengintegrasikan Manajer Insiden dengan PagerDuty, PagerDuty buat insiden yang sesuai setiap kali Manajer Insiden membuat insiden. Insiden di PagerDuty menggunakan alur kerja paging dan kebijakan eskalasi yang Anda tetapkan di sana selain yang ada di Manajer Insiden. PagerDuty melampirkan peristiwa timeline dari Manajer Insiden sebagai catatan tentang insiden Anda.

1. Perluas integrasi pihak ketiga, lalu pilih kotak centang Aktifkan PagerDuty integrasi.
2. Untuk Select secret, pilih rahasia di AWS Secrets Manager mana Anda menyimpan kredensi untuk mengakses akun Anda PagerDuty .

   Untuk informasi tentang menyimpan PagerDuty kredensil Anda dalam rahasia Secrets Manager, lihat. Menyimpan kredensyal PagerDuty akses secara rahasia AWS Secrets Manager
3. Untuk PagerDuty layanan, pilih layanan dari PagerDuty akun Anda di mana Anda ingin membuat PagerDuty insiden.
4. Lanjutkan dengan menambahkan tag opsional dan membuat rencana respons.

Menambahkan tag dan membuat rencana respons

Untuk menambahkan tag dan membuat rencana respons

1. (Opsional) Di area Tag, terapkan satu atau beberapa pasangan nama/nilai kunci tag ke rencana respons.

   Tag adalah metadata opsional yang Anda tetapkan ke sumber daya. Dengan tag, Anda dapat mengkategorikan sumber daya dengan berbagai cara, seperti berdasarkan tujuan, pemilik, atau lingkungan. Misalnya, Anda mungkin ingin menandai rencana respons untuk mengidentifikasi jenis insiden yang dimaksudkan untuk mitigasi, jenis saluran eskalasi yang dikandungnya, atau rencana eskalasi yang akan dikaitkan dengannya. Untuk informasi selengkapnya tentang menandai sumber daya Manajer Insiden, lihatMenandai sumber daya di Manajer Insiden.
2. Pilih Buat rencana respons.

Mengidentifikasi potensi penyebab insiden dari layanan lain sebagai “temuan” di Manajer Insiden

Di Manajer Insiden, temuan adalah informasi tentang AWS CodeDeploy penyebaran atau pembaruan AWS CloudFormation tumpukan yang terjadi sekitar waktu insiden, dan yang melibatkan satu atau lebih sumber daya yang mungkin terkait dengan insiden tersebut. Setiap temuan dapat diperiksa sebagai penyebab potensial insiden tersebut. Informasi tentang penyebab potensial ini ditambahkan ke halaman Detail insiden untuk suatu insiden. Dengan informasi tentang penerapan dan perubahan ini, responden tidak perlu mencari informasi ini secara manual. Ini mengurangi waktu yang dibutuhkan untuk mengevaluasi penyebab potensial, yang dapat mengurangi mean time to recover (MTTR) dari suatu insiden.

Saat ini, Manajer Insiden mendukung pengumpulan temuan dari dua Layanan AWS: AWS CodeDeploydan AWS CloudFormation.

Temuan adalah fitur opt-in. Anda dapat mengaktifkannya di panduan Dapatkan persiapan, saat Anda pertama kali melakukan orientasi ke Manajer Insiden, atau nanti di halaman Pengaturan.

Saat Anda mengaktifkan fitur Temuan, Manajer Insiden membuat peran layanan untuk Anda. Peran layanan ini mencakup izin yang diperlukan untuk mengambil temuan dari CodeDeploy dan. CloudFormation

Untuk bekerja dengan temuan dalam skenario lintas akun, aktifkan fitur di akun manajemen. Setelah itu, setiap akun aplikasi dalam organisasi AWS Resource Access Manager (AWS RAM) harus membuat peran layanan yang sesuai.

Lihat topik berikut untuk membantu Anda menggunakan fitur Temuan.

Topik

- Mengaktifkan dan membuat peran layanan untuk temuan
- Konfigurasikan izin untuk dukungan temuan lintas akun

Mengaktifkan dan membuat peran layanan untuk temuan

Saat Anda mengaktifkan fitur Temuan, Manajer Insiden membuat peran layanan yang dinamai `IncidentManagerIncidentAccessServiceRole` atas nama Anda. Peran layanan ini memberikan izin yang dibutuhkan Manajer Insiden untuk mengumpulkan informasi tentang CodeDeploy penerapan dan pembaruan CloudFormation tumpukan yang terjadi sekitar waktu insiden dibuat.

> **Note**
>
> Jika Anda menggunakan Manajer Insiden dengan organisasi, peran layanan dibuat di akun manajemen. Untuk bekerja dengan temuan di seluruh akun lain dalam organisasi, peran layanan harus dibuat di setiap akun aplikasi. Untuk informasi tentang menggunakan CloudFormation templat untuk membuat peran ini di akun aplikasi Anda, lihat langkah 4 diSiapkan dan konfigurasikan manajemen insiden lintas akun.

Peran layanan ini dikaitkan dengan kebijakan AWS terkelola. Untuk informasi tentang izin dalam kebijakan ini, lihatAWS kebijakan terkelola: AWSIncident ManagerIncidentAccessServiceRolePolicy.

Untuk informasi tentang mengaktifkan temuan selama proses orientasi Manajer Insiden, lihat. Memulai dengan Manajer Insiden

Untuk informasi tentang mengaktifkan temuan setelah Anda menyelesaikan proses orientasi, lihat. Mengelola fitur Temuan

Konfigurasikan izin untuk dukungan temuan lintas akun

Untuk menggunakan fitur Temuan di seluruh akun dengan organisasi yang disiapkan AWS RAM, setiap akun aplikasi harus mengonfigurasi izin bagi Manajer Insiden untuk mengambil peran layanan akun manajemen atas namanya.

Izin ini dapat dikonfigurasi dalam akun aplikasi dengan menerapkan AWS CloudFormation template yang disediakan oleh AWS, yang menciptakan peran. `IncidentManagerIncidentAccessServiceRole`

Untuk informasi tentang mengunduh dan menerapkan template ini di akun aplikasi, lihat langkah 4 diMengelola insiden di seluruh Akun AWS dan Wilayah di Manajer Insiden.

Membuat insiden secara otomatis atau manual di Manajer Insiden

Manajer Insiden, alat di AWS Systems Manager, membantu Anda mengelola dan merespons insiden dengan cepat. Anda dapat mengonfigurasi Amazon CloudWatch dan Amazon EventBridge untuk secara otomatis membuat insiden berdasarkan CloudWatch alarm dan EventBridge peristiwa. Anda juga dapat membuat insiden secara manual di halaman daftar insiden atau dengan menggunakan tindakan StartIncidentAPI dari AWS CLI atau AWS SDK. Manajer Insiden menghapus duplikasi insiden yang dibuat dari CloudWatch alarm atau EventBridge peristiwa yang sama ke dalam insiden yang sama.

Untuk insiden yang dibuat secara otomatis oleh CloudWatch alarm atau EventBridge peristiwa, Manajer Insiden mencoba membuat insiden yang Wilayah AWS sama dengan aturan acara atau alarm. Jika Manajer Insiden tidak tersedia di Wilayah AWS, CloudWatch atau EventBridge secara otomatis membuat insiden di salah satu Wilayah yang tersedia yang ditentukan dalam kumpulan replikasi Anda. Untuk informasi selengkapnya, lihat Mengelola insiden di seluruh Akun AWS dan Wilayah di Manajer Insiden.

Ketika sistem membuat insiden, Manajer Insiden secara otomatis mengumpulkan informasi tentang AWS sumber daya yang terlibat dalam insiden tersebut dan menambahkan informasi ini ke tab Item Terkait. Jika Anda menentukan runbook dalam rencana respons Anda, saat sistem membuat insiden, Manajer Insiden dapat mengirimkan informasi tentang AWS sumber daya yang terlibat dalam insiden tersebut ke runbook. Sistem kemudian dapat menargetkan sumber daya tersebut ketika memulai runbook dan mencoba untuk memperbaiki masalah.

Ketika sistem membuat insiden, itu juga menciptakan workitem operasional induk (OpsItem) di OpsCenter, komponen Systems Manager, dan menautkannya ke insiden sebagai item terkait. Anda dapat menggunakan ini OpsItem untuk melacak pekerjaan terkait dan analisis insiden masa depan. Panggilan untuk OpsCenter mengeluarkan biaya. Untuk informasi selengkapnya tentang OpsCenter harga, lihat harga Systems Manager.

> **Important**
>
> Perhatikan detail penting berikut.
>
> - Jika Manajer Insiden tidak tersedia, sistem hanya dapat gagal dan membuat insiden di tempat lain Wilayah AWS jika Anda telah menentukan setidaknya dua Wilayah dalam

kumpulan replikasi Anda. Untuk informasi tentang mengonfigurasi set replikasi, lihat. Memulai dengan Manajer Insiden

- Insiden yang dibuat oleh failover lintas wilayah tidak memanggil runbook yang ditentukan dalam paket respons.

Membuat insiden secara otomatis dengan alarm CloudWatch

CloudWatch menggunakan CloudWatch metrik Anda untuk mengingatkan Anda tentang perubahan di lingkungan Anda dan untuk secara otomatis melakukan tindakan insiden awal. CloudWatch Bekerja dengan Systems Manager dan Incident Manager untuk membuat insiden dari template rencana respons saat alarm masuk ke status alarm. Ini membutuhkan prasyarat berikut:

- Manajer Insiden dikonfigurasi dan set replikasi dibuat. Langkah ini membuat peran terkait layanan Manajer Insiden di akun Anda, memberikan izin yang diperlukan.
- Rencana respons Manajer Insiden yang dikonfigurasi. Untuk mempelajari cara mengonfigurasi rencana respons Manajer Insiden, lihat Membuat dan mengonfigurasi rencana respons di Manajer Insiden di bagian Persiapan insiden di panduan ini.
- CloudWatch Metrik yang dikonfigurasi memantau aplikasi Anda. Untuk memantau praktik terbaik, lihat Pemantauan di bagian Persiapan insiden dari panduan ini.

Untuk membuat alarm dengan aksi insiden Mulai

1. Buat alarm di CloudWatch. Untuk informasi selengkapnya, lihat Menggunakan CloudWatch alarm Amazon di Panduan CloudWatch Pengguna Amazon.
2. Saat memilih tindakan untuk menjalankan alarm, pilih tindakan Add Systems Manager.
3. Pilih Buat insiden dan pilih paket Respons untuk insiden ini.
4. Selesaikan langkah-langkah yang tersisa di panduan jenis alarm yang Anda pilih.

> **Tip**
>
> Anda juga dapat menambahkan tindakan buat insiden ke alarm yang ada.

Membuat insiden secara otomatis dengan acara EventBridge

EventBridge aturan memperhatikan pola acara. Jika acara cocok dengan pola yang ditentukan, Manajer Insiden membuat insiden menggunakan rencana respons yang dipilih.

Membuat insiden menggunakan acara mitra SaaS

Anda dapat mengonfigurasi EventBridge untuk menerima acara dari aplikasi dan layanan mitra perangkat lunak sebagai layanan (SaaS), yang memungkinkan integrasi pihak ketiga. Setelah mengonfigurasi EventBridge untuk menerima acara dari mitra pihak ketiga, Anda dapat membuat aturan yang cocok dengan acara mitra untuk membuat insiden. Untuk melihat daftar integrasi pihak ketiga, lihat Menerima acara dari mitra SaaS.

Konfigurasikan EventBridge untuk menerima acara dari integrasi SaaS.

1. Buka EventBridge konsol Amazon di https://console.aws.amazon.com/events/.
2. Di panel navigasi, pilih Sumber peristiwa mitra.
3. Gunakan bilah pencarian untuk menemukan mitra yang Anda inginkan dan pilih Siapkan untuk mitra itu.
4. Pilih Salin untuk menyalin ID akun Anda ke clipboard.

> **Note**
>
> Untuk mengintegrasikan dengan Salesforce, gunakan langkah-langkah yang dijelaskan dalam panduan AppFlow pengguna Amazon.

5. Kunjungi situs web mitra dan ikuti petunjuk untuk membuat sumber acara mitra. Gunakan ID akun Anda untuk ini. Sumber acara yang Anda buat hanya tersedia di akun Anda.
6. Kembali ke EventBridge konsol dan pilih Sumber acara Partner di panel navigasi.
7. Pilih tombol di sebelah sumber acara mitra, dan pilih Kaitkan dengan bus acara.

Buat aturan yang memicu peristiwa dari mitra SaaS

1. Buka EventBridge konsol Amazon di https://console.aws.amazon.com/events/.
2. Di panel navigasi, pilih Aturan.
3. Pilih Buat aturan.

4. Masukkan nama dan deskripsi untuk aturan.

   Aturan tidak boleh memiliki nama yang sama dengan aturan lain di Wilayah yang sama dan di bus kejadian yang sama.
5. Untuk bus acara, pilih bus acara yang sesuai dengan mitra ini.
6. Untuk Tipe aturan, pilih Aturan dengan pola peristiwa.
7. Pilih Selanjutnya.
8. Untuk sumber Acara, pilih AWS acara atau acara EventBridge mitra.
9. Untuk pola Acara, pilih Formulir pola acara.
10. Untuk sumber Acara, pilih EventBridgemitra
11. Untuk Mitra, pilih nama mitra.
12. Untuk Tipe kejadian, pilih Semua kejadian atau pilih tipe kejadian yang akan digunakan untuk aturan ini. Jika Anda memilih Semua Acara, semua acara yang dipancarkan oleh sumber acara mitra ini akan cocok dengan aturan.

    Jika Anda ingin menyesuaikan pola acara, pilih Edit, buat perubahan, lalu pilih Simpan.
13. Pilih Berikutnya.
14. Untuk Pilih target, pilih Rencana respons Manajer Insiden, lalu pilih paket Respons.

    > **Note**
    >
    > Saat memilih paket respons, semua paket respons yang Anda miliki dan telah dibagikan dengan akun Anda akan muncul di daftar tarik-turun Paket respons.
15. EventBridge dapat membuat peran IAM yang diperlukan agar aturan Anda berjalan:
    - Untuk membuat peran IAM secara otomatis, pilih Buat peran baru untuk sumber daya khusus ini.
    - Untuk menggunakan peran IAM yang Anda buat sebelumnya, pilih Gunakan peran yang sudah ada.
16. Pilih Berikutnya.
17. (Opsional) Masukkan satu atau lebih tanda untuk aturan. Untuk informasi selengkapnya, lihat EventBridgetag Amazon di Panduan EventBridge Pengguna Amazon.
18. Pilih Berikutnya.
19. Tinjau aturan Anda lalu pilih Buat aturan.

Membuat insiden menggunakan acara AWS layanan

EventBridge juga menerima acara dari AWS layanan yang tercantum dalam Acara dari AWS Layanan yang Didukung. Mirip dengan cara Anda mengonfigurasi aturan untuk mitra SaaS, Anda dapat mengonfigurasinya untuk AWS layanan.

Buat aturan yang memicu peristiwa dari layanan AWS

1. Buka EventBridge konsol Amazon di https://console.aws.amazon.com/events/.
2. Di panel navigasi, pilih Aturan.
3. Pilih Buat aturan.
4. Masukkan nama dan deskripsi untuk aturan.

   Aturan tidak boleh memiliki nama yang sama dengan aturan lain di Wilayah yang sama dan di bus peristiwa yang sama.
5. Untuk Bus peristiwa, pilih default.
6. Untuk Tipe aturan, pilih Aturan dengan pola peristiwa.
7. Pilih Selanjutnya.
8. Untuk sumber Acara, pilih AWS acara atau acara EventBridge mitra.
9. Untuk pola Acara, pilih Formulir pola acara.
10. Untuk Sumber peristiwa, pilih Layanan AWS .
11. Untuk nama Layanan, pilih layanan yang memantau insiden.
12. Untuk Tipe kejadian, pilih Semua kejadian atau pilih tipe kejadian yang akan digunakan untuk aturan ini. Jika Anda memilih Semua Acara, semua acara yang dipancarkan oleh sumber acara mitra ini akan cocok dengan aturan.

    Jika Anda ingin menyesuaikan pola acara, pilih Edit, buat perubahan, lalu pilih Simpan.
13. Pilih Berikutnya.
14. Untuk Pilih target, pilih Rencana respons Manajer Insiden, lalu pilih paket Respons.

    > **Note**
    >
    > Saat memilih paket respons, semua paket respons yang Anda miliki dan telah dibagikan dengan akun Anda akan muncul di daftar tarik-turun Paket respons.
15. EventBridge dapat membuat peran IAM yang diperlukan agar aturan Anda berjalan:

- Untuk membuat peran IAM secara otomatis, pilih Buat peran baru untuk sumber daya khusus ini.
- Untuk menggunakan peran IAM yang Anda buat sebelumnya, pilih Gunakan peran yang sudah ada.

16. Pilih Berikutnya.
17. (Opsional) Masukkan satu atau lebih tanda untuk aturan. Untuk informasi selengkapnya, lihat EventBridgetag Amazon di Panduan EventBridge Pengguna Amazon.
18. Pilih Berikutnya.
19. Tinjau aturan Anda lalu pilih Buat aturan.

Membuat insiden secara manual

Responden dapat melacak insiden secara manual menggunakan konsol Manajer Insiden dengan menggunakan rencana respons yang telah ditentukan sebelumnya. Gunakan langkah-langkah berikut untuk membuat insiden.

1. Buka konsol Manajer Insiden.
2. Pilih Mulai insiden.
3. Untuk paket Respons, pilih paket respons dari daftar.
4. (Opsional) Untuk mengganti judul yang disediakan oleh rencana respons yang ditentukan, masukkan judul Insiden.
5. (Opsional) Untuk mengesampingkan dampak yang diberikan oleh rencana respons yang ditentukan, masukkan Dampak insiden.

Izin IAM yang diperlukan untuk memulai insiden secara manual

Untuk memulai insiden secara manual, pengguna memerlukan izin untuk mengakses konsol Manajer Insiden, melihat paket respons, dan memulai insiden. Ketika pengguna memulai insiden, Manajer Insiden menggunakan sesi akses maju (FAS) untuk melakukan `StartEngagement` panggilan sebagai bagian dari. `StartIncident`

Kebijakan IAM berikut memberikan izin yang diperlukan untuk memulai insiden secara manual, melihat rencana respons yang dapat dibuat dengan insiden, dan melihat dan mengedit insiden setelah dibuat.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ssm-incidents:StartIncident",
                "ssm-incidents:GetResponsePlan",
                "ssm-incidents:ListResponsePlans",
                "ssm-incidents:TagResource",
                "ssm-incidents:GetIncidentRecord",
                "ssm-incidents:ListIncidentRecords",
                "ssm-incidents:UpdateIncidentRecord"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm-contacts:StartEngagement"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:CalledViaFirst": "ssm-incidents.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm:CreateOpsItem"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:CalledViaFirst": "ssm-incidents.amazonaws.com"
                }
            }
        }
    ]
}
```

Kebijakan ini mencakup izin berikut:

- ssm-incidents: StartIncident - Memungkinkan pengguna untuk memulai insiden secara manual menggunakan konsol atau API. Ini menciptakan catatan insiden baru dari rencana respons.
- ssm-incidents: GetResponsePlan - Memungkinkan pengguna untuk mengambil informasi tentang rencana respons tertentu.
- ssm-incidents: ListResponsePlans - Memungkinkan pengguna untuk membuat daftar semua paket respons di akun mereka.
- ssm-incidents: TagResource - Memungkinkan menambahkan tag ke sumber daya Manajer Insiden, termasuk insiden dan rencana respons.
- ssm-incidents: GetIncidentRecord - Memungkinkan pengguna untuk mengambil informasi rinci tentang insiden tertentu.
- ssm-incidents: ListIncidentRecords - Memungkinkan pengguna untuk membuat daftar semua insiden di akun mereka.
- ssm-incidents: UpdateIncidentRecord - Memungkinkan pengguna untuk memperbarui rincian insiden yang ada.
- ssm-contacts: StartEngagement (dengan kondisi) - Memungkinkan Manajer Insiden untuk memulai keterlibatan dengan kontak. Kondisi ini memastikan ini hanya dapat dipanggil melalui Manajer Insiden.
- ssm: CreateOpsItem (dengan kondisi) - Memungkinkan Manajer Insiden membuat OpsItem in OpsCenter. Kondisi ini memastikan ini hanya dapat dipanggil melalui Manajer Insiden.

Kunci CalledViaFirst kondisi aws: memastikan bahwa izin tertentu (sepertiStartEngagement) hanya dapat digunakan ketika permintaan datang melalui layanan Manajer Insiden. Pendekatan ini menggunakan FAS alih-alih peran terkait layanan, yang mencegah potensi panggilan lintas akun yang dapat menimbulkan risiko keamanan.

Melihat detail insiden di konsol Manajer Insiden

AWS Systems Manager Incident Manager melacak insiden Anda dari saat terdeteksi hingga resolusi dan melalui analisis pasca-insiden. Anda dapat menemukan semua insiden di halaman daftar Insiden di konsol Manajer Insiden, dengan tautan langsung ke detail Insiden.

Topik

- Melihat daftar insiden di konsol
- Melihat detail insiden di konsol

Melihat daftar insiden di konsol

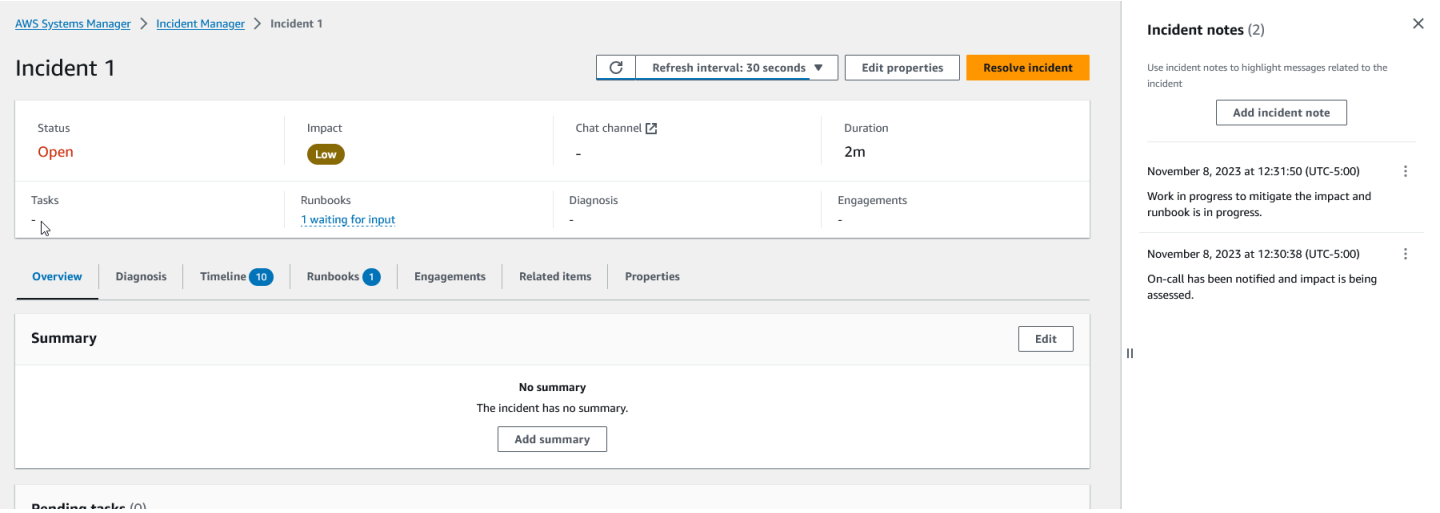
Halaman daftar Insiden berisi tiga bagian: Insiden terbuka, Insiden Terselesaikan, dan Analisis. Anda dapat melacak insiden baru secara manual dan membuat analisis dari halaman ini. Untuk mempelajari selengkapnya tentang melacak insiden secara manual, lihat Membuat insiden secara manual di bagian Pembuatan insiden di panduan ini. Untuk mempelajari tentang analisis pasca-insiden, lihat Menjalankan analisis pasca-insiden di Incident Manager bagian panduan ini.

Detail Insiden menampilkan insiden Terbuka di ubin dengan judul, dampak, durasi, dan saluran obrolan untuk insiden tersebut. Setelah Anda menyelesaikan suatu insiden, itu pindah ke daftar Insiden Terselesaikan. Analisis ada di tab kedua.

Melihat detail insiden di konsol

Halaman detail Insiden memberikan wawasan dan alat terperinci yang dapat Anda gunakan untuk mengelola insiden. Dari halaman ini, Anda dapat memulai runbook untuk mengurangi insiden, menambahkan catatan insiden, melibatkan penyelesai lain, dan melihat detail insiden seperti garis waktu, metrik, properti, dan sumber daya terkait.

Seperti yang ditunjukkan pada gambar berikut, halaman detail Insiden mencakup beberapa bagian: Spanduk teratas, Catatan insiden, dan tujuh tab yang berisi informasi dan sumber daya tambahan. Secara default, bagian Top banner dan catatan Insiden ditampilkan di semua halaman detail Insiden.



Topik ini menjelaskan elemen halaman Detail insiden dan tindakan yang dapat Anda lakukan dari halaman.

Spanduk teratas

Spanduk teratas di setiap halaman detail insiden mencakup informasi berikut:

- Status — Status saat ini dari suatu insiden dapat Terbuka atau Terselesaikan.
- Dampak — Dampak insiden terhadap lingkungan Anda. Itu bisa tinggi, sedang, dan rendah. Untuk mengubah dampak insiden, pilih Edit properti.
- Saluran obrolan — Tautan untuk mengakses saluran obrolan tempat Anda dapat melihat pembaruan dan pemberitahuan insiden.
- Durasi — Jumlah waktu yang berlalu sebelum responden menyelesaikan insiden tersebut.
- Runbook — Status untuk runbook yang terkait dengan insiden ini. Status dapat menunggu masukan, berhasil, atau tidak berhasil. Jika status runbook menunggu masukan, Anda dapat memilih runbook untuk melihat detail tindakan. Anda dapat memilih gagal untuk melihat runbook yang Timed out, Gagal, atau Dibatalkan.
- Keterlibatan — Jumlah total keterlibatan dan status setiap keterlibatan. Saat Anda membuat keterlibatan, statusnya Terlibat. Setelah Anda mengakui keterlibatan, status berubah dari Terlibat menjadi Diakui. Manajer Insiden tidak mendukung pengakuan keterlibatan pihak ketiga. Keterlibatan tersebut tetap dalam status Terlibat.

Anda dapat mengedit judul insiden, dampak, dan saluran obrolan dengan memilih Edit di sudut kanan atas spanduk.

Catatan insiden

Sisi kanan layar menampilkan bagian Catatan insiden. Dengan catatan, Anda dapat berkolaborasi dan berkomunikasi dengan pengguna lain yang mengerjakan suatu insiden. Anda dapat menjelaskan mitigasi yang Anda terapkan, akar penyebab potensial yang Anda identifikasi, atau status insiden saat ini. Sebagai praktik terbaik, gunakan bagian Catatan insiden untuk memposting pembaruan status dan tindakan yang Anda atau orang lain lakukan pada suatu insiden. Jika Anda perlu berkomunikasi dengan resolver lain secara real time, gunakan saluran obrolan yang tersedia di Manajer Insiden.

Untuk menambahkan catatan, pilih tombol Tambahkan catatan kejadian, lalu masukkan catatan Anda. Catatan dapat berisi pembaruan tentang status insiden atau informasi relevan lainnya yang memberikan visibilitas kepada pengguna lain. Jika diperlukan, Anda juga dapat mengedit atau menghapus catatan insiden.

> **Note**
>
> Setiap pengguna dengan izin IAM untuk menjalankan `ssm-incidents:UpdateTimelineEvent` dan `ssm-incidents:DeleteTimelineEvent` tindakan dapat mengedit dan menghapus catatan. Namun, saat Anda membagikan insiden dengan akun lain, kebijakan sumber daya tidak menyertakan `ssm-incidents:DeleteTimelineEvent` tindakan tersebut. Ini mencegah pengguna yang berbagi insiden dengan Anda menghapus catatan. Anda dapat melihat jejak audit untuk catatan dari peristiwa Manajer Insiden di AWS CloudTrail konsol.

Tab

Halaman detail insiden memiliki tujuh tab, sehingga memudahkan responden untuk menemukan dan melihat informasi selama insiden. Tab menampilkan penghitung di nama tab, yang menunjukkan jumlah pembaruan pada tab. Untuk informasi lebih lanjut tentang isi setiap tab serta tindakan yang tersedia, lanjutkan membaca.

Gambaran Umum

Tab Ikhtisar adalah halaman arahan untuk responden. Ini berisi ringkasan insiden, daftar peristiwa timeline terbaru, dan langkah runbook saat ini.

Responden menggunakan Ringkasan untuk menangkap tindakan apa yang telah diambil, hasil dari setiap perubahan, kemungkinan langkah selanjutnya, dan informasi tentang dampak insiden tersebut. Untuk memperbarui ringkasan, pilih Edit di sudut kanan atas bagian Ringkasan.

> **Important**
>
> Jika beberapa responden mengedit bidang ringkasan secara bersamaan, responden yang mengirimkan hasil editannya terakhir akan menimpa semua input lainnya.

Bagian peristiwa timeline terbaru berisi garis waktu yang diisi oleh Manajer Insiden dengan lima peristiwa terbaru. Gunakan bagian ini untuk memahami status kejadian dan apa yang baru saja terjadi. Untuk melihat timeline lengkap, lanjutkan ke tab Timeline.

Halaman ikhtisar juga menampilkan langkah runbook saat ini. Langkah ini mungkin merupakan langkah otomatis yang berjalan di AWS lingkungan Anda, atau mungkin serangkaian instruksi manual untuk responden. Untuk melihat runbook lengkap, termasuk langkah sebelumnya dan yang akan datang, pilih tab Runbook.

Diagnosis

Tab Diagnosis berisi informasi penting tentang aplikasi dan sistem yang Anda AWS hosting, termasuk informasi tentang metrik dan, jika diaktifkan, temuan.

Bekerja dengan metrik

Manajer Insiden menggunakan Amazon CloudWatch untuk mengisi metrik dan grafik alarm yang ditemukan di tab ini. Untuk mempelajari lebih lanjut tentang praktik terbaik manajemen insiden untuk mendefinisikan alarm dan metrik, lihat Pemantauan di bagian Perencanaan insiden di panduan pengguna ini.

Untuk menambahkan metrik

- Pilih Tambahkan di sudut kanan atas tab ini.
  - Untuk menambahkan metrik dari CloudWatch dasbor yang ada, pilih Dari CloudWatch dasbor yang ada.
    a. Pilih Dasbor. Ini menambahkan semua metrik dan alarm yang merupakan bagian dari dasbor yang dipilih.

b. (Opsional) Anda juga dapat Memilih metrik dari dasbor untuk melihat metrik tertentu.

- Tambahkan satu metrik dengan memilih Dari CloudWatch dan menempelkan sumber metrik. Untuk menyalin sumber metrik:

  a. Buka CloudWatch konsol di https://console.aws.amazon.com/cloudwatch/.

  b. Di panel navigasi, pilih Metrik.

  c. Pada tab Semua metrik, masukkan istilah pencarian di bidang pencarian, seperti nama metrik atau nama sumber daya, dan pilih Enter.

     Misalnya, jika Anda mencari `CPUUtilization` metrik, Anda akan melihat ruang nama dan dimensi yang terkait dengan metrik ini.

  d. Pilih salah satu hasil dari penelusuran Anda untuk melihat metrik.

  e. Pilih tab Sumber dan salin sumbernya.

Grafik alarm metrik hanya dapat ditambahkan ke detail insiden melalui rencana respons terkait, atau dengan memilih Dari CloudWatch dasbor yang ada saat menambahkan metrik.

Untuk menghapus metrik, pilih Hapus, lalu pilih metrik yang ingin Anda hapus dari dropdown Metrik yang disediakan.

Melihat temuan dari AWS CodeDeploy dan AWS CloudFormation

Setelah Temuan diaktifkan dan semua izin yang diperlukan dikonfigurasi, temuan apa pun yang mungkin terkait dengan insiden tertentu dilampirkan pada insiden tersebut. Responden dapat melihat informasi tentang temuan ini di halaman Detail insiden.

Untuk melihat temuan dari CodeDeploy dan CloudFormation

1. Buka konsol Manajer Insiden.
2. Pilih nama insiden untuk diselidiki.
3. Pada tab Diagnosis, di area Temuan, bandingkan waktu mulai dari setiap temuan yang dilaporkan dengan waktu mulai kejadian.
4. Untuk melihat detail lebih lanjut tentang temuan, di kolom Referensi, pilih tautan ke CodeDeploy atau CloudFormation temuan.

Garis Waktu

Gunakan tab Timeline untuk melacak peristiwa yang terjadi selama insiden. Manajer Insiden secara otomatis mengisi peristiwa timeline yang mengidentifikasi kejadian signifikan selama insiden tersebut. Responden dapat menambahkan peristiwa khusus berdasarkan kejadian yang terdeteksi secara manual. Selama analisis pasca-insiden, tab timeline memberikan wawasan berharga tentang bagaimana mempersiapkan dan menanggapi insiden dengan lebih baik di masa depan. Untuk informasi lebih lanjut tentang analisis pasca-insiden, lihatMenjalankan analisis pasca-insiden di Incident Manager.

Untuk menambahkan acara timeline kustom, pilih Tambah. Pilih tanggal menggunakan kalender, lalu masukkan waktu. Semua waktu ditampilkan di zona waktu lokal Anda. Berikan deskripsi singkat tentang peristiwa yang muncul di timeline.

Untuk mengedit acara kustom yang ada, pilih acara di timeline dan pilih Edit. Anda dapat mengubah waktu, tanggal, dan deskripsi acara khusus. Anda hanya dapat mengedit acara khusus.

Runbook

Tab Runbooks pada halaman detail insiden adalah tempat responden dapat melihat langkah-langkah runbook dan memulai runbook baru.

Untuk memulai runbook baru, pilih Mulai runbook di bagian Runbooks. Gunakan kolom pencarian untuk menemukan runbook yang ingin Anda mulai. Berikan Parameter yang diperlukan dan Versi runbook yang ingin Anda gunakan saat memulai runbook. Runbook yang dimulai selama insiden dari tab Runbooks menggunakan izin akun yang saat ini masuk.

Untuk menavigasi ke definisi runbook di Systems Manager, pilih judul runbook di bawah Runbooks. Untuk menavigasi ke instance runbook yang sedang berjalan di Systems Manager, pilih detail eksekusi di bawah Rincian eksekusi. Halaman-halaman ini menampilkan template yang digunakan untuk memulai runbook dan detail spesifik dari contoh dokumen otomatisasi yang sedang berjalan.

Bagian langkah Runbook menampilkan daftar langkah yang secara otomatis diambil oleh runbook yang dipilih atau dilakukan responden secara manual. Langkah-langkah berkembang saat mereka menjadi langkah saat ini, menampilkan informasi yang diperlukan untuk menyelesaikan langkah, atau rincian tentang apa yang dilakukan langkah tersebut. Langkah-langkah runbook otomatis diselesaikan setelah otomatisasi selesai. Langkah-langkah manual mengharuskan responden untuk memilih Langkah berikutnya di bagian bawah setiap langkah. Setelah langkah selesai, output langkah muncul sebagai dropdown.

Untuk membatalkan eksekusi runbook, pilih Batalkan runbook. Ini akan menghentikan eksekusi runbook dan tidak menyelesaikan langkah lebih lanjut di runbook.

Keterlibatan

Tab Keterlibatan pada detail insiden mendorong keterlibatan responden dan tim. Dari tab ini, Anda dapat melihat siapa yang telah terlibat, siapa yang telah merespons, serta responden mana yang akan terlibat sebagai bagian dari rencana eskalasi. Responden dapat melibatkan kontak lain langsung dari tab ini. Untuk mempelajari lebih lanjut tentang membuat rencana kontak dan eskalasi, lihat bagian Membuat dan mengonfigurasi kontak di Manajer Insiden dan Membuat rencana eskalasi untuk keterlibatan responden di Manajer Insiden bagian dari panduan ini.

Anda dapat mengonfigurasi rencana respons dengan kontak dan rencana eskalasi untuk memulai keterlibatan secara otomatis di awal insiden. Untuk mempelajari lebih lanjut tentang mengonfigurasi rencana respons, lihat Membuat dan mengonfigurasi rencana respons di Manajer Insiden bagian panduan ini.

Anda dapat menemukan informasi tentang setiap kontak di tabel. Tabel ini mencakup informasi berikut:

- Nama - Tautan ke halaman detail kontak yang menampilkan metode kontak dan rencana keterlibatan mereka.
- Rencana eskalasi — Tautan ke rencana eskalasi yang melibatkan kontak.
- Sumber kontak - Mengidentifikasi layanan yang melibatkan kontak ini, seperti AWS Systems Manager atau PagerDuty.
- Terlibat — Menampilkan kapan rencana melibatkan kontak, atau kapan harus melibatkan kontak sebagai bagian dari rencana eskalasi.
- Diakui - Menampilkan apakah kontak mengakui keterlibatan.

Untuk mengakui keterlibatan, responden dapat melakukan salah satu hal berikut:

- Panggilan telepon — Masuk **1** saat diminta.
- SMS — Membalas pesan dengan kode yang disediakan, atau masukkan kode yang disediakan pada tab Keterlibatan insiden.
- Email — Masukkan kode yang disediakan di tab Keterlibatan insiden.

Item terkait

Tab Item terkait digunakan untuk mengumpulkan sumber daya yang terkait dengan mitigasi insiden. Sumber daya ini dapat berupa ARNs, tautan ke sumber daya eksternal, atau file yang diunggah ke bucket Amazon S3. Tabel menampilkan judul deskriptif dan baik ARN, link, atau rincian bucket. Sebelum menggunakan bucket S3, tinjau Praktik Terbaik Keamanan untuk Amazon S3 di Panduan Pengguna Amazon S3.

Saat mengunggah file ke bucket Amazon S3, pembuatan versi diaktifkan atau ditangguhkan pada bucket tersebut. Saat pembuatan versi diaktifkan di bucket, file yang diunggah dengan nama yang sama dengan file yang ada ditambahkan sebagai versi baru dari file tersebut. Jika pembuatan versi ditangguhkan, file yang diunggah dengan nama yang sama dengan file yang ada menimpa file yang ada. Untuk mempelajari lebih lanjut tentang pembuatan versi, lihat Menggunakan pembuatan versi di bucket S3 di Panduan Pengguna Amazon S3.

Saat menghapus item terkait file, file akan dihapus dari insiden tetapi tidak dihapus dari bucket Amazon S3. Untuk mempelajari lebih lanjut tentang menghapus objek dari bucket Amazon S3, lihat Menghapus objek Amazon S3 di Panduan Pengguna Amazon S3.

Properti

Tab Properties memberikan rincian berikut tentang insiden tersebut.

Di bagian Properti insiden, Anda dapat melihat yang berikut:

- Status — Menjelaskan status insiden saat ini. Insiden tersebut dapat dibuka atau diselesaikan.
- Waktu mulai — Waktu ketika insiden dibuat di Manajer Insiden.
- Waktu yang diselesaikan — Waktu insiden diselesaikan di Manajer Insiden.
- Nama Sumber Daya Amazon (ARN) — ARN dari insiden tersebut. Gunakan ARN saat mereferensikan insiden dari obrolan atau perintah dengan AWS Command Line Interface ()AWS CLI.
- Rencana Respons - Mengidentifikasi rencana respons untuk insiden yang dipilih. Memilih rencana respons akan membuka halaman detail rencana respons.
- Induk OpsItem — Mengidentifikasi yang OpsItem dibuat sebagai induk dari insiden tersebut. Orang tua OpsItem dapat memiliki beberapa insiden terkait dan item tindakan tindak lanjut. Memilih induk OpsItem membuka halaman OpsItems detail di OpsCenter.

- Analisis — Mengidentifikasi analisis yang dibuat dari insiden ini. Buat analisis dari insiden yang diselesaikan untuk meningkatkan proses respons insiden Anda. Pilih analisis untuk membuka halaman detail analisis.
- Pemilik — Akun tempat insiden itu dibuat.

Di bagian Tag, Anda dapat melihat dan mengedit kunci tag dan nilai yang terkait dengan catatan insiden. Untuk informasi selengkapnya tentang tag di Manajer Insiden, lihatMenandai sumber daya di Manajer Insiden.

Menjalankan analisis pasca-insiden di Incident Manager

Analisis pasca-insiden memandu Anda untuk mengidentifikasi peningkatan respons insiden Anda, termasuk waktu untuk mendeteksi dan mitigasi. Analisis juga dapat membantu Anda memahami akar penyebab insiden tersebut. Manajer Insiden membuat item tindakan yang direkomendasikan untuk meningkatkan respons insiden Anda.

Manfaat analisis pasca-insiden

- Tingkatkan respons insiden
- Memahami akar penyebab masalah
- Atasi akar penyebab dengan item tindakan yang dapat dikirimkan
- Menganalisis dampak insiden
- Menangkap dan berbagi pembelajaran dalam suatu organisasi

Apa yang tidak menggunakan analisis untuk

Analisis tidak bersalah dan tidak memanggil orang dengan nama.

“Terlepas dari apa yang kami temukan, kami memahami dan benar-benar percaya bahwa setiap orang melakukan pekerjaan terbaik yang mereka bisa, mengingat apa yang mereka ketahui pada saat itu, keterampilan dan kemampuan mereka, sumber daya yang tersedia, dan situasi yang dihadapi.” - Norm Kerth, Retrospektif Proyek: Buku Pegangan untuk Tinjauan Tim

Rincian analisis

Halaman detail analisis memandu Anda melalui pengumpulan informasi, menilai peningkatan, dan membuat item tindakan. Halaman detail analisis mirip dengan detail insiden dengan beberapa perbedaan utama seperti metrik historis, garis waktu yang dapat diedit, dan pertanyaan untuk meningkatkan insiden masa depan.

Gambaran Umum

Gambaran umum adalah ringkasan dari insiden tersebut. Ringkasan ini mencakup latar belakang, apa yang terjadi, mengapa itu terjadi, bagaimana hal itu dikurangi, durasi, dan item tindakan utama untuk mencegah insiden terjadi lagi. Ikhtisar adalah tingkat tinggi. Anda akan menjelajahi detail lebih lanjut di tab Pertanyaan analisis.

Metrik

Gunakan tab metrik untuk memvisualisasikan metrik utama dalam aplikasi Anda selama durasi kejadian. Anda dapat menambahkan grafik metrik di sini yang memiliki satu atau lebih metrik yang digambarkan dalam grafik yang sama. Metrik yang digunakan selama insiden secara otomatis diisi di tab ini. Kami menyarankan Anda menambahkan deskripsi, judul, dan anotasi titik waktu utama selama kejadian.

Beberapa poin waktu penting yang dapat Anda pertimbangkan saat menganalisis grafik metrik:

- Perubahan penerapan
- Perubahan konfigurasi
- Waktu mulai insiden
- Waktu alarm
- Waktu pertunangan
- Waktu mulai mitigasi
- Insiden diselesaikan waktu

Batasan

- CloudWatch alarm dan ekspresi metrik tidak diimpor dari insiden.
- Metrik yang berada di Wilayah yang tidak didukung Manajer Insiden tidak diimpor dari insiden tersebut.
- Metrik dalam akun aplikasi memerlukan konfigurasi `CloudWatch-CrossAccountSharingRole` sebelum membuat analisis. Untuk informasi selengkapnya tentang peran tersebut, lihat CloudWatch Konsol Lintas Akun Lintas Wilayah di panduan CloudWatch pengguna.

Garis Waktu

Jelaskan titik-titik waktu penting pada garis waktu saat Anda menyelam lebih dalam untuk memahami insiden tersebut. Garis waktu insiden secara otomatis diisi di tab ini. Anda dapat menghapus titik waktu yang tidak relevan dengan analisis. Anda juga dapat menambahkan dan mengedit titik waktu untuk menggambarkan insiden dan dampaknya dengan lebih akurat.

Gunakan tab timeline untuk menjawab pertanyaan yang Anda temukan di tab Pertanyaan tentang respons insiden.

Pertanyaan

Gunakan pertanyaan Manajer Insiden untuk meningkatkan waktu penyelesaian insiden dalam aplikasi Anda dan mengurangi terjadinya insiden. Saat Anda menjawab pertanyaan, perbarui tab Metrik dan Garis Waktu untuk akurasi. Pertanyaan-pertanyaan berfokus pada aspek-aspek kunci dari respons insiden ini:

- Deteksi — Bisakah Anda meningkatkan waktu untuk mendeteksi? Apakah ada pembaruan metrik dan alarm yang dapat mendeteksi insiden lebih dini?
- Diagnosis — Dapatkah Anda meningkatkan waktu untuk diagnosis? Apakah ada pembaruan pada rencana respons atau rencana eskalasi Anda yang melibatkan perespons yang tepat lebih dini?
- Mitigasi — Bisakah Anda meningkatkan waktu untuk mitigasi? Apakah ada langkah-langkah runbook yang dapat Anda tambahkan atau tingkatkan?
- Pencegahan — Dapatkah Anda mencegah terjadinya insiden di masa depan? Untuk menemukan akar penyebab insiden, Amazon menggunakan pendekatan 5-Mengapa dalam penyelidikan masalah.

Tindakan

Manajer Insiden membuat item tindakan yang direkomendasikan untuk Anda tinjau saat Anda menyelesaikan pertanyaan. Anda dapat memilih untuk menerima dan menyelesaikan tindakan ini dari tab ini atau Anda dapat mengabaikan tindakan ini. Anda dapat meninjau item tindakan yang diberhentikan dengan memilih item tindakan yang diberhentikan. Item tindakan adalah jenis OpsItem yang terkait dengan analisis dan insiden di OpsCenter.

Daftar periksa

Sebelum menutup analisis, gunakan daftar periksa untuk meninjau tindakan yang harus diambil responden. Saat responden menyelesaikan tindakan dalam daftar periksa, ikon di sebelah tindakan berubah dari elips menjadi tanda centang, yang menunjukkan bahwa tindakan telah selesai. Jika Anda belum menyelesaikan item daftar periksa, Manajer Insiden akan menampilkan pesan untuk mengonfirmasi bahwa responden ingin menutup analisis tanpa menyelesaikannya.

Template analisis

Template analisis menyediakan serangkaian pertanyaan yang menyelam jauh ke dalam akar penyebab insiden. Anda dapat menggunakan jawaban Anda untuk pertanyaan-pertanyaan ini untuk meningkatkan kinerja aplikasi dan respons insiden.

AWS Template standar

Manajer Insiden menyediakan templat pertanyaan standar berdasarkan respons AWS insiden dan praktik terbaik analisis masalah, berjudul`AWSIncidents-PostIncidentAnalysisTemplate`.

Buat template analisis

Kami mendorong Anda untuk menggunakan `AWSIncidents-PostIncidentAnalysisTemplate` templat default dan menambahkan pertanyaan atau bagian tambahan yang sesuai untuk kasus penggunaan Anda. Buat templat analisis berdasarkan templat default Gunakan templat ini sebagai titik awal untuk membuat templat analisis di akun manajemen Anda. Anda kemudian dapat menduplikasi templat analisis Anda ke setiap Wilayah tempat Anda mengaktifkan Manajer Insiden.

Buat template analisis

1. Panggil `GetDocument` tindakan dan gunakan `Name` parameternya untuk mengunduh`AWSIncidents-PostIncidentAnalysisTemplate`. Untuk informasi selengkapnya tentang `GetDocument` sintaks, lihat Referensi API Systems Manager.
2. Konten dalam respons berisi blok bangunan JSON untuk analisis. Gunakan blok bangunan pertanyaan untuk memasukkan pertanyaan tambahan dalam analisis. Kami menyarankan Anda menambahkan pertanyaan atau bagian di `Incident questions` bagian ini.
3. Untuk membuat template baru, gunakan `CreateDocument` operasi dengan JSON yang diperbarui dari langkah sebelumnya. Anda harus menyertakan yang berikut *`Analysis_Template_Name`* ini, di mana nama template Anda,

   - `DocumentFormat: "JSON"`
   - `DocumentType: "ProblemAnalysisTemplate"`
   - `Name: "`*`Analysis_Template_Name`*`"`

Buat analisis

1. Untuk membuat analisis, pilih Buat analisis dari halaman detail insiden insiden dari insiden tertutup.
2. Pilih templat analisis untuk membuat analisis ini, dan masukkan nama deskriptif analisis.
3. Pilih Buat.

Cetak analisis insiden yang diformat

Anda dapat menghasilkan salinan analisis lengkap atau tidak lengkap yang diformat untuk dicetak. Anda juga dapat menyimpan salinan ini sebagai PDF. Anda dapat mencetak satu analisis pada satu waktu. Pencetakan batch dari beberapa analisis saat ini tidak didukung.

Untuk mencetak analisis yang diformat

1. Buka konsol Manajer Insiden.
2. Pilih tab Analisis.
3. Pilih judul analisis yang ingin Anda cetak.
4. Di sudut kanan atas halaman detail analisis, pilih Cetak.
5. Dalam kotak dialog Analisis insiden cetak, kosongkan bagian analisis yang tidak ingin Anda sertakan dalam versi cetak. Secara default, semua bagian dipilih.
6. Pilih Cetak untuk membuka kontrol cetak lokal untuk perangkat Anda.
7. Pilih tujuan atau format pencetakan Anda. Anda dapat memilih printer lokal atau jaringan, atau Anda dapat menyimpan analisis ke PDF. Buat perubahan apa pun, jika diinginkan, pada opsi pencetakan yang tersisa, lalu pilih Cetak.

> **Note**
>
> Kontrol cetak lokal mengacu pada antarmuka pengguna yang disediakan oleh browser web dan perangkat Anda.
> Tujuan pencetakan adalah tujuan yang dikonfigurasi untuk, dan dapat diakses dari, perangkat Anda.

Tutorial Manajer Insiden

Tutorial AWS Systems Manager Incident Manager ini membantu Anda membangun sistem manajemen insiden yang lebih kuat. Tutorial ini mencakup kegiatan umum yang terjadi selama insiden atau mendukung respons insiden.

Topik

- Tutorial: Menggunakan runbook Automation Systems Manager dengan Incident Manager
- Tutorial: Mengelola insiden keamanan di Manajer Insiden

Tutorial: Menggunakan runbook Automation Systems Manager dengan Incident Manager

Anda dapat menggunakan runbook AWS Systems Manager Otomasi untuk menyederhanakan tugas pemeliharaan, penerapan, dan remediasi umum untuk layanan. AWS Dalam tutorial ini, Anda akan membuat runbook khusus untuk mengotomatiskan respons insiden di Manajer Insiden. Skenario untuk tutorial ini melibatkan CloudWatch alarm Amazon yang ditetapkan untuk EC2 metrik Amazon. Ketika instance memasuki status yang memicu alarm, Manajer Insiden secara otomatis melakukan tugas-tugas berikut:

1. Membuat insiden di Manajer Insiden.
2. Memulai runbook yang mencoba untuk memulihkan masalah.
3. Menerbitkan hasil buku runbook ke halaman detail insiden di Manajer Insiden.

Proses yang dijelaskan dalam tutorial ini juga dapat digunakan dengan EventBridge acara Amazon dan jenis AWS sumber daya lainnya. Dengan mengotomatiskan respons remediasi Anda terhadap alarm dan peristiwa, Anda dapat mengurangi dampak insiden pada organisasi Anda dan sumber dayanya.

Tutorial ini menjelaskan cara mengedit CloudWatch alarm yang ditetapkan ke EC2 instans Amazon untuk rencana respons Manajer Insiden. Jika Anda tidak memiliki alarm, instans, atau paket respons yang dikonfigurasi, kami sarankan Anda mengonfigurasi sumber daya tersebut sebelum memulai. Untuk informasi selengkapnya, lihat topik berikut.

- Menggunakan CloudWatch alarm Amazon di CloudWatch Panduan Pengguna Amazon

- EC2 Instans Amazon di EC2 Panduan Pengguna Amazon
- EC2Instans Amazon di EC2 Panduan Pengguna Amazon
- Membuat dan mengonfigurasi rencana respons di Manajer Insiden

> **Important**
>
> Anda akan dikenakan biaya dengan membuat AWS sumber daya dan menggunakan langkah-langkah otomatisasi runbook. Untuk informasi selengkapnya, lihat harga AWS.

Topik

- Tugas 1: Membuat runbook
- Tugas 2: Membuat peran IAM
- Tugas 3: Menghubungkan runbook ke rencana respons Anda
- Tugas 4: Menetapkan CloudWatch alarm ke rencana respons Anda
- Tugas 5: Memverifikasi hasil

Tugas 1: Membuat runbook

Gunakan prosedur berikut untuk membuat runbook di konsol Systems Manager. Ketika dipanggil dari insiden Manajer Insiden, runbook memulai ulang EC2 instans Amazon dan memperbarui insiden dengan informasi tentang eksekusi runbook. Sebelum memulai, verifikasi bahwa Anda memiliki izin untuk membuat runbook. Untuk informasi selengkapnya, lihat Menyiapkan Otomatisasi di Panduan AWS Systems Manager Pengguna.

> **Important**
>
> Tinjau detail penting berikut tentang membuat runbook tutorial ini:
>
> - Runbook dimaksudkan untuk insiden yang dibuat dari sumber CloudWatch alarm. Jika Anda menggunakan runbook ini untuk jenis insiden lain, misalnya insiden yang dibuat secara manual, maka peristiwa timeline di langkah runbook pertama tidak akan ditemukan dan sistem mengembalikan kesalahan.
> - Runbook membutuhkan CloudWatch alarm termasuk dimensi yang disebut`InstanceId`. Alarm untuk metrik EC2 instans Amazon memiliki dimensi ini. Jika Anda menggunakan

runbook ini dengan metrik lain (atau dengan sumber insiden lain, seperti EventBridge), maka Anda harus mengubah `JsonDecode2` langkah untuk mencocokkan data yang diambil dalam skenario Anda.

- Runbook mencoba untuk memulihkan masalah yang memicu alarm dengan memulai ulang instance Amazon. EC2 Untuk kejadian nyata, Anda mungkin tidak ingin memulai ulang instance. Perbarui runbook dengan tindakan remediasi spesifik yang Anda ingin sistem ambil.

Untuk informasi selengkapnya tentang membuat runbook, lihat Bekerja dengan runbook di AWS Systems Manager Panduan Pengguna.

Untuk membuat runbook

1. Buka AWS Systems Manager konsol di https://console.aws.amazon.com/systems-manager/.
2. Di panel navigasi, pilih Dokumen.
3. Pilih Otomatisasi.
4. Untuk Nama, masukkan nama deskriptif untuk runbook, seperti. **`IncidentResponseRunbook`**
5. Pilih tab Editor, dan kemudian pilih Edit.
6. Tempelkan konten berikut ke editor:

```
description: This runbook attempts to restart an Amazon EC2 instance that caused an
 incident.
schemaVersion: '0.3'
parameters:
  IncidentRecordArn:
    type: String
    description: The incident
mainSteps:
  - name: ListTimelineEvents
    action: 'aws:executeAwsApi'
    outputs:
      - Selector: '$.eventSummaries[0].eventId'
        Name: eventId
        Type: String
    inputs:
      Service: ssm-incidents
      Api: ListTimelineEvents
      incidentRecordArn: '{{IncidentRecordArn}}'
```

```
      filters:
        - key: eventType
          condition:
            equals:
              stringValues:
                - SSM Incident Trigger
    description: This step retrieves the ID of the first timeline event with the
  CloudWatch alarm details.
  - name: GetTimelineEvent
    action: 'aws:executeAwsApi'
    inputs:
      Service: ssm-incidents
      Api: GetTimelineEvent
      incidentRecordArn: '{{IncidentRecordArn}}'
      eventId: '{{ListTimelineEvents.eventId}}'
    outputs:
      - Name: eventData
        Selector: $.event.eventData
        Type: String
    description: This step retrieves the timeline event itself.
  - name: JsonDecode
    action: 'aws:executeScript'
    inputs:
      Runtime: python3.8
      Handler: script_handler
      Script: |-
        import json

        def script_handler(events, context):
          data = json.loads(events["eventData"])
          return data
      InputPayload:
        eventData: '{{GetTimelineEvent.eventData}}'
    outputs:
      - Name: rawData
        Selector: $.Payload.rawData
        Type: String
    description: This step parses the timeline event data.
  - name: JsonDecode2
    action: 'aws:executeScript'
    inputs:
      Runtime: python3.8
      Handler: script_handler
      Script: |-
```

```
        import json

        def script_handler(events, context):
          data = json.loads(events["rawData"])
          return data
      InputPayload:
        rawData: '{{JsonDecode.rawData}}'
    outputs:
      - Name: InstanceId
        Selector:
'$.Payload.detail.configuration.metrics[0].metricStat.metric.dimensions.InstanceId'
        Type: String
    description: This step parses the CloudWatch event data.
  - name: RestartInstance
    action: 'aws:executeAutomation'
    inputs:
      DocumentName: AWS-RestartEC2Instance
      DocumentVersion: $DEFAULT
      RuntimeParameters:
        InstanceId: '{{JsonDecode2.InstanceId}}'
    description: This step restarts the Amazon EC2 instance
```

7. Pilih Buat otomatisasi.

Tugas 2: Membuat peran IAM

Gunakan tutorial berikut untuk membuat peran AWS Identity and Access Management (IAM) yang memberikan izin Manajer Insiden untuk mengintitiasi runbook yang ditentukan dalam rencana respons. Runbook dalam tutorial ini memulai ulang instance Amazon EC2 . Anda akan menentukan peran IAM ini di tugas berikutnya ketika Anda menghubungkan runbook ke rencana respons Anda.

Buat peran IAM yang mengintitiasi runbook dari rencana respons

1. Buka konsol IAM di https://console.aws.amazon.com/iam/.
2. Di panel navigasi, pilih Peran, lalu pilih Buat peran.
3. Di bawah Jenis entitas Tepercaya, verifikasi bahwa AWS layanan dipilih.
4. Di bawah Kasus penggunaan, di bidang Kasus penggunaan untuk AWS layanan lain, masukkan**`Incident Manager`**.
5. Pilih Manajer Insiden, lalu pilih Berikutnya.

6. Pada halaman Tambahkan izin, pilih Buat kebijakan. Editor izin akan terbuka di jendela atau tab browser baru.
7. Di editor, pilih tab JSON.
8. Salin dan tempel kebijakan izin berikut ke editor JSON. Ganti *account_ID* dengan Akun AWS ID Anda.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Resource": [
                "arn:aws:ssm:*:account_ID:automation-definition/
IncidentResponseRunbook:*",
                "arn:aws:ssm:*::automation-definition/AWS-RestartEC2Instance:*"
            ],
            "Action": "ssm:StartAutomationExecution"
        },
        {
            "Effect": "Allow",
            "Resource": "arn:aws:ssm:*:*:automation-execution/*",
            "Action": "ssm:GetAutomationExecution"
        },
        {
            "Effect": "Allow",
            "Resource": "arn:aws:ssm-incidents:*:*:*",
            "Action": "ssm-incidents:*"
        },
        {
            "Effect": "Allow",
            "Resource": "arn:aws:iam::*:role/AWS-SystemsManager-
AutomationExecutionRole",
            "Action": "sts:AssumeRole"
        },
        {
            "Effect": "Allow",
            "Resource": "*",
            "Action": [
                "ec2:StopInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:StartInstances"
            ]
```

```
        }
    ]
}
```

9. Pilih Berikutnya: Tag
10. (Opsional) Jika perlu, tambahkan tag ke kebijakan Anda.
11. Pilih Berikutnya: Tinjauan.
12. Di bidang Nama, masukkan nama yang membantu Anda mengidentifikasi peran ini sebagai yang digunakan untuk tutorial ini.
13. (Opsional) Masukkan deskripsi di bidang Deskripsi.
14. Pilih Buat kebijakan.
15. Arahkan kembali ke jendela browser atau tab untuk peran yang Anda buat. Halaman Tambahkan izin ditampilkan.
16. Pilih tombol refresh (terletak di sebelah tombol Buat Kebijakan), lalu masukkan nama kebijakan batas yang Anda buat ke dalam kotak filter.
17. Pilih kebijakan izin yang Anda buat, lalu pilih Berikutnya.
18. Pada halaman Nama, tinjau, dan buat, untuk nama Peran, masukkan nama yang membantu Anda mengidentifikasi peran ini sebagai yang digunakan untuk tutorial ini.
19. (Opsional) Masukkan deskripsi di bidang Deskripsi.
20. Tinjau detail peran, tambahkan tag jika diperlukan, dan pilih Buat peran.

Tugas 3: Menghubungkan runbook ke rencana respons Anda

Dengan menghubungkan runbook ke rencana respons Manajer Insiden Anda, Anda memastikan proses mitigasi yang konsisten, berulang, dan tepat waktu. Runbook juga berfungsi sebagai titik awal bagi resolver untuk menentukan tindakan selanjutnya.

Untuk menetapkan runbook ke rencana respons Anda

1. Buka konsol Manajer Insiden.
2. Pilih paket Respons.
3. Untuk paket Respons, pilih paket respons yang ada dan pilih Edit. Jika Anda tidak memiliki rencana respons yang ada, pilih Buat rencana respons untuk membuat rencana baru.

   Lengkapi bidang-bidang berikut:

   a. Di bagian Runbook, pilih Pilih runbook yang ada.
   b. Untuk Pemilik, verifikasi bahwa Dimiliki oleh saya dipilih.
   c. Untuk Runbook, pilih runbook yang Anda buat. Tugas 1: Membuat runbook
   d. Untuk Versi, pilih Default pada saat eksekusi.
   e. Di bagian Input, untuk IncidentRecordArnparameter, pilih Insiden ARN.
   f. Di bagian Izin eksekusi, pilih peran IAM yang Anda buat. Tugas 2: Membuat peran IAM
4. Simpan perubahan Anda.

Tugas 4: Menetapkan CloudWatch alarm ke rencana respons Anda

Gunakan prosedur berikut untuk menetapkan CloudWatch alarm untuk EC2 instans Amazon ke paket respons Anda.

Untuk menetapkan CloudWatch alarm ke rencana respons Anda

1. Buka CloudWatch konsol di https://console.aws.amazon.com/cloudwatch/.
2. Di panel navigasi, di bawah Alarm, pilih Semua alarm.
3. Pilih alarm untuk EC2 instans Amazon yang ingin Anda sambungkan ke paket respons Anda.
4. Pilih Tindakan, dan kemudian pilih Edit. Verifikasi bahwa metrik memiliki dimensi yang disebut`InstanceId`.
5. Pilih Berikutnya.
6. Untuk panduan Konfigurasi tindakan, pilih tindakan Add Systems Manager.
7. Pilih Buat insiden.
8. Pilih paket respons yang Anda buatTugas 3: Menghubungkan runbook ke rencana respons Anda.
9. Pilih Perbarui alarm.

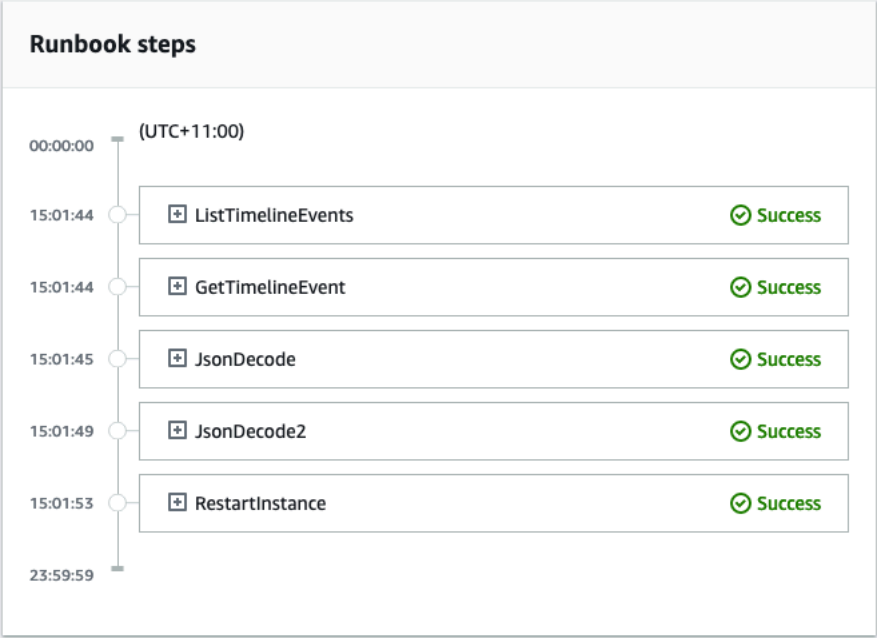
Tugas 5: Memverifikasi hasil

Untuk memverifikasi bahwa CloudWatch alarm membuat insiden dan kemudian memproses runbook yang ditentukan dalam rencana respons Anda, Anda harus memicu alarm. Setelah Anda memicu alarm dan runbook selesai diproses, Anda dapat memverifikasi hasil runbook dengan menggunakan

prosedur berikut. Untuk informasi tentang memicu alarm, lihat set-alarm-statedi Referensi AWS CLI Perintah.

1. Buka konsol Manajer Insiden.
2. Pilih insiden yang dibuat oleh CloudWatch alarm.
3. Pilih tab Runbooks.
4. Lihat tindakan yang dilakukan pada EC2 instans Amazon Anda di bagian Langkah Runbook.

   Gambar berikut menunjukkan bagaimana langkah-langkah yang diambil oleh runbook yang Anda buat dalam tutorial ini dilaporkan di konsol. Setiap langkah dicantumkan dengan stempel waktu dan pesan status.



   Untuk melihat semua detail di CloudWatch alarm, perluas langkah JsonDecode2, lalu perluas Output.

> **Important**
>
> Anda harus membersihkan setiap perubahan sumber daya yang Anda terapkan selama tutorial ini yang tidak ingin Anda simpan. Ini termasuk perubahan pada sumber daya Manajer Insiden seperti rencana sumber daya dan insiden, perubahan CloudWatch alarm, dan peran IAM yang Anda buat untuk tutorial ini.

Tutorial: Mengelola insiden keamanan di Manajer Insiden

Anda dapat menggunakan AWS Security Hub, Amazon EventBridge, dan Manajer Insiden bersama-sama untuk mengidentifikasi dan mengelola insiden keamanan di aplikasi yang AWS di-hosted Anda. Tutorial ini memandu Anda melalui konfigurasi EventBridge aturan yang membuat insiden berdasarkan temuan Security Hub yang dikirim secara otomatis.

> **Note**
>
> Tutorial ini menggunakan EventBridge Security Hub. Anda mungkin dikenakan biaya dari menggunakan layanan ini.

Prasyarat

- Siapkan Security Hub. Untuk informasi selengkapnya, lihat Menyiapkan AWS Security Hub.
- Buat atau perbarui temuan di Security Hub. Untuk informasi lebih lanjut, lihat Temuan di AWS Security Hub.
- Konfigurasikan rencana respons yang akan digunakan Manajer Insiden sebagai templat saat membuat insiden keamanan Anda. Untuk informasi selengkapnya, lihat Mempersiapkan Insiden di Manajer Insiden.

Untuk tutorial ini, kita menggunakan pola yang telah ditentukan untuk membuat EventBridge aturan. Untuk membuat aturan menggunakan pola kustom, lihat Menggunakan pola kustom untuk membuat aturan dalam panduan AWS Security Hub pengguna.

Buat EventBridge aturan

1. Buka EventBridge konsol Amazon di https://console.aws.amazon.com/events/.
2. Di panel navigasi, pilih Aturan.
3. Pilih Buat aturan.
4. Masukkan Nama dan Deskripsi untuk aturan tersebut.

   Aturan tidak boleh memiliki nama yang sama dengan aturan lain di Wilayah yang sama dan di bus peristiwa yang sama.
5. Untuk Bus peristiwa, pilih default.
6. Untuk Tipe aturan, pilih Aturan dengan pola peristiwa.

7. Pilih Selanjutnya.
8. Untuk sumber Acara, pilih AWS acara atau acara EventBridge mitra.
9. Untuk pola Acara, pilih Formulir pola acara.
10. Untuk Sumber peristiwa, pilih Layanan AWS .
11. Untuk AWS layanan, pilih Security Hub.
12. Untuk jenis Acara, pilih Temuan Security Hub - Imported.
13. Secara default, EventBridge mengkonfigurasi pola acara tanpa nilai filter apa pun. Untuk setiap atribut, `attribute name` opsi Any dipilih. Perbarui filter ini untuk membuat insiden berdasarkan temuan keamanan yang paling memengaruhi lingkungan Anda.
14. Klik Berikutnya.
15. Untuk Jenis target, pilih Layanan AWS .
16. Untuk Pilih target, pilih Rencana respons Manajer Insiden.
17. Untuk paket Respons, pilih paket respons yang akan digunakan sebagai templat untuk insiden yang dibuat.
18. EventBridge dapat membuat peran IAM yang diperlukan agar aturan Anda berjalan.
    - Untuk membuat peran IAM secara otomatis, pilih Buat peran baru untuk sumber daya tertentu.
    - Untuk menggunakan peran IAM yang sudah ada di akun Anda, pilih Gunakan peran yang ada.
19. (Opsional) Masukkan satu atau lebih tanda untuk aturan.
20. Pilih Berikutnya.
21. Tinjau detail aturan dan pilih Buat aturan.

Sekarang setelah Anda membuat EventBridge aturan ini, temuan keamanan yang cocok dengan nilai atribut yang Anda tentukan akan membuat insiden di Manajer Insiden. Anda dapat melakukan triase, mengelola, memantau, dan membuat analisis pasca-insiden dari insiden ini.

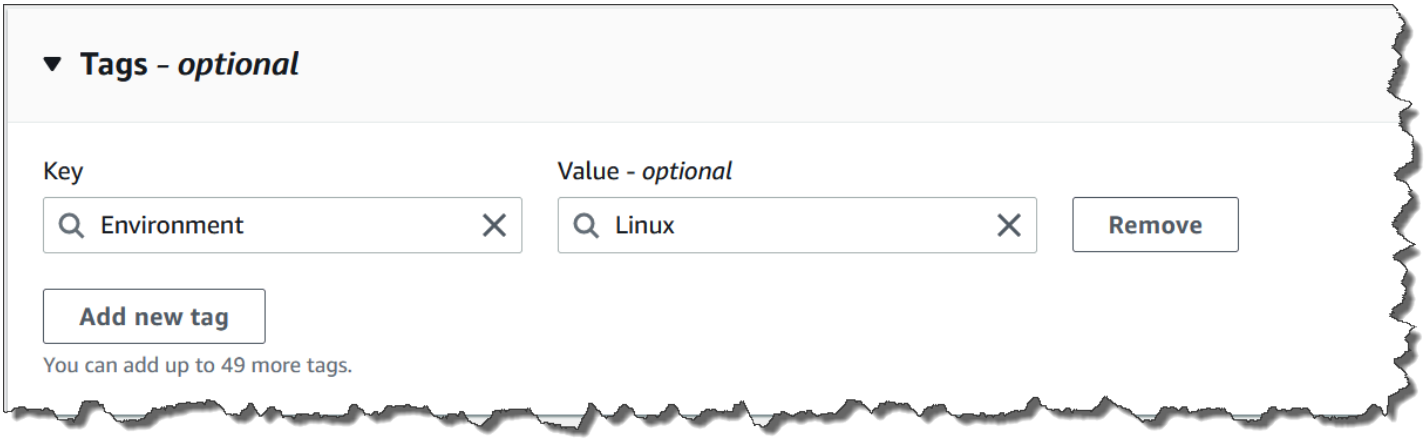
Menandai sumber daya di Manajer Insiden

Tag adalah metadata opsional yang dapat Anda tetapkan ke sumber daya Manajer Insiden dalam set Wilayah AWS replikasi yang ditentukan. Anda dapat menetapkan tag ke rencana respons, catatan insiden, dan kontak. Anda juga dapat menambahkan tag ke jadwal panggilan dan rotasi. Anda juga dapat menambahkan tag ke set replikasi itu sendiri. Tag memungkinkan Anda untuk mengkategorikan dan mengontrol akses ke sumber daya ini dengan cara yang berbeda. Setiap tag terdiri dari kunci dan nilai opsional, yang keduanya Anda tentukan. Kami menyarankan Anda merancang satu set kunci tag yang memenuhi kebutuhan Anda untuk setiap jenis sumber daya Manajer Insiden. Menggunakan satu set kunci tag yang konsisten memudahkan Anda mengelola sumber daya ini dan mengelola akses ke sana. Anda dapat mencari dan memfilter sumber daya berdasarkan tag. Untuk informasi selengkapnya tentang mengontrol akses ke sumber daya menggunakan tag, lihat Mengontrol akses ke AWS sumber daya menggunakan tag di Panduan Pengguna IAM.

Anda dapat menentukan tag di bagian default Insiden saat membuat rencana respons. Tag ini diterapkan pada catatan insiden saat insiden dibuat menggunakan rencana respons.

> **Note**
>
> Tag tidak memiliki arti semantik. Mereka ditafsirkan secara ketat sebagai serangkaian karakter.

Anda dapat menambah atau menghapus tag dengan menggunakan konsol Manajer Insiden. Tangkapan layar berikut menampilkan area Tag pada halaman konsol, dengan bidang untuk menambahkan kunci dan nilai tag, dan tombol untuk menambah dan menghapus tag.



Untuk bekerja dengan tag secara terprogram, gunakan tindakan API berikut:

- TagResource
- UntagResource
- ListTagsForResource

> **Important**
>
> Tag yang diterapkan pada rencana respons, catatan insiden, kontak, jadwal panggilan dan rotasi, dan set replikasi hanya dapat dilihat dan dimodifikasi dari akun pemilik sumber daya.

Keamanan di Manajer Insiden AWS Systems Manager

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 berjalan Layanan AWS di dalamnya 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 Manajer Insiden AWS Systems Manager, lihat AWS Layanan dalam Lingkup oleh AWS Layanan Program Kepatuhan .
- 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 Manajer Insiden. Topik berikut menunjukkan cara mengonfigurasi Manajer Insiden untuk memenuhi tujuan keamanan dan kepatuhan Anda. Anda juga mempelajari cara menggunakan Layanan AWS yang lain yang membantu Anda memantau dan mengamankan sumber daya Manajer Insiden Anda.

Topik

- Perlindungan data di Manajer Insiden
- Identity and Access Management untuk Manajer Insiden AWS Systems Manager
- Bekerja dengan kontak bersama dan rencana respons di Manajer Insiden
- Validasi kepatuhan untuk Manajer Insiden AWS Systems Manager
- Ketahanan di Manajer Insiden AWS Systems Manager
- Keamanan infrastruktur di Manajer Insiden AWS Systems Manager
- Bekerja dengan Manajer Insiden AWS Systems Manager dan antarmuka titik akhir VPC ()AWS PrivateLink
- Analisis konfigurasi dan kerentanan di Manajer Insiden

- Praktik terbaik keamanan di Manajer Insiden AWS Systems Manager

Perlindungan data di Manajer Insiden

Model tanggung jawab AWS bersama model berlaku untuk perlindungan data di Manajer Insiden AWS Systems Manager. 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 kredensil dan mengatur pengguna individu dengan AWS IAM Identity Center atau AWS Identity and Access Management (IAM). Dengan cara itu, setiap pengguna hanya diberi izin yang diperlukan untuk memenuhi tanggung jawab tugasnya. Kami juga menyarankan supaya Anda mengamankan data dengan cara-cara berikut:

- Gunakan autentikasi multi-faktor (MFA) pada setiap akun.
- Gunakan SSL/TLS untuk berkomunikasi dengan sumber daya. AWS Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Siapkan API dan 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 Manajer Insiden 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.

Secara default, Manajer Insiden mengenkripsi data dalam perjalanan menggunakan SSL/TLS.

Enkripsi data

Manajer Insiden menggunakan kunci AWS Key Management Service (AWS KMS) untuk mengenkripsi sumber daya Manajer Insiden Anda. Untuk informasi selengkapnya AWS KMS, lihat Panduan AWS KMS Pengembang. AWS KMS menggabungkan perangkat keras dan perangkat lunak yang aman dan sangat tersedia untuk menyediakan sistem manajemen kunci yang diskalakan untuk cloud. Incident Manager mengenkripsi data Anda menggunakan kunci yang Anda tentukan dan mengenkripsi metadata menggunakan kunci yang dimiliki. AWS Untuk menggunakan Manajer Insiden, Anda harus menyiapkan set replikasi Anda, yang mencakup pengaturan enkripsi. Manajer Insiden memerlukan enkripsi data untuk digunakan.

Anda dapat menggunakan kunci yang AWS dimiliki untuk mengenkripsi set replikasi Anda atau Anda dapat menggunakan kunci terkelola pelanggan Anda sendiri yang Anda buat AWS KMS untuk mengenkripsi Wilayah dalam kumpulan replikasi Anda. Incident Manager hanya mendukung AWS KMS kunci enkripsi simetris untuk mengenkripsi data Anda yang dibuat di dalamnya. AWS KMS Manajer Insiden tidak mendukung AWS KMS kunci dengan materi kunci yang diimpor, penyimpanan kunci khusus, Kode Otentikasi Pesan berbasis Hash (HMAC), atau jenis kunci lainnya. Jika Anda menggunakan kunci terkelola pelanggan, Anda menggunakan AWS KMS konsol atau AWS KMS APIs membuat kunci terkelola pelanggan secara terpusat dan menentukan kebijakan utama yang mengontrol cara Manajer Insiden dapat menggunakan kunci yang dikelola pelanggan. Saat Anda menggunakan kunci yang dikelola pelanggan untuk enkripsi dengan Manajer Insiden, kunci yang dikelola AWS KMS pelanggan harus berada di Wilayah yang sama dengan sumber daya. Untuk mempelajari lebih lanjut tentang menyiapkan enkripsi data di Manajer Insiden, lihatSiapkan penyihir.

Ada biaya tambahan untuk menggunakan kunci yang dikelola AWS KMS pelanggan. Untuk informasi selengkapnya, lihat AWS KMS konsep - kunci KMS di Panduan AWS Key Management Service Pengembang dan AWS KMS harga.

> **Important**
>
> Jika Anda menggunakan AWS KMS key (kunci KMS) untuk mengenkripsi kumpulan replikasi dan data Manajer Insiden, tetapi kemudian memutuskan untuk menghapus set replikasi, pastikan untuk menghapus set replikasi sebelum menonaktifkan atau menghapus kunci KMS.

Untuk mengizinkan Manajer Insiden menggunakan kunci terkelola pelanggan Anda untuk mengenkripsi data Anda, Anda harus menambahkan pernyataan kebijakan berikut ke kebijakan kunci kunci yang dikelola pelanggan Anda. Untuk mempelajari lebih lanjut tentang menyiapkan dan mengubah kebijakan utama di akun Anda, lihat Menggunakan kebijakan utama AWS KMS di Panduan AWS Key Management Service Pengembang. Kebijakan ini memberikan izin berikut:

- Memungkinkan Manajer Insiden melakukan operasi hanya-baca untuk menemukan Manajer Insiden di akun Anda. AWS KMS key
- Memungkinkan Manajer Insiden menggunakan kunci KMS untuk membuat hibah dan menjelaskan kunci, tetapi hanya ketika itu bertindak atas nama kepala sekolah di akun yang memiliki izin untuk menggunakan Manajer Insiden. Jika prinsipal yang ditentukan dalam pernyataan kebijakan tidak memiliki izin untuk menggunakan kunci KMS dan menggunakan Manajer Insiden, panggilan gagal, bahkan ketika itu berasal dari layanan Manajer Insiden.

```
        {
        "Sid": "Allow CreateGrant through AWS Systems Manager Incident Manager",
        "Effect": "Allow",
        "Principal": {
          "AWS": "arn:aws:iam::111122223333:user/ssm-lead"
        },
        "Action": [
          "kms:CreateGrant",
          "kms:DescribeKey"
        ],
        "Resource": "*",
        "Condition": {
          "StringLike": {
            "kms:ViaService": [
              "ssm-incidents.amazonaws.com",
              "ssm-contacts.amazonaws.com"
            ]
          }
```

```
        }
      }
```

Ganti `Principal` nilai dengan prinsipal IAM yang membuat set replikasi Anda.

Incident Manager menggunakan konteks enkripsi dalam semua permintaan AWS KMS untuk operasi kriptografi. Anda dapat menggunakan konteks enkripsi ini untuk mengidentifikasi peristiwa CloudTrail log di mana Manajer Insiden menggunakan kunci KMS Anda. Incident Manager menggunakan konteks enkripsi berikut:

- `contactArn=`*`ARN of the contact or escalation plan`*

Identity and Access Management untuk Manajer Insiden AWS Systems Manager

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 diautentikasi (masuk) dan diberi wewenang (memiliki izin) untuk menggunakan sumber daya Manajer Insiden. IAM adalah Layanan AWS yang dapat Anda gunakan tanpa biaya tambahan.

Topik

- Audiens
- Mengautentikasi dengan identitas
- Mengelola akses menggunakan kebijakan
- Bagaimana Manajer Insiden AWS Systems Manager bekerja dengan IAM
- Contoh kebijakan berbasis identitas untuk Manajer Insiden AWS Systems Manager
- Contoh kebijakan berbasis sumber daya untuk Manajer Insiden AWS Systems Manager
- Pencegahan Deputi Bingung Lintas Layanan di Manajer Insiden
- Menggunakan peran terkait layanan untuk Manajer Insiden
- AWS kebijakan terkelola untuk Manajer Insiden AWS Systems Manager
- Memecahkan masalah Manajer Insiden AWS Systems Manager identitas dan akses

Audiens

Cara Anda menggunakan AWS Identity and Access Management (IAM) berbeda, tergantung pada pekerjaan yang Anda lakukan di Manajer Insiden.

Pengguna layanan — Jika Anda menggunakan layanan Manajer Insiden untuk melakukan pekerjaan Anda, administrator Anda memberi Anda kredensi dan izin yang Anda butuhkan. Saat Anda menggunakan lebih banyak fitur Manajer Insiden untuk melakukan pekerjaan Anda, Anda mungkin memerlukan izin tambahan. Memahami cara akses dikelola dapat membantu Anda meminta izin yang tepat dari administrator Anda. Jika Anda tidak dapat mengakses fitur di Manajer Insiden, lihatMemecahkan masalah Manajer Insiden AWS Systems Manager identitas dan akses.

Administrator layanan — Jika Anda bertanggung jawab atas sumber daya Manajer Insiden di perusahaan Anda, Anda mungkin memiliki akses penuh ke Manajer Insiden. Tugas Anda adalah menentukan fitur dan sumber daya Manajer Insiden 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 lebih lanjut tentang bagaimana perusahaan Anda dapat menggunakan IAM dengan Manajer Insiden, lihatBagaimana Manajer Insiden AWS Systems Manager bekerja dengan IAM.

Administrator IAM — Jika Anda seorang administrator IAM, Anda mungkin ingin mempelajari detail tentang cara menulis kebijakan untuk mengelola akses ke Manajer Insiden. Untuk melihat contoh kebijakan berbasis identitas Manajer Insiden yang dapat Anda gunakan di IAM, lihat. Contoh kebijakan berbasis identitas untuk Manajer Insiden AWS Systems Manager

Mengautentikasi dengan identitas

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

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

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

Untuk manajemen akses terpusat, kami sarankan Anda menggunakan AWS IAM Identity Center. Anda dapat membuat pengguna dan grup di Pusat 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 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 suatu organisasi, maka 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 Manajer Insiden AWS Systems Manager bekerja dengan IAM

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

Fitur IAM yang dapat Anda gunakan dengan Manajer Insiden AWS Systems Manager

Fitur IAM	Dukungan Manajer Insiden
Kebijakan berbasis identitas	Ya
Kebijakan berbasis sumber daya	Ya
Tindakan kebijakan	Ya
Sumber daya kebijakan	Ya
Kunci kondisi kebijakan	Tidak
ACLs	Tidak
ABAC (tanda dalam kebijakan)	Tidak
Kredensial sementara	Ya
Izin principal	Ya
Peran layanan	Ya
Peran terkait layanan	Ya

Untuk mendapatkan pandangan tingkat tinggi tentang cara kerja Manajer Insiden dan AWS layanan lainnya dengan sebagian besar fitur IAM, lihat AWS layanan yang bekerja dengan IAM di Panduan Pengguna IAM.

Manajer Insiden tidak mendukung kebijakan yang menolak akses ke sumber daya yang digunakan bersama AWS RAM.

Kebijakan berbasis identitas untuk Manajer Insiden

Mendukung kebijakan berbasis identitas: Ya

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

Dengan kebijakan berbasis identitas IAM, Anda dapat menentukan secara spesifik apakah tindakan dan sumber daya diizinkan atau ditolak, serta kondisi yang menjadi dasar dikabulkan atau ditolaknya tindakan tersebut. 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 Manajer Insiden

Untuk melihat contoh kebijakan berbasis identitas Manajer Insiden, lihat. Contoh kebijakan berbasis identitas untuk Manajer Insiden AWS Systems Manager

Kebijakan berbasis sumber daya dalam Manajer Insiden

Mendukung kebijakan berbasis sumber daya: Ya

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.

Layanan Manajer Insiden hanya mendukung dua jenis kebijakan berbasis sumber daya yang disebut menggunakan AWS RAM konsol atau PutResourcePolicy tindakan, yang dilampirkan ke rencana respons atau kontak. Kebijakan ini mendefinisikan prinsip mana yang dapat melakukan tindakan pada rencana respons, kontak, rencana eskalasi, dan insiden. Manajer Insiden menggunakan kebijakan berbasis sumber daya untuk berbagi sumber daya di seluruh akun.

Manajer Insiden tidak mendukung kebijakan yang menolak akses ke sumber daya yang digunakan bersama AWS RAM.

Untuk mempelajari cara melampirkan kebijakan berbasis sumber daya ke rencana respons atau kontak, lihat. Mengelola insiden di seluruh Akun AWS dan Wilayah di Manajer Insiden

Contoh kebijakan berbasis sumber daya dalam Manajer Insiden

Untuk melihat contoh kebijakan berbasis sumber daya Manajer Insiden, lihat. Contoh kebijakan berbasis sumber daya untuk Manajer Insiden AWS Systems Manager

Tindakan kebijakan untuk Manajer Insiden

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 Manajer Insiden, lihat Tindakan yang ditentukan oleh Manajer Insiden AWS Systems Manager dalam Referensi Otorisasi Layanan.

Tindakan kebijakan di Manajer Insiden menggunakan awalan berikut sebelum tindakan:

```
ssm-incidents
ssm-contacts
```

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

```
"Action": [
      "ssm-incidents:GetResponsePlan",
      "ssm-contacts:GetContact"
         ]
```

Anda juga dapat menentukan beberapa tindakan menggunakan wildcard (*). Sebagai contoh, untuk menentukan semua tindakan yang dimulai dengan kata `Get`, sertakan tindakan berikut:

```
"Action": "ssm-incidents:Get*"
```

Untuk melihat contoh kebijakan berbasis identitas Manajer Insiden, lihat. Contoh kebijakan berbasis identitas untuk Manajer Insiden AWS Systems Manager

Incident Manager menggunakan tindakan di dua ruang nama yang berbeda, ssm-incidents dan ssm-contacts. Saat membuat kebijakan untuk Manajer Insiden, pastikan untuk menggunakan namespace yang benar untuk tindakan tersebut. Insiden SSM digunakan untuk rencana respons dan tindakan terkait insiden. Kontak SSM digunakan untuk tindakan yang terkait dengan kontak dan keterlibatan kontak. Misalnya:

- `ssm-contacts:GetContact`
- `ssm-incidents:GetResponsePlan`

Sumber daya kebijakan untuk Manajer Insiden

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 tipe sumber daya Manajer Insiden dan jenisnya ARNs, lihat Sumber Daya yang ditentukan oleh Manajer Insiden AWS Systems Manager dalam Referensi Otorisasi Layanan. Untuk mempelajari tindakan yang dapat menentukan ARN setiap sumber daya, lihat Tindakan yang ditentukan oleh Manajer Insiden AWS Systems Manager.

Untuk melihat contoh kebijakan berbasis identitas Manajer Insiden, lihat. Contoh kebijakan berbasis identitas untuk Manajer Insiden AWS Systems Manager

Sumber daya Manajer Insiden digunakan untuk membuat insiden, berkolaborasi dalam saluran obrolan, menyelesaikan insiden, dan melibatkan responden. Jika pengguna memiliki akses ke paket respons, mereka memiliki akses ke semua insiden yang dibuat darinya. Jika pengguna memiliki akses ke kontak atau rencana eskalasi, mereka dapat melibatkan kontak atau kontak dalam rencana eskalasi.

Kunci kondisi kebijakan untuk Manajer Insiden

Mendukung kunci kondisi kebijakan khusus layanan: Tidak

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.

Daftar kontrol akses (ACLs) di Manajer Insiden

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.

Kontrol akses berbasis atribut (ABAC) dengan Manajer Insiden

Mendukung ABAC (tag dalam kebijakan): Tidak

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 kredensil sementara dengan Manajer Insiden

Mendukung kredensial sementara: Ya

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

Anda menggunakan kredensi sementara jika Anda masuk AWS Management Console menggunakan metode apa pun kecuali nama pengguna dan kata sandi. Misalnya, ketika Anda mengakses AWS menggunakan tautan masuk tunggal (SSO) perusahaan Anda, proses tersebut secara otomatis membuat kredensil sementara. Anda juga akan 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 kredenal sementara secara manual menggunakan API AWS CLI atau AWS . Anda kemudian dapat menggunakan kredensyal sementara tersebut untuk mengakses. AWS AWS merekomendasikan agar Anda secara dinamis menghasilkan kredensi sementara alih-alih menggunakan kunci akses jangka panjang. Untuk informasi selengkapnya, lihat Kredensial keamanan sementara di IAM.

Izin utama lintas layanan untuk Manajer Insiden

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 Manajer Insiden

Mendukung peran layanan: Ya

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 Manajer Insiden. Edit peran layanan hanya jika Manajer Insiden memberikan panduan untuk melakukannya.

Memilih peran IAM di Manajer Insiden

Saat Anda membuat sumber daya rencana respons di Manajer Insiden, Anda harus memilih peran untuk mengizinkan Manajer Insiden menjalankan dokumen otomatisasi Systems Manager atas nama Anda. Jika sebelumnya Anda telah membuat peran layanan atau peran terkait layanan, Manajer Insiden memberi Anda daftar peran yang dapat dipilih. Penting untuk memilih peran yang memungkinkan akses untuk menjalankan instance dokumen otomatisasi Anda. Untuk informasi selengkapnya, lihat Mengintegrasikan runbook Otomasi Systems Manager di Incident Manager untuk remediasi insiden. Saat Anda membuat Pengembang Amazon Q di saluran obrolan aplikasi obrolan untuk digunakan selama insiden, Anda dapat memilih peran layanan yang memungkinkan Anda menggunakan perintah langsung dari obrolan. Untuk mempelajari selengkapnya tentang membuat saluran obrolan untuk kolaborasi insiden, lihatMembuat dan mengintegrasikan saluran obrolan untuk responden di Manajer Insiden. Untuk mempelajari selengkapnya tentang kebijakan IAM di Pengembang Amazon Q di aplikasi obrolan, lihat Mengelola izin untuk menjalankan perintah

menggunakan Pengembang Amazon Q dalam aplikasi obrolan dalam panduan Administrator Pengembang Amazon Q dalam aplikasi obrolan.

Peran terkait layanan untuk Manajer Insiden

Mendukung peran terkait layanan: Ya

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

Untuk informasi tentang membuat atau mengelola peran terkait layanan Manajer Insiden, lihat. Menggunakan peran terkait layanan untuk Manajer Insiden

Contoh kebijakan berbasis identitas untuk Manajer Insiden AWS Systems Manager

Secara default, pengguna dan peran tidak memiliki izin untuk membuat atau memodifikasi sumber daya Manajer Insiden. 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 Manajer Insiden, termasuk format ARNs untuk setiap jenis sumber daya, lihat Kunci tindakan, sumber daya, dan kondisi Manajer Insiden AWS Systems Manager di Referensi Otorisasi Layanan.

Topik

- Praktik terbaik kebijakan
- Menggunakan konsol Manajer Insiden
- Mengizinkan pengguna melihat izin mereka sendiri
- Mengakses rencana respons

Praktik terbaik kebijakan

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

- Mulailah dengan kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit — Untuk mulai memberikan izin kepada pengguna dan beban kerja Anda, gunakan kebijakan AWS terkelola yang memberikan izin untuk banyak kasus penggunaan umum. Mereka tersedia di Anda Akun AWS. Kami menyarankan Anda mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola AWS pelanggan yang khusus untuk kasus penggunaan Anda. Untuk informasi selengkapnya, lihat Kebijakan yang dikelola AWS atau Kebijakan yang dikelola AWS untuk fungsi tugas dalam Panduan Pengguna IAM.
- Menerapkan izin dengan hak akses paling rendah – Ketika Anda menetapkan izin dengan kebijakan IAM, hanya berikan izin yang diperlukan untuk melakukan tugas. Anda melakukannya dengan mendefinisikan tindakan yang dapat diambil pada sumber daya tertentu dalam kondisi tertentu, yang juga dikenal sebagai izin dengan hak akses paling rendah. Untuk informasi selengkapnya tentang cara menggunakan IAM untuk mengajukan izin, lihat Kebijakan dan izin dalam IAM dalam Panduan Pengguna IAM.
- Gunakan kondisi dalam kebijakan IAM untuk membatasi akses lebih lanjut – Anda dapat menambahkan suatu kondisi ke kebijakan Anda untuk membatasi akses ke tindakan dan sumber daya. Sebagai contoh, Anda dapat menulis kondisi kebijakan untuk menentukan bahwa semua permintaan harus dikirim menggunakan SSL. Anda juga dapat menggunakan ketentuan untuk memberikan akses ke tindakan layanan jika digunakan melalui yang spesifik Layanan AWS, seperti 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 Manajer Insiden

Untuk mengakses Manajer Insiden AWS Systems Manager konsol, Anda harus memiliki set izin minimum. Izin ini harus memungkinkan Anda untuk membuat daftar dan melihat detail tentang sumber daya Manajer Insiden 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 dapat menyelesaikan insiden menggunakan konsol Manajer Insiden, lampirkan juga kebijakan yang `IncidentManagerResolverAccess` AWS dikelola Manajer Insiden ke entitas. Untuk informasi selengkapnya, lihat Menambah izin untuk pengguna dalam Panduan Pengguna IAM.

```
IncidentManagerResolverAccess
```

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:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Mengakses rencana respons

Dalam contoh ini, Anda ingin memberi pengguna IAM di akun Amazon Web Services Anda akses ke salah satu paket respons Manajer Insiden Anda. `examplepl an` Anda juga ingin mengizinkan pengguna untuk menambahkan, memperbarui, dan menghapus paket respons.

Kebijakan memberikan`ssm-incidents:ListResponsePlans`,`ssm-incidents:GetResponsePlan`, `ssm-incidents:UpdateResponsePlan` dan `ssm-incident:ListResponsePlan` izin kepada pengguna.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"ListResponsePlans",
         "Effect":"Allow",
```

```
            "Action":[
               "ssm-incidents:ListResponsePlans"
            ],
            "Resource":"arn:aws:ssm-incidents:::*"
         },
         {
            "Sid":"ViewSpecificResponsePlanInfo",
            "Effect":"Allow",
            "Action":[
               "ssm-incidents:GetResponsePlan"
            ],
            "Resource":"arn:aws:ssm-incidents:*:111122223333:response-plan/exampleplan"
         },
         {
            "Sid":"ManageResponsePlan",
            "Effect":"Allow",
            "Action":[
               "ssm-incidents:UpdateResponsePlan"
            ],
            "Resource":"arn:aws:ssm-incidents:*:111122223333:response-plan/exampleplan/*"
         }
      ]
}
```

Contoh kebijakan berbasis sumber daya untuk Manajer Insiden AWS Systems Manager

Manajer Insiden AWS Systems Manager mendukung kebijakan izin berbasis sumber daya untuk rencana respons dan kontak Manajer Insiden.

Manajer Insiden tidak mendukung kebijakan berbasis sumber daya yang menolak akses ke sumber daya yang digunakan bersama. AWS RAM

Untuk mempelajari cara membuat rencana respons atau kontak, lihat Membuat dan mengonfigurasi rencana respons di Manajer Insiden dan Membuat dan mengonfigurasi kontak di Manajer Insiden.

Membatasi akses rencana respons Manajer Insiden oleh organisasi

Contoh berikut memberikan izin kepada pengguna di organisasi dengan ID organisasi: `o-abc123def45` untuk menanggapi insiden yang dibuat menggunakan paket respons. `myplan`

`Condition`Blok menggunakan `StringEquals` kondisi dan kunci `aws:PrincipalOrgID` kondisi, yang merupakan kunci kondisi AWS Organizations tertentu. Untuk informasi selengkapnya tentang kunci kondisi ini, lihat Menentukan kondisi dalam kebijakan.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "OrganizationAccess",
      "Effect": "Allow",
      "Principal": “*”,
      "Condition": {
         "StringEquals": {"aws:PrincipalOrgID":"o-abc123def45"}
      },
      "Action": [
        "ssm-incidents:GetResponsePlan",
        "ssm-incidents:StartIncident",
        "ssm-incidents:UpdateIncidentRecord",
        "ssm-incidents:GetIncidentRecord",
        "ssm-incidents:CreateTimelineEvent",
        "ssm-incidents:UpdateTimelineEvent",
        "ssm-incidents:GetTimelineEvent",
        "ssm-incidents:ListTimelineEvents",
        "ssm-incidents:UpdateRelatedItems",
        "ssm-incidents:ListRelatedItems"
      ],
      "Resource": [
        "arn:aws:ssm-incidents:*:111122223333:response-plan/myplan",
        "arn:aws:ssm-incidents:*:111122223333:incident-record/myplan/*"
      ]
    }
  ]
}
```

Memberikan akses kontak Manajer Insiden ke kepala sekolah

Contoh berikut memberikan izin kepada kepala sekolah dengan `arn:aws:iam::999988887777:root` ARN untuk membuat keterlibatan ke kontak. `mycontact`

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

```
        {
            "Sid": "PrincipalAccess",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::999988887777:root"
            },
            "Action": [
                "ssm-contacts:GetContact",
                "ssm-contacts:StartEngagement",
                "ssm-contacts:DescribeEngagement",
                "ssm-contacts:ListPagesByContact"
            ],
            "Resource": [
                "arn:aws:ssm-contacts:*:111122223333:contact/mycontact"
                "arn:aws:ssm-contacts:*:111122223333:engagement/mycontact/*"
            ]
        }
    ]
}
```

Pencegahan Deputi Bingung Lintas Layanan di Manajer Insiden

Masalah Deputi yang membingungkan adalah masalah keamanan informasi yang terjadi ketika entitas tanpa izin untuk melakukan tindakan memanggil entitas yang lebih istimewa untuk melakukan tindakan. Ini dapat memungkinkan aktor jahat untuk menjalankan perintah atau memodifikasi sumber daya yang jika tidak, mereka tidak akan memiliki izin untuk menjalankan atau mengakses.

Pada tahun AWS, peniruan lintas layanan dapat menyebabkan skenario wakil yang membingungkan. Peniruan lintas layanan adalah ketika satu layanan (layanan panggilan) memanggil layanan lain (layanan yang disebut). Aktor jahat dapat menggunakan layanan panggilan untuk mengubah sumber daya di layanan lain menggunakan izin yang biasanya tidak mereka miliki.

AWS menyediakan prinsip layanan dengan akses terkelola ke sumber daya di akun Anda untuk membantu Anda melindungi keamanan sumber daya Anda. Sebaiknya gunakan kunci konteks kondisi `aws:SourceAccount`global `aws:SourceArn`dan global dalam kebijakan sumber daya Anda. Kunci ini membatasi izin yang Manajer Insiden AWS Systems Manager memberikan layanan lain ke sumber daya itu. Jika Anda menggunakan kedua kunci konteks kondisi global, `aws:SourceAccount` nilai dan akun yang direferensikan dalam `aws:SourceArn` nilai harus menggunakan ID akun yang sama saat digunakan dalam pernyataan kebijakan yang sama.

Nilai `aws:SourceArn` harus ARN dari catatan insiden yang terkena dampak. Jika Anda tidak mengetahui ARN lengkap sumber daya, atau jika Anda menentukan beberapa sumber daya, gunakan kunci kondisi konteks `aws:SourceArn` global dengan `*` wildcard untuk bagian ARN yang tidak diketahui. Misalnya, Anda dapat mengatur `aws:SourceArn` kearn`:aws:ssm-incidents::`*111122223333*`:*`.

Dalam contoh kebijakan kepercayaan berikut, kami menggunakan kunci `aws:SourceArn` kondisi untuk membatasi akses ke peran layanan berdasarkan ARN catatan insiden. Hanya catatan insiden yang dibuat dari rencana respons `myresponseplan` yang dapat menggunakan peran ini.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Principal": { "Service": "ssm-incidents.amazonaws.com" },
    "Action": "sts:AssumeRole",
    "Condition": {
      "ArnLike": {
        "aws:SourceArn": "arn:aws:ssm-incidents:*:111122223333:incident-record/
myresponseplan/*"
      }
    }
  }
}
```

Menggunakan peran terkait layanan untuk Manajer Insiden

Manajer Insiden AWS Systems Manager menggunakan AWS Identity and Access Management peran terkait layanan (IAM). Peran terkait layanan adalah jenis peran IAM unik yang ditautkan langsung ke Manajer Insiden. Peran terkait layanan telah ditentukan sebelumnya oleh Manajer Insiden dan mencakup semua izin yang diperlukan layanan untuk memanggil AWS layanan lain atas nama Anda.

Peran terkait layanan membuat pengaturan Manajer Insiden lebih mudah karena Anda tidak perlu menambahkan izin yang diperlukan secara manual. Manajer Insiden mendefinisikan izin dari peran terkait layanannya, dan kecuali ditentukan lain, hanya Manajer Insiden yang dapat mengambil perannya. Izin yang ditentukan mencakup kebijakan kepercayaan dan kebijakan izin, dan kebijakan izin tersebut tidak dapat dilampirkan ke entitas IAM lainnya.

Anda dapat menghapus peran tertaut layanan hanya setelah menghapus sumber daya terkait terlebih dahulu. Ini melindungi sumber daya Manajer Insiden 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 bisa digunakan dengan IAM dan carilah layanan yang memiliki opsi Ya di kolom Peran Terkait Layanan. Pilih Ya dengan sebuah tautan untuk melihat dokumentasi peran terkait layanan untuk layanan tersebut.

Izin peran terkait layanan untuk Manajer Insiden

Manajer Insiden menggunakan peran terkait layanan bernama. AWSServiceRoleforIncidentManager Peran ini memungkinkan Manajer Insiden untuk mengelola catatan insiden Manajer Insiden dan sumber daya terkait atas nama Anda.

Peran AWSService RoleforIncidentManager terkait layanan mempercayai layanan berikut untuk mengambil peran:

- `ssm-incidents.amazonaws.com`

Kebijakan izin peran `AWSIncidentManagerServiceRolePolicy`memungkinkan Manajer Insiden menyelesaikan tindakan berikut pada sumber daya yang ditentukan:

- Tindakan: `ssm-incidents:ListIncidentRecords` pada semua sumber daya yang terkait dengan tindakan.
- Tindakan: `ssm-incidents:CreateTimelineEvent` pada semua sumber daya yang terkait dengan tindakan.
- Tindakan: `ssm:CreateOpsItem` pada semua sumber daya yang terkait dengan tindakan.
- Tindakan: `ssm:AssociateOpsItemRelatedItem` pada `all resources related to the action.`
- Tindakan: `ssm-contacts:StartEngagement` pada semua sumber daya yang terkait dengan tindakan.
- Tindakan: `cloudwatch:PutMetricData` pada CloudWatch metrik di dalam `AWS/IncidentManager` dan ruang nama `AWS/Usage`

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

Membuat peran terkait layanan untuk Manajer Insiden

Anda tidak perlu membuat peran terkait layanan secara manual. Saat Anda membuat set replikasi di, API AWS Management Console, atau AWS API AWS CLI, Manajer Insiden membuat peran terkait layanan untuk Anda.

Jika Anda menghapus peran terkait layanan ini, dan ingin membuatnya lagi, Anda dapat mengulangi proses yang sama untuk membuat kembali peran tersebut di akun Anda. Saat Anda membuat kumpulan replikasi, Manajer Insiden membuat peran terkait layanan untuk Anda lagi.

Mengedit peran terkait layanan untuk Manajer Insiden

Manajer Insiden tidak mengizinkan Anda mengedit peran AWSService RoleforIncidentManager terkait layanan. Setelah membuat peran terkait layanan, Anda tidak dapat mengubah nama peran karena berbagai entitas mungkin mereferensikan peran tersebut. Namun, Anda dapat menyunting penjelasan peran menggunakan IAM. Untuk informasi selengkapnya, lihat Mengedit Peran Tertaut Layanan dalam Panduan Pengguna IAM.

Menghapus peran terkait layanan untuk Manajer Insiden

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

Untuk menghapus peran terkait layanan, Anda harus menghapus set replikasi terlebih dahulu. Menghapus set replikasi akan menghapus semua data yang dibuat dan disimpan di Manajer Insiden, termasuk rencana respons, kontak, dan rencana eskalasi. Anda juga akan kehilangan semua insiden yang dibuat sebelumnya. Alarm dan EventBridge aturan apa pun yang menunjuk ke rencana respons yang dihapus tidak akan lagi membuat insiden pada alarm atau pencocokan aturan. Untuk menghapus kumpulan replikasi, Anda harus menghapus setiap Wilayah di set.

> **Note**
>
> Jika layanan Manajer Insiden 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 Regions dalam set replikasi yang digunakan oleh AWSService RoleforIncidentManager

1. Buka konsol Manajer Insiden dan pilih Pengaturan dari navigasi kiri.
2. Pilih Wilayah di set Replikasi.
3. Pilih Hapus.
4. Untuk mengonfirmasi penghapusan Wilayah, masukkan nama Wilayah dan pilih Hapus.
5. Ulangi langkah-langkah ini sampai Anda menghapus semua Wilayah di set replikasi Anda. Saat menghapus Wilayah terakhir, konsol memberi tahu Anda bahwa ia menghapus set replikasi dengannya.

Untuk menghapus peran tertaut layanan secara manual menggunakan IAM

Gunakan konsol IAM, the AWS CLI, atau AWS API untuk menghapus peran AWSService RoleforIncidentManager terkait layanan. Untuk informasi selengkapnya, silakan lihat Menghapus Peran Terkait Layanan di Panduan Pengguna IAM.

Wilayah yang Didukung untuk peran terkait layanan Manajer Insiden

Manajer Insiden mendukung penggunaan peran terkait layanan di semua Wilayah tempat layanan tersedia. Untuk informasi selengkapnya, lihat AWS Wilayah dan Titik Akhir.

AWS kebijakan terkelola untuk Manajer Insiden AWS Systems Manager

Kebijakan AWS terkelola adalah kebijakan mandiri yang dibuat dan dikelola oleh AWS. AWS Kebijakan terkelola dirancang untuk memberikan izin bagi banyak kasus penggunaan umum sehingga Anda dapat mulai menetapkan izin kepada pengguna, grup, dan peran.

Perlu diingat bahwa kebijakan AWS terkelola mungkin tidak memberikan izin hak istimewa paling sedikit untuk kasus penggunaan spesifik Anda karena tersedia untuk digunakan semua pelanggan.

AWS Kami menyarankan Anda untuk mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola pelanggan yang khusus untuk kasus penggunaan Anda.

Anda tidak dapat mengubah izin yang ditentukan dalam kebijakan AWS terkelola. Jika AWS memperbarui izin yang ditentukan dalam kebijakan AWS terkelola, pembaruan akan memengaruhi semua identitas utama (pengguna, grup, dan peran) yang dilampirkan kebijakan tersebut. AWS kemungkinan besar akan memperbarui kebijakan AWS terkelola saat baru Layanan AWS diluncurkan atau operasi API baru tersedia untuk layanan yang ada.

Untuk informasi selengkapnya, lihat Kebijakan terkelola AWS dalam Panduan Pengguna IAM.

AWS kebijakan terkelola: AWSIncident ManagerIncidentAccessServiceRolePolicy

Anda dapat melampirkan `AWSIncidentManagerIncidentAccessServiceRolePolicy` ke entitas IAM Anda. Manajer Insiden juga melampirkan kebijakan ini ke peran Manajer Insiden yang memungkinkan Manajer Insiden melakukan tindakan atas nama Anda.

Kebijakan ini memberikan izin hanya-baca yang memungkinkan Manajer Insiden membaca sumber daya tertentu lainnya Layanan AWS untuk mengidentifikasi temuan yang terkait dengan insiden di layanan tersebut.

Detail izin

Kebijakan ini mencakup izin berikut.

- `cloudformation`— Memungkinkan kepala sekolah untuk menggambarkan tumpukan. AWS CloudFormation Ini diperlukan bagi Manajer Insiden untuk mengidentifikasi CloudFormation peristiwa dan sumber daya yang terkait dengan suatu insiden.
- `codedeploy`— Memungkinkan kepala sekolah untuk membaca penerapan. AWS CodeDeploy Ini diperlukan bagi Manajer Insiden untuk mengidentifikasi CodeDeploy penyebaran dan target yang terkait dengan suatu insiden.

- `autoscaling`— Memungkinkan prinsipal untuk menentukan apakah instans Amazon Elastic Compute Cloud (EC2) adalah bagian dari grup Auto Scaling. Ini diperlukan agar Manajer Insiden dapat memberikan temuan untuk EC2 instance yang merupakan bagian dari grup Auto Scaling.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "IncidentAccessPermissions",
            "Effect": "Allow",
            "Action": [
                "cloudformation:DescribeStackEvents",
                "cloudformation:DescribeStackResources",
                "codedeploy:BatchGetDeployments",
                "codedeploy:ListDeployments",
                "codedeploy:ListDeploymentTargets",
                "autoscaling:DescribeAutoScalingInstances"
            ],
            "Resource": "*"
        }
    ]
}
```

Untuk melihat detail selengkapnya tentang kebijakan, termasuk versi terbaru dari dokumen kebijakan JSON, lihat AWSIncidentManagerIncidentAccessServiceRolePolicydalam Panduan Referensi Kebijakan AWS Terkelola.

Kebijakan terkelola AWS : **`AWSIncidentManagerServiceRolePolicy`**

Anda tidak dapat melampirkan `AWSIncidentManagerServiceRolePolicy` ke entitas IAM Anda. Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan Manajer Insiden melakukan tindakan atas nama Anda. Untuk informasi selengkapnya, lihat Menggunakan peran terkait layanan untuk Manajer Insiden.

Kebijakan ini memberikan izin Manajer Insiden untuk membuat daftar insiden, membuat peristiwa timeline, membuat, mengaitkan item terkait OpsItems, memulai keterlibatan OpsItems, dan mempublikasikan CloudWatch metrik yang terkait dengan insiden.

Detail izin

Kebijakan ini mencakup izin berikut.

- `ssm-incidents`— Memungkinkan kepala sekolah untuk membuat daftar insiden dan membuat peristiwa timeline. Ini diperlukan agar responden dapat berkolaborasi selama insiden di dasbor insiden.
- `ssm`— Memungkinkan kepala sekolah untuk membuat OpsItems dan mengaitkan item terkait. Ini diperlukan untuk membuat orang tua OpsItem ketika insiden dimulai.
- `ssm-contacts`— Memungkinkan kepala sekolah untuk memulai keterlibatan. Ini diperlukan untuk Manajer Insiden untuk melibatkan kontak selama insiden.
- `cloudwatch`— Memungkinkan kepala sekolah untuk mempublikasikan metrik. CloudWatch Ini diperlukan untuk Manajer Insiden untuk mempublikasikan metrik yang terkait dengan insiden dan metrik penggunaan.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "UpdateIncidentRecordPermissions",
            "Effect": "Allow",
            "Action": [
                "ssm-incidents:ListIncidentRecords",
                "ssm-incidents:CreateTimelineEvent"
            ],
            "Resource": "*"
        },
        {
            "Sid": "RelatedOpsItemPermissions",
            "Effect": "Allow",
            "Action": [
                "ssm:CreateOpsItem",
                "ssm:AssociateOpsItemRelatedItem"
            ],
            "Resource": "*"
        },
        {
            "Sid": "IncidentEngagementPermissions",
```

```
            "Effect": "Allow",
            "Action": "ssm-contacts:StartEngagement",
            "Resource": "*"
        },
        {
            "Sid": "PutCloudWatchMetricPermission",
            "Effect": "Allow",
            "Action": [
                "cloudwatch:PutMetricData"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "cloudwatch:namespace": [
                         "AWS/IncidentManager",
                         "AWS/Usage"
                     ]
                 }
             }
         }
    ]
}
```

Untuk melihat detail selengkapnya tentang kebijakan, termasuk versi terbaru dari dokumen kebijakan JSON, lihat AWSIncidentManagerServiceRolePolicydalam Panduan Referensi Kebijakan AWS Terkelola.

AWS kebijakan terkelola: **`AWSIncidentManagerResolverAccess`**

Anda dapat melampirkan `AWSIncidentManagerResolverAccess` ke entitas IAM Anda untuk memungkinkan mereka memulai, melihat, dan memperbarui insiden. Ini juga memungkinkan mereka untuk membuat peristiwa timeline pelanggan dan item terkait di dasbor insiden. Anda juga dapat melampirkan kebijakan ini ke Pengembang Amazon Q dalam peran layanan aplikasi obrolan atau langsung ke peran terkelola pelanggan yang terkait dengan saluran obrolan apa pun yang digunakan untuk kolaborasi insiden. Untuk mempelajari selengkapnya tentang kebijakan IAM di Pengembang Amazon Q di aplikasi obrolan, lihat Mengelola izin untuk menjalankan perintah menggunakan Pengembang Amazon Q dalam aplikasi obrolan di Panduan Administrator Pengembang Amazon Q di aplikasi obrolan.

Detail izin

Kebijakan ini mencakup izin berikut.

- `ssm-incidents`— Memungkinkan Anda memulai insiden, daftar rencana respons, daftar insiden, memperbarui insiden, membuat daftar peristiwa garis waktu, membuat acara garis waktu khusus, memperbarui peristiwa garis waktu khusus, menghapus peristiwa garis waktu khusus, mencantumkan item terkait, membuat item terkait, dan memperbarui item terkait.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "StartIncidentPermissions",
            "Effect": "Allow",
            "Action": [
                "ssm-incidents:StartIncident"
            ],
            "Resource": "*"
        },
        {
            "Sid": "ResponsePlanReadOnlyPermissions",
            "Effect": "Allow",
            "Action": [
                "ssm-incidents:ListResponsePlans",
                "ssm-incidents:GetResponsePlan"
            ],
            "Resource": "*"
        },
        {
            "Sid": "IncidentRecordResolverPermissions",
            "Effect": "Allow",
            "Action": [
                "ssm-incidents:ListIncidentRecords",
                "ssm-incidents:GetIncidentRecord",
                "ssm-incidents:UpdateIncidentRecord",
                "ssm-incidents:ListTimelineEvents",
                "ssm-incidents:CreateTimelineEvent",
                "ssm-incidents:GetTimelineEvent",
                "ssm-incidents:UpdateTimelineEvent",
                "ssm-incidents:DeleteTimelineEvent",
                "ssm-incidents:ListRelatedItems",
```

```
                "ssm-incidents:UpdateRelatedItems"
            ],
            "Resource": "*"
        }
    ]
}
```

Untuk melihat detail selengkapnya tentang kebijakan, termasuk versi terbaru dari dokumen kebijakan JSON, lihat AWSIncidentManagerResolverAccessdalam Panduan Referensi Kebijakan AWS Terkelola.

Pengelola Insiden memperbarui kebijakan AWS terkelola

Lihat detail tentang pembaruan kebijakan AWS terkelola untuk Manajer Insiden sejak layanan ini mulai melacak perubahan ini. Untuk peringatan otomatis tentang perubahan pada halaman ini, berlangganan umpan RSS di halaman riwayat Dokumen Manajer Insiden.

Perubahan	Deskripsi	Tanggal
`AWSIncidentManagerServiceRolePolicy` — Pembaruan kebijakan	Manajer Insiden menambahkan izin baru yang memungkinkan Manajer Insiden mempublikasikan metrik dalam `AWS/Usage` namespace ke akun Anda.	Januari 27, 2025
AWSIncidentManagerIncidentAccessServiceRolePolicy — Pembaruan kebijakan	Manajer Insiden telah menambahkan izin baru untuk`AWSIncidentManagerIncidentAccessServiceRolePolicy` , untuk mendukung fitur Temuan, yang memungkinkannya memeriksa apakah sebuah EC2 instance	Februari 20, 2024

Perubahan	Deskripsi	Tanggal
	merupakan bagian dari grup Auto Scaling.	
`AWSIncidentManager IncidentAccessServiceRolePolicy` – Kebijakan baru	Manajer Insiden menambahkan kebijakan baru yang memberikan izin Manajer Insiden untuk memanggil orang lain Layanan AWS sebagai bagian dari mengelola insiden.	17 November 2023
`AWSIncidentManager ServiceRolePolicy` — Pembaruan kebijakan	Manajer Insiden menambahkan izin baru yang memungkinkan Manajer Insiden mempublikasikan metrik ke akun Anda.	Desember 16, 2022
`AWSIncidentManager ResolverAccess` – Kebijakan baru	Manajer Insiden menambahkan kebijakan baru untuk memungkinkan Anda memulai insiden, daftar rencana respons, mencantumkan insiden, memperbarui insiden, membuat daftar peristiwa garis waktu, membuat peristiwa garis waktu khusus, memperbarui peristiwa garis waktu khusus, menghapus peristiwa garis waktu khusus, mencantumkan item terkait, membuat item terkait, dan memperbarui item terkait.	26 April 2021

Perubahan	Deskripsi	Tanggal
`AWSIncidentManagerServiceRolePolicy` – Kebijakan baru	Manajer Insiden menambahkan kebijakan baru untuk memberikan izin Manajer Insiden untuk membuat daftar insiden, membuat peristiwa garis waktu, membuat OpsItems, mengaitkan item terkait OpsItems, dan memulai keterlibatan yang terkait dengan insiden.	26 April 2021
Manajer Insiden mulai melacak perubahan	Manajer Insiden mulai melacak perubahan untuk kebijakan yang AWS dikelola.	26 April 2021

Memecahkan masalah Manajer Insiden AWS Systems Manager identitas dan akses

Gunakan informasi berikut untuk membantu Anda mendiagnosis dan memperbaiki masalah umum yang mungkin Anda temui saat bekerja dengan Manajer Insiden dan IAM.

Topik

- Saya tidak berwenang untuk melakukan tindakan di Manajer Insiden
- Saya tidak berwenang untuk melakukan iam: PassRole
- Saya ingin mengizinkan orang di luar akun Amazon Web Services saya untuk mengakses sumber daya Manajer Insiden saya

Saya tidak berwenang untuk melakukan tindakan di Manajer Insiden

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 `ssm-incidents:`*`GetWidget`* rekaan.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform: ssm-
incidents: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 `ssm-incidents:`*`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 bahwa Anda tidak berwenang untuk melakukan `iam:PassRole` tindakan, kebijakan Anda harus diperbarui agar Anda dapat meneruskan peran ke Manajer Insiden.

Beberapa Layanan AWS memungkinkan Anda untuk meneruskan peran yang ada ke layanan tersebut alih-alih membuat peran layanan baru atau peran terkait layanan. Untuk melakukannya, Anda harus memiliki izin untuk meneruskan peran ke layanan.

Contoh kesalahan berikut terjadi ketika pengguna IAM bernama `marymajor` mencoba menggunakan konsol untuk melakukan tindakan di Manajer Insiden. 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 akun Amazon Web Services saya untuk mengakses sumber daya Manajer Insiden 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 mengetahui apakah Manajer Insiden mendukung fitur ini, lihatBagaimana Manajer Insiden AWS Systems Manager 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.

Bekerja dengan kontak bersama dan rencana respons di Manajer Insiden

Dengan berbagi kontak, sebagai pemilik kontak, Anda dapat berbagi informasi kontak, rencana eskalasi, dan keterlibatan dengan orang lain Akun AWS atau dalam organisasi. AWS

Dengan berbagi rencana respons, sebagai pemilik rencana respons, Anda dapat berbagi rencana respons dan insiden terkait dengan orang lain Akun AWS atau di dalam AWS organisasi.

Pemilik rencana kontak atau respons dapat berbagi kontak dan rencana respons dengan:

- Khusus Akun AWS di dalam atau di luar organisasinya di AWS Organizations

- Unit organisasi di dalam organisasinya di AWS Organizations
- Seluruh organisasinya di AWS Organizations

Daftar Isi

- Prasyarat untuk berbagi kontak dan rencana respons
- Layanan terkait
- Berbagi rencana kontak atau respons
- Berhenti berbagi kontak bersama atau rencana tanggapan
- Mengidentifikasi kontak bersama atau rencana tanggapan
- Izin rencana kontak dan respons bersama
- Tagihan dan pengukuran
- Batas instans

Prasyarat untuk berbagi kontak dan rencana respons

Untuk berbagi kontak atau rencana tanggapan dengan organisasi atau unit organisasi Anda di AWS Organizations:

- Anda harus memiliki sumber daya di Anda Akun AWS. Anda tidak dapat membagikan kontak atau paket respons yang telah dibagikan kepada Anda.
- Anda harus mengaktifkan berbagi dengan AWS Organizations. Untuk informasi selengkapnya, lihat Mengaktifkan Berbagi dengan AWS Organizations di Panduan AWS RAM Pengguna.

Layanan terkait

Berbagi rencana kontak dan respons terintegrasi dengan AWS Resource Access Manager (AWS RAM). Dengan AWS RAM, Anda dapat berbagi AWS sumber daya Anda dengan apa pun Akun AWS atau melalui AWS Organizations. Anda berbagi sumber daya yang Anda miliki dengan membuat pembagian sumber daya. Pembagian sumber daya menentukan sumber daya yang akan dibagikan, dan konsumen yang akan dibagikan. Konsumen dapat berupa individu Akun AWS, unit organisasi, atau seluruh organisasi di AWS Organizations.

Untuk informasi selengkapnya AWS RAM, lihat Panduan AWS RAM Pengguna.

Berbagi rencana kontak atau respons

Setelah Anda membagikan rencana respons, konsumen memiliki akses ke semua insiden masa lalu, saat ini, dan masa depan yang dibuat menggunakan rencana respons tersebut.

Setelah Anda berbagi kontak, konsumen memiliki akses ke informasi kontak, rencana keterlibatan, rencana eskalasi, dan keterlibatan yang terjadi selama insiden. Konsumen juga dapat melakukan kontak atau rencana eskalasi selama insiden.

Jika Anda bagian dari organisasi AWS Organizations dan berbagi dalam organisasi Anda diaktifkan, konsumen di organisasi Anda secara otomatis diberikan akses ke kontak bersama atau paket respons. Jika tidak, konsumen menerima undangan untuk bergabung dengan pembagian sumber daya dan diberikan akses ke kontak bersama atau rencana tanggapan setelah menerima undangan.

Anda dapat membagikan paket kontak atau respons yang Anda miliki dengan menggunakan AWS RAM konsol atau AWS CLI.

> **Note**
>
> Saat ini, kemampuan untuk menambahkan kontak yang dibagikan dari akun lain ke paket respons tidak didukung.

Untuk berbagi kontak atau paket respons yang Anda miliki dengan menggunakan AWS RAM konsol

Lihat Membuat Sumber Daya Bersama di Panduan Pengguna AWS RAM .

Untuk berbagi kontak atau rencana tanggapan yang Anda miliki dengan menggunakan AWS CLI

Gunakan perintah create-resource-share.

Berhenti berbagi kontak bersama atau rencana tanggapan

Ketika pemilik sumber daya berhenti berbagi kontak atau rencana respons dengan konsumen, kontak, rencana respons, rencana eskalasi, keterlibatan, dan insiden tidak lagi muncul di konsol konsumen.

> **Note**
>
> Konsumen terus melihat kontak, rencana respons, rencana eskalasi, keterlibatan, atau insiden tanpa pembaruan, jika mereka melihatnya di konsol, hingga mereka menyegarkan halaman atau menjauh dari halaman.

Untuk berhenti berbagi kontak bersama atau rencana respons yang Anda miliki, Anda harus menghapusnya dari pembagian sumber daya. Anda dapat melakukan ini dengan menggunakan AWS RAM konsol atau AWS CLI.

Untuk berhenti berbagi kontak bersama atau paket respons yang Anda miliki dengan menggunakan AWS RAM konsol

Lihat Memperbarui Sumber Daya Bersama di Panduan Pengguna AWS RAM .

Untuk berhenti berbagi kontak bersama atau rencana respons yang Anda miliki dengan menggunakan AWS CLI

Gunakan perintah disassociate-resource-share.

Mengidentifikasi kontak bersama atau rencana tanggapan

Pemilik dan konsumen dapat mengidentifikasi kontak bersama dan rencana respons dengan menggunakan konsol Manajer Insiden dan AWS CLI.

Untuk mengidentifikasi kontak bersama atau rencana respons dengan menggunakan konsol Manajer Insiden

> **Note**
>
> Kontak, rencana respons, rencana eskalasi, keterlibatan, dan insiden umumnya tidak dapat diidentifikasi sebagai sumber daya bersama di konsol Manajer Insiden. Di tempat-tempat di mana Nama Sumber Daya Amazon (ARN) terlihat, ARN berisi ID akun pemilik.

Untuk mengidentifikasi kontak bersama atau rencana respons dengan menggunakan AWS CLI

Gunakan ListContactsperintah ListResponsePlansatau. Perintah mengembalikan kontak dan rencana respons yang Anda miliki serta rencana kontak dan respons yang dibagikan dengan Anda. ARN menunjukkan Akun AWS ID pemilik kontak atau rencana respons.

Izin rencana kontak dan respons bersama

Izin untuk pemilik

Pemilik dapat memperbarui, melihat, berbagi, berhenti berbagi, dan menggunakan kontak dan rencana respons. Kontak dan rencana respons mencakup keterlibatan dan insiden terkait.

Izin untuk konsumen

Konsumen hanya dapat menggunakan dan melihat rencana respons dan kontak. Kontak dan rencana respons mencakup keterlibatan dan insiden terkait.

Tagihan dan pengukuran

Pemilik sumber daya ditagih untuk sumber daya tersebut. Konsumen tidak ditagih untuk sumber daya yang dibagikan dengan mereka. Tidak ada biaya tambahan yang terkait dengan berbagi sumber daya.

Batas instans

Berbagi sumber daya tidak memengaruhi batas sumber daya di akun pemilik atau konsumen. Hanya akun pemilik yang digunakan untuk menghitung batas sumber daya.

Validasi kepatuhan untuk Manajer Insiden AWS Systems Manager

Auditor pihak ketiga menilai keamanan dan kepatuhan Manajer Insiden AWS Systems Manager sebagai bagian dari beberapa program AWS kepatuhan. Program ini mencakup SOC, PCI, FedRAMP, HIPAA, dan lainnya.

Untuk mempelajari apakah an Layanan AWS berada dalam lingkup program kepatuhan tertentu, lihat Layanan AWS di Lingkup oleh Program Kepatuhan Layanan AWS dan pilih program kepatuhan yang Anda minati. Untuk informasi umum, lihat Program AWS Kepatuhan Program AWS .

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

Tanggung jawab kepatuhan Anda saat menggunakan Layanan AWS ditentukan oleh sensitivitas data Anda, tujuan kepatuhan perusahaan Anda, dan hukum dan peraturan yang berlaku. AWS menyediakan sumber daya berikut untuk membantu kepatuhan:

- Kepatuhan dan Tata Kelola Keamanan – Panduan implementasi solusi ini membahas pertimbangan arsitektur serta memberikan langkah-langkah untuk menerapkan fitur keamanan dan kepatuhan.
- Referensi Layanan yang Memenuhi Syarat HIPAA — Daftar layanan yang memenuhi syarat HIPAA. Tidak semua memenuhi Layanan AWS syarat HIPAA.
- AWS Sumber Daya AWS — Kumpulan buku kerja dan panduan ini mungkin berlaku untuk industri dan lokasi Anda.
- AWS Panduan Kepatuhan Pelanggan - Memahami model tanggung jawab bersama melalui lensa kepatuhan. Panduan ini merangkum praktik terbaik untuk mengamankan Layanan AWS dan memetakan panduan untuk kontrol keamanan di berbagai kerangka kerja (termasuk Institut Standar dan Teknologi Nasional (NIST), Dewan Standar Keamanan Industri Kartu Pembayaran (PCI), dan Organisasi Internasional untuk Standardisasi (ISO)).
- Mengevaluasi Sumber Daya dengan Aturan dalam Panduan AWS Config Pengembang — AWS Config Layanan menilai seberapa baik konfigurasi sumber daya Anda mematuhi praktik internal, pedoman industri, dan peraturan.
- AWS Security Hub— Ini Layanan AWS memberikan pandangan komprehensif tentang keadaan keamanan Anda di dalamnya AWS. Security Hub menggunakan kontrol keamanan untuk sumber daya AWS Anda serta untuk memeriksa kepatuhan Anda terhadap standar industri keamanan dan praktik terbaik. Untuk daftar layanan dan kontrol yang didukung, lihat Referensi kontrol Security Hub.
- Amazon GuardDuty — Ini Layanan AWS mendeteksi potensi ancaman terhadap beban kerja Akun AWS, kontainer, dan data Anda dengan memantau lingkungan Anda untuk aktivitas mencurigakan dan berbahaya. GuardDuty dapat membantu Anda mengatasi berbagai persyaratan kepatuhan, seperti PCI DSS, dengan memenuhi persyaratan deteksi intrusi yang diamanatkan oleh kerangka kerja kepatuhan tertentu.
- AWS Audit ManagerIni Layanan AWS membantu Anda terus mengaudit AWS penggunaan Anda untuk menyederhanakan cara Anda mengelola risiko dan kepatuhan terhadap peraturan dan standar industri.

Ketahanan di Manajer Insiden AWS Systems Manager

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 Availability Zone, Anda dapat mendesain dan mengoperasikan aplikasi dan basis data yang secara otomatis

mengalami kegagalan 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.

Manajer Insiden adalah layanan global-regional dan saat ini tidak mendukung Availability Zone.

Selain infrastruktur AWS global, Manajer Insiden menawarkan beberapa fitur untuk membantu mendukung ketahanan data dan kebutuhan cadangan Anda. Selama penyihir Persiapan Anda diminta untuk menyiapkan set replikasi. Kumpulan replikasi regional ini memastikan bahwa data dan sumber daya Anda dapat diakses dari beberapa Wilayah, membuat manajemen insiden di seluruh jaringan cloud lebih mudah dikelola. Replikasi ini juga memastikan bahwa data Anda aman dan dapat diakses jika salah satu Wilayah Anda mati.

Untuk informasi selengkapnya tentang menggunakan set replikasi Manajer Insiden, lihatMengkonfigurasi set replikasi Manajer Insiden.

Keamanan infrastruktur di Manajer Insiden AWS Systems Manager

Sebagai layanan terkelola, Manajer Insiden AWS Systems Manager 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 Incident Manager 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.

Bekerja dengan Manajer Insiden AWS Systems Manager dan antarmuka titik akhir VPC ()AWS PrivateLink

Anda dapat membuat koneksi pribadi antara VPC Anda dan Manajer Insiden AWS Systems Manager dengan membuat antarmuka VPC endpoint. Titik akhir antarmuka didukung oleh AWS PrivateLink. Dengan AWS PrivateLink, Anda dapat mengakses operasi API Manajer Insiden secara pribadi tanpa gateway internet, perangkat NAT, koneksi VPN, atau AWS Direct Connect koneksi.. Instans di VPC Anda tidak memerlukan alamat IP publik untuk berkomunikasi dengan operasi API Manajer Insiden. Lalu lintas antara VPC dan Manajer Insiden tetap berada dalam jaringan Amazon.

Setiap titik akhir antarmuka diwakili oleh satu atau beberapa Antarmuka Jaringan Elastis di subnet Anda.

Untuk informasi selengkapnya, lihat Antarmuka VPC endpoint (AWS PrivateLink) dalam Panduan Pengguna Amazon VPC.

Pertimbangan untuk titik akhir VPC Manajer Insiden

Sebelum menyiapkan titik akhir VPC antarmuka untuk Pengelola Insiden, pastikan Anda meninjau properti dan batasan dan kuota titik akhir Antarmuka di Panduan AWS PrivateLink Pengguna Amazon VPC.

Incident Manager mendukung panggilan ke semua tindakan API-nya dari VPC Anda. Untuk menggunakan semua Manajer Insiden, Anda harus membuat dua titik akhir VPC: satu untuk `ssm-incidents` dan satu untuk. `ssm-contacts`

Membuat titik akhir VPC antarmuka untuk Manajer Insiden

Anda dapat membuat titik akhir VPC untuk Pengelola Insiden menggunakan konsol VPC Amazon atau (). AWS Command Line Interface AWS CLI Untuk informasi selengkapnya, lihat Membuat titik akhir antarmuka dalam Panduan Pengguna Amazon VPC.

Buat titik akhir VPC untuk Manajer Insiden menggunakan nama layanan yang didukung untuk Manajer Insiden di Anda. Wilayah AWS Contoh berikut menunjukkan format titik akhir antarmuka untuk IPv4 dan titik akhir dual-stack.

IPv4 format titik akhir

- `com.amazonaws.`*`region`*`.ssm-incidents`
- `com.amazonaws.`*`region`*`.ssm-contacts`

Format titik akhir tumpukan ganda (IPv4 dan IPv6)

- `aws.api.region.ssm-incidents`
- `aws.api.region.ssm-contacts`

Untuk daftar titik akhir yang didukung untuk semua Wilayah, lihat titik akhir dan kuota Manajer AWS Systems Manager Insiden di Panduan Referensi AWS Umum.

Jika Anda mengaktifkan DNS pribadi untuk titik akhir antarmuka, Anda dapat membuat permintaan API ke Manajer Insiden menggunakan nama DNS Regional default dalam format. Contoh berikut menunjukkan format nama DNS Regional default.

- `ssm-incidents.region.amazonaws.com`
- `ssm-contacts.region.amazonaws.com`

Untuk informasi selengkapnya, lihat Mengakses layanan melalui titik akhir antarmuka dalam Panduan Pengguna Amazon VPC.

Membuat kebijakan titik akhir VPC untuk Manajer Insiden

Anda dapat melampirkan kebijakan titik akhir ke titik akhir VPC Anda yang mengontrol akses ke Manajer Insiden. Kebijakan titik akhir menentukan informasi berikut:

- Prinsipal yang dapat melakukan tindakan.
- Tindakan yang dapat dilakukan.
- Sumber daya di mana tindakan ini dapat dilakukan.

Untuk informasi selengkapnya, lihat Mengontrol Akses ke Layanan dengan titik akhir VPC dalam Panduan Pengguna Amazon VPC.

Contoh: Kebijakan titik akhir VPC untuk tindakan Manajer Insiden

Berikut ini adalah contoh kebijakan endpoint untuk Manajer Insiden. Saat dilampirkan ke titik akhir, kebijakan ini memberikan akses ke tindakan Manajer Insiden yang terdaftar untuk semua prinsip di semua sumber daya.

```
{
```

```
    "Statement":[
       {
          "Principal":"*",
          "Effect":"Allow",
          "Action":[
             "ssm-contacts:ListContacts",
             "ssm-incidents:ListResponsePlans",
             "ssm-incidents:StartIncident"
          ],
          "Resource":"*"
       }
    ]
}
```

Analisis konfigurasi dan kerentanan di Manajer Insiden

Konfigurasi dan kontrol TI adalah tanggung jawab bersama antara AWS dan Anda, pelanggan kami. Untuk informasi selengkapnya, lihat model tanggung jawab AWS bersama.

Praktik terbaik keamanan di Manajer Insiden AWS Systems Manager

Manajer Insiden AWS Systems Manager menyediakan banyak fitur keamanan untuk dipertimbangkan saat Anda mengembangkan dan menerapkan kebijakan keamanan Anda sendiri. Praktik terbaik berikut adalah pedoman umum dan tidak mewakili solusi keamanan yang lengkap. Karena praktik terbaik ini mungkin tidak sesuai atau cukup untuk lingkungan Anda, anggap sebagai pertimbangan yang membantu dan bukan sebagai resep.

Topik

- Praktik terbaik keamanan preventif untuk Manajer Insiden
- Praktik terbaik keamanan Detektif untuk Manajer Insiden

Praktik terbaik keamanan preventif untuk Manajer Insiden

Terapkan akses hak akses paling rendah

Saat memberikan izin, Anda memutuskan siapa yang mendapatkan izin apa untuk sumber daya Manajer Insiden mana. Anda mengaktifkan tindakan tertentu yang ingin Anda izinkan pada

sumber daya tersebut. Oleh karena itu, berikan hanya izin yang diperlukan untuk melakukan tugas. Menerapkan akses hak akses paling rendah adalah hal mendasar dalam mengurangi risiko keamanan dan dampak yang dapat diakibatkan oleh kesalahan atau niat jahat.

Alat bantu berikut tersedia untuk menerapkan akses hak akses paling rendah:

- Mengontrol akses ke AWS sumber daya menggunakan kebijakan dan batas Izin untuk entitas IAM
- Kebijakan Kontrol Layanan

Membuat dan mengelola kontak

Saat mengaktifkan kontak, Manajer Insiden menjangkau perangkat untuk mengonfirmasi aktivasi. Pastikan informasi perangkat sudah benar sebelum mengaktifkan perangkat. Ini mengurangi kemungkinan bahwa Manajer Insiden menghubungi perangkat atau orang yang salah selama aktivasi.

Tinjau kontak dan rencana eskalasi Anda secara teratur untuk memastikan bahwa hanya kontak yang perlu dihubungi selama insiden yang dihubungi. Tinjau kontak secara teratur untuk menghapus informasi yang sudah ketinggalan zaman atau salah. Jika kontak tidak lagi diberi tahu saat insiden terjadi, hapus mereka dari rencana eskalasi terkait atau hapus dari Manajer Insiden.

Jadikan saluran obrolan pribadi

Anda dapat menjadikan saluran obrolan insiden Anda pribadi untuk menerapkan akses hak istimewa paling sedikit. Pertimbangkan untuk menggunakan saluran obrolan yang berbeda dengan daftar pengguna cakupan bawah untuk setiap templat rencana respons. Ini memastikan hanya responden yang benar yang ditarik ke saluran obrolan yang mungkin berisi informasi sensitif.

Slack saluran yang dibuat di Amazon Q Developer dalam aplikasi obrolan mewarisi izin peran IAM yang digunakan untuk mengonfigurasi Pengembang Amazon Q dalam aplikasi obrolan. Ini memungkinkan responden di Pengembang Amazon Q dalam aplikasi obrolan diaktifkan Slack saluran untuk memanggil tindakan apa pun yang tercantum dalam daftar izin, seperti Manajer Insiden APIs dan mengambil grafik metrik.

Tetap perbarui AWS alat

AWS secara teratur merilis versi terbaru dari alat dan plugin yang dapat Anda gunakan dalam AWS operasi Anda. Memperbarui sumber daya ini untuk memastikan pengguna dan instans di akun Anda memiliki akses ke fitur fungsionalitas dan keamanan terbaru di alat ini.

- AWS CLI — The AWS Command Line Interface (AWS CLI) adalah alat open source yang memungkinkan Anda untuk berinteraksi dengan AWS layanan menggunakan perintah di shell baris perintah Anda. Untuk memperbarui AWS CLI, Anda menjalankan perintah yang sama yang digunakan untuk menginstal AWS CLI. Kami merekomendasikan membuat tugas terjadwal pada mesin lokal Anda untuk menjalankan perintah yang sesuai untuk sistem operasi Anda setidaknya sekali setiap dua minggu. Untuk informasi tentang perintah instalasi, lihat Menginstal Antarmuka Baris AWS Perintah di Panduan Pengguna Antarmuka Baris AWS Perintah.
- AWS Tools for Windows PowerShell — Alat untuk Windows PowerShell adalah seperangkat PowerShell modul yang dibangun di atas fungsionalitas yang diekspos oleh AWS SDK for .NET. Alat untuk Windows PowerShell memungkinkan Anda untuk melakukan skrip operasi pada AWS sumber daya Anda dari baris PowerShell perintah. Secara berkala, saat versi terbaru dari Alat untuk Windows PowerShell dirilis, Anda harus memperbarui versi yang Anda jalankan secara lokal. Untuk selengkapnya, lihat AWS Tools for Windows PowerShell Memperbarui Windows atau Memperbarui AWS Tools for Windows PowerShell di Linux atau macOS.

Konten terkait

Praktik terbaik keamanan untuk Systems Manager

Praktik terbaik keamanan Detektif untuk Manajer Insiden

Identifikasi dan audit semua sumber daya Manajer Insiden Anda

Identifikasi aset IT Anda adalah aspek penting dari tata kelola dan keamanan. Identifikasi sumber daya Systems Manager Anda untuk menilai postur keamanan mereka dan mengambil tindakan pada area kelemahan potensial. Buat grup sumber daya untuk sumber daya Manajer Insiden Anda. Untuk informasi selengkapnya, lihat Apa yang dimaksud dengan grup sumber daya? dalam AWS Resource Groups Panduan Pengguna.

Gunakan AWS CloudTrail

AWS CloudTrail menyediakan catatan tindakan yang diambil oleh pengguna, peran, atau AWS layanan di Manajer Insiden. Dengan menggunakan informasi yang dikumpulkan oleh AWS CloudTrail, Anda dapat menentukan permintaan yang dibuat untuk Manajer Insiden, alamat IP dari mana permintaan dibuat, siapa yang membuat permintaan, kapan dibuat, dan detail tambahan. Untuk informasi selengkapnya, lihat Logging panggilan Manajer Insiden AWS Systems Manager API menggunakan AWS CloudTrail.

Pantau saran AWS keamanan

Periksa secara teratur nasihat keamanan yang diposting di Trusted Advisor untuk Anda Akun AWS. Anda dapat melakukan ini secara terprogram menggunakan. describe-trusted-advisor-checks

Selanjutnya, secara aktif memantau alamat email utama yang terdaftar untuk masing-masing Anda Akun AWS. AWS akan menghubungi Anda, menggunakan alamat email ini, tentang masalah keamanan yang muncul yang mungkin memengaruhi Anda.

AWS Masalah operasional dengan dampak luas diposting di AWS Service Health Dashboard. Masalah operasional juga diposting ke akun individu melalui AWS Health Dashboard. Lihat informasi yang lebih lengkap dalam dokumentasi AWS Health.

Konten terkait

Amazon Web Services: Gambaran Umum Proses Keamanan (whitepaper)

Memulai: Ikuti Praktik Terbaik Keamanan saat Anda Mengkonfigurasi AWS Sumber Daya Anda (Blog AWS Keamanan)

Praktik Terbaik IAM

Praktik Terbaik Keamanan di AWS CloudTrail

Pemantauan di Manajer Insiden

AWS Systems Manager Incident Manager terintegrasi dengan layanan berikut yang menawarkan kemampuan pemantauan dan pencatatan:

CloudWatch metrik

Gunakan CloudWatch metrik untuk mengambil statistik tentang titik data untuk operasi Manajer Insiden AWS Systems Manager Anda sebagai kumpulan data deret waktu yang diurutkan, yang dikenal sebagai metrik. Anda dapat menggunakan metrik ini untuk memverifikasi bahwa sistem Anda bekerja sesuai harapan. Untuk informasi selengkapnya, lihat Metrik pemantauan di Manajer Insiden dengan Amazon CloudWatch.

CloudTrail log

Gunakan AWS CloudTrail untuk menangkap informasi terperinci tentang panggilan yang dilakukan AWS APIs. Anda dapat menyimpan panggilan ini sebagai file log di Amazon Simple Storage Service.. Anda dapat menggunakan CloudTrail log ini untuk menentukan informasi seperti panggilan mana yang dibuat, alamat IP sumber dari mana panggilan itu berasal, siapa yang melakukan panggilan, dan kapan panggilan dilakukan. CloudTrail Log berisi informasi tentang panggilan ke tindakan API untuk Manajer Insiden. lUntuk informasi selengkapnya, lihatLogging panggilan Manajer Insiden AWS Systems Manager API menggunakan AWS CloudTrail.

Trusted Advisor

AWS Trusted Advisor dapat membantu Anda memantau AWS sumber daya Anda untuk meningkatkan kinerja, keandalan, keamanan, dan efektivitas biaya. Empat Trusted Advisor cek tersedia untuk semua pengguna; lebih dari 50 cek tersedia untuk pengguna dengan paket dukungan Bisnis atau Perusahaan. Untuk Manajer Insiden, Trusted Advisor periksa apakah konfigurasi set replikasi menggunakan lebih dari satu Wilayah AWS untuk mendukung failover dan respons regional. Untuk informasi lebih lanjut, lihat AWS Trusted Advisor dalam Panduan Pengguna AWS Dukungan .

Metrik pemantauan di Manajer Insiden dengan Amazon CloudWatch

Incident Manager menyediakan metrik agregat yang dapat Anda pantau di Amazon. CloudWatch Anda dapat menggunakan metrik ini untuk mengidentifikasi tren rencana insiden dan respons.

Metrik ini meliputi:

- Jumlah insiden yang dibuat selama periode waktu tertentu
- Waktu untuk menanggapi dan menyelesaikan insiden tersebut
- Jumlah insiden yang diselesaikan

Anda dapat memantau metrik Manajer Insiden untuk lebih memahami kesehatan operasional Anda, dan mengambil tindakan yang berarti untuk mendorong keunggulan operasional respons insiden Anda. Metrik Manajer Insiden tersedia di semua Wilayah Manajer Insiden. Metrik Anda akan tersedia untuk dilihat di Amazon CloudWatch untuk semua Wilayah yang Anda tentukan dalam set replikasi saat masuk ke Manajer Insiden. Anda dapat melihat metrik yang dipublikasikan di Wilayah tempat tindakan untuk insiden tersebut diambil. Tidak ada biaya tambahan untuk metrik ini.

Di CloudWatch konsol, Anda dapat membuat dasbor dengan metrik berikut untuk:

- Ukur dan tinjau beban insiden yang ada
- Lacak apakah beban insiden Anda meningkat, menurun, atau tetap sama
- Lebih efektif menggunakan Manajer Insiden untuk mengurangi frekuensi, durasi, dan dampak insiden Anda

Halaman ini menjelaskan metrik Manajer Insiden yang tersedia di CloudWatch konsol.

> **Important**
>
> Untuk peristiwa yang dibuat pelanggan, jika nilai sumber dalam `TriggerDetails` diberi nama menggunakan karakter non-ASCII, metrik untuk acara tersebut tidak akan dilaporkan dalam metrik Amazon CloudWatch , yang tidak mendukung teks non-ASCII. `source`dapat disediakan secara terprogram saja, seperti dengan menggunakan SDK atau. AWS CLI

Manajer Insiden mengirimkan metrik berikut ke CloudWatch.

Metrik	Deskripsi
`NumberOfCreateIncidents`	Jumlah insiden yang dibuat.

Metrik	Deskripsi
	Dimensi Valid: [] (Dimensi kosong), [`ResponsePlan Impact`], [], [`Source`], [`ResponsePlan ,Impact`], [`ResponsePlan ,Source`] Unit: Jumlah
`NumberOfResolveIncidents`	Jumlah insiden diselesaikan. Dimensi Valid: [] (Dimensi kosong), [`ResponsePlan Impact`], [], [`Source`], [`ResponsePlan ,Impact`], [`ResponsePlan ,Source`] Unit: Jumlah
`TimeToFirstAcknowledgement`	Perbedaan waktu antara insiden menciptakan waktu dan waktu pengakuan pertama dibuat untuk insiden tersebut. Dimensi Valid: [] (Dimensi kosong), [`ResponsePlan Impact`], [], [`Source`], [`ResponsePlan ,Impact`], [`ResponsePlan ,Source`] Unit: Detik
`TimeToResolveIncident`	Perbedaan waktu antara kapan insiden itu dibuat dan kapan itu diselesaikan. Dimensi yang Valid:] (Dimensi kosong), [`ResponsePlan Impact`], [`Source`], [`ResponsePlan ,Impact`], [`ResponsePlan ,Source`] Unit: Detik

Melihat metrik Manajer Insiden di konsol CloudWatch

Untuk melihat metrik Manajer Insiden di konsol CloudWatch

1. Buka CloudWatch konsol di https://console.aws.amazon.com/cloudwatch/.

2. Di panel navigasi, pilih Metrik.
3. Pilih `IncidentManager` namespace.
4. Pada tab Metrik, pilih dimensi, lalu pilih metrik.

Untuk informasi selengkapnya tentang bekerja dengan CloudWatch metrik, lihat topik berikut di Panduan CloudWatch Pengguna Amazon:

- Metrik-metrik
- Menggunakan CloudWatch metrik Amazon

Dimensi untuk Metrik

Metrik Incident Manager menggunakan `IncidentManager` namespace dan menyediakan metrik untuk dimensi berikut:

Dimensi	Deskripsi
`By Response Plan`	Lihat metrik agregat berdasarkan rencana respons.
`By Impact Level`	Lihat metrik agregat berdasarkan tingkat keparahan.
`By Source`	Lihat metrik untuk insiden yang dibuat secara manual, berdasarkan CloudWatch alarm, atau EventBridge peristiwa.
`Across All Incidents`	Lihat metrik agregat untuk semua insiden di Wilayah saat ini. AWS
`Response Plan name and Source`	Lihat metrik agregat untuk setiap kombinasi rencana respons dan sumber.
`Response Plan Name and Impact Level`	Lihat metrik agregat untuk setiap kombinasi rencana respons dan tingkat keparahan.

Logging panggilan Manajer Insiden AWS Systems Manager API menggunakan AWS CloudTrail

Manajer Insiden AWS Systems Manager terintegrasi dengan AWS CloudTrail, layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atau Layanan AWS. CloudTrail menangkap semua panggilan API untuk Manajer Insiden sebagai peristiwa. Panggilan yang diambil termasuk panggilan dari konsol Manajer Insiden dan panggilan kode ke operasi API Manajer Insiden. Dengan menggunakan informasi yang dikumpulkan oleh CloudTrail, Anda dapat menentukan permintaan yang dibuat untuk Manajer Insiden, alamat IP dari mana permintaan dibuat, kapan dibuat, dan detail tambahan.

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

- Baik permintaan tersebut dibuat dengan kredensial pengguna root atau pengguna.
- Apakah permintaan dibuat atas nama pengguna IAM Identity Center.
- Apakah permintaan tersebut dibuat dengan kredensial keamanan sementara untuk satu peran atau pengguna gabungan.
- Apakah permintaan tersebut dibuat oleh Layanan AWS lain.

CloudTrail aktif di Anda Akun AWS ketika Anda membuat akun dan Anda secara otomatis memiliki akses ke riwayat CloudTrail Acara. Riwayat CloudTrail Acara menyediakan catatan yang dapat dilihat, dapat dicari, dapat diunduh, dan tidak dapat diubah dari 90 hari terakhir dari peristiwa manajemen yang direkam dalam file. Wilayah AWS Untuk informasi selengkapnya, lihat Bekerja dengan riwayat CloudTrail Acara di Panduan AWS CloudTrail Pengguna. Tidak ada CloudTrail biaya untuk melihat riwayat Acara.

Untuk catatan acara yang sedang berlangsung dalam 90 hari Akun AWS terakhir Anda, buat jejak atau penyimpanan data acara CloudTrailDanau.

CloudTrail jalan setapak

> Jejak memungkinkan CloudTrail untuk mengirimkan file log ke bucket Amazon S3. Semua jalur yang dibuat menggunakan AWS Management Console Multi-region. Anda dapat membuat jalur Single-region atau Multi-region dengan menggunakan. AWS CLI Membuat jejak Multi-wilayah disarankan karena Anda menangkap aktivitas Wilayah AWS di semua akun Anda. Jika Anda membuat jejak wilayah Tunggal, Anda hanya dapat melihat peristiwa yang dicatat di jejak.

Wilayah AWS Untuk informasi selengkapnya tentang jejak, lihat Membuat jejak untuk Anda Akun AWS dan Membuat jejak untuk organisasi di Panduan AWS CloudTrail Pengguna.

Anda dapat mengirimkan satu salinan acara manajemen yang sedang berlangsung ke bucket Amazon S3 Anda tanpa biaya CloudTrail dengan membuat jejak, namun, ada biaya penyimpanan Amazon S3. Untuk informasi selengkapnya tentang CloudTrail harga, lihat AWS CloudTrail Harga. Untuk informasi tentang harga Amazon S3, lihat Harga Amazon S3.

CloudTrail Menyimpan data acara danau

CloudTrail Lake memungkinkan Anda menjalankan kueri berbasis SQL pada acara Anda. CloudTrail Lake mengonversi peristiwa yang ada dalam format JSON berbasis baris ke format Apache ORC. ORC adalah format penyimpanan kolumnar yang dioptimalkan untuk pengambilan data dengan cepat. Peristiwa digabungkan ke dalam penyimpanan data peristiwa, yang merupakan kumpulan peristiwa yang tidak dapat diubah berdasarkan kriteria yang Anda pilih dengan menerapkan pemilih acara tingkat lanjut. Penyeleksi yang Anda terapkan ke penyimpanan data acara mengontrol peristiwa mana yang bertahan dan tersedia untuk Anda kueri. Untuk informasi lebih lanjut tentang CloudTrail Danau, lihat Bekerja dengan AWS CloudTrail Danau di Panduan AWS CloudTrail Pengguna.

CloudTrail Penyimpanan data acara danau dan kueri menimbulkan biaya. Saat Anda membuat penyimpanan data acara, Anda memilih opsi harga yang ingin Anda gunakan untuk penyimpanan data acara. Opsi penetapan harga menentukan biaya untuk menelan dan menyimpan peristiwa, dan periode retensi default dan maksimum untuk penyimpanan data acara. Untuk informasi selengkapnya tentang CloudTrail harga, lihat AWS CloudTrail Harga.

Acara manajemen Manajer Insiden di CloudTrail

Acara manajemen memberikan informasi tentang operasi manajemen yang dilakukan pada sumber daya di Anda Akun AWS. Ini juga dikenal sebagai operasi pesawat kontrol. Secara default, CloudTrail mencatat peristiwa manajemen.

Manajer Insiden AWS Systems Manager mencatat semua operasi pesawat kontrol Manajer Insiden sebagai peristiwa manajemen. Untuk daftar operasi bidang Manajer Insiden AWS Systems Manager kontrol yang dicatat oleh Manajer Insiden CloudTrail, lihat Referensi Manajer Insiden AWS Systems Manager API.

Contoh acara Manajer Insiden

Peristiwa mewakili permintaan tunggal dari sumber manapun dan mencakup informasi tentang operasi API yang diminta, tanggal dan waktu operasi, parameter permintaan, dan sebagainya. CloudTrail file log bukanlah jejak tumpukan yang diurutkan dari panggilan API publik, sehingga peristiwa tidak muncul dalam urutan tertentu.

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan `StartIncident` tindakan.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "1234567890abcdef0",
        "arn": "arn:aws:iam::246873129580111122223333:user/nikki_wolf",
        "accountId": "abcdef01234567890",
        "accessKeyId": "021345abcdef6789",
        "userName": "nikki_wolf"
    },
    "eventTime": "2024-04-22T23:20:10Z",
    "eventSource": "ssm-incidents.amazonaws.com",
    "eventName": "StartIncident",
    "awsRegion": "us-east-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "aws-cli/2.0.58 Python/3.7.4 Darwin/19.6.0 exe/x86_64 command/
ssmincidents.start-incident",
    "requestParameters": {
        "responsePlanArn": "arn:aws:ssm-incidents::555555555555:response-plan/security-
test-response-plan-non-dedupe-v1",
        "clientToken": "12345678-1111-2222-3333-abcdefghijkl"
    },
    "responseElements": {
        "incidentRecordArn": "arn:aws:ssm-incidents::444455556666:incident-record/
security-test-response-plan-non-dedupe-v1/abcdefgh-abcd-1234-1234-1234567890"
    },
    "requestID": "abcdefgh-1234-abcd-1234-1234567abcdef",
    "eventID": "12345678-1234-1234-abcd-abcdef1234567",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "12345678901234567"
```

```
}
```

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan `DeleteContactChannel` tindakan.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "1234567890abcdef0",
        "arn": "arn:aws:iam::246873129580111122223333:user/nikki_wolf",
        "accountId": "abcdef01234567890",
        "accessKeyId": "021345abcdef6789",
        "userName": "nikki_wolf"
    },
    "eventTime": "2024-04-08T02:27:21Z",
    "eventSource": "ssm-contacts.amazonaws.com",
    "eventName": "DeleteContactChannel",
    "awsRegion": "us-east-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Apache-HttpClient/UNAVAILABLE (Java/1.8.0_282)",
    "requestParameters": {
        "contactChannelId": "arn:aws:ssm-contacts:us-west-2:555555555555:device/
bnuomysohc/abcdefgh-abcd-1234-1234-1234567890"
    },
    "responseElements": null,
    "requestID": "abcdefgh-1234-abcd-1234-1234567abcdef",
    "eventID": "12345678-1234-1234-abcd-abcdef1234567",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "12345678901234567"
}
```

Untuk informasi tentang konten CloudTrail rekaman, lihat konten CloudTrail rekaman di Panduan AWS CloudTrail Pengguna.

Integrasi produk dan layanan dengan Manajer Insiden

Manajer Insiden AWS Systems Manager, alat di, terintegrasi dengan produk, layanan, dan alat berikut.

Integrasi dengan Layanan AWS

Manajer Insiden terintegrasi dengan Layanan AWS dan alat yang dijelaskan dalam tabel berikut.

AWS CDK	AWS CDK Ini adalah kerangka kerja pengembangan untuk menggunakan kode untuk menentukan infrastruktur cloud Anda dan menggunakan AWS CloudFormation untuk penyediaan. AWS CDK Mendukung beberapa bahasa pemrograman termasuk TypeScript, JavaScript, Python, Java, dan C #/.Net. Untuk informasi tentang menggunakan Manajer Insiden AWS CDK dengan, lihat bagian berikut di Referensi AWS CDK API: • @aws-cdk/aws-ssmincidents modul • @aws-cdk/aws-ssmcontacts modul
Pengembang Amazon Q dalam aplikasi obrolan	Pengembang Amazon Q dalam aplikasi obrolan memungkinkan DevOps dan tim pengemban gan perangkat lunak untuk menggunakan ruang obrolan program pesan untuk memantau dan menanggapi peristiwa operasional di ruang obrolan mereka AWS Cloud. Menggunakan Amazon Q Developer dalam aplikasi obrolan dengan Manajer Insiden, Anda dapat membuat saluran obrolan yang dapat digunakan responden untuk memantau dan menanggapi insiden. Pengembang Amazon Q dalam aplikasi obrolan mendukung Slack

	ruang obrolan, Microsoft Teams saluran, dan ruang obrolan Amazon Chime sebagai saluran obrolan. Sebagai bagian dari membuat saluran obrolan, Anda juga membuat topik di Amazon Simple Notification Service (Amazon SNS). Amazon SNS adalah layanan terkelola yang menyediakan pengiriman pesan dari penerbit ke pelanggan. Dalam rencana respons insiden, saat Anda mengaitkan saluran obrolan yang telah Anda buat dengan paket, Anda juga memilih satu atau beberapa topik yang terkait dengan saluran obrolan. Topik SNS ini digunakan untuk mengirim pemberitahuan tentang insiden ke responden insiden. Untuk informasi selengkapnya, lihat Membuat dan mengintegrasikan saluran obrolan untuk responden di Manajer Insiden.

AWS CloudFormation	AWS CloudFormation adalah layanan yang dapat Anda gunakan untuk membuat template dengan semua sumber daya yang Anda butuhkan untuk aplikasi Anda, dan kemudian mengkonfigurasi dan menyediakan sumber daya untuk Anda. Ini juga akan mengkonfi gurasi semua dependensi, sehingga Anda dapat lebih fokus pada aplikasi Anda dan kurang mengelola sumber daya. Untuk informasi tentang penggunaan AWS CloudFormation dengan Manajer Insiden, lihat topik berikut di Panduan AWS CloudFormation Pengguna: • Referensi tipe sumber daya Manajer Insiden • Referensi tipe sumber daya referensi tipe sumber daya kontak
Amazon CloudWatch	CloudWatchmemantau AWS sumber daya Anda dan aplikasi yang Anda jalankan AWS secara real time. Anda dapat menggunak an CloudWatch untuk mengumpulkan dan melacak metrik, yang merupakan variabel yang dapat Anda ukur untuk sumber daya dan aplikasi Anda. Anda dapat mengonfigurasi CloudWatch alarm untuk membuat insiden di Manajer Insiden. CloudWatch Bekerja dengan Systems Manager dan Incident Manager untuk membuat insiden dari template rencana respons saat alarm masuk ke status alarm. Untuk informasi selengkapnya, lihat Membuat insiden secara otomatis dengan alarm CloudWatch .

Amazon Chime	Amazon Chime adalah tempat kerja online yang menggabungkan rapat, obrolan, dan panggilan bisnis. Anda dapat bertemu, mengobrol, dan melakukan panggilan bisnis di dalam dan di luar organisasi Anda menggunak an Amazon Chime. Anda dapat mengintegrasikan ruang Amazon Chime ke dalam operasi Manajer Insiden Anda dengan membuat saluran obrolan untuk Amazon Chime di Amazon Q Developer dalam aplikasi obrolan, lalu menambahkan saluran tersebut ke paket respons. Untuk informasi selengkapnya, lihat Membuat dan mengintegrasikan saluran obrolan untuk responden di Manajer Insiden.
Amazon EventBridge	EventBridgeadalah layanan tanpa server yang menggunakan peristiwa untuk menghubun gkan komponen aplikasi, sehingga memudahka n Anda untuk membangun aplikasi berbasis peristiwa yang dapat diskalakan. Anda dapat mengonfigurasi EventBridge aturan untuk melihat pola peristiwa di AWS sumber daya Anda dan membuat insiden di Manajer Insiden saat peristiwa cocok dengan pola yang telah Anda tetapkan. Aturan Anda dapat memantau pola acara di lusinan aplikasi Layanan AWS dan layanan pihak ketiga. Untuk informasi selengkapnya, lihat Membuat insiden secara otomatis dengan acara EventBridge .

AWS Secrets Manager	Secrets Manager membantu Anda mengelola, mengambil, dan memutar kredensyal database, kredensyal aplikasi, OAuth token, kunci API, dan rahasia lainnya sepanjang siklus hidupnya. Ketika Anda mengintegrasikan Manajer Insiden dengan PagerDuty layanan, Anda membuat rahasia di Secrets Manager yang berisi PagerDuty kredensil Anda. Untuk informasi selengkapnya, lihat Menyimpan kredensyal PagerDuty akses secara rahasia AWS Secrets Manager.

AWS Systems Manager	Systems Manager adalah hub operasi yang dapat Anda gunakan untuk melihat dan mengontrol infrastruktur aplikasi Anda dan solusi end-to-end manajemen yang aman untuk lingkungan cloud. Alat Systems Manager berikut terintegrasi langsung dengan Incident Manager: • Automation — Runbook Otomasi mendefini sikan tindakan yang dilakukan Systems Manager pada sumber daya Anda AWS . Di Manajer Insiden, runbook mendefini sikan serangkaian langkah otomatis dan manual untuk digunakan untuk menyelesa ikan insiden Anda. Untuk informasi tentang membuat runbook Otomasi untuk digunakan dengan Manajer Insiden, lihatMengintegrasikan runbook Otomasi Systems Manager di Incident Manager untuk remediasi insiden. • OpsCenter OpsCenter Menyediakan lokasi pusat di mana insinyur operasi dan profesion al TI dapat mengelola item pekerjaan operasional, yang disebut OpsItems, terkait dengan AWS sumber daya. Anda dapat membuat OpsItems langsung dari analisis pasca-insiden untuk menindaklanjuti pekerjaan terkait. Untuk informasi selengkapnya, lihat Menjalankan analisis pasca-insiden di Incident Manager.

AWS Trusted Advisor	Trusted Advisoradalah alat yang tersedia untuk AWS pelanggan dengan paket dukungan Dasar atau Pengembang. Trusted Advisor memeriksa AWS lingkungan Anda, dan kemudian membuat rekomendasi ketika ada peluang untuk menghemat uang, meningkat kan ketersediaan dan kinerja sistem, atau membantu menutup kesenjangan keamanan. Untuk Manajer Insiden, Trusted Advisor periksa apakah konfigurasi set replikasi menggunakan lebih dari satu Wilayah AWS untuk mendukung failover dan respons Regional.

Integrasi dengan produk dan layanan lainnya

Anda dapat mengintegrasikan atau menggunakan Manajer Insiden dengan layanan pihak ketiga yang dijelaskan dalam tabel berikut.

Awan Jira	Dengan menggunakan ini AWS Service Management Connector, Anda dapat menginteg rasikan Incident Manager dengan Jira Cloud (Atlassian), platform alur kerja berbasis cloud pihak ketiga. Setelah Anda mengonfigurasi integrasi dengan Jira Cloud, saat Anda membuat insiden baru di Manajer Insiden, integrasi akan menciptak an insiden di Jira Cloud juga. Jika Anda memperbarui insiden di Manajer Insiden, itu membuat pembaruan ini untuk insiden terkait di Jira Cloud. Jika Anda menyelesaikan insiden di Manajer Insiden atau Jira Cloud, integrasi akan menyelesaikan insiden di kedua layanan berdasarkan preferensi yang Anda konfigura sikan.

	Untuk informasi selengkapnya, lihat Mengintegrasikan Manajer Insiden AWS Systems Manager (Jira Cloud) di Panduan AWS Service Management Connector Administrator.
Manajemen Layanan Jira	Dengan menggunakan ini AWS Service Management Connector, Anda dapat mengintegrasikan Manajer Insiden dengan Jira Service Management, platform alur kerja berbasis cloud pihak ketiga. Setelah Anda mengonfigurasi integrasi dengan Manajemen Layanan Jira, saat Anda membuat insiden baru di Manajer Insiden, integrasi akan menciptakan insiden di Manajemen Layanan Jira juga. Jika Anda memperbarui insiden di Manajer Insiden, itu membuat pembaruan ini untuk insiden terkait di Manajemen Layanan Jira. Jika Anda menyelesaikan insiden di Manajer Insiden atau Manajemen Layanan Jira, integrasi akan menyelesaikan insiden di kedua layanan berdasarkan preferensi yang Anda konfigurasikan. Untuk informasi selengkapnya, lihat Mengonfigurasi Manajemen Layanan JIRA di Panduan AWS Service Management Connector Administrator.

Microsoft Teams	Microsoft Teamsmenyediakan alat berbasis cloud kolaboratif untuk perpesanan tim, konferensi audio dan video, dan berbagi file. Anda dapat mengintegrasikan a Microsoft Teams salurkan ke operasi Manajer Insiden Anda dengan membuat saluran obrolan untuk Microsoft Team di Amazon Q Developer dalam aplikasi obrolan, dan kemudian menambahkan saluran itu ke rencana respons. Untuk informasi selengkapnya, lihat Membuat dan mengintegrasikan saluran obrolan untuk responden di Manajer Insiden.

PagerDuty	PagerDutyadalah alat respons insiden yang mendukung alur kerja paging dan kebijakan eskalasi. Ketika Anda mengintegrasikan Manajer Insiden dengan PagerDuty, Anda dapat menambahk an PagerDuty layanan ke paket respons Anda. Setelah itu, insiden terkait dibuat PagerDuty setiap kali insiden dibuat di Manajer Insiden. Insiden di PagerDuty menggunakan alur kerja paging dan kebijakan eskalasi yang Anda tetapkan di sana selain yang ada di Manajer Insiden. PagerDutymelampirkan peristiwa timeline dari Manajer Insiden sebagai catatan tentang insiden Anda. Untuk mengintegrasikan Manajer Insiden dengan PagerDuty, Anda harus terlebih dahulu membuat rahasia AWS Secrets Manager yang berisi PagerDuty kredensil Anda. Untuk informasi tentang menambahkan Kunci PagerDuty REST API dan detail lain yang diperlukan ke rahasia AWS Secrets Manager, lihatMenyimpan kredensyal PagerDuty akses secara rahasia AWS Secrets Manager. Untuk informasi tentang menambahkan PagerDuty layanan dari PagerDuty akun Anda ke paket respons di Manajer Insiden, lihat langkah-langkah untuk Mengintegrasikan PagerDuty layanan ke dalam paket respons dalam topikMembuat rencana respons.

ServiceNow	Dengan menggunakan ini AWS Service Management Connector, Anda dapat menginteg rasikan Manajer Insiden dengan ServiceNo wplatform alur kerja berbasis cloud pihak ketiga. Setelah Anda mengonfigurasi integrasi dengan ServiceNow, saat Anda membuat insiden baru di Manajer Insiden, integrasi akan membuat insiden ServiceNow juga. Jika Anda memperbarui insiden di Manajer Insiden, itu membuat pembaruan ini untuk insiden terkait di ServiceNow. Jika Anda menyelesaikan insiden di Manajer Insiden atau ServiceNo w, integrasi menyelesaikan insiden di kedua layanan berdasarkan preferensi yang Anda konfigurasikan. Untuk informasi selengkapnya, lihat Menginteg rasikan Manajer Insiden AWS Systems Manager ServiceNow dalam Panduan AWS Service Management Connector Administrator.
Slack	Slackmenyediakan alat berbasis cloud kolaborat if untuk perpesanan tim, konferensi audio dan video, dan berbagi file. Anda dapat mengintegrasikan a Slack salurkan ke operasi Manajer Insiden Anda dengan membuat saluran obrolan untuk Slack di Amazon Q Developer dalam aplikasi obrolan, dan kemudian menambahkan saluran itu ke rencana respons. Untuk informasi selengkapnya, lihat Membuat dan mengintegrasikan saluran obrolan untuk responden di Manajer Insiden.

Terraform	HashiCorp Terraform adalah alat perangkat lunak infrastruktur sumber terbuka sebagai kode (IAc) yang menyediakan alur kerja antarmuka baris perintah (CLI) untuk mengelola berbagai layanan cloud. Untuk Manajer Insiden, Anda dapat menggunakan Terraform untuk mengelola atau menyediakan hal-hal berikut: Sumber daya Kontak Manajer Insiden SSM • aws_ssmcontacts_contact • aws_ssmcontacts_contact_channel • aws_ssmcontacts_plan • aws_ssmcontacts_rotation Sumber data Kontak SSM • aws_ssmcontacts_contact • aws_ssmcontacts_contact_channel • aws_ssmcontacts_plan • aws_ssmcontacts_rotation Sumber daya Manajer Insiden SSM • aws_ssmincidents_replication_set • aws_ssmincidents_response_plan Sumber data Manajer Insiden SSM • aws_ssmincidents_replication_set • aws_ssmincidents_response_plan

Menyimpan kredensyal PagerDuty akses secara rahasia AWS Secrets Manager

Setelah Anda mengaktifkan integrasi dengan PagerDuty untuk rencana respons, Manajer Insiden bekerja dengan PagerDuty cara berikut:

- Manajer Insiden membuat insiden terkait PagerDuty saat Anda membuat insiden baru di Manajer Insiden.
- Alur kerja paging dan kebijakan eskalasi yang Anda buat PagerDuty digunakan di lingkungan. PagerDuty Namun, Manajer Insiden tidak mengimpor PagerDuty konfigurasi Anda.
- Manajer Insiden menerbitkan peristiwa timeline sebagai catatan untuk insiden di PagerDuty, hingga maksimum 2.000 catatan.
- Anda dapat memilih untuk menyelesaikan PagerDuty insiden secara otomatis ketika Anda menyelesaikan insiden terkait di Manajer Insiden.

Untuk mengintegrasikan Manajer Insiden dengan PagerDuty, Anda harus terlebih dahulu membuat rahasia AWS Secrets Manager yang berisi PagerDuty kredensil Anda. Ini memungkinkan Manajer Insiden untuk berkomunikasi dengan PagerDuty layanan Anda. Anda kemudian dapat menyertakan PagerDuty layanan dalam paket respons yang Anda buat di Manajer Insiden.

Rahasia yang Anda buat di Secrets Manager ini harus berisi, dalam format JSON yang tepat, berikut ini:

- Kunci API dari PagerDuty akun Anda. Anda dapat menggunakan Kunci API REST Akses Umum atau Kunci API REST Token Pengguna.
- Alamat email pengguna yang valid dari PagerDuty subdomain Anda.
- Wilayah PagerDuty layanan tempat Anda menerapkan subdomain Anda.

> **Note**
>
> Semua layanan dalam PagerDuty subdomain disebarkan ke wilayah layanan yang sama.

Prasyarat

Sebelum membuat rahasia di Secrets Manager, pastikan Anda memenuhi persyaratan berikut.

Kunci KMS

Anda harus mengenkripsi rahasia yang Anda buat dengan kunci terkelola pelanggan yang telah Anda buat di AWS Key Management Service (AWS KMS). Anda menentukan kunci ini ketika Anda membuat rahasia yang menyimpan PagerDuty kredensyal Anda.

> **Important**
>
> Secrets Manager menyediakan opsi untuk mengenkripsi rahasia dengan Kunci yang dikelola AWS, tetapi mode enkripsi ini tidak didukung.

Kunci yang dikelola pelanggan harus memenuhi persyaratan berikut:

- Jenis kunci: Pilih Simetris.
- Penggunaan kunci: Pilih Enkripsi dan dekripsi.
- Regionalitas: Jika Anda ingin mereplikasi paket respons Anda ke beberapa Wilayah AWS, pastikan Anda memilih kunci Multi-Wilayah.

Kebijakan kunci

Pengguna yang mengonfigurasi paket respons harus memiliki izin untuk `kms:GenerateDataKey` dan `kms:Decrypt` dalam kebijakan berbasis sumber daya kunci. Kepala `ssm-incidents.amazonaws.com` layanan harus memiliki izin untuk `kms:GenerateDataKey` dan `kms:Decrypt` dalam kebijakan berbasis sumber daya kunci.

Kebijakan berikut menunjukkan izin ini. Ganti masing-masing *`user input placeholder`* dengan informasi Anda sendiri.

```
{
    "Version": "2012-10-17",
    "Id": "key-consolepolicy-3",
    "Statement": [
        {
            "Sid": "Enable IAM user permissions",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::account-id:root"
```

```
            },
            "Action": "kms:*",
            "Resource": "*"
        },
        {
            "Sid": "Allow creator of response plan to use the key",
            "Effect": "Allow",
            "Principal": {
                "AWS": "IAM_ARN_of_principal_creating_response_plan"
            },
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey*"
            ],
            "Resource": "*"
        },
        {
            "Sid": "Allow Incident Manager to use the key",
            "Effect": "Allow",
            "Principal": {
                "Service": "ssm-incidents.amazonaws.com"
            },
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey*"
            ],
            "Resource": "*"
        }
    ]
}
```

Untuk informasi tentang membuat kunci terkelola pelanggan baru, lihat Membuat kunci KMS enkripsi simetris di Panduan AWS Key Management Service Pengembang. Untuk informasi selengkapnya tentang AWS KMS kunci, lihat AWS KMS konsep.

Jika kunci terkelola pelanggan yang sudah ada memenuhi semua persyaratan sebelumnya, Anda dapat mengedit kebijakannya untuk menambahkan izin ini. Untuk informasi tentang memperbarui kebijakan dalam kunci terkelola pelanggan, lihat Mengubah kebijakan kunci di Panduan AWS Key Management Service Pengembang.

> **Tip**
>
> Anda dapat menentukan kunci kondisi untuk membatasi akses lebih jauh. Misalnya, kebijakan berikut mengizinkan akses melalui Secrets Manager di Wilayah Timur AS (Ohio) (us-east-2) saja:
>
> ```
> {
>  "Sid": "Enable IM Permissions",
>  "Effect": "Allow",
>  "Principal": {
>  "Service": "ssm-incidents.amazonaws.com"
>  },
>  "Action": ["kms:Decrypt", "kms:GenerateDataKey*"],
>  "Resource": "*",
>  "Condition": {
>  "StringEquals": {
>  "kms:ViaService": "secretsmanager.us-east-2.amazonaws.com"
>  }
>  }
> }
> ```

`GetSecretValue`izin

Identitas IAM (pengguna, peran, atau grup) yang membuat rencana respons harus memiliki izin IAM. `secretsmanager:GetSecretValue`

Untuk menyimpan kredensyal PagerDuty akses secara rahasia AWS Secrets Manager

1. Ikuti langkah-langkah melalui Langkah 3a di Buat AWS Secrets Manager rahasia di Panduan AWS Secrets Manager Pengguna.
2. Untuk Langkah 3b, untuk pasangan kunci/nilai, lakukan hal berikut:
   - Pilih tab Plaintext.
   - Ganti isi default kotak dengan struktur JSON berikut:

```
{
 "pagerDutyToken": "pagerduty-token",
 "pagerDutyServiceRegion": "pagerduty-region",
 "pagerDutyFromEmail": "pagerduty-email"
```

```
}
```

- Dalam sampel JSON yang Anda tempel, ganti *`placeholder values`* sebagai berikut:
  - *`pagerduty-token`*: Nilai Kunci API REST Akses Umum atau Kunci API REST Token Pengguna dari PagerDuty akun Anda.

    Untuk informasi terkait, lihat Kunci Akses API di Pangkalan PagerDuty Pengetahuan.
  - *`pagerduty-region`*: Wilayah layanan pusat PagerDuty data yang menghosting PagerDuty subdomain Anda.

    Untuk informasi terkait, lihat Wilayah Layanan di Pangkalan PagerDuty Pengetahuan.
  - *`pagerduty-email`*: Alamat email yang valid untuk pengguna yang termasuk dalam PagerDuty subdomain Anda.

    Untuk informasi terkait, lihat Mengelola Pengguna di Pangkalan PagerDuty Pengetahuan.

Contoh berikut menunjukkan rahasia JSON lengkap yang berisi PagerDuty kredensil yang diperlukan:

```
{
    "pagerDutyToken": "y_NbAkKc66ryYEXAMPLE",
    "pagerDutyServiceRegion": "US",
    "pagerDutyFromEmail": "JohnDoe@example.com"
}
```

3. Pada Langkah 3c, untuk kunci Enkripsi, pilih kunci terkelola pelanggan yang Anda buat yang memenuhi persyaratan yang tercantum di bagian Prasyarat sebelumnya.
4. Pada Langkah 4c, untuk izin Sumber Daya, lakukan hal berikut:
   - Perluas izin Sumber Daya.
   - Pilih Edit izin.
   - Ganti isi default kotak kebijakan dengan struktur JSON berikut:

```
{
    "Effect": "Allow",
    "Principal": {
        "Service": "ssm-incidents.amazonaws.com"
    },
    "Action": "secretsmanager:GetSecretValue",
```

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

- Pilih Simpan.

5. Pada Langkah 4d, untuk Replikasi rahasia, lakukan hal berikut jika Anda mereplikasi rencana respons Anda ke lebih dari satu: Wilayah AWS
   - Perluas rahasia Replikasi.
   - Untuk Wilayah AWS, pilih Wilayah tempat Anda mereplikasi rencana respons Anda.
   - Untuk kunci Enkripsi, pilih kunci terkelola pelanggan yang Anda buat, atau direplikasi ke, Wilayah ini yang memenuhi persyaratan yang tercantum di bagian Prasyarat.
   - Untuk setiap tambahan Wilayah AWS, pilih Tambah Wilayah dan pilih nama Wilayah dan kunci yang dikelola pelanggan.
6. Selesaikan langkah-langkah yang tersisa di Buat AWS Secrets Manager rahasia di Panduan AWS Secrets Manager Pengguna.

Untuk informasi tentang cara menambahkan PagerDuty layanan ke alur kerja insiden Manajer Insiden, lihat Mengintegrasikan PagerDuty layanan ke dalam paket respons dalam topikMembuat rencana respons.

Informasi terkait

Cara Mengotomatiskan Respons Insiden dengan PagerDuty dan Manajer Insiden AWS Systems Manager (Blog AWS Cloud Operasi dan Migrasi)

Enkripsi rahasia AWS Secrets Manager di Panduan AWS Secrets Manager Pengguna

Pemecahan Masalah Manajer AWS Insiden Systems Manager

Jika Anda mengalami masalah saat menggunakan Manajer Insiden AWS Systems Manager, Anda dapat menggunakan informasi berikut untuk menyelesaikannya sesuai dengan praktik terbaik kami. Jika masalah yang Anda temui berada di luar cakupan informasi berikut, atau jika masih ada setelah Anda mencoba menyelesaikannya, hubungi AWS Dukungan.

Topik

- Pesan galat: ValidationException – We were unable to validate the AWS Secrets Manager secret
- Masalah pemecahan masalah lainnya

Pesan galat: `ValidationException – We were unable to validate the AWS Secrets Manager secret`

Masalah 1: Identitas AWS Identity and Access Management (IAM) (pengguna, peran, atau grup) yang membuat paket respons tidak memiliki izin `secretsmanager:GetSecretValue` IAM. Identitas IAM harus memiliki izin ini untuk memvalidasi rahasia Secrets Manager.

- Solusi: Tambahkan `secretsmanager:GetSecretValue` izin yang hilang ke kebijakan IAM untuk identitas IAM yang membuat rencana respons. Untuk selengkapnya, lihat Menambahkan izin identitas IAM (konsol) atau Menambahkan kebijakan IAM (AWS CLI) di Panduan Pengguna IAM.

Masalah 2: Rahasia tidak memiliki kebijakan berbasis sumber daya yang dilampirkan yang memungkinkan identitas IAM untuk menjalankan `GetSecretValue`tindakan, atau kebijakan berbasis sumber daya menolak izin untuk identitas.

- Solusi: Buat atau tambahkan `Allow` pernyataan ke kebijakan berbasis sumber daya rahasia yang memberikan izin untuk `secrets:GetSecretValue` identitas IAM. Atau, jika Anda menggunakan `Deny` pernyataan yang menyertakan identitas IAM, perbarui kebijakan agar identitas dapat menjalankan tindakan. Untuk selengkapnya, lihat Melampirkan kebijakan izin ke AWS Secrets Manager rahasia di Panduan AWS Secrets Manager Pengguna.

Masalah 3: Rahasia tidak memiliki kebijakan berbasis sumber daya yang dilampirkan yang memungkinkan akses ke kepala layanan Manajer Insiden,. `ssm-incidents.amazonaws.com`

- Solusi: Buat atau perbarui kebijakan berbasis sumber daya untuk rahasia tersebut dan sertakan izin berikut:

```
{
    "Effect": "Allow",
    "Principal": {
        "Service": ["ssm-incidents.amazonaws.com"]
    },
    "Action": "secretsmanager:GetSecretValue",
    "Resource": "*"
}
```

Masalah 4: Yang AWS KMS key dipilih untuk mengenkripsi rahasia bukanlah kunci yang dikelola pelanggan, atau kunci terkelola pelanggan yang dipilih tidak memberikan izin IAM `kms:Decrypt` dan `kms:GenerateDataKey*` kepada kepala layanan Manajer Insiden. Sebagai alternatif, identitas IAM yang membuat rencana respons mungkin tidak memiliki izin IAM. `GetSecretValue`

- Solusi: Pastikan Anda memenuhi persyaratan yang dijelaskan di bawah Prasyarat dalam topik. Menyimpan kredensyal PagerDuty akses secara rahasia AWS Secrets Manager

Masalah 5: ID rahasia yang berisi Kunci API REST Akses Umum atau Kunci API REST Token Pengguna tidak valid.

- Solusi: Pastikan Anda memasukkan ID rahasia Secrets Manager secara akurat, tanpa spasi tambahan. Anda harus bekerja di tempat Wilayah AWS yang sama yang menyimpan rahasia yang ingin Anda gunakan. Anda tidak dapat menggunakan rahasia yang dihapus.

Masalah 6: Dalam kasus yang jarang terjadi, layanan Secrets Manager mungkin mengalami masalah, atau Manajer Insiden mungkin mengalami kesulitan berkomunikasi dengannya.

- Solusi: Tunggu beberapa menit, lalu coba lagi. Periksa apakah ada masalah yang mungkin memengaruhi salah satu layanan. AWS Health Dashboard

Masalah pemecahan masalah lainnya

Jika langkah sebelumnya tidak menyelesaikan masalah, Anda dapat menemukan bantuan tambahan dari sumber daya berikut:

- Untuk masalah IAM khusus untuk Manajer Insiden saat Anda mengakses konsol Manajer Insiden, lihatMemecahkan masalah Manajer Insiden AWS Systems Manager identitas dan akses.
- Untuk masalah autentikasi dan otorisasi umum saat Anda mengakses AWS Management Console, lihat Memecahkan Masalah IAM di Panduan Pengguna IAM

Riwayat dokumen untuk Manajer Insiden

Perubahan	Deskripsi	Tanggal
Ubah persyaratan izin untuk membuat insiden secara manual	Izin IAM yang diperlukan bagi pengguna untuk membuat insiden secara manual telah berubah dan tidak lagi menggunakan peran terkait layanan. Sebagai gantinya, Manajer Insiden sekarang menggunakan sesi akses maju (FAS) untuk menelepon `ssm-contacts:StartEngagement` sebagai bagian dari. `ssm-incidents:StartIncident` Untuk informasi selengkapnya, lihat Izin IAM yang diperlukan untuk memulai insiden secara manual.	10 Juni 2025
Memperbarui ke kebijakan terkelola `AWSServiceRoleforIncidentManagerPolicy`	Manajer Insiden telah menambahkan izin baru `AWSServiceRoleforIncidentManagerPolicy` yang memungkinkan Manajer Insiden mempublikasikan metrik dalam `AWS/Usage` namespace ke akun Anda. Untuk informasi selengkapnya, lihat pembaruan Manajer Insiden ke kebijakan AWS terkelola.	Januari 28, 2025

Memperbarui ke kebijakan terkelola `AWSIncidentManagerIncidentAccessServiceRolePolicy`	Manajer Insiden telah menambahkan izin baru untuk`AWSIncidentManagerIncidentAccessServiceRolePolicy` , untuk mendukung fitur Temuan, yang memungkinkannya memeriksa apakah sebuah EC2 instance merupakan bagian dari grup Auto Scaling. Untuk informasi selengkapnya, lihat pembaruan Manajer Insiden ke kebijakan AWS terkelola.	Februari 20, 2024
Dukungan HashiCorp Terraform tambahan: Rotasi on-call	Terraform telah menambahkan dukungannya untuk Manajer Insiden. Anda sekarang dapat menyediakan atau mengelola sumber daya panggilan Manajer Insiden menggunakan Terraform. Untuk informasi tentang ini dan integrasi pihak ketiga lainnya dengan Manajer Insiden, lihat Integrasi dengan produk dan layanan lain.	Februari 2, 2024

Fitur baru: Temuan dari yang lain Layanan AWS	Temuan memberi Anda informasi tentang perubahan yang terkait dengan AWS CloudFormation tumpukan dan AWS CodeDeploy penyebaran yang terjadi sekitar waktu yang sama ketika insiden dibuat di Manajer Insiden. Di konsol Manajer Insiden, Anda dapat melihat informasi ringkasan tentang perubahan tersebut dan, dalam banyak kasus, mengakses tautan ke CloudFormation atau CodeDeploy konsol untuk detail lengkap tentang perubahan tersebut. Temuan mengurangi waktu yang dibutuhkan untuk mengevaluasi potensi penyebab insiden. Mereka juga mengurangi kemungkinan responden mengakses akun atau konsol yang salah untuk menyelidiki penyebab suatu insiden. Fitur ini juga memperkenalkan kebijakan terkelola baru`AWSIncidentManagerIncidentAccessServiceRolePolicy`, yang memungkinkan Manajer Insiden membaca sumber daya lain Layanan AWS untuk mengidentifikasi temuan yang terkait dengan insiden. Untuk	15 November 2023

	informasi selengkapnya, lihat topik berikut: • Bekerja dengan temuan • AWS kebijakan terkelola : AWSIncidentManager IncidentAccessServ iceRolePolicy	
Daftar integrasi yang diperbaru i dengan Manajer Insiden	Topik Integrasi produk dan layanan dengan Manajer Insiden telah diperluas untuk mencantumkan dan menjelask an semua Layanan AWS alat pihak ketiga yang dapat Anda integrasikan dengan Manajer Insiden ke dalam operasi deteksi dan respons insiden Anda.	9 Juni 2023

Integrasi dengan AWS Trusted Advisor	Trusted Advisor sekarang memeriksa bahwa konfigurasi set replikasi menggunakan lebih dari satu Wilayah AWS untuk mendukung failover dan respons regional. Untuk insiden yang dibuat oleh CloudWatch alarm atau EventBridge peristiwa, Manajer Insiden membuat insiden yang Wilayah AWS sama dengan aturan alarm atau peristiwa. Jika Manajer Insiden sementara tidak tersedia di Wilayah itu, sistem mencoba membuat insiden di Wilayah lain dalam kumpulan replikasi. Jika set replikasi hanya mencakup satu Wilayah, sistem gagal membuat catatan insiden sementara Manajer Insiden tidak tersedia. Untuk membantu menghindari situasi ini, Trusted Advisor laporkan saat kumpulan replikasi dikonfigurasi hanya untuk satu Wilayah. Untuk informasi tentang bekerja dengan Trusted Advisor, lihat AWS Trusted Advisordi Panduan AWS Dukungan Pengguna.	28 April 2023

Gunakan Microsoft Teams sebagai saluran obrolan dalam rencana respons	Melalui integrasi dengan Microsoft Teams dan Pengembang Amazon Q dalam aplikasi obrolan, Anda sekarang dapat menggunakan Microsoft Teams saluran obrolan dalam rencana respons Anda. Ini selain dukungan untuk Slack dan saluran obrolan Amazon Chime. Selama insiden, Manajer Insiden mengirimkan pemberitahuan status langsung ke saluran obrolan untuk memberi tahu semua responden. Responden juga dapat berkomunikasi satu sama lain dan AWS CLI perintah terkait insiden dalam Microsoft Teams aplikasi untuk memperbarui dan berinteraksi dengan insiden. Untuk informasi selengkapnya, lihat Bekerja dengan saluran obrolan di Manajer Insiden.	4 April 2023

Fitur baru: Jadwal panggilan	Jadwal panggilan di Manajer Insiden menentukan siapa yang diberi tahu ketika insiden terjadi yang memerlukan intervensi operator. Jadwal panggilan terdiri dari satu atau lebih rotasi yang Anda buat untuk jadwal tersebut. Setiap rotasi dapat mencakup hingga 30 kontak. Setelah Anda membuat jadwal panggilan , Anda dapat memasukkannya sebagai eskalasi dalam rencana eskalasi Anda. Ketika insiden yang terkait dengan rencana eskalasi itu terjadi, Manajer Insiden memberi tahu operator (atau operator) yang sedang menelepon sesuai dengan jadwal. Untuk informasi selengkapnya, lihat Bekerja dengan jadwal panggilan di Manajer Insiden.	Maret 28, 2023

Cetak analisis insiden yang diformat atau simpan sebagai PDF	Halaman analisis insiden sekarang menyertakan tombol Cetak untuk menghasilkan versi analisis yang diformat untuk dicetak. Dengan menggunakan tujuan printer yang dikonfigurasi untuk perangkat Anda, Anda dapat menyimpan analisis insiden sebagai PDF atau mengirimk annya ke printer lokal atau jaringan. Untuk informasi selengkapnya, lihat Mencetak analisis insiden yang diformat.	Januari 17, 2023

PagerDuty integrasi: Manajer Insiden sekarang menyalin peristiwa timeline insiden ke PagerDuty insiden	Saat Anda mengaktifkan integrasi dengan PagerDuty dalam rencana respons, Manajer Insiden menambahk an peristiwa timeline yang dibuat dari rencana tersebut ke catatan insiden yang sesuai. PagerDuty PagerDuty menambahkan peristiwa timeline sebagai catatan pada insiden tersebut, hingga maksimal 2.000 catatan. Untuk mempelajari lebih lanjut tentang perubahan ini, lihat topik berikut: • Simpan kredenal PagerDuty akses secara rahasia AWS Secrets Manager • Integrasikan PagerDuty layanan ke dalam rencana respons	15 Desember 2022
Integrasi Manajer Insiden dengan CloudWatch metrik.	Anda sekarang dapat memiliki metrik terkait insiden yang diterbitkan di. CloudWatch Untuk informasi selengkap nya, lihat CloudWatchmetrik. Ini AWSIncidentManager ServiceRolePolicy telah menyertakan izin tambahan untuk memungkinkan layanan kami mempublikasikan metrik atas nama Anda.	15 Desember 2022

Meluncurkan catatan Insiden dan memperbarui layar Detail Insiden	Anda dapat berkolaborasi dan berkomunikasi dengan pengguna lain yang mengerjakan insiden menggunakan catatan Insiden. Selain itu, Anda dapat melihat status runbook dan keterlibatan dari layar Detail Insiden. Untuk informasi lebih lanjut, lihat Detail Insiden.	16 November 2022

Integrasikan rencana PagerDuty eskalasi dan alur kerja paging ke dalam rencana respons Manajer Insiden	Anda sekarang dapat mengintegrasikan Manajer Insiden dengan PagerDuty dan menambahkan PagerDuty layanan ke rencana respons. Setelah Anda mengonfigurasi integrasi, Manajer Insiden dapat membuat insiden yang sesuai PagerDuty untuk setiap insiden baru yang dibuat di Manajer Insiden. PagerDuty menggunakan alur kerja paging dan kebijakan eskalasi yang Anda tentukan di lingkungan. PagerDuty Untuk informasi selengkapnya, lihat topik berikut: • Integrasi produk dan layanan dengan Manajer Insiden • Simpan kredenal PagerDuty akses secara rahasia AWS Secrets Manager • Integrasikan PagerDuty layanan ke dalam rencana respons dalam topik Membuat rencana respons • Pemecahan Masalah	16 November 2022

Meluncurkan catatan Insiden dan memperbarui layar Detail Insiden.	Anda dapat berkolaborasi dan berkomunikasi dengan pengguna lain yang mengerjakan insiden menggunakan catatan Insiden. Selain itu, Anda dapat melihat status runbook dan keterlibatan dari layar Detail Insiden. Untuk informasi lebih lanjut, lihat Detail Insiden.	16 November 2022
Menandai dukungan untuk set replikasi	Anda sekarang dapat menetapkan tag ke set replikasi Anda. Manajer Insiden AWS Systems Manager Ini menambah dukungan yang ada untuk menetapkan tag ke rencana respons, catatan insiden, dan kontak dalam set replikasi yang Wilayah AWS ditentukan. Untuk informasi, lihat topik berikut: • Siapkan penyihir • Menandai sumber daya Manajer Insiden	2 November 2022

Integrasi Manajer Insiden dengan Manajemen Layanan Atlassian Jira	Anda dapat menginteg rasikan Manajer Insiden dengan Manajemen Layanan Jira dengan menggunakan Konektor Manajemen AWS Layanan untuk Manajemen Layanan Jira. Setelah Anda mengonfigurasi integrasi, insiden baru yang dibuat di Manajer Insiden membuat insiden yang sesuai di Jira. Jika Anda memperbarui insiden di Manajer Insiden, pembaruan akan ditambahk an ke insiden terkait di Jira. Jika Anda menyelesaikan insiden di Manajer Insiden atau Jira, insiden terkait juga diselesaikan, berdasarkan preferensi yang dikonfigurasi. Untuk informasi selengkap nya, lihat Mengonfigurasi Manajemen Layanan JIRA di Panduan Administrator Konektor Manajemen AWS Layanan.	6 Oktober 2022

Dukungan penandaan yang ditingkatkan	Manajer Insiden mendukung penetapan tag ke rencana respons, catatan insiden, dan kontak dalam Wilayah AWS set replikasi yang ditentuka n. Manajer Insiden juga mendukung penetapan tag secara otomatis ke insiden yang dibuat dari rencana respons. Untuk informasi selengkapnya, lihat Menandai sumber daya Manajer Insiden.	28 Juni 2022

Integrasi Manajer Insiden dengan ServiceNow	Anda dapat mengintegrasikan Manajer Insiden ServiceNowdengan menggunakan Konektor Manajemen AWS Layanan untuk ServiceNow. Setelah Anda mengonfigurasi integrasi, insiden baru yang dibuat di Manajer Insiden membuat insiden yang sesuai di ServiceNow. Jika Anda memperbarui insiden di Manajer Insiden, pembaruan akan ditambahkan ke insiden terkait di ServiceNow. Jika Anda menyelesaikan insiden di Manajer Insiden atau ServiceNow, insiden terkait juga diselesaikan, berdasarkan preferensi yang dikonfigurasi. Untuk informasi selengkapnya, lihat Mengintegrasikan Manajer AWS Systems Manager Insiden di ServiceNow.	9 Juni 2022

Impor detail kontak	Ketika insiden dibuat, Manajer Insiden dapat memberi tahu responden dengan menggunakan pemberita huan suara atau SMS. Untuk memastikan bahwa responden melihat bahwa pemberitahuan panggilan atau SMS berasal dari Manajer Insiden, kami menyarankan agar semua responden mengunduh file format kartu virtual Manajer Insiden (.vcf) ke buku alamat di perangkat seluler mereka. Untuk informasi selengkapnya, lihat Mengimpor detail kontak ke buku alamat Anda.	Mei 18, 2022

Beberapa peningkatan fitur untuk meningkatkan pembuatan dan remediasi insiden	Manajer Insiden meluncurkan peningkatan fitur berikut untuk meningkatkan pembuatan dan remediasi insiden: • Membuat insiden secara otomatis di lain Wilayah AWS: Jika Manajer Insiden tidak tersedia Wilayah AWS saat Amazon CloudWatch atau Amazon EventBridge membuat insiden, layanan ini sekarang secara otomatis membuat insiden di salah satu Wilayah yang tersedia yang ditentukan dalam kumpulan replikasi Anda. Untuk informasi selengkap nya, lihat Manajemen insiden Lintas Wilayah. • Secara otomatis mengisi parameter runbook dengan metadata insiden: Anda sekarang dapat mengonfig urasi Manajer Insiden untuk mengumpulkan informasi tentang AWS sumber daya dari insiden. Manajer Insiden kemudian dapat mengisi parameter runbook dengan informasi yang dikumpulkan. Untuk informasi selengkapnya, lihat Tutorial: Menggunakan runbook Otomasi Systems	Mei 17, 2022

	Manager dengan Manajer Insiden. • Secara otomatis mengumpulkan informasi AWS sumber daya: Ketika sistem membuat insiden, Manajer Insiden sekarang secara otomatis mengumpulkan informasi tentang AWS sumber daya yang terlibat dalam insiden tersebut. Manajer Insiden kemudian menambahkan informasi ini ke tab Item terkait.	
Dukungan multi-runbook	Manajer Insiden sekarang mendukung menjalankan beberapa runbook selama insiden untuk halaman detail insiden.	Januari 14, 2022
Manajer Insiden diluncurkan di baru Wilayah AWS	Manajer Insiden sekarang tersedia di Wilayah baru ini: us-west-1, sa-east-1, ap-northeast-2, ap-south-1, ca-central-1, eu-west-2, dan eu-west-3. Untuk informasi selengkapnya tentang Wilayah Manajer Insiden dan kuota, lihat panduan Referensi Umum AWS referensi.	November 8, 2021
Pengakuan keterlibatan konsol	Anda sekarang dapat mengakui keterlibatan langsung dari konsol Manajer Insiden.	5 Agustus 2021

Tab properti	Manajer Insiden memperkenalkan tab properti ke halaman detail insiden, memberikan informasi lebih lanjut tentang insiden, orang tua OpsItem, dan analisis pasca-insiden terkait.	Agustus 3, 2021
Peluncuran Manajer Insiden	Incident Manager adalah konsol manajemen insiden yang dirancang untuk membantu pengguna mengurangi dan memulihkan dari insiden yang memengaruhi aplikasi yang dihosting mereka AWS .	10 Mei 2021

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