Manual do usuário

Incident Manager

Incident Manager: Manual do usuário

Table of Contents

O que é o AWS Systems Manager Incident Manager? ... 1
Principais componentes e recursos ... 1
Benefícios do uso do Incident Manager ... 3
Serviços relacionados ... 5
Acessando o Incident Manager ... 5
Regiões e cotas do Incident Manager ... 5
Preços do Incident Manager ... 6
O ciclo de vida do incidente ... 6
Alertas e engajamento ... 7
Triagem ... 8
Investigação e mitigação ... 9
Análise pós-incidente ... 10
Configuração ... 11
Inscreva-se para um Conta da AWS ... 11
Criar um usuário com acesso administrativo ... 12
Conceder acesso programático ... 13
Perfil necessário para a configuração do Incident Manager ... 14
Conceitos básicos ... 15
Pré-requisitos ... 15
Assistente Prepare-se ... 15
Incident management entre regiões e entre contas ... 22
Incident management entre regiões ... 22
Gerenciamento de incidentes entre contas ... 23
Práticas recomendadas ... 23
Definir e configurar incident management entre regiões e entre regiões ... 23
Limitações ... 25
Preparação para incidentes ... 27
Monitorar ... 29
Trabalhar com configurações gerais ... 29
Conjunto de replicação ... 30
Como gerenciar tags de um conjunto de replicação ... 31
Como gerenciar o atributo Descobertas ... 32
Como trabalhar com contatos ... 33
Canais de contato ... 33

Planos de engajamento ... 34
Criar um contato ... 35
Importar detalhes de contato para seu catálogo de endereços ... 36
Trabalhando com programações de plantão ... 36
Criando uma programação de plantão ... 37
Gerenciando uma programação de plantão existente ... 42
Como trabalhar com planos de escalação ... 48
Estágios ... 48
Criar um plano de escalação ... 49
Trabalhar com canais de chat ... 49
Tarefa 1: Criar ou atualizar tópicos do Amazon SNS para seu canal de chat ... 50
Tarefa 2: criar um canal de chat no AWS Chatbot ... 52
Tarefa 3: adicionar o canal de chat a um plano de resposta no Incident Manager ... 55
Como interagir pelo canal de chat ... 55
Trabalho com runbooks ... 56
Permissões do IAM necessárias para iniciar e executar fluxos de trabalho do runbook ... 57
Trabalho com parâmetros de runbook ... 60
Defina um runbook ... 62
Modelo de runbook do Incident Manager ... 63
Como trabalhar com planos de resposta ... 64
Criar um plano de resposta ... 65
Como trabalhar com descobertas ... 72
Habilite e crie um perfil de serviço para descobertas ... 73
Configurar permissões para suporte de descobertas entre contas ... 73
Como criar incidentes ... 74
Como configurar criação automática de incidentes com alarmes do CloudWatch ... 75
Criação automática de incidentes com eventos do EventBridge ... 76
Criação de incidentes usando eventos de parceiros SaaS ... 76
Criação de incidentes usando eventos de serviço da AWS ... 78
Criação manual de incidentes ... 79
Rastreamento de incidentes ... 81
Lista de incidentes ... 81
Detalhes do incidente ... 81
Banner superior ... 82
Notas de incidentes ... 83
Guias ... 83

Visão geral ... 83
Diagnóstico ... 84
Linha do tempo ... 86
Runbooks ... 86
Engajamentos ... 87
Itens relacionados ... 88
Propriedades ... 88
Como realizar uma análise pós-incidente ... 90
Detalhes da análise ... 90
Visão geral ... 90
Métricas ... 91
Cronograma ... 91
Perguntas ... 92
Ações ... 92
Lista de verificação ... 92
Modelos de análise ... 93
AWS modelo padrão ... 93
Criar um modelo de análise ... 93
Criar uma análise ... 94
Imprima uma análise de incidentes formatada ... 94
Tutoriais ... 95
Usar runbooks com o Incident Manager ... 95
Tarefa 1: Criar o runbook ... 96
Tarefa 2: Criar um perfil do IAM ... 99
Tarefa 3: Conectar o runbook ao seu plano de resposta ... 101
Tarefa 4: Atribuir um CloudWatch alarme ao seu plano de resposta ... 102
Tarefa 5: verificar os resultados ... 102
Gerenciar incidentes de segurança ... 103
Marcar recursos ... 106
Segurança ... 108
Proteção de dados ... 109
Criptografia de dados ... 110
Identity and Access Management ... 112
Público ... 113
Autenticando com identidades ... 113
Gerenciando acesso usando políticas ... 117

Como AWS Systems Manager Incident Manager funciona com o IAM 120
Exemplos de políticas baseadas em identidade 129
Exemplos de políticas baseadas em atributos 133
Prevenção do problema do substituto confuso entre serviços 135
Usar perfis vinculados ao serviço 136
AWS políticas gerenciadas para o Incident Manager 139
Solução de problemas 146
Usar contatos compartilhados e planos de resposta no Incident Manager 148
Pré-requisitos para compartilhar contatos e planos de resposta 149
Serviços relacionados 149
Compartilhar um plano de contato ou resposta 150
Interromper um compartilhamento de um contato ou plano de resposta 150
Identificar um contato ou um plano de resposta compartilhado 151
Permissões compartilhadas de contatos e de planos de resposta 152
Faturamento e medição 152
Limites de instâncias 152
Validação de conformidade 152
Resiliência 154
Segurança da infraestrutura 154
Trabalhar com endpoints da VPC (AWS PrivateLink) 155
Considerações sobre os endpoints da VPC do Incident Manager 156
Criação de um endpoint da VPC de interface para o Incident Manager 156
Criar uma política de endpoint da VPC do Incident Manager 156
Análise de configuração e vulnerabilidade 157
Melhores práticas de segurança 157
Práticas recomendadas de segurança preventiva no Incident Manager 158
Práticas recomendadas de segurança preventiva no Incident Manager 159
Registro e monitoramento 161
Métricas do Amazon CloudWatch 161
Como visualizar métricas do Incident Manager no console do CloudWatch 163
Dimensões para métricas 164
Log de chamadas de API do Incident Manager usando o AWS CloudTrail 165
Informações sobre o Incident Manager no CloudTrail 165
Noções básicas sobre as entradas do arquivo de log do Incident Manager 166
Integrações de produtos e serviços 169
Integração com Serviços da AWS 169

Integração com outros produtos e serviços 174
Armazenando credenciais de PagerDuty acesso em segredo AWS Secrets Manager 180
Solução de problemas 186
A mensagem de erro: `ValidationException – We were unable to validate the AWS Secrets Manager secret` 186
Outros casos de solução de problemas 188
Glossário do AWS 189
Histórico de documentos 190
..... ccviii

O que é o AWS Systems Manager Incident Manager?

O Incident Manager, um recurso do AWS Systems Manager, fornece um console de gerenciamento de incidentes que ajuda você a mitigar e se recuperar de incidentes que afetam suas aplicações hospedadas na AWS.

No contexto de AWS, um incidente é qualquer interrupção ou redução não planejada na qualidade dos serviços que pode ter um impacto significativo nas operações comerciais. Portanto, é crucial que as organizações estabeleçam uma estratégia de resposta para mitigar e se recuperar de incidentes com eficiência e implementem ações para evitar futuros incidentes.

O Incident Manager ajuda a reduzir o tempo de resolução de incidentes ao:

- Fornecer planos automatizados para engajar com eficiência as pessoas responsáveis por responder aos incidentes.
- Fornecer dados relevantes de solução de problemas.
- Habilitar ações de resposta automatizadas usando runbooks de automação predefinidos.
- Fornecer métodos para colaborar e se comunicar com todas as partes interessadas.

Os recursos e fluxos de trabalho incorporados ao Incident Manager são baseados nas melhores práticas de resposta a incidentes que a Amazon vem desenvolvendo quase desde o início. O Incident Manager se integra com Serviços da AWS Amazon CloudWatch, AWS CloudTrail, AWS Systems Manager e Amazon EventBridge.

Principais componentes e recursos

Esta seção descreve os recursos do Incident Manager que você usa para configurar seus planos de resposta a incidentes.

Plano de resposta

Um plano de resposta funciona como um modelo que define o que deve estar em vigor quando ocorre um incidente. Ele inclui informações como:

- Quem é obrigado a responder quando ocorre um incidente.
- A resposta automatizada estabelecida para mitigar o incidente.
- A ferramenta de colaboração que os respondentes devem usar para se comunicar e receber notificações automáticas sobre o incidente.

Detecção de incidente

Você pode configurar alarmes do Amazon CloudWatch e eventos do Amazon EventBridge para criar incidentes quando condições ou alterações que afetam seus AWS recursos forem detectadas.

Suporte à automação do Runbook

Você pode iniciar runbooks de automação a partir do Incident Manager para automatizar sua resposta crítica aos incidentes e fornecer etapas detalhadas aos primeiros respondentes.

Engajamento e escalonamento

Um plano de engajamento especifica que todos devem ser notificados sobre cada incidente exclusivo. Você pode especificar contatos individuais adicionados ao Incident Manager ou especificar uma agenda de plantão criada no Incident Manager. Os planos de engajamento também especificam um caminho de escalonamento para ajudar a garantir a visibilidade entre as partes interessadas e a participação ativa durante o processo de resposta a incidentes.

Agenda de plantão

Uma agenda de plantão no Incident Manager consiste em uma ou mais rotações que você cria para a agenda. Para cada rotação, é possível incluir até 30 contatos. Quando adicionado a um plano de escalonamento ou plano de resposta, a agenda de plantão define quem é notificado quando ocorre um incidente que requer intervenção do respondente. As agendas de plantão ajudam a garantir a cobertura completa e redundante 24 horas por dia, 7 dias por semana, conforme necessário para sua resposta a incidentes.

Colaboração ativa

Os respondentes de incidentes respondem ativamente aos incidentes por meio da integração com o AWS Chatbot cliente. AWS Chatbot suporta a criação de canais de bate-papo para o Incident Manager que usa Slack, Microsoft Teams, ou Amazon Chime. Os respondentes podem se comunicar diretamente uns com os outros, receber notificações automatizadas sobre incidentes e, em Slack e Microsoft Teams, executar diretamente algumas operações da interface de linha de comandos (CLI) do Incident Manager.

Diagnóstico do incidente

Os respondentes podem visualizar informações atualizadas no console do Incident Manager durante um incidente. Com base nas mudanças nas informações, os respondentes podem, então, criar itens de acompanhamento e corrigi-los usando runbooks de automação.

Descobertas de outros serviços

Para dar suporte aos respondentes no diagnóstico de incidentes, ative o atributo Descobertas no Incident Manager. As descobertas são informações sobre AWS CodeDeploy implantações e AWS CloudFormation atualizações de pilha que ocorreram na época de um incidente e que envolveram um ou mais recursos provavelmente relacionados ao incidente. Ter essas informações economiza tempo na avaliação de possíveis causas, o que pode reduzir o tempo médio de recuperação (MTTR) de um incidente.

Análise pós-incidente

Depois que um incidente é resolvido, você usa uma análise pós-incidente para identificar melhorias na resposta a incidentes, incluindo o tempo de detecção e mitigação. Uma análise também pode ajudá-lo a entender a causa raiz dos incidentes. O Incident Manager cria itens de ação de acompanhamento recomendados que você pode usar para melhorar sua resposta a incidentes.

Benefícios do uso do Incident Manager

Conheça os benefícios de usar o Incident Manager nas operações de detecção e resposta a incidentes.

Esta seção descreve as vantagens que sua organização pode obter ao implementar um plano de resposta do Incident Manager.

Diagnostique problemas de forma eficiente e imediata

Os alarmes do Amazon CloudWatch e os eventos do Amazon EventBridge configurados podem criar incidentes automaticamente quando há alguma interrupção não planejada ou redução na qualidade dos seus serviços.

Os alarmes do CloudWatch detectam e relatam quando há alterações no valor da métrica ou expressão relativa a um limite por um número de períodos. Os eventos do EventBridge são criados como resultado de uma alteração em um ambiente, aplicativo ou serviço que você especificou em uma regra do EventBridge. Ao criar um alarme ou evento, você pode especificar uma ação para um incidente a ser criado no Incident Manager e o plano de resposta apropriado para facilitar o engajamento, a escalação e a mitigação do incidente.

O Incident Manager fornece a capacidade de coletar e rastrear automaticamente as métricas relacionadas a um incidente, por meio do uso das métricas do CloudWatch. Além das métricas

automatizadas geradas para o incidente quando ele é criado por meio de um alarme do CloudWatch, você pode adicionar métricas manualmente em tempo real para fornecer contexto e dados adicionais aos respondentes em um incidente.

Use o cronograma de incidentes do Incident Manager para exibir pontos de interesse em ordem cronológica. Os respondentes também podem usar a linha do tempo para adicionar eventos personalizados para descrever o que fizeram ou o que aconteceu. Os pontos de interesse automatizados incluem:

- Um alarme do CloudWatch ou uma regra do EventBridge cria um incidente.
- As métricas de incidentes são reportadas ao Incident Manager.
- Os respondentes estão engajados.
- As etapas do Runbook foram concluídas com êxito.

Interaja de forma eficaz

O Incident Manager reúne os respondedores de incidentes por meio do uso de contatos, agendas de plantão, planos de escalonamento e canais de bate-papo. Você define contatos individuais diretamente no Incident Manager e especifica as preferências de contato (e-mail, SMS ou voz). Você adiciona contatos às rotações de agendamento de plantão para determinar quem está envolvido para lidar com incidentes durante um determinado período. Usando os contatos definidos e as agendas de plantão, você cria planos de escalonamento para envolver os respondentes necessários no momento certo durante um incidente.

Colabore em tempo real

A comunicação durante um incidente é a chave para uma resolução mais rápida. Usando um AWS Chatbot cliente configurado para usar Slack, Microsoft Teams, ou o Amazon Chime, você pode reunir os respondentes em seu canal de bate-papo conectado preferido, onde eles interagem diretamente com o incidente e entre si. O Incident Manager também exibe as ações em tempo real dos respondedores de incidentes no canal de bate-papo, fornecendo contexto para outras pessoas.

Automatize a restauração de serviços

O Incident Manager permite que seus respondentes se concentrem nas principais tarefas necessárias para resolver um incidente por meio do uso de runbooks de automação. No Incident Manager, os runbooks são uma série predefinida de ações tomadas para resolver um incidente. Eles combinam o poder das tarefas automatizadas com etapas manuais, conforme necessário, deixando os respondentes mais disponíveis para analisar e responder ao impacto.

Previna futuros incidentes

Usando a análise pós-incidente do Incident Manager, sua equipe pode desenvolver planos de resposta mais robustos e efetuar mudanças em seus aplicativos para evitar futuros incidentes e tempo de inatividade. A análise pós-incidente também fornece aprendizado iterativo e aprimoramento de runbooks, planos de resposta e métricas.

Serviços relacionados

O Incident Manager se integra a vários outros Serviços da AWS serviços e ferramentas de terceiros para ajudá-lo a detectar e resolver incidentes, interagir indiretamente com suas operações de API e gerenciar a infraestrutura. Para obter mais informações, consulte Integrações de produtos e serviços com o Incident Manager.

Acessando o Incident Manager

Você pode acessar o Incident Manager de qualquer uma das seguintes formas:

- Pelo console do Incident Manager
- AWS CLI Para obter mais informações, consulte Conceitos básicos do AWS CLI no AWS Command Line Interface Manual do usuário. Para obter informações sobre os comandos da CLI para o Incident Manager, consulte ssm-incidents e ssm-contacts na AWS CLI Referência de Comandos.
- Incident Manager API Para obter mais informações, consulte a AWS Systems Manager Incident Manager Referência de API.
- AWS SDKs Para obter mais informações, consulte Ferramentas para criar na AWS.

Regiões e cotas do Incident Manager

O Incident Manager não é suportado em todos os Regiões da AWS suportados pelo Systems Manager.

Para ver informações sobre regiões e cotas do Incident Manager, consulte AWS Systems Manager Incident Manager endpoints e cotas no Referência geral da Amazon Web Services.

Preços do Incident Manager

O uso do Incident Manager é cobrado. Para mais informações, consulte AWS valores do Systems Manager.

> **Note**
>
> Outros Serviços da AWS, AWS conteúdos e conteúdos de terceiros disponibilizados em conjunto com este serviço podem estar sujeitos a cobranças separadas e regidos por termos adicionais.

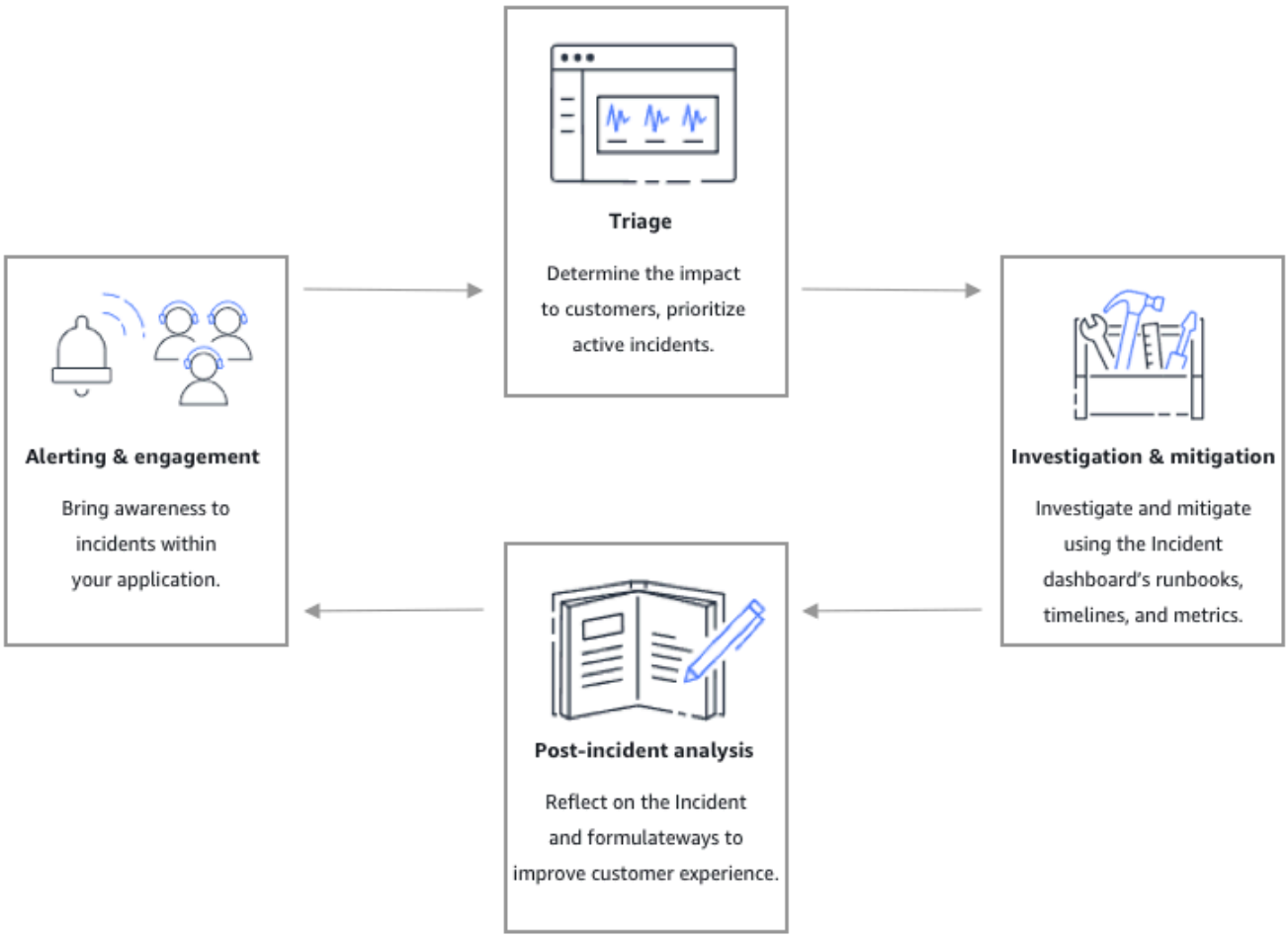
Para obter uma visão geral do Trusted Advisor, um serviço que ajuda você a otimizar os custos, a segurança e a performance do AWS ambiente, consulte AWS Trusted Advisor no AWS Support Manual do usuário.

O ciclo de vida do incidente no Incident Manager

O AWS Systems Manager Incident Manager fornece uma estrutura passo a passo com base nas práticas recomendadas para identificar e reagir a incidentes, como interrupções no serviço ou ameaças à segurança. O foco principal do Incident Manager é ajudar a restaurar os serviços ou aplicativos afetados ao normal o mais rápido possível por meio de uma solução completa de gerenciamento do ciclo de vida de incidentes.

O Incident Manager fornece ferramentas e práticas recomendadas para cada fase do ciclo de vida do incidente:

- Alertas e engajamento
- Triagem
- Investigação e mitigação
- Análise pós-incidente



Alertas e engajamento

A fase de alerta e engajamento do ciclo de vida do incidente visa conscientizar sobre incidentes nos aplicativos e serviços. Essa fase começa antes que um incidente seja detectado e exige uma compreensão profunda dos aplicativos. Você pode usar as métricas do Amazon CloudWatch para monitorar dados sobre o desempenho dos aplicativos ou utilizar o Amazon EventBridge para agregar alertas de diferentes fontes, aplicativos e serviços. Depois de configurar o monitoramento de seus aplicativos, você pode começar a alertar sobre métricas que fogem da norma histórica. Para saber mais sobre como monitorar as práticas recomendadas, consulte Monitorar.

Para dar suporte aos respondentes no diagnóstico de incidentes, ative o atributo Descobertas no Incident Manager. As Descobertas são informações sobre implantações do AWS CodeDeploy e atualizações de pilha do AWS CloudFormation da época de um incidente. Ter essas informações

economiza tempo na avaliação de possíveis causas, o que pode reduzir o tempo médio de recuperação (MTTR) de um incidente.

Agora que você monitora incidentes nos aplicativos, é possível definir um plano de resposta a incidentes para usar durante incidentes. Para saber mais sobre como criar planos de resposta, consulte Como trabalhar com planos de resposta no Incident Manager. Os eventos do Amazon EventBridge ou os Alarmes do CloudWatch podem criar automaticamente um incidente usando planos de resposta como modelo. Para saber mais sobre como criar incidentes, consulte Criação de incidentes no Incident Manager.

Os planos de resposta lançam os respectivos planos de escalonamento e planos de engajamento para envolver os primeiros a responder no incidente. Para obter mais informações sobre como configurar planos de escalonamento, consulte Criar um plano de escalação. Simultaneamente, o AWS Chatbot notifica os respondentes usando um canal de chat direcionando os respondentes para a página de detalhes do incidente. Usando o canal de chat e os detalhes do incidente, a equipe pode se comunicar e fazer a triagem de um incidente. Para obter mais informações sobre configuração de canais de chat no Incident Manager, consulte Tarefa 2: criar um canal de chat no AWS Chatbot.

Triagem

A triagem é quando os respondentes tentam determinar o impacto nos clientes. A visualização dos detalhes do incidente no console do Incident Manager fornece aos respondentes cronogramas e métricas para ajudar a avaliar o incidente. A avaliação do impacto de um incidente também estabelece as bases para o tempo de resposta, resolução e comunicação do incidente. Os respondentes priorizam os incidentes usando classificações de impacto de 1 (crítico) a 5 (sem impacto).

Sua organização pode definir o escopo exato de cada classificação de impacto da maneira que preferir. A tabela a seguir fornece exemplos de como normalmente é definido cada nível de impacto.

Código de impacto	Nome do impacto	Escopo definido por amostra
1	`Critical`	Falha total do aplicativo que afeta a maioria dos clientes.
2	`High`	Falha total do aplicativo que afeta uma parte dos clientes.

Código de impacto	Nome do impacto	Escopo definido por amostra
3	`Medium`	Falha parcial do aplicativo que afeta o cliente.
4	`Low`	Falhas intermitentes que têm impacto limitado nos clientes.
5	`No Impact`	Os clientes não estão sendo afetados no exato momento, mas é necessária uma ação urgente para evitar um impacto.

Investigação e mitigação

A visualização de detalhes do incidente fornece à equipe runbooks, cronogramas e métricas. Para ver como você pode lidar com um incidente, consulte os Detalhes do incidente.

Os runbooks geralmente fornecem etapas de investigação e podem extrair dados ou tentar as soluções mais comuns automaticamente. Os runbooks também fornecem etapas claras e reproduzíveis, que sua equipe já tenha achado útil ao mitigar incidentes. A guia runbook foca na etapa atual do runbook e mostra as etapas anteriores e as próximas.

O Incident Manager faz uma integração com o Systems Manager Automation para criar runbooks. Use runbooks para:

- Gerenciar instâncias e recursos da AWS
- Executar scripts automaticamente
- Gerenciar recursos do AWS CloudFormation

Para obter mais informações sobre as ações de automação, consulte Referência de ações do Systems Manager Automation no Guia do usuário do AWS Systems Manager.

A guia Cronograma mostra quais ações foram tomadas. A linha do tempo registra cada um com um carimbo de data/hora e detalhes criados automaticamente. Para adicionar eventos personalizados

à linha do tempo, consulte a seção Linha do tempo na página Detalhes do incidente deste guia do usuário.

A guia Diagnóstico mostra métricas preenchidas automaticamente e métricas adicionadas manualmente. Essa visualização fornece informações valiosas sobre as atividades do aplicativo durante um incidente.

A guia Engajamentos permite adicionar mais contatos ao incidente e ajuda a fornecer os recursos para que o contato envolvido se atualize rapidamente depois de acionado. Os contatos são engajados seguindo os planos de escalonamento ou planos de engajamento pessoal definidos.

Pelo canal de chat, é possível interagir diretamente com o incidente e com outros respondentes da sua equipe. Com o AWS Chatbot, é possível configurar canais de chat no Slack, no Microsoft Teams e no Amazon Chime. Nos canais do Slack e do Microsoft Teams, os respondentes podem interagir com incidentes diretamente do canal de chat usando vários comandos do `ssm-incidents`. Para obter mais informações, consulte Como interagir pelo canal de chat.

Análise pós-incidente

O Incident Manager fornece toda a estrutura para refletir sobre um incidente, tomar as medidas necessárias para evitar que o incidente ocorra novamente no futuro e para melhorar as atividades gerais de resposta a incidentes. Entre as melhorias estão:

- Alterações nos aplicativos envolvidos em um incidente. Sua equipe pode usar esse tempo para melhorar o sistema e torná-lo mais tolerante a falhas.
- Mudanças no plano de resposta a incidentes. Reserve um tempo para incorporar as lições aprendidas.
- Mudanças nos runbooks. Sua equipe pode se aprofundar nas etapas necessárias para a resolução e nas etapas que podem automatizar.
- Alterações nos alertas. Depois de um incidente, sua equipe pode ter notado pontos críticos nas métricas que podem ser usados para alertar a equipe muito antes sobre um incidente.

O Incident Manager facilita essas possíveis melhorias aplicando um questionário de análise pós-incidente e itens de ação junto com o cronograma do incidente. Para saber mais sobre as melhorias por meio de análise, consulte Como realizar uma análise pós-incidente no Incident Manager.

Configurando o AWS Systems Manager Incident Manager

Recomendamos configurar o AWS Systems Manager Incident Manager na conta que você usa para gerenciar suas operações. Antes de usar o Incident Manager pela primeira vez, execute as seguintes tarefas:

Tópicos

- Inscreva-se para um Conta da AWS
- Criar um usuário com acesso administrativo
- Conceder acesso programático
- Perfil necessário para a configuração do Incident Manager

Inscreva-se para um Conta da AWS

Se você não tiver um Conta da AWS, conclua as etapas a seguir para criar um.

Para se inscrever em um Conta da AWS

1. Abra https://portal.aws.amazon.com/billing/signup.
2. Siga as instruções on-line.

   Parte do procedimento de inscrição envolve receber uma chamada telefônica e digitar um código de verificação no teclado do telefone.

   Quando você se inscreve em um Conta da AWS, um Usuário raiz da conta da AWSé criado. O usuário-raiz tem acesso a todos os Serviços da AWS e recursos na conta. Como prática recomendada de segurança, atribua o acesso administrativo a um usuário e use somente o usuário-raiz para executar tarefas que exigem acesso de usuário-raiz.

AWS envia um e-mail de confirmação após a conclusão do processo de inscrição. A qualquer momento, é possível visualizar as atividades da conta atual e gerenciar sua conta acessando https://aws.amazon.com/ e selecionando Minha conta.

Criar um usuário com acesso administrativo

Depois de se inscrever em um Conta da AWS, proteja seu Usuário raiz da conta da AWS AWS IAM Identity Center, habilite e crie um usuário administrativo para que você não use o usuário root nas tarefas diárias.

Proteja seu Usuário raiz da conta da AWS

1. Faça login AWS Management Consolecomo proprietário da conta escolhendo Usuário raiz e inserindo seu endereço de Conta da AWS e-mail. Na próxima página, digite sua senha.

   Para obter ajuda ao fazer login usando o usuário-raiz, consulte Signing in as the root user (Fazer login como usuário-raiz) no Guia do usuário do Início de Sessão da AWS .

2. Habilite a autenticação multifator (MFA) para o usuário-raiz.

   Para obter instruções, consulte Habilitar um dispositivo de MFA virtual para seu usuário Conta da AWS raiz (console) no Guia do usuário do IAM.

Criar um usuário com acesso administrativo

1. Habilitar o IAM Identity Center.

   Para obter instruções, consulte Habilitar AWS IAM Identity Center no Guia do usuário do AWS IAM Identity Center .

2. No Centro de Identidade do IAM, conceda o acesso administrativo para um usuário.

   Para ver um tutorial sobre como usar o Diretório do Centro de Identidade do IAM como fonte de identidade, consulte Configurar o acesso do usuário com o padrão Diretório do Centro de Identidade do IAM no Guia AWS IAM Identity Center do usuário.

Iniciar sessão como o usuário com acesso administrativo

- Para fazer login com seu usuário do Centro de Identidade do IAM, use a URL de login que foi enviada ao seu endereço de e-mail quando você criou o usuário do Centro do Usuário do IAM.

  Para obter ajuda para fazer login usando um usuário do IAM Identity Center, consulte Como fazer login no portal de AWS acesso no Guia Início de Sessão da AWS do usuário.

Atribuir acesso a usuários adicionais

1. No Centro de Identidade do IAM, crie um conjunto de permissões que siga as práticas recomendadas de aplicação de permissões com privilégio mínimo.

   Para obter instruções, consulte Create a permission set no Guia do usuário do AWS IAM Identity Center .

2. Atribua usuários a um grupo e, em seguida, atribua o acesso de autenticação única ao grupo.

   Para obter instruções, consulte Add groups no Guia do usuário do AWS IAM Identity Center .

Conceder acesso programático

Os usuários precisam de acesso programático se quiserem interagir com pessoas AWS fora do AWS Management Console. A forma de conceder acesso programático depende do tipo de usuário que está acessando AWS.

Para conceder acesso programático aos usuários, selecione uma das seguintes opções:

Qual usuário precisa de acesso programático?	Para	Por
Identificação da força de trabalho (Usuários gerenciados no Centro de Identidade do IAM)	Use credenciais temporári as para assinar solicitações programáticas para AWS SDKs ou APIs. AWS CLI AWS	Siga as instruções da interface que deseja utilizar. • Para o AWS CLI, consulte Configurando o AWS CLI para uso AWS IAM Identity Center no Guia do AWS Command Line Interface usuário. • Para AWS SDKs, ferrament as e AWS APIs, consulte a autenticação do IAM Identity Center no Guia de referência de AWS SDKs e ferramentas.

Qual usuário precisa de acesso programático?	Para	Por
IAM	Use credenciais temporári as para assinar solicitações programáticas para AWS SDKs ou APIs. AWS CLI AWS	Siga as instruções em Como usar credenciais temporárias com AWS recursos no Guia do usuário do IAM.
IAM	(Não recomendado) Use credenciais de longo prazo para assinar solicitaç ões programáticas para AWS SDKs AWS CLI ou APIs. AWS	Siga as instruções da interface que deseja utilizar. • Para isso AWS CLI, consulte Autenticação usando credenciais de usuário do IAM no Guia do AWS Command Line Interface usuário. • Para AWS SDKs e ferramentas, consulte Autenticar usando credencia is de longo prazo no Guia de referência de AWS SDKs e ferramentas. • Para AWS APIs, consulte Gerenciamento de chaves de acesso para usuários do IAM no Guia do usuário do IAM.

Perfil necessário para a configuração do Incident Manager

Antes de começar, sua conta deve ter a permissão do IAM `iam:CreateServiceLinkedRole`. O Incident Manager usa essa permissão para criar o `AWSServiceRoleforIncidentManager` em sua conta. Para ter mais informações, consulte Usar perfis vinculados ao serviço do Incident Manager.

Conceitos básicos do Incident Manager

Esta seção explica o Prepare-se no console do Incident Manager. Você precisa concluir o Prepare-se no console antes de poder iniciar o gerenciamento de incidentes. O assistente orienta você na configuração do conjunto de replicação, de pelo menos um contato e um plano de escalação, além do primeiro plano de resposta. Os guias a seguir ajudarão você a entender o Incident Manager e o ciclo de vida do incidente:

- O que é o AWS Systems Manager Incident Manager?
- O ciclo de vida do incidente no Incident Manager

Pré-requisitos

Se você estiver usando o Incident Manager pela primeira vez, consulte o Configurando o AWS Systems Manager Incident Manager. Recomendamos configurar o Incident Manager na conta que você usa para gerenciar suas operações.

Recomendamos que você realize a configuração rápida do Systems Manager antes de iniciar o assistente Prepare-se do Incident Manager. Use a Configuração rápida do Systems Manager para configurar os serviços e os atributos da AWS conforme as práticas recomendadas. O Incident Manager usa os recursos do Systems Manager para gerenciar incidentes associados a suas contas da Contas da AWS e os benefícios de ter o Systems Manager configurado primeiro.

Assistente Prepare-se

Na primeira vez que usar o Incident Manager, você poderá acessar o assistente Prepare-se na página inicial do serviço Incident Manager. Para acessar o assistente Prepare-se depois de realizar a configuração pela primeira vez, escolha Preparar na página da lista Incidentes.

1. Abra o console do Incident Manager.
2. Na página inicial do serviço Incident Manager, escolha Prepare-se.

Configurações gerais

1. Em Configurações gerais, escolha Arquivos.

2. Leia os Termos e condições. Se você concordar com os termos e condições do Incident Manager, selecione Eu li e concordo com os termos e condições do Incident Manager e escolha Próximo.
3. Na área Regiões, sua atual Região da AWS aparece como a primeira região em seu conjunto de replicação. Para adicionar mais regiões ao seu conjunto de replicação, escolha-as na lista de regiões.

   Recomendamos incluir pelo menos duas regiões. Caso uma região esteja temporariamente indisponível, as atividades relacionadas a incidentes ainda podem ser roteadas para a outra região.

   > **Note**
   >
   > A criação do conjunto de replicação cria o perfil `AWSServiceRoleforIncidentManager` vinculado a serviços na conta. Para saber mais sobre esse perfil, consulte Usar perfis vinculados ao serviço do Incident Manager.

4. Para configurar a criptografia do conjunto de replicação, faça um dos seguintes procedimentos:

   > **Note**
   >
   > Todos os recursos do Incident Manager são criptografados. Para saber mais sobre como seus dados são criptografados, consulte Proteção de dados no Incident Manager. Para obter mais informações sobre o conjunto de replicação do Incident Manager, consulte Como usar o conjunto de replicação do Incident Manager.

   - Para usar uma AWS chave própria, escolha Usar AWS chave própria.
   - Para usar sua própria AWS KMS chave, escolha Escolher uma AWS KMS key existente. Para cada região selecionada na etapa 3, escolha uma chave AWS KMS ou insira um nome do recurso da Amazon (ARN) do AWS KMS.

     > **Tip**
     >
     > Se você não tiver uma AWS KMS key disponível, escolha Criar uma AWS KMS key.

5. (Opcional) Na área Tags insira uma ou mais tags para o conjunto de replicação. Uma tag inclui uma chave e, opcionalmente, um valor.

Tags são metadados opcionais que você atribui a um recurso. As tags permitem categorizar um recurso de diferentes formas, como por finalidade, proprietário ou ambiente. Para obter mais informações, consulte Marcando recursos no Incident Manager.

6. (Opcional) Na área Acesso ao serviço, para ativar o atributo Descobertas, escolha a caixa de seleção Criar perfil de serviço para descobertas nesta conta.

   Uma descoberta é uma informação sobre uma implantação de código ou alteração na infraestrutura que ocorreu na mesma época em que um incidente foi criado. Cada descoberta pode ser examinada como uma possível causa do incidente. As informações sobre essas possíveis causas são adicionadas à página Detalhes do incidente. Com informações sobre essas implantações e mudanças prontamente disponíveis, os respondentes não precisam pesquisar essas informações manualmente.

   > **Tip**
   >
   > Para ver informações sobre o perfil a ser criado, escolha Exibir permissões.

7. Escolha Criar.

   Para saber mais sobre conjuntos de replicação e resiliência, consulte Resiliência em AWS Systems Manager Incident Manager.

Contatos (opcional)

1. Escolha Criar contato.

   O Incident Manager engaja os contatos durante um incidente. Para obter mais informações sobre contatos, consulte Como trabalhar com contatos do Incident Manager.

2. Em Nome, insira o nome do contato.
3. Em Alias exclusivo, insira um alias para identificar esse contato.
4. Na seção Canal de contato, faça o seguinte para definir como o contato será engajado durante incidentes:

   a. Em Tipo, escolha E-mail, SMS ou Voz.
   b. Em Nome do canal, insira um nome exclusivo para ajudá-lo a identificar o canal.
   c. Em Detalhes, insira o endereço de e-mail ou número de telefone do contato.

Os números de telefone devem ter de 9 a 15 caracteres e começar com +, seguidos pelo código do país e pelo número do assinante.

d. Para criar outro canal de contato, escolha Adicionar um novo canal de contato. Recomendamos definir pelo menos dois canais para cada contato.

5. Na área Plano de engajamento, faça o seguinte para definir por quais canais notificar o contato e por quanto tempo esperar por uma confirmação em cada canal. Selecione os canais de contato a serem usados para interagir com o contato durante incidentes.

> **Note**
>
> Recomendamos definir pelo menos dois dispositivos no plano de engajamento.

a. Em Nome do canal de contato, escolha um canal especificado na área Canal de contato.

b. Em Tempo de engajamento (min), insira o número de minutos de espera antes de interagir com o canal de contato.

   Recomendamos que você selecione pelo menos um dispositivo para engajar no início de um engajamento, especificando **0** (zero) minutos de tempo de espera.

c. Para adicionar mais canais de contato ao plano de engajamento, escolha Adicionar engajamento.

6. (Opcional) Na área Tags insira uma ou mais tags para o contato. Uma tag inclui uma chave e, opcionalmente, um valor.

   Tags são metadados opcionais que você atribui a um recurso. As tags permitem categorizar um recurso de diferentes formas, como por finalidade, proprietário ou ambiente. Para obter mais informações, consulte Marcando recursos no Incident Manager.

7. Para criar o registro de contato e enviar códigos de ativação para os canais de contato definidos, escolha Próximo.

8. (Opcional) Na página Ativação do canal de contato, insira o código de ativação enviado para cada canal.

   Você pode gerar novos códigos de ativação posteriormente se não conseguir inseri-los agora.

9. Repita a etapa quatro até adicionar todos os seus contatos ao Incident Manager.

10. Depois que todos os contatos forem inseridos, escolha Concluir.

(Opcional) Planos de escalação

1. Escolha Criar plano de escalação.

   Um plano de escalação escala os contatos durante um incidente, garantindo que o Incident Manager envolva os respondentes corretos durante um incidente. Para obter mais informações sobre planos de escalação, consulte Como trabalhar com planos de escalação no Incident Manager.
2. Em Nome, insira um nome exclusivo para o plano de escalação.
3. Em Alias, insira um alias exclusivo para ajudá-lo a identificar o plano de escalação.
4. Na área do Estágio 1, faça o seguinte:

   a. Em Canal de escalação, escolha os canais de contato para engajar.

   b. Se você quiser que um contato possa interromper a progressão dos estágios do plano de escalação, selecione Confirmação interrompe a progressão do plano.

   c. Para adicionar mais canais a um estágio, escolha Adicionar canal de escalação.
5. Para criar um novo estágio no plano de escalação, escolha Adicionar estágio e adicione os detalhes do estágio.
6. (Opcional) Na área Tags adicione uma ou mais tags ao plano de escalação. Uma tag inclui uma chave e, opcionalmente, um valor.

   Tags são metadados opcionais que você atribui a um recurso. As tags permitem categorizar um recurso de diferentes formas, como por finalidade, proprietário ou ambiente. Para obter mais informações, consulte Marcando recursos no Incident Manager.
7. Escolha Criar plano de escalação.

Plano de resposta

1. Selecione Criar plano de resposta. Use o plano de resposta para reunir os contatos e os planos de escalação criados. Ao usar o assistente Prepare-se, as seções a seguir são opcionais, especialmente se for a primeira vez que você configura um plano de resposta:

   - Canal de chat
   - Runbooks
   - Engajamentos
   - Integrações de terceiros

Para obter informações sobre como adicionar esses elementos aos planos de resposta posteriormente, consulte Preparação para incidentes no Incident Manager.

2. Em Nome, insira um nome exclusivo e identificável para o plano de resposta. O nome é usado para criar o ARN do plano de resposta ou em planos de resposta sem nome de exibição.
3. (Opcional) Em Nome de exibição, insira um nome para ajudá-lo a identificar esse plano de resposta ao criar incidentes.
4. Em Título, insira um título para ajudar a identificar o tipo de incidente relacionado a esse plano de resposta. O valor que você especifica está incluído no título de cada incidente. O alarme ou o evento que iniciou o incidente também é adicionado ao título.
5. Em Impacto, selecione o nível de impacto que você espera para incidentes relacionados a esse plano de resposta, como **`Critical`** ou **`Low`**.
6. (Opcional) Em Resumo, insira uma breve descrição usada para fornecer uma visão geral do incidente. O Incident Manager preenche automaticamente as informações relevantes no resumo durante um incidente.
7. (Opcional) Em Cadeia de desduplicação, insira uma cadeia de caracteres de desduplicação. O Incident Manager usa essa string para evitar que a mesma causa raiz crie vários incidentes na mesma conta.

   Uma sequência de desduplicação é um termo ou frase que o sistema usa para verificar incidentes duplicados. Se você especificar uma string de desduplicação, o Incident Manager pesquisará incidentes abertos que contenham a mesma string `dedupeString` no campo ao criar o incidente. Se uma duplicação for detectada, o Incident Manager desduplica o incidente mais recente no incidente existente.

   > **Note**
   >
   > Por padrão, o Incident Manager desduplica automaticamente vários incidentes criados pelo mesmo alarme do Amazon CloudWatch ou no evento do Amazon EventBridge. Você não precisa inserir sua própria sequência de desduplicação para evitar a duplicação desses tipos de recursos.

8. (Opcional) Na área Tags adicione uma ou mais tags ao plano de resposta. Uma tag inclui uma chave e, opcionalmente, um valor.

Tags são metadados opcionais que você atribui a um recurso. As tags permitem categorizar um recurso de diferentes formas, como por finalidade, proprietário ou ambiente. Para obter mais informações, consulte Marcando recursos no Incident Manager.

9. Selecione os contatos e os planos de escalação a serem aplicados ao incidente no menu suspenso Engajamentos.
10. Selecione Criar plano de resposta.

Depois de criar um plano de resposta, você pode associar os alarmes do Amazon CloudWatch ou os eventos do Amazon EventBridge ao plano de resposta. Isso criará automaticamente um incidente com base em um alarme ou evento. Para obter mais informações, consulte Criação de incidentes no Incident Manager.

Incident management entre regiões e entre contas no Incident Manager

Você pode configurar o Incident Manager, um recurso do AWS Systems Manager, para lidar com várias Regiões da AWS e contas. Esta seção descreve as práticas recomendadas, etapas de configuração e limitações conhecidas ao trabalhar entre regiões e entre contas.

Tópicos

- Incident management entre regiões
- Gerenciamento de incidentes entre contas

Incident management entre regiões

O Incident Manager oferece suporte à criação automática e manual de incidentes em várias Regiões da AWS. Ao se integrar inicialmente ao Incident Manager usando o assistente Prepare-se, você pode especificar até três Regiões da AWS no conjunto de replicação. Para incidentes automaticamente criados por alarmes do Amazon CloudWatch ou eventos do Amazon EventBridge, o Incident Manager cria um incidente na mesma Região da AWS como a regra de alarme ou evento. Se o Incident Manager não estiver disponível na Região da AWS, o CloudWatch ou o EventBridge criarão automaticamente o incidente em uma das regiões disponíveis especificadas no conjunto de replicação.

> **Important**
>
> Observe os seguintes detalhes importantes.
>
> - Recomendamos que você especifique pelo menos duas Regiões da AWS no conjunto de replicação. Se você não especificar pelo menos duas regiões, o sistema falhará em criar incidentes durante o período em que o Incident Manager não estiver disponível.
> - Os incidentes criados por um failover entre regiões não invocam os runbooks especificados nos planos de resposta.

Para obter mais informações sobre integração com o Incident Manager e especificação de regiões adicionais, consulte Conceitos básicos do Incident Manager.

Gerenciamento de incidentes entre contas

O Incident Manager usa AWS Resource Access Manager (AWS RAM) para compartilhar os recursos do Incident Manager entre contas de gerenciamento e aplicativos. Esta seção descreve as práticas recomendadas entre contas, como configurar a funcionalidade entre contas para o Incident Manager e as limitações conhecidas da funcionalidade entre contas no Incident Manager.

Uma conta de gerenciamento é a conta na qual você executa o gerenciamento de operações. No caso de uma organização, a conta de gerenciamento é proprietária dos planos de resposta, contatos, planos de escalação, runbooks e outros recursos do AWS Systems Manager.

A conta de aplicativo é a conta que controla os recursos que compõem os seus aplicativos. Esses recursos podem ser instâncias do Amazon EC2, tabelas do Amazon DynamoDB ou qualquer outro recurso que você usa para criar aplicativos no Nuvem AWS. As contas de aplicativo também controlam os alarmes do Amazon CloudWatch e os do Amazon EventBridge que criam incidentes no Incident Manager.

O AWS RAM usa compartilhamentos de recursos para compartilhar recursos entre contas. Você pode compartilhar o plano de resposta e os recursos de contato entre contas no AWS RAM. Ao compartilhar esses recursos, as contas de aplicativos e as contas de gerenciamento podem interagir com engajamentos e incidentes. Compartilhar um plano de resposta compartilha todos os incidentes passados e futuros criados usando esse plano de resposta. Compartilhar um contato compartilha todos os engajamentos passados e futuros do plano de contato ou resposta.

Práticas recomendadas

Siga estas práticas recomendadas ao compartilhar seus recursos do Incident Manager entre contas:

- Atualize regularmente o compartilhamento de recursos com planos de resposta e contatos.
- Analise regularmente os princípios de compartilhamento de recursos.
- Configure o Incident Manager, os runbooks e os canais de chat na sua conta de gerenciamento.

Definir e configurar incident management entre regiões e entre regiões

As etapas a seguir descrevem como instalar e configurar os recursos do Incident Manager ativando a funcionalidade entre contas. Você pode ter configurado alguns serviços e recursos ativando a funcionalidade entre contas no passado. Use essas etapas como uma lista de verificação dos requisitos antes de iniciar seu primeiro incidente usando recursos entre contas.

1. (Opcional) Criar organizações e unidades organizacionais usando o AWS Organizations. Siga as etapas no Tutorial: criar e configurar uma organização no Guia do usuário do AWS Organizations.
2. (Opcional) Use o recurso de configuração rápida do Systems Manager para configurar os perfis AWS Identity and Access Management corretos para usar ao configurar seus runbooks entre contas. Para obter mais informações, consulte Configuração Rápida no Guia do usuário do AWS Systems Manager.
3. Siga as etapas listadas em Como executar automações em várias Regiões da AWS e contas no Guia do usuário do AWS Systems Manager para criar runbooks em seus documentos de automação do Systems Manager. Um runbook pode ser executado por uma conta de gerenciamento ou por uma de suas contas de aplicativo. Dependendo do seu caso de uso, você precisará instalar o modelo do AWS CloudFormationapropriado para os perfis necessários para criar e visualizar runbooks durante um incidente.
   - Como executar um runbook na conta de gerenciamento. A conta de gerenciamento deve baixar e instalar o modelo do `AWS-SystemsManager-AutomationReadOnlyRole` CloudFormation. Ao instalar o `AWS-SystemsManager-AutomationReadOnlyRole`, especifique os IDs de conta de todas as contas de aplicativo. Esse perfil permitirá que as contas de aplicativos leiam o status do runbook na página de detalhes do incidente. A conta de aplicativo deve instalar o modelo do `AWS-SystemsManager-AutomationAdministrationReadOnlyRole` CloudFormation. A página de detalhes do incidente usa esse perfil para obter o status de automação da conta de gerenciamento.
   - Como executar um runbook em uma conta de aplicativo. A conta de gerenciamento deve baixar e instalar o modelo do `AWS-SystemsManager-AutomationAdministrationReadOnlyRole` CloudFormation. Esse perfil permite que a conta de gerenciamento leia o status do runbook na conta de aplicativo. A conta de aplicativo deve baixar e instalar o modelo do `AWS-SystemsManager-AutomationReadOnlyRole`CloudFormation. Ao instalar o `AWS-SystemsManager-AutomationReadOnlyRole`, especifique o ID da conta, da conta de gerenciamento e de outras contas de aplicativo. A conta de gerenciamento e as outras contas de aplicativo assumem esse perfil para ler o status do runbook.
4. (Opcional) Em cada conta de aplicativo da organização, baixe e instale o modelo `AWS-SystemsManager-IncidentManagerIncidentAccessServiceRole` do CloudFormation. Ao instalar o `AWS-SystemsManager-IncidentManagerIncidentAccessServiceRole`, especifique o ID da conta, da conta de gerenciamento. Esse perfil fornece as permissões que o Incident Manager precisa para acessar informações sobre implantações do AWS CodeDeploy

e atualizações de pilha do AWS CloudFormation. Essas informações são relatadas como descobertas de um incidente se o atributo Descobertas estiver ativado. Para obter mais informações, consulte Como trabalhar com descobertas no Incident Manager.

5. Para configurar e criar contatos, planos de escalação, canais de chat e planos de resposta, siga as etapas detalhadas em Preparação para incidentes no Incident Manager.
6. Adicione seus contatos e recursos do plano de resposta ao compartilhamento de recursos existente ou a um novo compartilhamento de recursos no AWS RAM. Para obter mais informações, consulte Comece a usar o AWS RAM no Manual do usuário do AWS RAM. Adicionar planos de resposta ao AWS RAM permite que as contas de aplicativos acessem incidentes e painéis de incidentes criados usando os planos de resposta. As contas de aplicativos também ganham a capacidade de associar alarmes do CloudWatch e eventos do EventBridge a um plano de resposta. Adicionar os contatos e os planos de escalação ao AWS RAM permite que as contas do aplicativo visualizem os engajamentos e engajem os contatos no painel de incidentes.
7. Adicionar a funcionalidade entre contas e entre regiões ao console do CloudWatch. Para obter etapas e informações, consulte Console do CloudWatch entre contas e entre regiões no Guia do usuário do Amazon CloudWatch. Adicionar essa funcionalidade garante que as contas de aplicativo e a conta de gerenciamento que você criou possam visualizar e editar métricas nos painéis de incidentes e análises.
8. Criar um barramento de eventos do Amazon EventBridge entre contas. Para obter etapas e informações, consulte Como enviar e receber eventos Amazon EventBridge entre contas da AWS. Você pode usar esse barramento de eventos para criar regras de eventos que detectem incidentes nas contas de aplicativo e criem incidentes na conta de gerenciamento.

Limitações

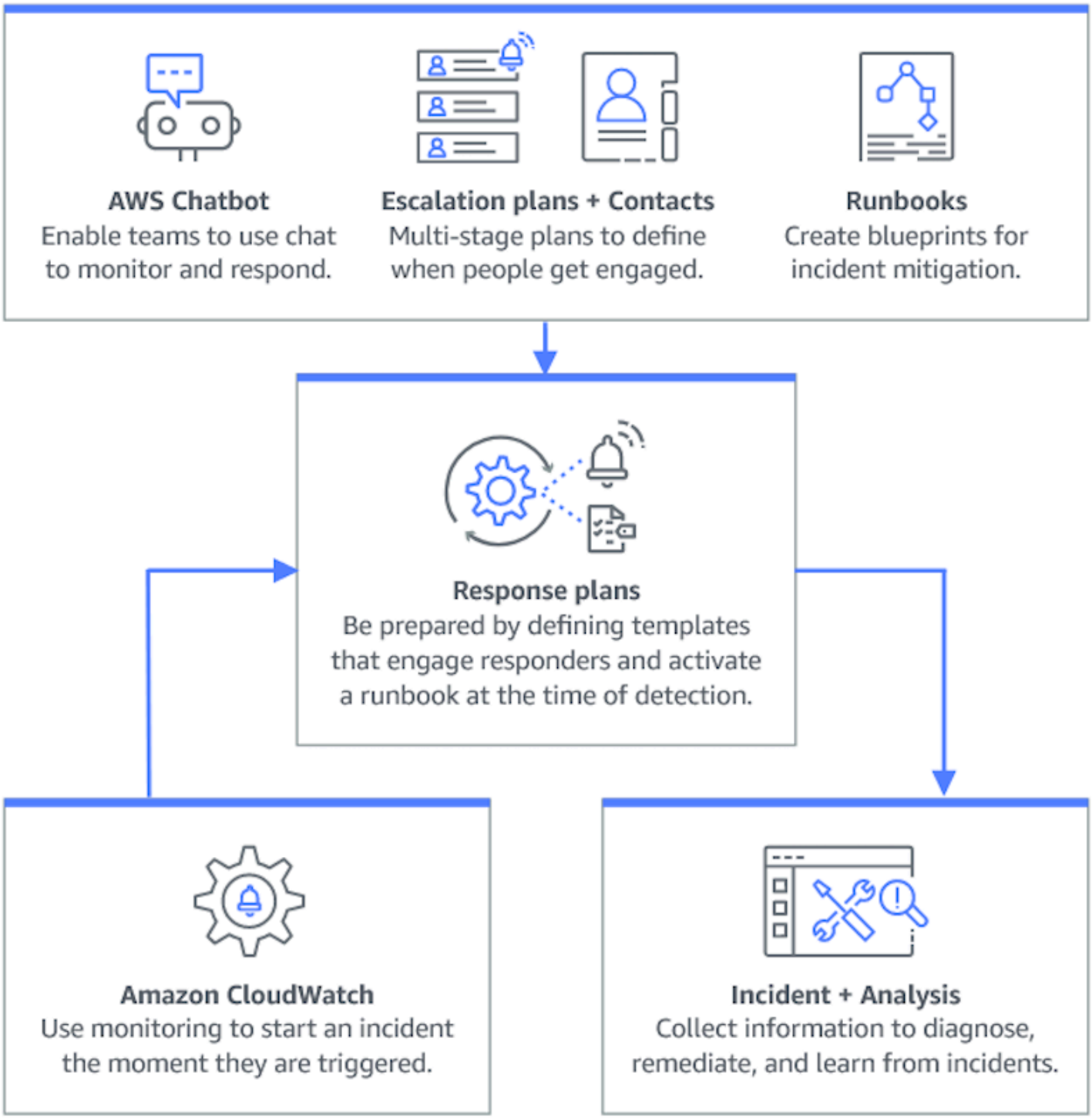
Aqui estão as limitações conhecidas da funcionalidade entre contas do Incident Manager:

- A conta que cria uma análise pós-incidente é a única que pode visualizá-la e alterá-la. Se você usar uma conta de aplicativo para criar uma análise pós-incidente, somente membros dessa conta poderão visualizá-la e alterá-la. O mesmo acontece se você usar uma conta de gerenciamento para criar uma análise pós-incidente.
- Os eventos da linha do tempo não são preenchidos em documentos de automação executados em contas de aplicativos. As atualizações dos documentos de automação executados nas contas de aplicativo estão visíveis na guia Runbook do incidente.

- Os tópicos do Amazon Simple Notification Service não podem ser usados entre contas. Os tópicos do Amazon SNS devem ser criados na mesma região e conta do plano de resposta em que são usados. Recomendamos usar a conta de gerenciamento para criar todos os tópicos e planos de resposta do SNS.
- Os planos de escalação só podem ser criados usando contatos da mesma conta. Um contato que foi compartilhado com você não pode ser adicionado a um plano de escalação da sua conta.
- As etiquetas aplicadas aos planos de resposta, registros de incidentes e contatos só podem ser visualizados e modificados na conta do proprietário do recurso.

Preparação para incidentes no Incident Manager

O planejamento de um incidente começa muito antes do ciclo de vida do incidente. Para se preparar para um incidente, considere cada um dos tópicos a seguir antes de criar planos de resposta. Use monitoramento, contatos, planos de escalação, canais de chat e runbooks para criar planos de resposta que automatizem a resposta.



Tópicos

- Monitorar
- Trabalhar com configurações gerais
- Como trabalhar com contatos do Incident Manager

- Trabalhando com programações de plantão no Incident Manager
- Como trabalhar com planos de escalação no Incident Manager
- Trabalhando com canais de chat no Incident Manager
- Trabalho com runbooks do Automation do Systems Manager no Incident Manager
- Como trabalhar com planos de resposta no Incident Manager
- Como trabalhar com descobertas no Incident Manager

Monitorar

Monitorar a integridade de seus aplicativos hospedados da AWS é fundamental para garantir o tempo de atividade e o desempenho dos aplicativos. Ao determinar as soluções de monitoramento, considere o seguinte:

- Criticidade do atributo — em caso de falha, qual o nível do impacto para os usuários na sequência.
- Falhas comuns — com que frequência o sistema falha; sistemas que requerem intervenção frequente devem ser monitorados de perto.
- Aumento da latência — qual foi o aumento ou a redução de tempo para concluir uma tarefa.
- Métricas do lado do cliente versus lado do servidor — se há discrepância entre métricas relacionadas no cliente e no servidor.
- Falhas de dependência — falhas para as quais sua equipe pode e deve se preparar.

Depois de criar planos de resposta, você pode usar as soluções de monitoramento para rastrear automaticamente os incidentes no momento em que eles acontecem no seu ambiente. Para obter mais informações sobre rastreamento e criação de incidentes, consulte Rastreamento de incidentes no Incident Manager.

Para obter mais informações sobre como criar aplicações de infraestrutura e workloads de alta performance mais seguras, resilientes e eficientes, consulte o whitepaper AWS arquitetada.

Trabalhar com configurações gerais

Depois de concluir o assistente de integração do Incident Manager, você pode gerenciar determinadas opções na página Configurações. Essas opções incluem seu conjunto de replicação, as tags aplicadas ao conjunto de replicação e o atributo Descobertas.

Tópicos

- Como usar o conjunto de replicação do Incident Manager
- Como gerenciar tags de um conjunto de replicação
- Como gerenciar o atributo Descobertas

Como usar o conjunto de replicação do Incident Manager

O conjunto de replicação do Incident Manager replica seus dados para muitas Regiões da AWS aumentando a redundância entre regiões e permitindo que o Incident Manager acesse recursos em diferentes regiões e reduza a latência para os usuários. O conjunto de replicação também é usado para criptografar seus dados com uma Chave gerenciada pela AWS ou com sua própria chave gerenciada pelo cliente. Todos os recursos do Incident Manager são criptografados por padrão. Para saber mais sobre como os recursos são criptografados, consulte Proteção de dados no Incident Manager. Para começar a usar o Incident Manager, primeiro crie seu conjunto de replicação usando o assistente Prepare-se. Para saber mais sobre como se preparar no Incident Manager, consulte Assistente Prepare-se.

Como editar seu conjunto de replicação

Na página Configurações do Incident Manager, você pode editar seu conjunto de replicação. Você pode adicionar regiões, excluir regiões e ativar ou desativar a proteção contra exclusão do conjunto de replicação. Você não pode editar a chave usada para criptografar seus dados. Para alterar a chave, exclua e recrie o conjunto de replicação.

Adicionar uma região

1. Abra o console do Incident Manager e escolha Configurações no painel de navegação esquerdo.
2. Selecione Adicionar região.
3. Selecione a Região.
4. Escolha Adicionar.

Excluir uma região

1. Abra o console do Incident Manager e escolha Configurações no painel de navegação esquerdo.
2. Selecione a região que deseja excluir.
3. Escolha Excluir.

4. Insira excluir na caixa de texto e escolha Excluir.

Como excluir seu conjunto de replicação

A exclusão da última região no conjunto de replicação exclui todo o conjunto de replicação. Antes de excluir a última região, desative a proteção contra exclusão ativando a Proteção contra exclusão na página Configurações. Depois de excluir o conjunto de replicação, você pode criar um novo conjunto de replicação usando o assistente Prepare-se.

Para excluir uma região do conjunto de replicação, aguarde 24 horas após a criação. Tentar excluir uma região do conjunto de replicação antes dessas 24 horas após a criação faz com que a exclusão falhe.

A exclusão do conjunto de replicação exclui todos os dados do Incident Manager.

Excluir o conjunto de replicação

1. Abra o console do Incident Manager e escolha Configurações no painel de navegação esquerdo.
2. Selecione a última região do conjunto de replicação.
3. Escolha Excluir.
4. Insira excluir na caixa de texto e escolha Excluir.

Como gerenciar tags de um conjunto de replicação

Tags são metadados opcionais que você atribui a um recurso. As tags permitem categorizar um recurso de diferentes formas, como por finalidade, proprietário ou ambiente.

Para gerenciar tags de um conjunto de replicação

1. Abra o console do Incident Manager e escolha Configurações no painel de navegação esquerdo.
2. Na área Tags, escolha Editar.
3. Para adicionar uma tag, faça o seguinte:
   a. Selecione Add new tag (Adicionar nova etiqueta).
   b. Digite uma chave e, opcionalmente, um valor para a tag.
   c. Escolha Salvar.
4. Para excluir uma tag, faça o seguinte:

a. Ao lado da tag que deseja excluir, escolha Remover.

b. Escolha Salvar.

Como gerenciar o atributo Descobertas

O atributo Descobertas ajuda os respondentes de sua organização a identificar possíveis causas-raiz dos incidentes logo após o início dos incidentes. Atualmente, o Incident Manager fornece descobertas para implantações do AWS CodeDeploy e atualizações de pilha do AWS CloudFormation.

Para obter suporte para descobertas entre contas, depois de ativar o atributo, você deve realizar uma etapa adicional de configuração em cada conta de aplicativo na organização.

Para usar o atributo, permita que o Incident Manager crie um perfil de serviço que inclua as permissões necessárias para acessar dados em seu nome.

Para ativar o atributo Descobertas

1. Abra o console do Incident Manager e escolha Configurações no painel de navegação esquerdo.
2. Na área Descobertas, escolha Criar perfil de serviço.
3. Revise as informações sobre o perfil de serviço a ser criado e escolha Criar.

Para desativar o atributo Descobertas

Para parar de usar o atributo Descobertas, exclua o perfil `IncidentManagerIncidentAccessServiceRole` de cada conta em que foi criado.

1. Abra o console do IAM em https://console.aws.amazon.com/iam/.
2. No painel de navegação à esquerda, escolha Roles.
3. Na caixa de pesquisa, insira **`IncidentManagerIncidentAccessServiceRole`**.
4. Escolha o nome do perfil e escolha Excluir.
5. Insira o nome do perfil na caixa de diálogo para confirmar que deseja excluir o perfil e escolha Excluir.

Como trabalhar com contatos do Incident Manager

Os contatos AWS Systems Manager Incident Manager respondem a incidentes. Um contato pode ter vários canais com os quais o Incident Manager pode interagir durante um incidente. Você pode definir o plano de engajamento de um contato para descrever como e quando o Incident Manager envolve o contato.

Tópicos

- Canais de contato
- Planos de engajamento
- Criar um contato
- Importar detalhes de contato para seu catálogo de endereços

Canais de contato

Canais de contato são os diversos métodos que o Incident Manager utiliza para envolver um contato.

O Incident Manager suporta os seguintes canais de contato:

- E-mail
- SMS
- Voz

Ativação do canal de contato

Para proteger sua privacidade e segurança, o Incident Manager envia um código de ativação do dispositivo para você quando você cria contatos. Para engajar seus dispositivos durante um incidente, é preciso ativá-los primeiro. Para fazer isso, insira o código de ativação do dispositivo na página de criação de contato.

Alguns recursos do Incident Manager incluem funcionalidades que enviam notificações para um canal de contato. Ao usar esses recursos, você concorda que esse serviço envie notificações sobre interrupções no serviço ou outros eventos para os canais de contato incluídos no fluxo de trabalho especificado. Isso inclui notificações enviadas a um contato como parte de uma rotação de horário de plantão. As notificações podem ser enviadas por e-mail, SMS ou chamada de voz, conforme especificado nos detalhes de um contato. Ao usar esses recursos, você confirma que está autorizado a adicionar os canais de contato fornecidos ao Incident Manager.

Cancelar recebimento

Você pode cancelar as notificações a qualquer momento removendo o dispositivo móvel usado como canal de contato. Os destinatários de notificações individuais também podem cancelar notificações a qualquer momento removendo o dispositivo de seus contatos.

Para remover um canal de contato de um contato

1. Navegue até o console do Incident Manager e escolha Contatos no painel de navegação à esquerda.
2. Selecione o contato com o canal de contato que você está removendo e escolha Editar.
3. Escolha Remover ao lado do canal de contato que você gostaria de remover.
4. Escolha Atualizar.

Desativação do canal de contato

Para desativar um dispositivo, responda CANCELAR INSCRIÇÃO. Responder CANCELAR INSCRIÇÃO impede que o Incident Manager envolva seu dispositivo.

Reativação do canal de contato

1. Responda INICIAR à mensagem do Incident Manager.
2. Navegue até o console do Incident Manager e escolha Contatos no painel de navegação à esquerda.
3. Selecione o contato com o canal de contato que você está removendo e escolha Editar.
4. Escolha Ativar dispositivos.
5. Insira o Código de ativação enviado ao dispositivo pelo Incident Manager.
6. Selecione Ativar.

Planos de engajamento

Os planos de engajamento definem quando o Incident Manager envolve os canais de contato. Você pode interagir com os canais de contato várias vezes em diferentes estágios desde o início de um engajamento. Você pode usar planos de engajamento em um plano de escalação ou plano de resposta. Para saber mais sobre como criar planos de resposta, consulte Como trabalhar com planos de escalação no Incident Manager.

Criar um contato

Use as etapas a seguir para criar um contato.

1. Abra o console do Incident Manager e escolha Contatos no painel de navegação à esquerda.
2. Escolha Criar contato.
3. Digite o nome completo do contato e forneça um alias exclusivo e identificável.
4. Defina um Canal de contato. Recomendamos ter dois ou mais tipos diferentes de canais de contato.
   a. Escolha o tipo: e-mail, SMS ou voz.
   b. Informe um nome identificável para o canal de contato.
   c. Forneça os detalhes do canal de contato, como e-mail: arosalez@example.com
5. Para definir mais de um canal de contato, escolha Adicionar canal de contato. Repita a etapa 4 para cada novo canal de contato adicionado.
6. Defina um plano de engajamento.

   > **Important**
   > Para engajar um contato, você deve definir um plano de engajamento.

   a. Escolha o nome do canal de contato.
   b. Defina quantos minutos esperar, desde o início do engajamento, até que o Incident Manager interaja com esse canal de contato.
   c. Para adicionar outro canal de contato, escolha Adicionar engajamento.
7. Depois de definir seu plano de engajamento, escolha Criar. O Incident Manager envia um código de ativação para cada um dos canais de contato definidos.
8. (Opcional) Para ativar os canais de contato, insira o código de ativação que o Incident Manager enviou para cada canal de contato definido.
9. (Opcional) Para enviar um novo código de ativação, escolha Enviar novo código.
10. Escolha Finish.

Depois de definir um contato e ativar seus canais de contato, você pode adicionar contatos aos planos de escalação para formar uma cadeia de escalação. Para saber mais sobre como criar planos

de resposta, consulte Como trabalhar com planos de escalação no Incident Manager. Você pode adicionar contatos a um plano de resposta para engajamento direto. Para saber mais sobre como criar planos de resposta, consulte Como trabalhar com planos de resposta no Incident Manager.

Importar detalhes de contato para seu catálogo de endereços

Quando um incidente é criado, o Incident Manager pode notificar os respondentes por voz ou SMS. Para garantir que os respondentes vejam que a chamada ou a notificação por SMS é do Incident Manager, recomendamos que todos os respondentes baixem o arquivo do Incident Manager em formato de cartão virtual (.vcf) para o catálogo de endereços nos dispositivos móveis. O arquivo está hospedado no Amazon CloudFront e está disponível na partição comercial da AWS.

Para baixar o arquivo.vcf do Incident Manager

1. Em seu dispositivo móvel, escolha ou insira o seguinte URL: https://d26vhuvd5b89k2.cloudfront.net/aws-incident-manager.vcf.
2. Salve ou importe o arquivo para o catálogo de endereços no dispositivo móvel.

Trabalhando com programações de plantão no Incident Manager

Uma escala de plantão no Incident Manager define quem é notificado quando ocorre um incidente que requer intervenção do operador. Uma escala de plantão consiste em uma ou mais rotações que você cria para a escala. Cada rotação pode conter até 30 contatos.

Depois de criar, inclua a escala de plantão como escalação no plano de escalação. Quando ocorre um incidente associado a esse plano de escalação, o Incident Manager notifica o operador (ou operadores) que estão de plantão de acordo com a escala. Esse contato pode então reconhecer o engajamento. Em seu plano de escalação, você pode designar uma ou mais programações de plantão, bem como um ou mais contatos individuais, em vários estágios de escalonamento. Para obter mais informações, consulte Como trabalhar com planos de escalação no Incident Manager.

> **Tip**
>
> Como prática recomendada, recomendamos adicionar contatos e programações de plantão como canais de encaminhamento em um plano de escalação. Em seguida, você deve escolher um plano de escalação como engajamento em um plano de resposta.

Essa abordagem fornece a cobertura mais completa para resposta a incidentes em sua organização.

Cada programação de plantão suporta até oito rotações. As rotações podem se sobrepor ou ser executadas simultaneamente. Isso aumenta o número de operadores notificados para responder quando ocorre um incidente. Você também pode criar rotações que são executadas consecutivamente. Isso oferece suporte a cenários como o gerenciamento de incidentes "follow the sun", em que há grupos em todo o mundo que oferecem suporte ao mesmo serviço.

Use os tópicos desta seção para ajudar a criar e gerenciar programações de plantão para suas operações de resposta a incidentes.

Tópicos

- Criando uma programação de plantão e uma rotação no Incident Manager
- Gerenciando uma programação de plantão existente no Incident Manager

Criando uma programação de plantão e uma rotação no Incident Manager

Crie uma programação de plantão com uma ou mais rotações de contatos para responder a incidentes durante seus turnos.

Antes de começar

Antes de criar uma programação de plantão, certifique-se de ter criado anteriormente os contatos que deseja adicionar às rotações na programação. Para obter mais informações, consulte Como trabalhar com contatos do Incident Manager.

Contabilizar as alterações do horário de verão (DST)

Ao criar uma rotação, você especifica o fuso horário global que serve como base para os horários e datas de cobertura de turnos especificadas para a rotação. Você pode usar qualquer fuso horário definido pela Internet Assigned Numbers Authority (IANA). Por exemplo: `America/Los_Angeles`, `UTC` e `Asia/Seoul`. Você pode adicionar mais de uma rotação a uma programação de plantão. No entanto, quando os respondentes de cada rotação estiverem localizados geograficamente em fusos horários diferentes, lembre-se de quaisquer alterações de horário de verão às quais cada rotação possa estar sujeita.

Por exemplo, `America/Los_Angeles` e `Europe/Dublin` seguem diferentes cronogramas de horário de verão. Como resultado, a diferença de horário entre as duas zonas pode variar de 6 a 8 horas, dependendo da época do ano. Por exemplo, uma programação de plantão “follow the sun” tem uma rotação no fuso horário `America/Los_Angeles` e uma rotação no `Europe/Dublin`. Neste exemplo, o cronograma pode conter uma diferença de turno de uma hora ou uma sobreposição de turno de uma hora devido às mudanças no horário de verão.

Para evitar essas situações, recomendamos a seguinte abordagem:

1. Use um único fuso horário para todas as rotações em uma programação de plantão.
2. Calcule os horários locais ao atribuir respondentes fora desse fuso horário específico.

Se decidir atribuir cada rotação ao fuso horário local, revise a programação antes de qualquer horário de verão. Em seguida, ajuste os tempos de mudança de rotação conforme necessário para evitar lacunas ou sobreposições não intencionais na cobertura de plantão antes que qualquer alteração no horário de verão entre em vigor.

Para criar uma programação de plantão

1. Abra o console do Incident Manager.
2. Na barra de navegação à esquerda, selecione Programações de plantão.
3. Escolha Criar programação de plantão.
4. Em Nome da programação, insira um nome para ajudá-lo a identificar a programação, como **`MyApp Primary On-call Schedule`**.
5. Em Alias da programação, insira um alias para a programação que seja exclusivo no atual Região da AWS, como **`my-app-primary-on-call-schedule`**.
6. (Opcional) Na área Tags, aplique um ou mais pares de nome/valor de chave de tag à programação de plantão.

   Tags são metadados opcionais que você atribui a um recurso. As tags permitem categorizar um recurso de diferentes formas, como por finalidade, proprietário ou ambiente. Por exemplo, você pode marcar uma programação para identificar o período em que ela é executada, os tipos de operadores que ela contém ou o plano de escalação que ela suporta. Para obter mais informações sobre como aplicar tags em recursos do Incident Manager, consulte Marcando recursos no Incident Manager.
7. Continue adicionando uma ou mais rotações à programação de plantão.

Criando uma rotação para uma programação de plantão no Incident Manager

Uma rotação em uma programação de plantão especifica quando o turno está em vigor. Também especifica os contatos pelos quais os turnos rodam. Você pode incluir até oito rotações em uma única programação de plantão.

Você pode adicionar qualquer pessoa que criou como contato no Incident Manager a uma rotação. Para obter informações sobre o gerenciamento de contatos, consulte Como trabalhar com contatos do Incident Manager.

Ao configurar sua rotação, você pode ver a aparência geral da programação em um calendário de pré-visualização no lado direito da página.

Para criar uma rotação para uma programação de plantão

1. Na seção Rotação 1 da página Criar programação de plantão, em Nome da rotação, insira um nome que identifique a rotação, como**`00:00 - 7:59 Support`**, ou **`Dublin Support Group`**.
2. Em Data de início, insira a data em que essa rotação se torna ativa no formato `YYYY/MM/DD`, como `2023/07/14`.
3. Em Fuso horário, selecione o fuso horário global que serve como base para os horários e datas de cobertura de turnos que você especificar para essa rotação.

   Você pode usar qualquer fuso horário definido pela Internet Assigned Numbers Authority (IANA). Por exemplo: "América/Los_Angeles", "UTC" ou "Ásia/Seul". Para obter mais informações, consulte Banco de dados de fuso horário no site da IANA.

   > **Warning**
   >
   > Você pode basear cada rotação em seu próprio fuso horário. No entanto, qualquer alteração do horário de verão nos fusos horários selecionados pode afetar as janelas de cobertura pretendidas. Para obter mais informações, consulte Contabilizar as alterações do horário de verão (DST) no início deste tópico.

4. Em Hora de início da rotação, insira a hora em que o turno dessa rotação começa no formato `hh:mm` de 24 horas, como `16:00`.

   Observe as diferenças na hora local para contatos em fusos horários diferentes daquele que você especificou. Por exemplo, se você escolher `America/Los_Angeles` como fuso horário

e `00:00` como horário de início da rotação, isso será igual a 8h em Dublin, Irlanda, e 13h30 em Bumbai, Índia.

5. Em Hora de término da rotação, insira a hora em que o turno dessa rotação termina no formato `hh:mm` de 24 horas, como `23:59`.

> **Note**
>
> O período entre o início e o final de uma rotação deve ser de pelo menos 30 minutos.

6. (Opcional) Para definir a duração da rotação para 24 horas, selecione a cobertura de 24 horas e insira a hora de início dessa rotação no campo Hora de início da rotação. O valor da Hora de término da rotação é atualizado automaticamente.

   Por exemplo, se quiser que o plantão tenha cobertura de 24 horas com a mudança de turno às 11h, escolha cobertura de 24 horas e insira **`11:00`** como horário de início.

7. Em Ativa nos dias, selecione os dias da semana em que essa rotação está ativa. Se seu plano de plantão excluir a cobertura de fim de semana, por exemplo, selecione todos os dias, exceto domingo e sábado.

8. Continue adicionando contatos à rotação.

Adicionando contatos a uma rotação em uma programação de plantão no Incident Manager

Para cada rotação em sua programação de plantão, você pode adicionar um ou mais contatos, até um total de 30. Você escolhe entre os contatos configurados na configuração do Incident Manager.

Quando você adiciona um contato a uma rotação, o contato pode receber notificações como parte das tarefas de plantão deles. As notificações podem ser enviadas por e-mail, SMS ou chamada de voz, conforme especificado nos detalhes de um contato.

Para obter informações sobre como gerenciar seus contatos e as opções de notificação de contatos, consulte Como trabalhar com contatos do Incident Manager.

Para adicionar contatos a uma rotação em uma programação de plantão

1. Na página Criar programação de plantão, na seção Contatos para a rotação, escolha Adicionar ou remover contatos.

2. Na caixa de diálogo Adicionar ou remover contatos, selecione os aliases dos contatos a serem incluídos na rotação.

   A ordem em que você seleciona os contatos é a ordem em que eles são listados primeiro na programação de alternância. Você pode alterar a ordem após adicionar os contatos.

3. Selecione a opção Confirmar.
4. Para alterar a posição de um contato no pedido, selecione o botão de rádio desse usuário e use os botões Para cima
   ( )
   e Para baixo
   ( )
   para atualizar o pedido do contato.
5. Continue especificando a recorrência e a duração do turno individual da rotação.

Especificando a recorrência e a duração do turno e adicionando tags a uma rotação no Incident Manager

A recorrência do turno especifica com que frequência os contatos em uma rotação entram e saem de uma chamada. A duração da recorrência pode ser especificada em vários dias, semanas ou meses.

Para especificar a recorrência e a duração do turno e adicionar tags a uma rotação

1. Na página Criar programação de plantão, na seção Configurações de recorrência da rotação, faça o seguinte:

   - Para o Tipo de recorrência do turno, especifique se cada turno de plantão dura vários dias, semanas ou meses escolhendo entre `Daily`, `Weekly` e `Monthly`.
   - Em Duração do turno, insira quantos dias, semanas ou meses um turno dura.

     Por exemplo, se você escolher `Daily` e digitar **`1`**, o turno de plantão de cada contato dura um dia. Se você escolher `Weekly` e digitar **`3`**, o turno de plantão de cada contato dura três semanas.

2. (Opcional) Na área Tags, aplique um ou mais pares de nome/valor de chave de tag à rotação.

   Tags são metadados opcionais que você atribui a um recurso. As tags permitem categorizar um recurso de diferentes formas, como por finalidade, proprietário ou ambiente. Por exemplo, você pode marcar uma rotação para identificar a localização dos contatos atribuídos a ela, o

tipo de cobertura que ela deve fornecer ou o plano de escalação que ela suportará. Para obter mais informações sobre como aplicar tags em recursos do Incident Manager, consulte Marcando recursos no Incident Manager.

3. (Recomendado) Use a visualização prévia do calendário para garantir que não haja lacunas não intencionais na cobertura de sua programação de plantão.
4. Escolha Criar.

Agora você pode adicionar a programação de plantão como um canal de encaminhamento em um plano de escalação. Para obter mais informações, consulte Criar um plano de escalação.

Gerenciando uma programação de plantão existente no Incident Manager

Use o conteúdo desta seção para ajudar a trabalhar com as programações de plantão que você já criou.

Tópicos

- Visualizando detalhes da programação de plantão
- Editando uma programação de plantão
- Copiando uma programação de plantão
- Criando uma substituição para uma rotação de programação de plantão
- Excluindo uma programação de plantão

Visualizando detalhes da programação de plantão

Você pode acessar um resumo rápido de uma programação de plantão na página Exibir detalhes da programação de plantão. Esta página também contém informações sobre quem está de plantão no momento e quem estará no próximo plantão. A página inclui uma exibição de calendário que mostra quais contatos estão de plantão em um horário específico.

Para visualizar os detalhes da programação de plantão

1. Abra o console do Incident Manager.
2. Na barra de navegação à esquerda, selecione Programações de plantão.
3. Na linha da programação de plantão a ser exibida, siga um destes procedimentos:
   - Para abrir uma exibição resumida do calendário, escolha o alias da programação.

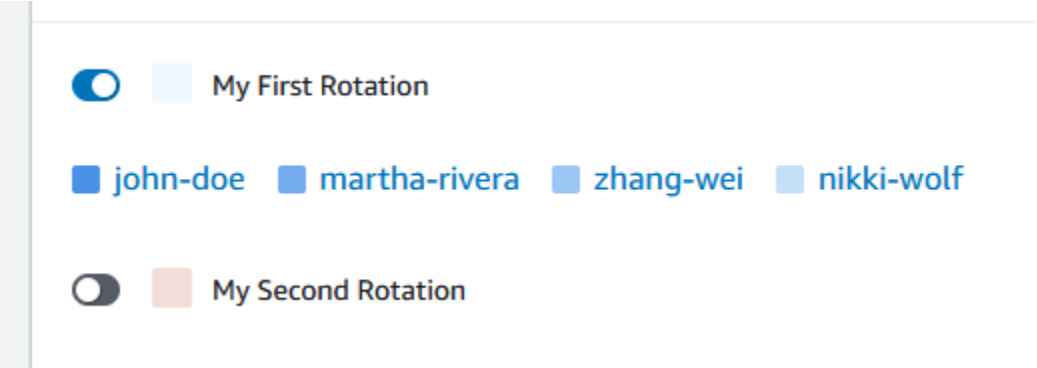
- ou -

Selecione o botão de seleção da linha e escolha Exibir.

- Para abrir uma visualização do calendário da programação, escolha Exibir calendário

  Na visualização do calendário, escolha o nome de um contato em uma data específica na programação para ver detalhes sobre o turno atribuído ou criar uma substituição.

- Para ativar ou desativar a exibição de uma rotação específica no calendário, escolha a chave ao lado do nome da rotação.



Editando uma programação de plantão

Você pode atualizar a configuração de uma programação de plantão e suas rotações, exceto os seguintes detalhes:

- O alias da programação
- Nomes de rotação
- Datas de início da rotação

Para usar um calendário existente como base para um novo calendário com a capacidade de alterar esses valores, você pode copiar o calendário. Para obter mais informações, consulte Copiando uma programação de plantão.

Para editar uma programação de plantão

1. Abra o console do Incident Manager.
2. Na barra de navegação à esquerda, selecione Programações de plantão.

3. Faça um dos seguintes procedimentos:
   - Selecione o botão de rádio na linha para edição da programação de plantão e, em seguida, escolha Editar.
   - Escolha o alias da programação de plantão para abrir a página Exibir detalhes da programação de plantão e, em seguida, escolha Editar.
4. Faça as modificações necessárias na programação de plantão e em suas rotações. Você pode alterar as opções de configuração de rotação, como horários de início e término, contatos e recorrência. É possível adicionar ou remover as rotações da programação, conforme necessário. A pré-visualização do calendário reflete suas alterações à medida que você as faz.

   Para obter mais informações sobre como trabalhar com a opção na página, consulte Criando uma programação de plantão e uma rotação no Incident Manager.
5. Escolha Atualizar.

> **Important**
>
> Se você editar uma programação que contém substituições, suas alterações podem afetar as substituições. Para garantir que suas substituições permaneçam configuradas conforme o esperado, recomendamos revisar cuidadosamente suas substituições de turno depois de atualizar a programação.

Copiando uma programação de plantão

Para usar a configuração de uma programação de plantão existente como ponto de partida para uma nova programação, você pode criar uma cópia do calendário e modificá-lo conforme necessário.

Copiando uma programação de plantão

1. Abra o console do Incident Manager.
2. Na barra de navegação à esquerda, selecione Programações de plantão.
3. Selecione o botão de rádio na linha para a programação de plantão copiar.
4. Escolha Copiar.
5. Faça as modificações necessárias no calendário e nas rotações dele. É possível alterar, adicionar ou remover as rotações, conforme necessário.

> **Note**
>
> Ao copiar uma programação existente, você deve especificar novas datas de início para cada rotação. As programações copiadas não oferecem suporte a rotações com datas de início no passado.

Para obter mais informações sobre como trabalhar com a opção na página, consulte Criando uma programação de plantão e uma rotação no Incident Manager.

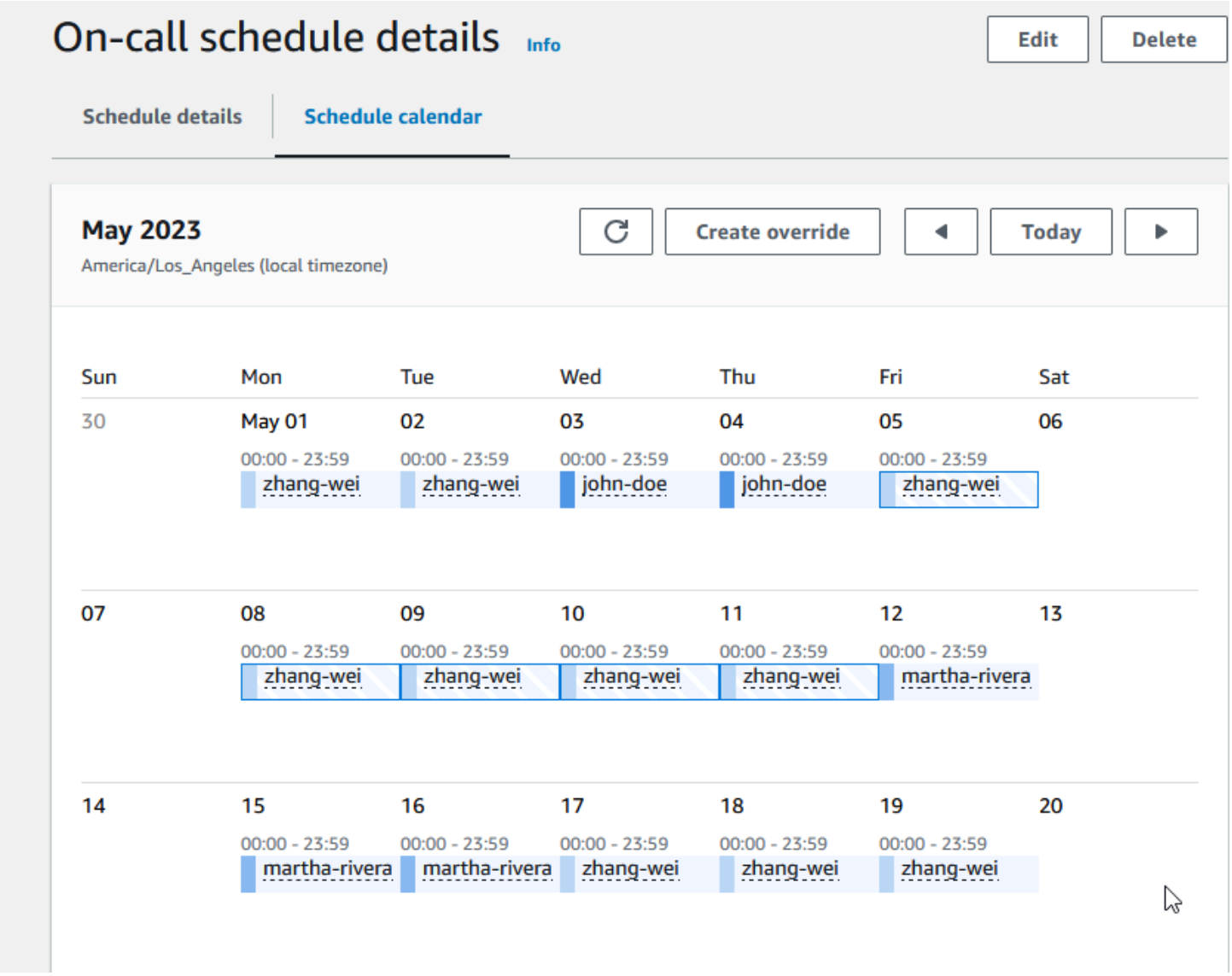
6. Selecione Criar cópia.

Criando uma substituição para uma rotação de programação de plantão

Se precisar fazer alterações pontuais em uma programação de rotação existente, você pode criar uma substituição. Uma substituição permite que você substitua todo ou parte do turno de um contato por outro contato. Você também pode criar uma substituição que se estenda por vários turnos.

Você só pode atribuir contatos a uma substituição que já estejam atribuídos à rotação.

Na pré-visualização do calendário, os turnos substituídos são mostrados com um fundo listrado em vez de um plano de fundo sólido. Na imagem a seguir, podemos ver que o contato Zhang Wei está de plantão em uma substituição que inclui partes dos turnos de John Doe e Martha Rivera, começando em 5 de maio e terminando em 11 de maio.



Para criar uma rotação para uma programação de plantão

1. Abra o console do Incident Manager.
2. Na barra de navegação à esquerda, selecione Programações de plantão.
3. Na linha da programação de plantão a ser exibida, siga um destes procedimentos:
   - Escolha o alias da programação e, em seguida, escolha a guia Calendário de programação.
   - Escolha Exibir calendário .
4. Faça um dos seguintes procedimentos:
   - Escolha Criar substituição.

- Escolha o nome de um contato na visualização prévia do calendário e, em seguida, escolha Substituir turno.

5. Na caixa de diálogo Criar substituição de turno, faça o seguinte:

> **Note**
>
> Uma substituição deve ter, pelo menos, 30 minutos de duração. Você só pode especificar uma substituição para turnos que ocorram em, no máximo, seis meses no futuro.

   a. Em Selecionar rotação, selecione o nome da rotação na qual criar uma substituição.
   b. Em Data de início, selecione ou insira a data em que a substituição começa.
   c. Em Hora de início, insira a hora em que a substituição começa no `hh:mm` formato.
   d. Em Data de término, selecione ou insira a data em que a substituição termina.
   e. Em Hora de início, insira a hora em que a substituição começa no `hh:mm` formato.
   f. Em Selecionar contato de substituição, selecione o nome do contato rotativo que está de plantão durante o período de substituição.

6. Escolha Criar substituição.

Depois de criar uma substituição, você pode identificá-la pelo fundo listrado. Quando você escolhe o nome do contato para um turno substituído, uma caixa de informações o identifica como um turno substituído. Você pode escolher Excluir substituição para removê-la e restaurar a atribuição original de plantão.

Excluindo uma programação de plantão

Quando não precisar mais de uma programação de plantão em particular, você pode excluí-la do Incident Manager.

Se algum plano de escalação ou plano de resposta atualmente usa a programação de plantão como um canal de encaminhamento, você deve removê-la desses planos antes de excluir a programação.

Para excluir uma programação de plantão

1. Abra o console do Incident Manager.
2. Na barra de navegação à esquerda, selecione Programações de plantão.

3. Selecione o botão de rádio na linha para a programação de plantão excluir.
4. Escolha Excluir.
5. Na caixa de diálogo Excluir agendamento de plantão?, digite **`confirm`** na caixa de texto.
6. Escolha Excluir.

Como trabalhar com planos de escalação no Incident Manager

O AWS Systems Manager Incident Manager fornece caminhos de escalação por meio de seus contatos definidos ou escalas de plantão, conhecidos coletivamente como canais de escalação. Você pode inserir vários canais de escalação em um incidente ao mesmo tempo. Se os contatos designados no canal de escalação não responderem, o Incident Manager escalará para o próximo conjunto de contatos. Você também pode escolher se o plano parará de escalar quando o usuário confirma o engajamento. Você pode adicionar planos de escalação a um plano de resposta para que a escalação comece automaticamente no começo de um incidente. Você também pode adicionar planos de escalação a um incidente ativo.

Tópicos

- Estágios
- Criar um plano de escalação

Estágios

Os planos de escalação usam estágios em que cada estágio tem a duração definida em minutos. Cada estágio tem as seguintes informações:

- Duração: o tempo que o plano aguarda até o início do próximo estágio. O primeiro estágio do plano de escalação inicia assim que o engajamento é iniciado.
- Canal de escalação: um canal de escalação é um único contato ou uma escala de plantão composta por vários contatos que alternam responsabilidades em um cronograma definido. O plano de escalação envolve cada canal usando o plano de engajamento definido. Você pode configurar cada canal de escalação para interromper a progressão do plano de escalação antes que ele passe para o próximo estágio. Cada estágio pode ter vários canais de escalação.

  Para obter informações sobre a configuração de contatos individuais, consulte Como trabalhar com contatos do Incident Manager. Para obter informações sobre a criação de escalas de plantão, consulte Trabalhando com programações de plantão no Incident Manager.

Criar um plano de escalação

1. Abra o console do Incident Manager e escolha Planos de escalação no painel de navegação à esquerda.
2. Escolha Criar plano de escalação.
3. Em Nome, insira um nome exclusivo para o plano de escalação, como **`My Escalation Plan`**.
4. Em Alias, insira um alias para ajudá-lo a identificar o plano, como **`my-escalation-plan`**.
5. Em Duração do estágio, insira os minutos que o Incident Manager deve aguardar para passar para o próximo estágio.
6. No canal de escalação, escolha um ou mais contatos ou escalas de plantão a acionar durante esse estágio.
7. (Opcional) Para permitir que um contato interrompa o plano de escalação depois de confirmar o engajamento, selecione Confirmação interrompe a progressão do plano.
8. Para adicionar outro canal a esse estágio, escolha Adicionar canal de escalação.
9. Para adicionar outro estágio ao plano de escalação, escolha Adicionar estágio.
10. Repita as etapas de 5 a 9 até terminar de adicionar os canais e estágios de escalação desejados para o plano de escalação.
11. (Opcional) Na área Tags, aplique um ou mais pares de nome/valor de chave de tag ao plano de escalação.

    Tags são metadados opcionais que você atribui a um recurso. As tags permitem categorizar um recurso de diferentes formas, como por finalidade, proprietário ou ambiente. Por exemplo, você pode aplicar tag no plano de escalação para identificar os tipos de incidentes onde ele deve ser usado, os tipos de canais de escalação que ele contém ou o plano de escalação que ele suporta. Para obter mais informações sobre como aplicar tags em recursos do Incident Manager, consulte Marcando recursos no Incident Manager.
12. Escolha Criar plano de escalação.

Trabalhando com canais de chat no Incident Manager

O Incident Manager, um recurso do AWS Systems Manager, permite que os respondentes se comuniquem diretamente pelos canais de chat durante um incidente. Um canal de chat é uma sala de chat que você configura no AWS Chatbot. Conectando esse canal a um plano de resposta no Incident Manager depois.

Durante um incidente, os respondentes usam o canal de chat para se comunicarem sobre o incidente. O Incident Manager também envia todas as atualizações e notificações sobre o incidente diretamente para o canal de chat. Ele envia essas notificações usando um ou mais tópicos do Amazon Simple Notification Service (Amazon SNS) que você especifica na configuração da sua sala do chat.

O AWS Chatbot e o Incident Manager oferecem suporte aos canais de chat nos seguintes aplicativos:

- Slack
- Microsoft Teams
- Amazon Chime

O processo de configuração de um canal de chat para uso em incidentes consiste em tarefas a serem realizadas em três serviços diferentes da Amazon Web Services.

Tarefas

- Tarefa 1: Criar ou atualizar tópicos do Amazon SNS para seu canal de chat
- Tarefa 2: criar um canal de chat no AWS Chatbot
- Tarefa 3: adicionar o canal de chat a um plano de resposta no Incident Manager
- Como interagir pelo canal de chat

Tarefa 1: Criar ou atualizar tópicos do Amazon SNS para seu canal de chat

O Amazon SNS é um serviço de mensagens gerenciado, que oferece entrega de mensagens de publicadores para assinantes (também conhecidos como produtores e consumidores). Os editores se comunicam de maneira assíncrona com os assinantes produzindo e enviando mensagens para um tópico, que é um canal de comunicação e um ponto de acesso lógico. O Incident Manager usa um ou mais tópicos que você associa a um plano de resposta para enviar notificações sobre um incidente aos respondentes do incidente.

Em um plano de resposta, você pode incluir um ou mais tópicos do Amazon SNS nas notificações de incidentes. Como prática recomendada, você deve criar um tópico SNS em cada Região da AWS adicionada ao conjunto de replicação.

> **Tip**
>
> Em um fluxo de trabalho de configuração mais linear, recomendamos configurar primeiro seus tópicos do Amazon SNS para uso com o Incident Manager. Depois de configurado, você pode criar o canal de chat.

Para criar ou atualizar tópicos do Amazon SNS para seu canal de chat

1. Siga as etapas de Criação de um tópico do Amazon SNS no Guia do desenvolvedor do Amazon Simple Notification Service.

   > **Note**
   >
   > Depois de criar, edite o tópico para atualizar sua política de acesso.

2. Selecione o tópico que você criou e anote ou copie o nome do recurso da Amazon (ARN) do tópico, no formato `arn:aws:sns:us-east-2:111122223333:My_SNS_topic`.
3. Selecione Editar e expanda a seção Política de acesso para configurar mais permissões de acesso, além das permissões padrão.
4. Adicione a seguinte declaração à matriz de Declarações da política:

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

   Substitua os *`valores de espaço reservado`* da seguinte forma:

- *sns-topic-arn* é o nome do recurso da Amazon (ARN) do tópico que você criou para esta região, no formato `arn:aws:sns:us-east-2:111122223333:My_SNS_topic`.
- *account-id* é o ID da Conta da AWS em que você está trabalhando, como `111122223333`.

5. Escolha Save changes (Salvar alterações).
6. Repita o processo em cada região incluída no seu conjunto de replicação.

Tarefa 2: criar um canal de chat no AWS Chatbot

Você pode criar um canal de chat no Slack, no Microsoft Teams ou no Amazon Chime. Você precisa de apenas um canal de chat para cada plano de resposta.

Nos seus canais de chat, recomendamos seguir o princípio do privilégio mínimo (não fornecer aos usuários mais permissões do que as necessárias para realizar suas tarefas). Você também deve revisar regularmente a associação aos seus canais de chat do AWS Chatbot. As avaliações ajudam a verificar se somente os respondentes adequados e outras partes interessadas têm acesso aos canais de chat.

Nos canais do Slack e nos canais do Microsoft Teams habilitados para AWS Chatbot, os respondedores de incidentes podem executar vários comandos da CLI do Incident Manager diretamente no aplicativo Slack ou no Microsoft Teams. Para obter mais informações, consulte Como interagir pelo canal de chat.

> **Important**
>
> Os usuários que você adiciona ao seu canal de chat devem ser os mesmos contatos listados no plano de escalonamento ou resposta. Você também pode adicionar outros usuários aos canais de chat, como partes interessadas e observadores de incidentes.

Para obter informações gerais sobre o AWS Chatbot, consulte O que é AWS Chatbot no AWS Chatbot Guia do administrador.

Escolha dentre esses aplicativos para criar seu canal:

Slack

As etapas desse procedimento fornecem as configurações de permissão recomendadas para permitir que todos os usuários do canal usem comandos de chat com o Incident Manager.

Usando comandos de chat compatíveis, seus respondentes podem atualizar e interagir com o incidente diretamente no canal de chat do Slack. Para obter mais informações, consulte Como interagir pelo canal de chat.

Para criar um canal de chat no Slack

- Siga as etapas do Tutorial: Comece a usar o Slack no Guia do administrador do AWS Chatbot e inclua o seguinte na configuração.
  - Na etapa 10, em Configurações do perfil, escolha Perfil do canal.
  - Na etapa 10d, em Modelos de política, selecione Permissões do Incident Manager.
  - Na etapa 11, em Políticas de barreira de proteção do canal, em Nome da política, escolha `AWSIncidentManagerResolverAccess`.
  - Na etapa 12, na seção tópicos do SNS, faça o seguinte:
    - Na Região 1, selecione uma Região da AWS que esteja incluída no seu conjunto de replicação.
    - Em Tópicos 1, selecione o tópico do SNS que você criou nessa região para usar para enviar notificações de incidentes ao canal de chat.
    - Para cada região adicional em seu conjunto de replicação, escolha Adicionar outra região e adicione mais regiões e tópicos do SNS.

Microsoft Teams

As etapas desse procedimento fornecem as configurações de permissão recomendadas para permitir que todos os usuários do canal usem comandos de chat com o Incident Manager. Usando comandos de chat compatíveis, seus respondentes podem atualizar e interagir com o incidente diretamente no canal de chat do Microsoft Teams. Para obter mais informações, consulte Como interagir pelo canal de chat.

Para criar um canal de chat no Microsoft Teams

- Siga as etapas do Tutorial: Comece a usar o Microsoft Teams no Guia do administrador do AWS Chatbot e inclua o seguinte na configuração:
  - Na etapa 10, em Configurações do perfil, escolha Perfil do canal.
  - Na etapa 10d, em Modelos de política, selecione Permissões do Incident Manager.

- Na etapa 11, em Políticas de barreira de proteção do canal, em Nome da política, escolha `AWSIncidentManagerResolverAccess`.
- Na etapa 12, na seção tópicos do SNS, faça o seguinte:
  - Na Região 1, selecione uma Região da AWS que esteja incluída no seu conjunto de replicação.
  - Em Tópicos 1, selecione o tópico do SNS que você criou nessa região para usar para enviar notificações de incidentes ao canal de chat.
  - Para cada região adicional em seu conjunto de replicação, escolha Adicionar outra região e adicione mais regiões e tópicos do SNS.

Amazon Chime

Para criar um canal de chat no Amazon Chime

- Siga as etapas do Tutorial: Comece a usar o Amazon Chime no Guia do administrador do AWS Chatbot e inclua o seguinte na configuração:
  - Na etapa 11, em Modelos de política, selecione Permissões do Incident Manager.
  - Na etapa 12, na seção tópicos do SNS, selecione os tópicos do SNS que enviarão notificações para o webhook do Amazon Chime:
    - Na Região 1, selecione uma Região da AWS que esteja incluída no seu conjunto de replicação.
    - Em Tópicos 1, selecione o tópico do SNS que você criou nessa região para usar para enviar notificações de incidentes ao canal de chat.
    - Para cada região adicional em seu conjunto de replicação, escolha Adicionar outra região e adicione mais regiões e tópicos do SNS.

> **Note**
>
> Os comandos de chat, que os respondedores de incidentes podem usar nos canais de chat do Slack e do Microsoft Teams, não são compatíveis com o Amazon Chime.

Tarefa 3: adicionar o canal de chat a um plano de resposta no Incident Manager

Ao criar ou atualizar um plano de resposta, você pode adicionar canais de chat para que os respondentes se comuniquem e recebam atualizações.

Ao seguir as etapas emCriar um plano de resposta, na seção (Opcional) Especificar um canal de chat de resposta a incidentes, selecione o canal que deseja usar para incidentes relacionados a esse plano de resposta.

Como interagir pelo canal de chat

Nos canais no Slack e no Microsoft Teams, o Incident Manager permite que os respondentes interajam com os incidentes diretamente do canal de chat usando os seguintes comandos do `ssm-incidents`:

- start-incident
- 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

Para executar comandos no canal de chat de um incidente ativo, use o formato a seguir. Substitua *`cli-options`* pela opção a ser incluída no comando.

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

Por exemplo:

```
@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
```

Trabalho com runbooks do Automation do Systems Manager no Incident Manager

Você pode usar runbooks da Automação do AWS Systems Manager, um recurso do AWS Systems Manager, para automatizar tarefas comuns de aplicativos e infraestrutura em seu ambiente Nuvem AWS.

Cada runbook define um fluxo de trabalho de runbook, que inclui as ações que o Systems Manager realiza nos nós gerenciados ou em outros tipos de recursos da AWS. Você pode usar runbooks para automatizar a manutenção, a implantação e a remediação de seus recursos AWS.

No Incident Manager, um runbook impulsiona a resposta e a mitigação de incidentes, e você especifica um runbook para usar como parte de um plano de resposta.

Em seus planos de resposta, você pode escolher entre dezenas de runbooks pré-configurados para tarefas comumente automatizadas ou criar runbooks personalizados. Quando você especifica um runbook em uma definição de plano de resposta, o sistema pode iniciar automaticamente o runbook quando um incidente começa.

> **Important**
>
> Os incidentes criados por um failover entre Regiões não invocam os runbooks especificados nos planos de resposta.

Para obter mais informações sobre Systems Manager Automation, runbooks e uso de runbooks com o Incident Manager, consulte os tópicos a seguir:

- Para adicionar um runbook a um plano de resposta, consulte Como trabalhar com planos de resposta no Incident Manager.
- Para saber mais sobre runbooks, consulte AWS Systems ManagerAutomação no Guia do usuário AWS Systems Manager e na Referência do runbook de automação AWS Systems Manager.
- Para obter informações sobre o custo do uso de runbook, consulte Preços do Systems Manager.
- Para obter informações sobre a invocação automática de runbooks quando um incidente é criado por um alarme do Amazon CloudWatch ou por um evento do Amazon EventBridge, consulte Tutorial: Uso de runbooks do Systems Manager Automation com o Incident Manager.

Tópicos

- Permissões do IAM necessárias para iniciar e executar fluxos de trabalho do runbook
- Trabalho com parâmetros de runbook
- Defina um runbook
- Modelo de runbook do Incident Manager

Permissões do IAM necessárias para iniciar e executar fluxos de trabalho do runbook

O Incident Manager exige permissões para executar runbooks como parte de sua resposta a incidentes. Para fornecer essas permissões, você usa perfis AWS Identity and Access Management (IAM), o perfil de serviço Runbook e a Automação *`AssumeRole`*.

O perfil de serviço Runbook é um perfil de serviço obrigatório. Esse perfil fornece ao Incident Manager as permissões necessárias para acessar e iniciar o fluxo de trabalho do runbook.

A Automação `AssumeRole` fornece as permissões necessárias para executar os comandos individuais especificados no runbook.

> **Note**
>
> Se nenhum `AssumeRole` for especificado, o Systems Manager Automation tentará usar o perfil de serviço Runbook para comandos individuais. Se você não especificar

umAssumeRole, deverá adicionar as permissões necessárias ao perfil de serviço do Runbook. Se você não fizer isso, o runbook não conseguirá executar esses comandos. No entanto, como uma prática recomendada de segurança, recomendamos usar um separado AssumeRole. Com um separado AssumeRole, é possível limitar as permissões necessárias que você deve adicionar a cada perfil.

Para obter mais informações sobre a Automação AssumeRole, consulte Configuração de um acesso ao perfil de serviço (assumir perfil) para automações no AWS Systems Manager Guia do usuário.

Você mesmo pode criar qualquer tipo de perfil manualmente no console do IAM e também pode permitir que o Incident Manager crie uma para você ao criar ou atualizar um plano de resposta.

Permissões de perfil de serviço runbook

As permissões do perfil de serviço do Runbook são fornecidas por meio de uma política semelhante à seguinte.

A primeira declaração permite que o Incident Manager inicie a StartAutomationExecution operação do Systems Manager. Essa operação então será executada em recursos representados pelos três formatos de Nome do recurso da Amazon (ARN).

A segunda instrução permite que o perfil de serviço do Runbook assuma um perfil em outra conta quando esse runbook é executado na conta afetada. Para obter mais informações, consulte Execução de automações em várias Regiões da AWS e contas no Guia do usuário AWS Systems Manager.

```
{
  "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"
        }
      }
    }
  ]
}
```

Permissões de automação AssumeRole

Ao criar ou atualizar um plano de resposta, você pode escolher entre várias políticas AWS gerenciadas para anexar ao AssumeRole criado pelo Incident Manager. Essas políticas fornecem permissões para executar várias operações comuns usadas em cenários de runbook do Incident Manager. Você pode escolher uma ou mais dessas políticas gerenciadas para fornecer permissões para sua política `AssumeRole`. A tabela a seguir descreve as políticas que você pode escolher ao criar uma `AssumeRole` no console do Incident Manager.

Nome da política gerenciada pela AWS	Descrição da política
`AmazonSSMAutomationRole`	Concede permissões para que o serviço Systems Manager Automation execute atividades definidas nos runbooks. Atribui essa política a administradores e usuários avançados confiáveis.
`AWSIncidentManagerResolverAccess`	Concede permissão para que os usuários iniciem, visualizem e atualizem incidentes. Você também pode usá-las para criar eventos do cronograma do cliente e itens relacionados no painel de incidentes.

Você pode usar essas políticas gerenciadas para conceder permissões para vários cenários comuns de resposta a incidentes. No entanto, as permissões necessárias para as tarefas específicas de que você precisa podem variar. Nesses casos, você precisa fornecer permissões adicionais de política

para seu `AssumeRole`. Para obter mais informações, consulte AWS Systems Manager Referência de runbook do Automation.

Trabalho com parâmetros de runbook

Ao adicionar um runbook a um plano de resposta, é possível especificar os parâmetros que esse runbook deve utilizar no tempo de execução. Planos de resposta oferecem suporte a parâmetros com valores estáticos e dinâmicos. Para valores estáticos, você insere o valor ao definir o parâmetro no plano de resposta. Para valores dinâmicos, o sistema determina o valor correto do parâmetro coletando informações do incidente. O Incident Manager oferece suporte aos seguintes parâmetros dinâmicos:

`Incident ARN`

Quando o Incident Manager cria um incidente, o sistema captura o nome do recurso da Amazon (ARN) do registro de incidente correspondente e o insere para esse parâmetro no runbook.

> **Note**
>
> Esse valor apenas pode ser atribuído a parâmetros do tipo `String`. Se atribuído a um parâmetro de qualquer outro tipo, o runbook não será executado.

`Involved resources`

Quando o Incident Manager cria um incidente, o sistema captura os ARNs dos recursos envolvidos nesse incidente. Esses ARNs de recursos são então atribuídos a esse parâmetro no runbook.

Sobre os recursos associados

O Incident Manager pode preencher os valores dos parâmetros do runbook com os ARNs dos recursos AWS especificados nos alarmes do CloudWatch, nos eventos do EventBridge e nos incidentes criados manualmente. Esta seção descreve os diferentes tipos de recursos para os quais o Incident Manager pode capturar ARNs ao preencher esse parâmetro.

Alarmes do CloudWatch

Quando um incidente é criado a partir de uma ação de alarme do CloudWatch, o Incident Manager extrai automaticamente os seguintes tipos de recursos das métricas associadas. Em seguida, ele preenche os parâmetros escolhidos com os seguintes recursos envolvidos:

Serviço da AWS	Tipo de recurso
Amazon DynamoDB	Índices secundários globais Streams Tabelas
Amazon EC2	Imagens Instâncias
AWS Lambda	Aliases de funções Versões da função Funções
Amazon Relational Database Service (Amazon RDS)	Clusters Instâncias de bancos de dados
Amazon Simple Storage Service (Amazon S3)	Buckets

Regras do EventBridge

Quando o sistema cria um incidente a partir de um evento do EventBridge, o Incident Manager preenche os parâmetros escolhidos com a `Resources` propriedade no evento. Para obter mais informações, consulte Eventos do Amazon EventBridge no Guia do usuário do Amazon EventBridge.

Incidentes criados manualmente

Quando você cria um incidente usando a ação da API StartIncident, o Incident Manager preenche os parâmetros escolhidos usando as informações na chamada de API. Especificamente, ele preenche os parâmetros usando itens do tipo `INVOLVED_RESOURCE` que são passados no `relatedItems` parâmetro.

> **Note**
>
> O valor `INVOLVED_RESOURCES` apenas pode ser atribuído a parâmetros do tipo `StringList`. Se atribuído a um parâmetro de qualquer outro tipo, o runbook não será executado.

Defina um runbook

Ao criar um runbook, você pode seguir as etapas fornecidas aqui ou seguir o guia mais detalhado fornecido na seção Trabalho com runbooks do Guia de Usuário do Systems Manager. Se você estiver criando um runbook com várias contas e várias Regiões, consulte Executar automações em várias Regiões da AWS e contas no Guia do Usuário do Systems Manager.

Defina um runbook

1. Abra o console do Systems Manager em https://console.aws.amazon.com/systems-manager/.
2. No painel de navegação, escolha Documents.
3. Escolha Create automation (Criar automação).
4. Insira um nome de runbook exclusivo e identificável.
5. Digite uma descrição do runbook.
6. Forneça um perfil do IAM para o documento de automação assumir. Isso permite que o runbook execute comandos automaticamente. Para obter mais informações, consulte Configurar um acesso ao perfil de serviço para fluxos de trabalho de automação.
7. (Opcional) Adicione todos os parâmetros de entrada com os quais o runbook começa. Você pode usar parâmetros dinâmicos ou estáticos ao iniciar um runbook. Os parâmetros dinâmicos usam valores do incidente em que o runbook é iniciado. Os parâmetros estáticos usam o valor que você fornece.
8. (Opcional) Adicione um tipo de Alvo.
9. (Opcional) Adicione tags.
10. Preencha as etapas que o runbook seguirá ao ser executado. Cada etapa exige:
    - Um nome.
    - Uma descrição da finalidade da etapa.
    - A ação a ser executada durante a etapa. Os runbooks usam o tipo de ação Pausa para descrever uma etapa manual.

- (Opcional) Propriedades do comando.

11. Depois de adicionar todas as etapas necessárias do runbook, escolha Criar automação.

Para habilitar a funcionalidade entre contas, compartilhe o runbook em sua conta de gerenciamento com todas as contas de aplicativos que usam o runbook durante um incidente.

Compartilhe um runbook

1. Abra o console do Systems Manager em https://console.aws.amazon.com/systems-manager/.
2. No painel de navegação, escolha Documents.
3. Na lista de documentos, selecione o documento que você deseja compartilhar e escolha View details (Visualizar detalhes). Na guia Permissions, verifique se você é o proprietário do documento. Somente o proprietário de um documento pode compartilhá-lo.
4. Escolha Editar.
5. Para compartilhar o comando publicamente, escolha Public (Público) e depois Save (Salvar). Para compartilhar o comando de forma privada, escolha Private (Privado), insira o ID da Conta da AWS e escolha Add permission (Adicionar permissão) e Save (Salvar).

Modelo de runbook do Incident Manager

O Incident Manager fornece o seguinte modelo de runbook para ajudar sua equipe a começar a criar runbooks na automação do Systems Manager. Você pode usar esse modelo como está ou editá-lo para incluir detalhes específicos de seu aplicativo e recursos.

Encontre o modelo de runbook do Incident Manager

1. Abra o console do Systems Manager em https://console.aws.amazon.com/systems-manager/.
2. No painel de navegação, escolha Documents.
3. Na área Documents, insira **`AWSIncidents-`** no campo de pesquisa para exibir todos os runbooks do Incident Manager.

> **Tip**
>
> Insira **`AWSIncidents-`** como texto livre em vez de usar a opção de filtro de Prefixo do nome do documento.

Usar um modelo

1. Abra o console do Systems Manager em https://console.aws.amazon.com/systems-manager/.
2. No painel de navegação, escolha Documents.
3. Escolha o modelo que você deseja atualizar na lista de documentos.
4. Escolha a guia Conteúdo e, em seguida, copie o conteúdo do documento.
5. No painel de navegação, escolha Documents.
6. Escolha Create automation (Criar automação).
7. Insira um nome exclusivo e identificável.
8. Escolha a guia Editor.
9. Escolha Editar.
10. Cole ou insira os detalhes copiados na área Editor de documentos.
11. Escolha Create automation (Criar automação).

`AWSIncidents-CriticalIncidentRunbookTemplate`

O `AWSIncidents-CriticalIncidentRunbookTemplate` é um modelo que fornece o ciclo de vida do incidente do Incident Manager em etapas manuais. Essas etapas são genéricas o suficiente para serem usadas na maioria dos aplicativos, mas detalhadas o suficiente para que os respondentes comecem a resolver incidentes.

Como trabalhar com planos de resposta no Incident Manager

Os planos de resposta permitem que você planeje como responder a um incidente que afeta seus usuários. Um plano de resposta funciona como um modelo com informações sobre quem engajar, a gravidade esperada do evento, os runbooks automáticos a iniciar e métricas a monitorar.

Práticas recomendadas

Você pode reduzir o impacto dos incidentes em suas equipes planejando bem antes a resposta a incidentes. As equipes devem considerar as seguintes práticas recomendadas ao criar um plano de resposta.

- Engajamento simplificado — identifique a equipe mais adequada para um incidente. Se você usar uma lista de distribuição muito ampla ou se engajar as equipes erradas, poderá causar confusão e atrasar o tempo de resposta durante um incidente.

- Escalação confiável — nos seus engajamentos no plano de resposta, recomendamos selecionar um plano de engajamento em vez de contatos ou horários de plantão. O plano de engajamento deve especificar cada contato ou os horários de plantão (que contêm vários contatos rotativos) a serem engajados durante incidentes. Como os respondentes especificados no plano de engajamento podem estar fora de área às vezes, você deve configurar os primeiros contatos substitutos a responder no plano de resposta, para cobrir casos assim. Com contatos substitutos, se os contatos primários e secundários não estiverem disponíveis ou se houver outras faltas não planejadas na cobertura, o Incident Manager ainda notificará um contato sobre o incidente.
- Runbooks — use os runbooks para fornecer etapas reproduzíveis e compreensíveis reduzindo o estresse que um respondente passa durante um incidente.
- Colaboração — use canais de chat para agilizar a comunicação durante incidentes. Os canais de chat ajudam os respondentes a ficarem atualizados com as informações. Eles também podem compartilhar informações com outros respondentes por meio desses canais.

Criar um plano de resposta

Use o procedimento a seguir para criar um plano de resposta e automatizar a resposta a incidentes.

Para criar um plano de resposta

1. Abra o console do Incident Manager e escolha Planos de resposta no painel de navegação esquerdo.
2. Selecione Criar plano de resposta.
3. Em Nome, insira um nome de plano de resposta exclusivo e identificável para usar no nome do recurso da Amazon (ARN) do plano de resposta.
4. (Opcional) Em Nome de exibição, insira um nome mais legível para humanos para ajudar a identificar o plano de resposta ao criar incidentes.
5. Continue especificando valores padrão para registros de incidentes.

Especificação de valores padrão do incidente

Para ajudá-lo a gerenciar incidentes com mais eficiência, você pode especificar valores padrão. O Incident Manager aplica esses valores a todos os incidentes associados a um plano de resposta.

Para especificar valores padrão de incidente

1. Em Título, insira um título para esse incidente para ajudá-lo a identificá-lo na página inicial do Incident Manager.
2. Em Impacto, escolha um nível de impacto para indicar o potencial escopo de um incidente criado nesse plano de resposta, como Crítico ou Baixo. Para obter informações sobre classificações de impacto no Incident Manager, consulte Triagem.
3. (Opcional) Em Resumo, insira um breve resumo do tipo de incidente criado nesse plano de resposta.
4. (Opcional) Em Cadeia de desduplicação, insira uma cadeia de caracteres de desduplicação. O Incident Manager usa essa string para evitar que a mesma causa raiz crie vários incidentes na mesma conta.

   Uma sequência de desduplicação é um termo ou frase que o sistema usa para verificar incidentes duplicados. Se você especificar uma string de desduplicação, o Incident Manager pesquisará incidentes abertos que contenham a mesma string `dedupeString` no campo ao criar o incidente. Se uma duplicação for detectada, o Incident Manager desduplica o incidente mais recente no incidente existente.

   > **Note**
   >
   > Por padrão, o Incident Manager desduplica automaticamente vários incidentes criados pelo mesmo alarme do Amazon CloudWatch ou no evento do Amazon EventBridge. Você não precisa inserir sua própria sequência de desduplicação para evitar a duplicação desses tipos de recursos.

5. (Opcional) Em Tags de incidentes, adicione chaves e valores de tag para atribuir aos incidentes criados a partir desse plano de resposta.

   Você deve ter a permissão `TagResource` para que o recurso de registro de incidentes defina tags de incidentes no plano de resposta.
6. Continue especificando um canal de chat opcional para que os resolvedores se comuniquem sobre incidentes.

(Opcional) Especificar um canal de chat de resposta a incidentes

Quando você inclui um canal de chat em um plano de resposta, os respondentes recebem atualizações de incidentes pelo canal. Eles podem interagir com o incidente diretamente do canal de chat usando comandos de chat.

Usando o AWS Chatbot, você pode criar um canal do Slack ou do Amazon Chime para usar em seus planos de resposta. Para obter informações sobre como criar um canal de chat no AWS Chatbot, consulte o Guia do administrador do AWS Chatbot.

> **Important**
>
> O Incident Manager deve ter permissões para publicar no tópico do Amazon Simple Notification Service (Amazon SNS) do canal de chat. Sem permissões para publicar nesse tópico do SNS, você não poderá adicioná-lo ao plano de resposta. O Incident Manager publica uma notificação de teste no tópico do SNS para verificar as permissões.

Para obter mais informações sobre canais de chat, consulte Trabalhando com canais de chat no Incident Manager.

Para especificar um canal de chat de resposta a incidentes

1. Em Canal de chat, selecione um canal de chat do AWS Chatbot em que os respondentes possam se comunicar durante um incidente.

   > **Tip**
   >
   > Para criar um novo canal de chat no AWS Chatbot, escolha Configurar novo cliente de Chatbot.

2. Em Tópicos de SNS do canal de chat, escolha tópicos adicionais de SNS para publicar durante o incidente. Adicionar tópicos do SNS em várias Regiões da AWS aumenta a redundância caso uma região esteja inativa no momento do incidente.
3. Continue selecionando os contatos, os horários de plantão e os planos de escalação a serem acionados durante um incidente.

(Opcional) Selecione recursos a acionar na resposta a incidentes

É importante identificar os respondentes mais adequados no caso de ocorrer um incidente. Recomendamos seguir estas práticas recomendadas:

1. Adicione o horário de plantão como canais de escalação em um plano de escalação.
2. Escolha um plano de escalação como engajamento em um plano de resposta.

Para obter mais informações sobre contatos e planos de escalação, consulte Como trabalhar com contatos do Incident Manager e Como trabalhar com planos de escalação no Incident Manager.

Para selecionar recursos a acionar na resposta a incidentes

1. Em Engajamentos, escolha qualquer número de planos de escalação, horários de plantão e contatos individuais.
2. Continue especificando se vai usar um runbook a ser executado como parte da mitigação de incidentes.

(Opcional) Especificar um runbook para mitigação de incidentes

Você pode usar runbooks da Automação do AWS Systems Manager, um recurso do AWS Systems Manager, para automatizar tarefas comuns de aplicativos e infraestrutura em seu ambiente Nuvem AWS.

Cada runbook define um fluxo de trabalho de runbook. Um fluxo de trabalho de runbook inclui as ações que o Systems Manager realiza nos nós gerenciados ou em outros tipos de recursos da AWS. No Incident Manager, um runbook impulsiona a resposta e a mitigação de incidentes.

Para obter mais informações sobre como usar runbooks em planos de resposta, consulte Trabalho com runbooks do Automation do Systems Manager no Incident Manager.

Para especificar um runbook para mitigação de incidentes:

1. Em Runbook, realize um destes procedimentos:
   - Escolha Clonar runbook a partir do modelo para fazer uma cópia do runbook padrão do Incident Manager. Em Nome do runbook, insira um nome descritivo para o novo runbook.
   - Escolha Selecionar runbook existente. Selecione o Proprietário, o Runbook e a Versão a usar.

> **Tip**
>
> Para criar um runbook do zero, escolha Configurar novo runbook.
> Para obter informações sobre como criar runbooks, consulte Trabalho com runbooks do Automation do Systems Manager no Incident Manager.

2. Na área Parâmetros, forneça todos os parâmetros solicitados para o runbook selecionado.

   Os parâmetros disponíveis são aqueles especificados pelo runbook. Um runbook pode exigir parâmetros diferentes dos outros. Alguns parâmetros podem ser obrigatórios e outros opcionais.

   Em muitos casos, você pode optar por inserir manualmente um valor estático para um parâmetro, como uma lista de IDs de instância do Amazon EC2. Você também pode permitir que o Incident Manager forneça os valores dos parâmetros que foram gerados dinamicamente por um incidente.

3. (Opcional) Em AutomationAssumeRole, especifique o perfil do IAM AWS Identity and Access Management a ser usado. Esse perfil deve ter as permissões necessárias para executar os comandos individuais especificados no runbook.

   > **Note**
   >
   > Se não for especificado `AssumeRole`, o Incident Manager tentará usar o perfil de serviço do Runbook para executar os comandos individuais especificados no runbook.

   Escolha uma das seguintes opções:

   - Inserir valor do ARN — insira manualmente o nome do recurso da Amazon (ARN) de um AssumeRole, no formato `arn:aws:iam::`*`account-id`*`:role/`*`assume-role-name`*. Por exemplo, **`arn:aws:iam::123456789012:role/MyAssumeRole`**.
   - Usar perfil de serviço existente — escolha um perfil com as permissões necessárias em uma lista de perfis existentes em sua conta.
   - Criar novo perfil de serviço — escolha entre as políticas gerenciadas da AWS a anexar ao seu AssumeRole. Depois de selecionar essa opção, em políticas gerenciadas do AWS, escolha uma ou mais políticas na lista.

Você pode aceitar o nome padrão sugerido para o novo perfil ou pode escolher um nome que preferir.

> **Note**
>
> Esse novo perfil de serviço do Runbook está associado ao runbook específico que você selecionou. Ele não pode ser usado com runbooks diferentes. Isso ocorre porque a seção Recursos da política não suportará outros runbooks.

4. Em Perfil de serviço do runbook, especifique o perfil do IAM a ser usado para fornecer as permissões necessárias para acessar e iniciar o fluxo de trabalho do próprio runbook.

   No mínimo, o perfil deve permitir a ação `ssm:StartAutomationExecution` para seu runbook específico. Para que o runbook funcione em várias contas, o perfil também deve permitir a ação `sts:AssumeRole` do perfil do `AWS-SystemsManager-AutomationExecutionRole` criado durante Incident management entre regiões e entre contas no Incident Manager.

   Escolha uma das seguintes opções:

   - Criar novo perfil de serviço — o Incident Manager cria um perfil de serviço do runbook para você com as permissões mínimas necessárias para iniciar o fluxo de trabalho do runbook.

     Em Nome do perfil, você pode aceitar o nome padrão sugerido ou pode inserir um nome que preferir. Recomendamos usar o nome sugerido ou manter o nome do runbook no nome. Isso é pelo fato de o novo AssumeRole estar associado ao runbook específico selecionado e que pode não ter as permissões necessárias para outros runbooks.
   - Usar perfil de serviço existente — um perfil do IAM criado anteriormente por você ou pelo Incident Manager concede as permissões necessárias.

     Em Nome do perfil, selecione o nome do perfil existente a usar.
5. Expanda Opções adicionais e escolha uma das opções a seguir para especificar a Conta da AWS onde o fluxo de trabalho do runbook deve ser executado.

   - Conta do proprietário do plano de resposta — inicie o fluxo de trabalho do runbook na Conta da AWS que o criou.
   - Conta afetada — inicie o fluxo de trabalho do runbook na conta que iniciou ou relatou o incidente.

Escolha Conta impactada ao usar o Incident Manager em cenários entre contas e o runbook precisa acessar recursos na conta afetada para poder fazer as correções.

6. Continue integrando opcionalmente um serviço PagerDuty ao plano de resposta.

(Opcional) Integrar um serviço PagerDuty ao plano de resposta

Integrar um serviço PagerDuty ao plano de resposta

Ao integrar o Incident Manager com o PagerDuty, o PagerDuty criará um incidente correspondente sempre que o Incident Manager criar um incidente. O incidente no PagerDuty usa o fluxo de trabalho de paginação e as políticas de escalação que você definiu lá, além das do Incident Manager. O PagerDuty anexa eventos da linha do tempo do Incident Manager como notas sobre seu incidente.

1. Expanda Integrações de terceiros e escolha a caixa de seleção Ativar integração com o PagerDuty.
2. Em Selecionar segredo, selecione o segredo no AWS Secrets Manager em que você armazena as credenciais para acessar sua conta do PagerDuty.

   Para obter informações sobre como armazenar suas credenciais do PagerDuty em um segredo do Secrets Manager, consulte Armazenando credenciais de PagerDuty acesso em segredo AWS Secrets Manager.
3. Em Serviço PagerDuty, selecione o serviço da sua conta do PagerDuty em que deseja criar o incidente do PagerDuty.
4. Continue adicionando tags opcionais e criando o plano de resposta.

Como adicionar tags e criar o plano de resposta

Como adicionar tags e criar o plano de resposta

1. (Opcional) Na área Tags, aplique um ou mais pares de nome/valor de chave de tag ao plano de resposta.

   Tags são metadados opcionais que você atribui a um recurso. Usando tags, você pode categorizar um recurso de diferentes formas, como por finalidade, proprietário ou ambiente. Por exemplo, você pode aplicar tag em um plano de resposta para identificar o tipo de incidente ao

qual ele se destina a mitigar, os tipos de canais de escalação que ele contém ou o plano de escalação que será associado a ele. Para obter mais informações sobre como aplicar tags em recursos do Incident Manager, consulte Marcando recursos no Incident Manager.

2. Selecione Criar plano de resposta.

Como trabalhar com descobertas no Incident Manager

No Incident Manager, uma descoberta são as informações sobre implantações do AWS CodeDeploy e atualizações de pilha do AWS CloudFormation da época de um incidente, e que envolveram um ou mais recursos provavelmente relacionados ao incidente. Cada descoberta pode ser examinada como uma possível causa do incidente. As informações sobre essas possíveis causas são adicionadas à página Detalhes do incidente. Com informações sobre essas implantações e mudanças prontamente disponíveis, os respondentes não precisam pesquisar essas informações manualmente. Isso reduz o tempo de avaliação de possíveis causas, o que pode reduzir o tempo médio de recuperação (MTTR) de um incidente.

Atualmente, o Incident Manager suporta a coleta de descobertas de dois Serviços da AWS: AWS CodeDeploy e AWS CloudFormation.

O Descobertas é um atributo opcional. Você pode ativá-lo no assistente Prepare-se, quando estiver se integrando pela primeira vez ao Incident Manager ou posteriormente na página Configurações.

Quando você ativa o atributo Descobertas, o Incident Manager cria um perfil de serviço para você. Esse perfil de serviço inclui as permissões necessárias para recuperar descobertas do CodeDeploy e do CloudFormation.

Para trabalhar com descobertas no cenário entre contas, ative o atributo na conta de gerenciamento. Depois disso, cada conta de aplicativo da organização do AWS Resource Access Manager (AWS RAM) deve criar um perfil de serviço correspondente.

Consulte os tópicos a seguir para ajudar você a usar o atributo Descobertas.

Tópicos

- Habilite e crie um perfil de serviço para descobertas
- Configurar permissões para suporte de descobertas entre contas

Habilite e crie um perfil de serviço para descobertas

Ao ativar o atributo Descobertas, o Incident Manager cria um perfil de serviço chamado `IncidentManagerIncidentAccessServiceRole` em seu nome. Esse perfil de serviço fornece as permissões que o Incident Manager precisa para coletar informações sobre implantações do CodeDeploy e atualizações de pilha do CloudFormation da época em que um incidente foi criado.

> **Note**
>
> Se você estiver usando o Incident Manager com uma organização, o perfil de serviço será criado na conta de gerenciamento. Para trabalhar com descobertas em outras contas da organização, o perfil de serviço deve ser criada em cada conta de aplicativo. Para obter informações sobre como usar um modelo do CloudFormation para criar esse perfil em suas contas de aplicativos, consulte a etapa 4 em Definir e configurar incident management entre regiões e entre regiões.

Esse perfil de serviço está associado a uma política gerenciada da AWS. Para obter mais informações sobre permissões desta política, consulte AWS política gerenciada: AWSIncidentManagerIncidentAccessServiceRolePolicy.

Para obter informações sobre como habilitar descobertas durante o processo de integração do Incident Manager, consulte Conceitos básicos do Incident Manager.

Para obter informações sobre como habilitar descobertas depois de concluir o processo de integração, consulte Como gerenciar o atributo Descobertas.

Configurar permissões para suporte de descobertas entre contas

Para usar o atributo Descobertas em contas com uma organização configurada no AWS RAM, cada conta de aplicativo deve configurar permissões para que o Incident Manager assuma o perfil de serviço da conta de gerenciamento em seu nome.

Essas permissões podem ser configuradas em uma conta de aplicativo implantando um modelo do AWS CloudFormation fornecido pela AWS, que cria o perfil `IncidentManagerIncidentAccessServiceRole`.

Para obter informações sobre como baixar e implantar esse modelo em uma conta de aplicativo, consulte a etapa 4 em Incident management entre regiões e entre contas no Incident Manager.

Criação de incidentes no Incident Manager

O Incident Manager, um recurso do AWS Systems Manager, ajuda você a gerenciar e responder rapidamente aos incidentes. Você pode configurar o Amazon CloudWatch e o Amazon EventBridge para criar incidentes automaticamente, com base nos alarmes do CloudWatch e nos eventos do EventBridge. Você também pode criar incidentes manualmente na página da lista de incidentes ou usando a ação da API StartIncident da AWS CLI ou do SDK da AWS. O Incident Manager desduplica incidentes criados a partir do mesmo alarme do CloudWatch ou evento do EventBridge no mesmo incidente.

Nos incidentes automaticamente criados por alarmes do CloudWatch ou eventos do EventBridge, o Incident Manager cria um incidente na mesma Região da AWS como a regra de alarme ou evento. Se o Incident Manager não estiver disponível na Região da AWS, o CloudWatch ou o EventBridge criarão automaticamente o incidente em uma das regiões disponíveis especificadas no conjunto de replicação. Para obter mais informações, consulte Incident management entre regiões e entre contas no Incident Manager.

Quando o sistema cria um incidente, o Incident Manager coleta automaticamente informações sobre os recursos da AWS envolvidos no incidente e adiciona essas informações à guia Itens relacionados. Se você especificou um runbook em seu plano de resposta, quando o sistema cria um incidente, o Incident Manager pode enviar as informações sobre os recursos da AWS envolvidos no incidente para o runbook. O sistema pode então direcionar esses recursos ao iniciar o runbook e tentar corrigir o problema.

Quando o sistema cria um incidente, ele também cria um item de trabalho operacional principal (OpsItem) no OpsCenter, um componente do Systems Manager, e o vincula ao incidente como um item relacionado. Você pode usar esse OpSitem para monitorar trabalhos relacionados e análises de futuros incidentes. As chamadas para o OpsCenter geram custos. Para obter mais informações sobre os preços do OpsCenter, consulte os Preços do Systems Manager.

> **Important**
>
> Observe os seguintes detalhes importantes.
>
> - Caso o Incident Manager não esteja disponível, o sistema só poderá fazer failover e criar incidentes em outras Regiões da AWS se você tiver especificado pelo menos duas regiões no conjunto de replicação. Para obter informações sobre como configurar um conjunto de replicação, consulte Conceitos básicos do Incident Manager.

- Os incidentes criados por um failover entre regiões não invocam os runbooks especificados nos planos de resposta.

Como configurar criação automática de incidentes com alarmes do CloudWatch

O CloudWatch usa suas métricas do CloudWatch para alertá-lo sobre mudanças no ambiente e para executar automaticamente a ação inicial do incidente. O CloudWatch trabalha com o Systems Manager e o Incident Manager para criar um incidente a partir de um modelo de plano de resposta quando um alarme entra em estado de alarme. Isso exige os seguintes pré-requisitos:

- Incident Manager configurado e conjunto de replicação criado. Essa etapa cria o perfil vinculado ao serviço Incident Manager em sua conta, fornecendo as permissões necessárias.
- Um plano de resposta do Incident Manager configurado. Para saber como configurar os planos de resposta do Incident Manager, consulte Como trabalhar com planos de resposta no Incident Manager na seção Preparação para incidentes deste guia.
- Métricas do CloudWatch configuradas para monitorar seu aplicativo. Para obter as práticas recomendadas de monitoramento, consulte Monitorar na seção Preparação para incidentes deste guia.

Para criar um alarme com uma ação Iniciar incidente

1. Crie um alarme no CloudWatch. Para obter mais informações, consulte Uso de alarmes do Amazon CloudWatch no Manual do usuário do Amazon CloudWatch.
2. Ao escolher a ação a ser executada pelo alarme, selecione Adicionar ação do Systems Manager.
3. Escolha Criar incidente e selecione o Plano de resposta para esse incidente.
4. Conclua as etapas restantes no guia do tipo de alarme selecionado.

> **Tip**
>
> Você também pode adicionar a ação de criação de incidente a qualquer alarme existente.

Criação automática de incidentes com eventos do EventBridge

As regras do EventBridge observam os padrões de eventos. Se o evento corresponder ao padrão definido, o Incident Manager cria um incidente usando o plano de resposta escolhido.

Criação de incidentes usando eventos de parceiros SaaS

Você pode configurar o EventBridge para receber eventos de aplicativos e serviços de parceiros de software como serviço (SaaS), permitindo a integração de terceiros. Depois de configurar o EventBridge para receber eventos de parceiros terceirizados, você pode criar regras que correspondam aos eventos do parceiro para criar incidentes. Para ver uma lista de integrações de terceiros, consulte Recebimento de eventos de um parceiro de SaaS.

Configure o EventBridge para receber eventos de uma integração SaaS.

1. Abra o console do Amazon EventBridge em https://console.aws.amazon.com/events/.
2. No painel de navegação, selecione Partner event sources (Origens de eventos do parceiro).
3. Use a barra de pesquisa para encontrar o parceiro que deseja e selecione Configurar para esse parceiro.
4. Selecione Copiar para copiar o ID da conta para a área de transferência.

> **Note**
>
> Para fazer a integração com o Salesforce, use as etapas descritas no Guia do usuário do Amazon AppFlow.

5. Acesse o site do parceiro e siga as instruções para criar uma origem de evento do parceiro. Use seu ID de conta para isso. A origem do evento criado estará disponível somente na sua conta.
6. Volte ao console do EventBridge e selecione Origens de eventos do parceiro no painel de navegação.
7. Selecione o botão ao lado da origem do evento do parceiro e selecione Associate with event bus (Associar ao barramento de eventos).

Criar uma regra que será acionada em um evento de um parceiro de SaaS

1. Abra o console do Amazon EventBridge em https://console.aws.amazon.com/events/.
2. No painel de navegação, escolha Rules (Regras).

3. Escolha Create rule (Criar regra).
4. Insira um nome e uma descrição para a regra.

   Uma regra não pode ter o mesmo nome que outra regra na mesma região e no mesmo barramento de eventos.
5. Em Barramento de eventos, escolha o barramento de eventos que corresponde a esse parceiro.
6. Em Rule type (Tipo de regra), escolha Rule with an event pattern (Regra com um padrão de evento).
7. Escolha Next (Próximo).
8. Em Event source (Origem do evento), escolha Eventos da AWS ou eventos de parceiro do EventBridge.
9. Na seção Padrão de evento, selecione Formulário de padrão de evento.
10. Em Origem do evento, escolha Parceiros do EventBridge
11. Em Parceiros, escolha o nome do parceiro.
12. Em Event type (Tipo de evento), selecione All Events (Todos os eventos) ou escolha o tipo de evento a ser usado para essa regra. Se você escolher All Events (Todos os eventos), todos os eventos emitidos por essa origem de evento do parceiro corresponderão à regra.

    Se quiser personalizar o padrão de evento, selecione Editar, faça as alterações e selecione Salvar.
13. Escolha Next (Próximo).
14. Em Selecionar um alvo, escolha Plano de resposta do Incident Manager e escolha um Plano de resposta.

    > **Note**
    >
    > Ao selecionar um plano de resposta, todos os planos de resposta que você possui e que foram compartilhados com sua conta aparecem na lista suspensa Plano de resposta.
15. Nesses casos, o Eventbridge pode criar o perfil do IAM necessário para a regra ser executada:

    - Para criar um perfil do IAM automaticamente, escolha Create a new role for this specific resource (Criar novo perfil para este recurso específico).
    - Para usar um perfil do IAM que você criou antes, escolha Use existing role (Usar perfil existente).

16. Escolha Next (Próximo).
17. (Opcional) Insira uma ou mais tags para a regra. Para obter mais informações, consulte Etiquetas do Amazon EventBridge no Guia do usuário do Amazon EventBridge.
18. Escolha Next (Próximo).
19. Revise sua regra e escolha Criar regra.

Criação de incidentes usando eventos de serviço da AWS

O EventBridge também recebe eventos dos serviços da AWS listados em Eventos de Serviços da AWS suportados. Da mesma forma que você configura regras para parceiros de SaaS, você pode configurá-las para serviços da AWS.

Crie uma regra que seja acionada em eventos de um serviço da AWS

1. Abra o console do Amazon EventBridge em https://console.aws.amazon.com/events/.
2. No painel de navegação, escolha Rules (Regras).
3. Escolha Create rule (Criar regra).
4. Insira um nome e uma descrição para a regra.

   Uma regra não pode ter o mesmo nome que outra regra na mesma região e no mesmo barramento de eventos.
5. Em Event Bus (Barramento de eventos), escolha default (padrão).
6. Em Rule type (Tipo de regra), escolha Rule with an event pattern (Regra com um padrão de evento).
7. Escolha Next (Próximo).
8. Em Event source (Origem do evento), escolha Eventos da AWS ou eventos de parceiro do EventBridge.
9. Na seção Padrão de evento, selecione Formulário de padrão de evento.
10. Em Event source (Origem do evento), escolha AWS services (Serviços da).
11. Em Nome do serviço, escolha o serviço que monitora um incidente.
12. Em Event type (Tipo de evento), selecione All Events (Todos os eventos) ou escolha o tipo de evento a ser usado para essa regra. Se você escolher All Events (Todos os eventos), todos os eventos emitidos por essa origem de evento do parceiro corresponderão à regra.

Se quiser personalizar o padrão de evento, selecione Editar, faça as alterações e selecione Salvar.

13. Escolha Next (Próximo).
14. Em Selecionar um alvo, escolha Plano de resposta do Incident Manager e escolha um Plano de resposta.

> **Note**
>
> Ao selecionar um plano de resposta, todos os planos de resposta que você possui e que foram compartilhados com sua conta aparecem na lista suspensa Plano de resposta.

15. Nesses casos, o Eventbridge pode criar o perfil do IAM necessário para a regra ser executada:
    - Para criar um perfil do IAM automaticamente, escolha Create a new role for this specific resource (Criar novo perfil para este recurso específico).
    - Para usar um perfil do IAM que você criou antes, escolha Use existing role (Usar perfil existente).
16. Escolha Next (Próximo).
17. (Opcional) Insira uma ou mais tags para a regra. Para obter mais informações, consulte Etiquetas do Amazon EventBridge no Guia do usuário do Amazon EventBridge.
18. Escolha Next (Próximo).
19. Revise sua regra e escolha Criar regra.

Criação manual de incidentes

Os respondentes podem rastrear manualmente um incidente usando o console do Incident Manager por um plano de resposta predefinido. Use as etapas a seguir para criar um incidente.

1. Abra o console do Incident Manager.
2. Selecione Iniciar incidente.
3. Em Plano de resposta, escolha um plano de resposta da lista.
4. (Opcional) Para substituir o título fornecido pelo plano de resposta definido, insira o Título do incidente.

5. (Opcional) Para substituir o impacto fornecido pelo plano de resposta definido, insira o Impacto do incidente.

Rastreamento de incidentes no Incident Manager

O AWS Systems Manager Incident Manager rastreia seus incidentes desde o momento em que são detectados até a resolução, passando depois pela análise pós-incidente. Você pode encontrar todos os incidentes na página Lista de incidentes no console do Incident Manager, com links diretos para os Detalhes do incidente.

Tópicos

- Lista de incidentes
- Detalhes do incidente

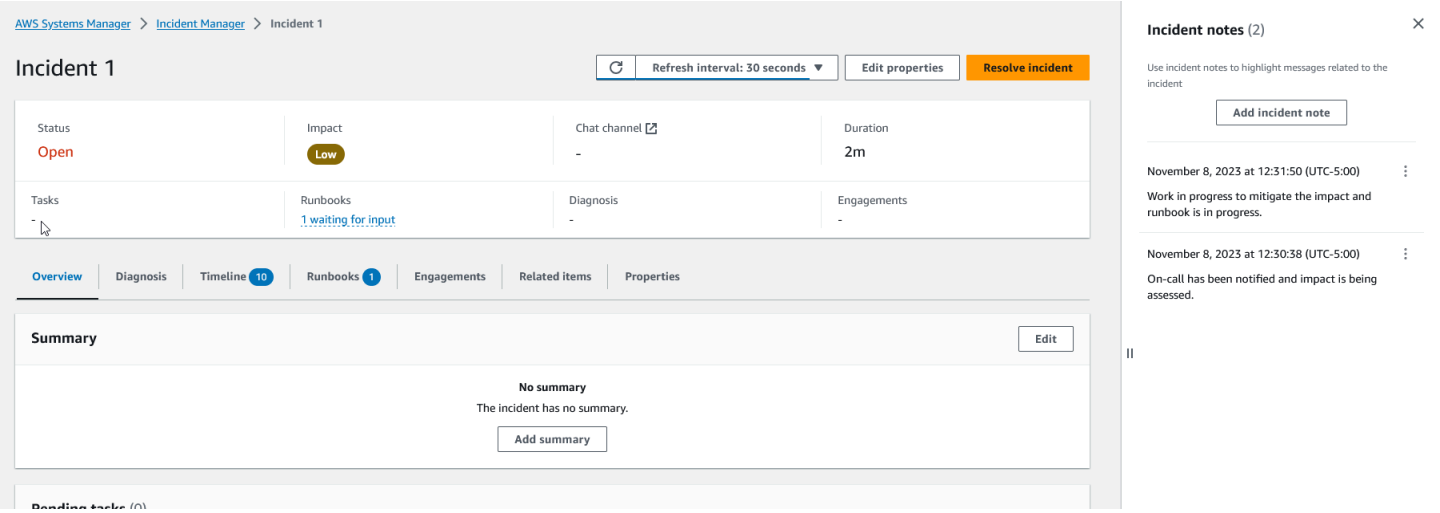
Lista de incidentes

A página Lista de incidentes contém três seções: Incidentes abertos, Incidentes resolvidos e Análises. Você pode rastrear manualmente novos incidentes e criar análises nesta página. Para saber mais sobre como rastrear manualmente um incidente, consulte Criação manual de incidentes na seção Criação de incidentes deste guia. Para saber mais sobre a análise pós-incidente, consulte a seção Como realizar uma análise pós-incidente no Incident Manager deste guia.

Os Detalhes do incidente exibem Incidentes abertos em blocos com o título, o impacto, a duração e o canal de chat desse incidente. Depois de resolver um incidente, ele passa para a lista de Incidentes resolvidos. Análises estão na segunda guia.

Detalhes do incidente

A página Detalhes do incidente fornece insights detalhados e ferramentas para você tratar um incidente. Nessa página, você pode iniciar runbooks para mitigar um incidente, adicionar notas de incidentes, envolver outros solucionadores e visualizar detalhes do incidente, como linhas do tempo, métricas, propriedades e recursos relacionados. A página Detalhes do incidente inclui as seguintes seções: banner superior, Notas do incidente e sete guias com informações e recursos adicionais. Por padrão, o banner superior e as seções Notas do incidente são exibidas em todas as páginas Detalhes do incidente.



Este tópico explica os elementos da página Detalhes do incidente e as ações que você pode executar na página.

Banner superior

O banner superior na página de detalhes de cada incidente inclui as seguintes informações:

- Status: o status atual de um incidente pode ser Aberto ou Resolvido.
- Impacto: o impacto do incidente no ambiente. Pode ser alto, médio ou baixo. Para alterar o impacto de um incidente, escolha Editar propriedades.
- Canal de chat: um link para acessar o canal de chat onde você pode ver atualizações e notificações de incidentes.
- Duração: o tempo decorrido até que um respondente resolva o incidente.
- Runbooks: os status dos runbooks associados a esse incidente. O status pode estar aguardando entrada, bem-sucedido ou malsucedido. Se o status de um runbook for aguardando entrada, você poderá selecionar o runbook para ver os detalhes da ação. Você pode selecionar malsucedido para visualizar os runbooks no statusAtingiu o tempo limite, Falhou ou Cancelados.
- Engajamentos: o número total de engajamentos e o status de cada engajamento. Quando você cria um engajamento, seu status é Engajado. Depois de confirmar o engajamento, o status muda de Engajado para Confirmado. O Incident Manager não oferece suporte à confirmação de engajamentos de terceiros. Esses engajamentos permanecem no status Engajado.

Você pode editar o título, o impacto e o canal de chat do incidente escolhendo Editar no canto superior direito do banner.

Notas de incidentes

O lado direito da tela exibe a seção Notas do incidente. Você pode colaborar e se comunicar com outros usuários que trabalham em um incidente usando notas. Você pode explicar as mitigações aplicadas, uma possível causa raiz identificada ou o status atual do incidente. Como prática recomendada, use a seção Notas do incidente para publicar atualizações de status e ações que você ou outras pessoas tomam em relação a um incidente. Se você precisar se comunicar com outros solucionadores em tempo real, use o canal de chat disponível no Incident Manager.

Para adicionar uma nota, escolha o botão Adicionar nota de incidente e, em seguida, insira sua nota. As notas podem conter atualizações sobre o status do incidente ou qualquer outra informação relevante que forneça visibilidade a outros usuários. Se necessário, você também pode editar ou excluir notas de incidentes.

> **Note**
>
> Qualquer usuário com permissão do IAM para executar as ações `ssm-incidents:UpdateTimelineEvent` e `ssm-incidents:DeleteTimelineEvent` pode editar e excluir notas. No entanto, quando você compartilha um incidente com outra conta, a política de recursos não inclui a ação `ssm-incidents:DeleteTimelineEvent`. Isso impede que o usuário com quem você compartilha o incidente exclua a nota. Você pode visualizar a trilha de auditoria de uma nota dos eventos do Incident Manager no console do AWS CloudTrail.

Guias

A página Detalhes do incidente tem sete guias, para facilitar para os respondentes localizarem e visualizarem informações durante um incidente. As guias exibem um contador no nome da guia, que indica o número de atualizações na guia. Para obter mais informações sobre o conteúdo de cada guia, bem como sobre as ações disponíveis, continue lendo.

Visão geral

A guia Visão geral é a página inicial dos respondentes. Ela contém o resumo do incidente, uma lista dos eventos recentes da Linha do tempo e a etapa atual do runbook.

Os respondentes usam o Resumo para acompanhar quais ações foram tomadas, os resultados de quaisquer alterações, possíveis próximas etapas e informações sobre o impacto do incidente. Para atualizar o resumo, escolha Editar no canto superior direito da seção Resumo.

> **Important**
>
> Se vários respondentes estiverem editando o campo de resumo simultaneamente, o respondente que enviou suas edições por último sobrescreverá todas as outras entradas.

A seção Eventos de linha do tempo recentes contém uma Linha do tempo preenchida pelo Incident Manager com os cinco eventos mais recentes. Use esta seção para entender o status do incidente e o que ocorreu recentemente. Para ver uma Linha do tempo completa, vá até a guia Linha do tempo.

A página de visão geral também exibe a etapa Runbook atual. Essa etapa pode ser uma etapa automática em execução no ambiente AWS ou pode ser um conjunto de instruções manuais para os respondentes. Para ver o runbook completo, incluindo as etapas anteriores e futuras, escolha a guia Runbook.

Diagnóstico

A guia Diagnóstico contém informações vitais sobre seus aplicativos e sistemas hospedados na AWS, incluindo informações sobre métricas e, se habilitada, descobertas.

Como trabalhar com métricas

O Incident Manager usa o Amazon CloudWatch para preencher os gráficos de métricas e alarmes encontrados nessa guia. Para saber mais sobre as práticas recomendadas de gerenciamento de incidentes para definir alarmes e métricas, consulte Monitorar na seção Planejamento de incidentes deste guia do usuário.

Para adicionar métricas

- Escolha Adicionar no canto superior direito dessa guia.
  - Para adicionar uma métrica de um painel existente do CloudWatch, escolha Do painel existente do CloudWatch.
    a. Escolha um Painel. Isso adiciona todas as métricas e alarmes que fazem parte do painel escolhido.

b. (Opcional) Você também pode Selecionar métricas no painel para visualizar métricas específicas.

- Adicione uma única métrica selecionando Do CloudWatch e colando uma origem de métrica. Para copiar uma origem de métrica:

  a. Abra o console do CloudWatch em https://console.aws.amazon.com/cloudwatch/.

  b. No painel de navegação, selecione Métricas.

  c. Na guia Todas as métricas, insira um termo de pesquisa no campo de pesquisa, como o nome de uma métrica ou nome do recurso e pressione Enter.

     Por exemplo, se você pesquisar a métrica `CPUUtilization`, verá os namespaces e as dimensões associados a essa métrica.

  d. Selecione um dos resultados da pesquisa para ver as métricas.

  e. Escolha a guia Origem e copie a origem.

Os gráficos de alarmes de métricas só podem ser adicionados aos detalhes do incidente por meio do plano de resposta relacionado ou selecionando Do painel existente do CloudWatch ao adicionar uma métrica.

Para remover métricas, escolha Remover e, em seguida, escolha as métricas que deseja remover do menu suspenso Métricas fornecido.

Como visualizar descobertas do AWS CodeDeploy e do AWS CloudFormation

Depois de habilitar Descobertas e configurar todas as permissões necessárias, todas as descobertas que possam estar relacionadas a um incidente específico serão anexadas ao incidente. Os respondentes podem ver informações sobre essas descobertas na página Detalhes do incidente.

Para ver as descobertas do CodeDeploy e do CloudFormation

1. Abra o console do Incident Manager.
2. Escolha o nome de um incidente a ser investigado.
3. Na guia Diagnóstico, na área Descobertas, compare os horários de início de qualquer descoberta relatada com o horário de início do incidente.
4. Para ver mais detalhes sobre uma descoberta, na coluna Referência, escolha o link para descoberta do CodeDeploy ou do CloudFormation.

Linha do tempo

Use a guia Linha do tempo para rastrear eventos que ocorrem durante um incidente. O Incident Manager preenche automaticamente os eventos da Linha do tempo que identificam ocorrências significativas durante o incidente. Os respondentes podem adicionar eventos personalizados com base nas ocorrências detectadas manualmente. Durante a análise pós-incidente, a guia da linha do tempo fornece informações valiosas sobre como se preparar e responder melhor aos incidentes no futuro. Para obter mais informações sobre análise pós-incidente, consulte Como realizar uma análise pós-incidente no Incident Manager.

Para adicionar um evento personalizado na linha do tempo, escolha Adicionar. Selecione uma data usando o calendário e, em seguida, insira uma hora. Todos os horários são exibidos no fuso horário local. Forneça uma breve descrição do evento que aparecerá na linha do tempo.

Para editar um evento personalizado existente, selecione o evento na linha do tempo e escolha Editar. Você pode alterar a hora, a data e a descrição dos eventos personalizados. Você só pode editar eventos personalizados.

Runbooks

A guia Runbooks da página de detalhes do incidente é onde os respondentes podem visualizar as etapas do runbook e iniciar novos runbooks.

Para iniciar um novo runbook, escolha Iniciar runbook na seção Runbooks. Use o campo de pesquisa para localizar o runbook que deseja iniciar. Forneça todos os Parâmetros necessários e a Versão do runbook que deseja usar ao iniciar o runbook. Os runbooks iniciados durante um incidente na guia Runbooks usam as permissões da conta atualmente conectada.

Para navegar até uma definição de runbook no Systems Manager, escolha o título do runbook em Runbooks. Para navegar até a instância do runbook em execução no Systems Manager, escolha os detalhes da execução em Detalhes da execução. Essas páginas exibem o modelo usado para iniciar o runbook e os detalhes específicos da instância atualmente em execução do documento de automação.

A seção Etapas do runbook exibe a lista de etapas que o runbook selecionado executa automaticamente ou que os respondentes executam manualmente. As etapas se expandem ao se tornarem a etapa atual, exibindo as informações necessárias para concluir a etapa ou os detalhes sobre o que a etapa faz. As etapas automáticas do runbook são resolvidas após a conclusão da automação. As etapas manuais exigem que os respondentes escolham Próxima etapa na parte

inferior de cada etapa. Após a conclusão de uma etapa, a saída da etapa aparece como uma lista suspensa.

Para cancelar a execução de um runbook, escolha Cancelar runbook. Isso interromperá a execução do runbook e não concluirá nenhuma etapa adicional no runbook.

Engajamentos

A guia Engajamentos dos detalhes do incidente impulsiona o engajamento dos respondentes e das equipes. Nessa guia, você pode ver quem foi engajado, quem respondeu e quais respondentes serão engajados como parte de um plano de escalação. Os respondentes podem interagir com outros contatos diretamente dessa guia. Para saber mais sobre a criação de contatos e planos de escalação, consulte as seções Como trabalhar com contatos do Incident Manager e Como trabalhar com planos de escalação no Incident Manager deste guia.

Você pode configurar planos de resposta com contatos e planos de escalação para iniciar automaticamente o engajamento no início de um incidente. Para saber mais sobre como configurar planos de resposta, consulte a seção Como trabalhar com planos de resposta no Incident Manager deste guia.

Você pode encontrar informações sobre cada contato na tabela. Essa tabela inclui as seguintes informações:

- Nome: links para a página de detalhes de contato que exibe seus métodos de contato e plano de engajamento.
- Plano de escalação: links para o plano de escalação que envolveu o contato.
- Fonte do contato: identifica o serviço que engajou esse contato, como o AWS Systems Manager ou o PagerDuty.
- Engajado: exibe quando o plano engajou um contato ou quando engajar um contato como parte do plano de escalação.
- Confirmado: mostra se o contato reconheceu o engajamento.

Para confirmar um engajamento, o respondente pode realizar um dos seguintes procedimentos:

- Chamada telefônica: digite **1** quando solicitado.
- SMS: responda à mensagem com o código fornecido ou insira o código fornecido na guia Engajamentos do incidente.

- E-mail: insira o código fornecido na guia Engajamentos do incidente.

Itens relacionados

A guia Itens relacionados é usada para coletar recursos relacionados à mitigação de incidentes. Esses recursos podem ser ARNs, links para recursos externos ou arquivos enviados para buckets do Amazon S3. A tabela exibe um título descritivo e um ARN, um link ou detalhes do bucket. Antes de usar buckets do S3, revise as Práticas recomendadas de segurança do Amazon S3 no Guia do usuário do Amazon S3.

Ao carregar arquivos em um bucket do Amazon S3, o versionamento é ativado ou suspenso nesse bucket. Quando o versionamento é ativado no bucket, os arquivos carregados com o mesmo nome de um arquivo existente são adicionados como uma nova versão do arquivo. Se o versionamento for suspenso, os arquivos carregados com o mesmo nome de um arquivo existente sobrescreverão o arquivo existente. Para saber mais sobre versionamento, consulte Como usar o versionamento nos buckets do S3 no Guia do usuário do Amazon S3.

Ao remover um item relacionado ao arquivo, o arquivo é removido do incidente, mas não é removido do bucket do Amazon S3. Para saber mais sobre como remover objetos de um bucket do Amazon S3, consulte Excluir objetos do Amazon S3 no Guia do usuário do Amazon S3.

Propriedades

A guia Propriedades fornece os seguintes detalhes sobre o incidente.

Na seção Propriedades de incidente, você pode ver o seguinte:

- Status: descreve o status atual do incidente. O incidente pode estar Aberto ou Resolvido.
- Horário de início: o horário em que o incidente foi criado no Incident Manager.
- Horário da resolução: o horário em que o incidente foi resolvido no Incident Manager.
- Nome do recurso da Amazon (ARN): o ARN do incidente. Use o ARN ao se referir ao incidente no chat ou com os comandos da AWS Command Line Interface (AWS CLI).
- Plano de resposta: identifica o plano de resposta para o incidente selecionado. A escolha do plano de resposta abre a página de detalhes do plano de resposta.
- OpsItem principal: identifica o OpsItem criado como o principal do incidente. Um OpSitem principal pode ter vários incidentes relacionados e itens de ação de acompanhamento. Selecionar o OpsItem principal abre a página de detalhes do OpsiTems no OpsCenter.

- Análise: identifica a análise criada desse incidente. Crie uma análise de um incidente resolvido para melhorar seu processo de resposta a incidentes. Escolha a análise para abrir a página de detalhes da análise.
- Proprietário: a conta na qual o incidente foi criado.

Na seção Tags, você pode visualizar e editar as chaves e os valores das tags associados ao registro do incidente. Para obter mais informações sobre tags no Incident Manager, consulte Marcando recursos no Incident Manager.

Como realizar uma análise pós-incidente no Incident Manager

A análise pós-incidente orienta você na identificação de melhorias na resposta a incidentes, incluindo o tempo de detecção e mitigação. Uma análise também pode ajudá-lo a entender a causa raiz dos incidentes. O Incident Manager cria itens de ação recomendados que você pode usar para melhorar sua resposta a incidentes.

Benefícios de uma análise pós-incidente

- Melhore a resposta a incidentes
- Entenda a causa raiz do problema
- Aborde as causas raízes com itens de ação de entrega
- Analise o impacto dos incidentes
- Capture e compartilhe aprendizados em uma organização

Para que não usar uma análise

Uma análise é irrepreensível e não chama as pessoas pelo nome.

“Independentemente do que descobrimos, entendemos e realmente acreditamos que todos fizeram o melhor trabalho possível, considerando o que sabiam na época, suas habilidades e aptidões, os recursos disponíveis e a situação em questão.” - Norm Kerth, “Project Retrospectives: A Handbook for Team Review” (“Retrospectivas de projetos: um manual para análise de equipes”)

Detalhes da análise

A página de detalhes da análise orienta você na coleta de informações, na avaliação de melhorias e na criação de itens de ação. A página de detalhes da análise é semelhante aos detalhes do incidente, com algumas diferenças importantes, como métricas históricas, cronograma editável e perguntas para melhorar futuros incidentes.

Visão geral

A visão geral é um resumo do incidente. Esse resumo inclui o histórico, o que ocorreu, por que aconteceu, como foi mitigado, a duração e os principais itens de ação para evitar que o incidente

aconteça novamente. A visão geral é de alto nível. Você explorará mais detalhes na guia Perguntas da análise.

Métricas

Use a guia de métricas para visualizar as principais métricas em seu aplicativo durante o incidente. Você pode adicionar aqui gráficos de métricas que tenham uma ou mais métricas representadas no mesmo gráfico. As métricas usadas durante um incidente são preenchidas automaticamente nessa guia. Recomendamos que você adicione uma descrição, título e anotações dos principais pontos temporais durante o incidente.

Alguns pontos temporais chave que você pode considerar ao analisar um gráfico métrico:

- Alteração na implantação
- Alteração de configuração
- Hora de início do incidente
- Hora do alarme
- Hora do engajamento
- Hora de início da mitigação
- Hora de resolução do incidente

Limitações

- Os alarmes e expressões métricas do CloudWatch não são importados de um incidente.
- As métricas que estão em uma região que o Incident Manager não suporta não são importadas do incidente.
- As métricas nas contas de aplicativos exigem a configuração do `CloudWatch-CrossAccountSharingRole` antes da criação da análise. Para obter mais informações sobre o perfil, consulte o console Cross-Account Cross-Region CloudWatch no guia do usuário do CloudWatch.

Cronograma

Descreva os principais momentos no cronograma à medida que você se aprofunda na compreensão do incidente. O cronograma de incidentes é preenchido automaticamente nessa guia. Você pode

excluir pontos temporais que não são relevantes para a análise. Você também pode adicionar e editar pontos temporais para descrever o incidente e seu impacto com mais precisão.

Use a guia Cronograma para responder às perguntas que você encontra na guia Perguntas sobre a resposta ao incidente.

Perguntas

Use as perguntas do Incident Manager para melhorar o tempo de resolução de incidentes em seu aplicativo e reduzir a ocorrência de incidentes. Ao responder às perguntas, atualize as guias Métricas e Cronograma para verificar a precisão. As perguntas se concentram nesses aspectos principais da resposta a incidentes:

- Detecção — Você poderia melhorar o tempo de detecção? Há atualizações nas métricas e alarmes que detectariam o incidente mais cedo?
- Diagnóstico — Você pode melhorar o tempo de diagnóstico? Há atualizações em seus planos de resposta ou planos de escalação que envolveriam os respondentes corretos mais cedo?
- Mitigação — Você pode melhorar o tempo de mitigação? Há etapas do runbook que você poderia adicionar ou melhorar?
- Prevenção — Você pode evitar que futuros incidentes ocorram? Para descobrir as causas básicas de um incidente, a Amazon usa a abordagem dos 5 porquês na investigação de problemas.

Ações

O Incident Manager cria itens de ação recomendados para você revisar ao responder às perguntas. Você pode optar por aceitar e concluir essas ações nessa guia ou pode ignorá-las. Você pode revisar itens de ação dispensados escolhendo Itens de ação dispensados. Os itens de ação são um tipo de OpsItem vinculado à análise e ao incidente no OpsCenter.

Lista de verificação

Antes de fechar uma análise, use a lista de verificação para revisar as ações que um respondente deve tomar. À medida que os respondentes concluem ações na lista de verificação, o ícone ao lado da ação muda de uma elipse para uma marca de seleção, indicando que a ação foi concluída. Se você não tiver concluído os itens da lista de verificação, o Incident Manager exibirá uma mensagem para confirmar que o respondente deseja fechar a análise sem concluí-la.

Modelos de análise

Um modelo de análise fornece um conjunto de perguntas que se aprofundam na causa raiz dos incidentes. Você pode usar suas respostas a essas perguntas para melhorar o desempenho do aplicativo e a resposta a incidentes.

AWS modelo padrão

O Incident Manager fornece um modelo padrão de perguntas com base nas melhores práticas de resposta a incidentes e análise de problemas AWS, intitulado `AWSIncidents-PostIncidentAnalysisTemplate`.

Criar um modelo de análise

Recomendamos que você use o `AWSIncidents-PostIncidentAnalysisTemplate` modelo padrão e adicione perguntas ou seções adicionais que sejam apropriadas para seus casos de uso. Crie modelos de análise com base no modelo padrão Use esse modelo como ponto de partida para criar modelos de análise em sua conta de gerenciamento. Em seguida, você pode duplicar seus modelos de análise em cada Região em que ativou o Incident Manager.

Criar um modelo de análise

1. Chame a `GetDocument` ação e use seu `Name` parâmetro para fazer o download `AWSIncidents-PostIncidentAnalysisTemplate`. Para obter mais informações sobre a `GetDocument` sintaxe, consulte Referência da API do Systems Manager.
2. O conteúdo da resposta contém os blocos de construção JSON para a análise. Use os blocos de construção da pergunta para inserir perguntas adicionais na análise. Recomendamos que você adicione perguntas ou seções na seção `Incident questions`.
3. Para criar o novo modelo, use a operação `CreateDocument` com o JSON atualizado da etapa anterior. Você deve incluir o seguinte, onde *`Analysis_Template_Name`* é o nome do seu modelo,

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

Criar uma análise

1. Para criar uma análise, escolha Criar análise na página de detalhes do incidente de um incidente fechado.
2. Escolha o modelo de análise a partir do qual criar essa análise e insira um nome descritivo da análise.
3. Escolha Criar.

Imprima uma análise de incidentes formatada

Você pode gerar uma cópia de uma análise completa ou incompleta formatada para impressão. Você também pode salvar essa cópia como PDF. É possível imprimir uma análise de cada vez. A impressão em lote de várias análises não é compatível no momento.

Para imprimir uma análise formatada

1. Abra o console do Incident Manager.
2. Escolha a guia Análise.
3. Selecione o título da análise que quer imprimir.
4. No canto superior direito da página de detalhes da análise, escolha Imprimir.
5. Na caixa de diálogo Imprimir análise de incidentes, limpe as seções da análise que não deseja incluir na versão impressa. Por padrão, todas as seções são selecionadas.
6. Escolha Imprimir para abrir os controles de impressão locais do seu dispositivo.
7. Escolha seu destino ou formato de impressão. Você pode escolher uma impressora local ou de rede ou salvar a análise em um PDF. Faça as alterações, se desejar, nas opções de impressão restantes e escolha Imprimir.

> **Note**
>
> Os Controles de impressão locais se referem à interface do usuário fornecida pelo seu navegador e dispositivo.
> Os Destinos de impressão são aqueles configurados e acessíveis a partir do seu dispositivo.

Tutoriais do Incident Manager

Esses tutoriais do AWS Systems Manager Incident Manager ajudam você a criar um sistema de gerenciamento de incidentes mais robusto. Esses tutoriais abrangem atividades comuns que ocorrem durante um incidente ou oferecem suporte à resposta a incidentes.

Tópicos

- Uso de runbooks do Automation do Systems Manager no Incident Manager
- Gerenciar incidentes de segurança no Incident Manager

Uso de runbooks do Automation do Systems Manager no Incident Manager

Você pode usar runbooks de AWS Systems Manager automação para simplificar as tarefas comuns de manutenção, implantação e remediação dos serviços. AWS Neste tutorial, você criará um runbook personalizado para automatizar uma resposta a incidentes no Incident Manager. O cenário deste tutorial envolve um CloudWatch alarme da Amazon atribuído a uma métrica do Amazon EC2. Quando a instância entra em um estado que aciona o alarme, o Incident Manager executa automaticamente as seguintes tarefas:

1. Cria um incidente no Incident Manager.
2. Inicia um runbook que tenta corrigir o problema.
3. Publica os resultados do runbook na página de detalhes do incidente no Incident Manager.

O processo descrito neste tutorial também pode ser usado com EventBridge eventos da Amazon e outros tipos de AWS recursos. Ao automatizar sua resposta de remediação a alarmes e eventos, você pode reduzir o impacto de um incidente em sua organização e em seus recursos.

Este tutorial descreve como editar um CloudWatch alarme atribuído a uma instância do Amazon EC2 para um plano de resposta do Incident Manager. Se você não tiver um alarme, uma instância ou um plano de resposta configurado, recomendamos que você configure esses recursos antes de começar. Para obter mais informações, consulte os tópicos a seguir.

- Usando CloudWatch alarmes da Amazon no Guia do CloudWatch usuário da Amazon
- Instâncias do Amazon EC2 no Guia do usuário do Amazon EC2

- Instâncias do Amazon EC2 no Guia do usuário do Amazon EC2
- Como trabalhar com planos de resposta no Incident Manager

> **Important**
>
> Você incorrerá em custos criando AWS recursos e usando as etapas de automação do runbook. Para obter mais informações, consulte Preços do AWS.

Tópicos

- Tarefa 1: Criar o runbook
- Tarefa 2: Criar um perfil do IAM
- Tarefa 3: Conectar o runbook ao seu plano de resposta
- Tarefa 4: Atribuir um CloudWatch alarme ao seu plano de resposta
- Tarefa 5: verificar os resultados

Tarefa 1: Criar o runbook

Use o procedimento a seguir para criar um runbook no console do Systems Manager. Quando invocado a partir de um incidente do Incident Manager, o runbook reinicia uma instância do Amazon EC2 e atualiza o incidente com informações sobre a execução do runbook. Antes de começar, verifique se você tem permissão para criar um runbook. Para obter mais informações, consulte Configuração de Automação no Guia do usuário do AWS Systems Manager .

> **Important**
>
> Analise os detalhes essenciais a seguir sobre como criar o runbook deste tutorial:
>
> - O runbook é destinado a um incidente criado a partir de uma fonte de CloudWatch alarme. Se você usar esse runbook para outros tipos de incidentes, por exemplo, incidentes criados manualmente, o evento do cronograma na primeira etapa do runbook não será encontrado e o sistema retornará um erro.
> - O runbook exige que o CloudWatch alarme inclua uma dimensão chamada`InstanceId`. Os alarmes para métricas de instância do Amazon EC2 têm essa dimensão. Se você usar esse runbook com outras métricas (ou com outras fontes de incidentes, como

EventBridge), precisará alterar a `JsonDecode2` etapa para corresponder aos dados capturados em seu cenário.

- O runbook tenta corrigir o problema que acionou o alarme reiniciando a instância do Amazon EC2. Para um incidente real, talvez você não queira reiniciar a instância. Atualize o runbook com as ações de remediação específicas que deseja que o sistema execute.

Para obter mais informações sobre a criação de runbooks, consulte Trabalhar com runbooks no Guia do usuário do AWS Systems Manager .

Para criar um runbook personalizado

1. Abra o AWS Systems Manager console em https://console.aws.amazon.com/systems-manager/.
2. No painel de navegação, escolha Documents.
3. Escolha Automação.
4. Em Name, insira um nome descritivo para o runbook, como **`IncidentResponseRunbook`**.
5. Escolha a guia Editor e depois escolha Edit (Editar).
6. Cole o seguinte conteúdo no 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. Escolha Criar automação.

Tarefa 2: Criar um perfil do IAM

Use o tutorial a seguir para criar uma função AWS Identity and Access Management (IAM) que dê permissão ao Incident Manager para iniciar um runbook especificado em um plano de resposta. O runbook deste tutorial reinicia uma instância do Amazon EC2. Você especificará esse perfil do IAM na próxima tarefa ao conectar o runbook ao seu plano de resposta.

Crie um perfil do IAM que inicie um runbook a partir de um plano de resposta

1. Abra o console do IAM em https://console.aws.amazon.com/iam/.
2. No painel de navegação, escolha Roles e Create role.
3. Verifique se o serviço da AWS está selecionado em Tipo de entidade confiável.
4. Em Caso de uso, no campo Casos de uso para outros serviços da AWS , insira **`Incident Manager`**.
5. Escolha Incident Manager e, em seguida, Next.
6. Na página Adicionar permissões, escolha Criar política. O editor de permissões abrirá em uma nova janela ou guia do navegador.

7. No editor de política, escolha a guia JSON.
8. Copie e cole o seguinte JSON na janela do editor de política de permissões. Substitua *account_ID* pelo seu Conta da AWS ID.

```
{
    "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. Escolha Próximo: etiquetas.
10. (Opcional) Se necessário, marque a sua política.
11. Selecione Next: Review (Próximo: revisar).
12. No campo Nome, insira um nome que o ajude a identificar esse perfil como sendo usado neste tutorial.
13. (Opcional) No campo Description, insira uma descrição.
14. Escolha Criar política.
15. Navegue de volta até a janela ou guia do navegador para o perfil que você está criando. A página Adicionar permissões é exibida.
16. Escolha o botão de atualização (localizado ao lado do botão Criar política) e, em seguida, insira o nome da política de permissões que você criou na caixa de filtro.
17. Escolha o grupo de mídias que você criou e, em seguida, escolha Next.
18. Na página Nomear, revisar e criar em Nome do perfil, insira um nome que o ajude a identificar esse perfil como sendo usado neste tutorial.
19. (Opcional) No campo Description, insira uma descrição.
20. Revise os detalhes do perfil, marque, se necessário, e escolha Criar perfil.

Tarefa 3: Conectar o runbook ao seu plano de resposta

Ao conectar o runbook ao seu plano de resposta do Incident Manager, você garante um processo de mitigação consistente, repetível e oportuno. O runbook também serve como ponto de partida para os resolvedores determinarem seu próximo curso de ação.

Para atribuir o runbook ao seu plano de resposta

1. Abra o console do Incident Manager.
2. Escolha os Planos de resposta.
3. Em Plano de resposta, escolha um plano de resposta existente e escolha Editar. Se não tiver um plano de resposta existente, escolha Criar plano de resposta para criar um novo plano.

   Preencha os seguintes campos:

   a. Na seção Runbook, escolha Selecionar runbook existente.

   b. Em Proprietário, verifique se a opção De minha propriedade está selecionada.
   c. Para Runbook, escolha o runbook que você criou em Tarefa 1: Criar o runbook.
   d. Em Versão, escolha Padrão no momento da execução.
   e. Na seção Entradas, para o parâmetro IncidentRecordArn, escolha ARN do incidente.
   f. Na seção Permissões de execução, escolha o perfil do IAM criado em Tarefa 2: Criar um perfil do IAM.
4. Salve as alterações.

Tarefa 4: Atribuir um CloudWatch alarme ao seu plano de resposta

Use o procedimento a seguir para atribuir um CloudWatch alarme para uma instância do Amazon EC2 ao seu plano de resposta.

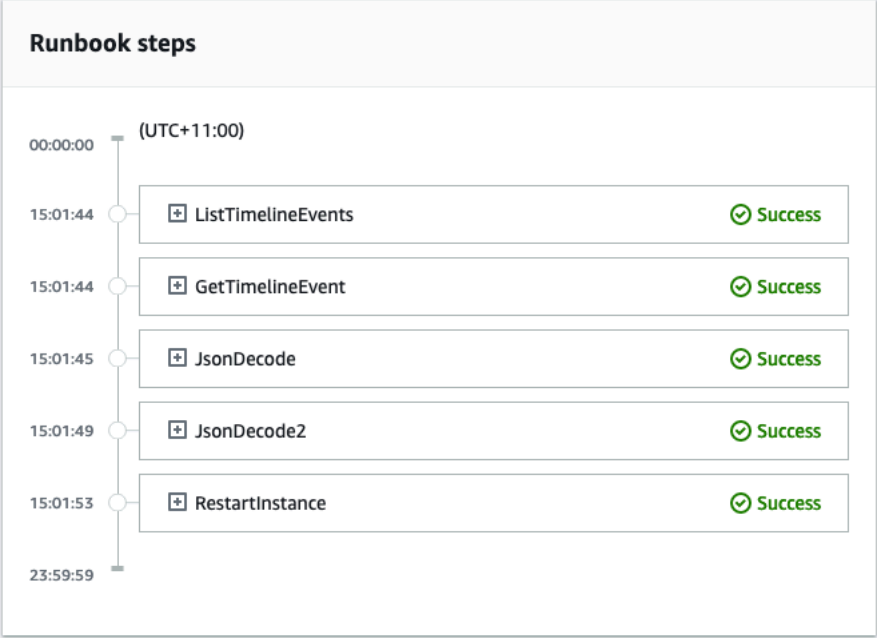
Para atribuir um CloudWatch alarme ao seu plano de resposta

1. Abra o CloudWatch console em https://console.aws.amazon.com/cloudwatch/.
2. No painel de navegação, escolha Alarmes, Todos os alarmes.
3. Escolha um alarme para uma instância do Amazon EC2 que deseja conectar ao plano de resposta.
4. Escolha Ações e, em seguida, escolha Editar. Verifique se a métrica tem uma dimensão chamada `InstanceId`.
5. Escolha Next.
6. Para Assistente de configuração de ações, escolha Adicionar ação do Systems Manager.
7. Escolha Criar incidente.
8. Escolha o plano de resposta criado em Tarefa 3: Conectar o runbook ao seu plano de resposta.
9. Escolha Create alarm (Criar alarme).

Tarefa 5: verificar os resultados

Para verificar se o CloudWatch alarme cria um incidente e, em seguida, processa o runbook especificado em seu plano de resposta, você deve acionar o alarme. Depois de acionar o alarme e o runbook concluir o processamento, você pode verificar os resultados do runbook usando o procedimento a seguir. Para obter informações sobre como acionar um alarme, consulte set-alarm-state na Referência de Comandos AWS CLI .

1. Abra o console do Incident Manager.
2. Escolha o incidente criado pelo CloudWatch alarme.
3. Escolha a guia Runbooks.
4. Veja as ações realizadas na sua instância do Amazon EC2 na seção Etapas do Runbook. A imagem a seguir é um exemplo que mostra as etapas executadas pelo runbook criado neste tutorial. Cada etapa é listada com um carimbo de data/hora e uma mensagem de status.



Para ver todos os detalhes no CloudWatch alarme, expanda a etapa JsonDecode2 e, em seguida, expanda Saída.

> **Important**
>
> Você deve limpar todas as alterações de recursos implementadas durante este tutorial que não deseje manter. Isso inclui alterações nos recursos do Incident Manager, como planos de recursos e incidentes, alterações CloudWatch nos alarmes e na função do IAM que você criou para este tutorial.

Gerenciar incidentes de segurança no Incident Manager

Você pode usar AWS Security Hub a Amazon EventBridge e o Incident Manager juntos para identificar e gerenciar incidentes de segurança em seus aplicativos AWS hospedados. Este tutorial

explica como configurar uma EventBridge regra que cria um incidente com base nas descobertas enviadas automaticamente pelo Security Hub.

> **Note**
>
> Este tutorial usa o EventBridge Security Hub. Você pode incorrer em custos com o uso desses serviços.

Pré-requisitos

- Configure o Security Hub. Para obter mais informações, consulte Configurar AWS Security Hub.
- Crie ou atualize descobertas no Security Hub. Para obter mais informações, consulte Descobertas no AWS Security Hub.
- Configure um plano de resposta que o Incident Manager usará como modelo ao criar seu incidente de segurança. Para ter mais informações, consulte Preparação para incidentes no Incident Manager.

Neste tutorial, usamos um padrão predefinido para criar a EventBridge regra. Para criar a regra usando um padrão personalizado, consulte Usando um padrão personalizado para criar a regra no guia do AWS Security Hub usuário.

Crie uma EventBridge regra

1. Abra o EventBridge console da Amazon em https://console.aws.amazon.com/events/.
2. No painel de navegação, escolha Regras.
3. Escolha Create rule.
4. Insira um Name (Nome) e uma Description (Descrição) para a regra.

   Uma regra não pode ter o mesmo nome que outra na mesma Região e barramento de eventos.
5. Em Event Bus (Barramento de eventos), escolha default (padrão).
6. Em Tipo de Regra, escolha Regra com Padrão de Evento.
7. Escolha Próximo.
8. Em Origem do evento, escolha AWS eventos ou eventos de EventBridge parceiros.
9. Em Padrão de evento, selecione Formulário de padrão de evento.
10. Em Fonte do evento, selecione Serviços da AWS .

11. Para o AWS serviço, selecione Security Hub.
12. Em Tipo de evento, escolha Security Hub Findings - Imported.
13. Por padrão, EventBridge configura o padrão do evento sem nenhum valor de filtro. Para cada atributo, a opção Qualquer ***nome de atributo*** é selecionada. Atualize esses filtros para criar incidentes com base nas descobertas de segurança que mais afetam seu ambiente.
14. Clique em Next.
15. Em Tipos de destino, escolha Serviço da AWS .
16. Em Selecionar um destino, escolha plano de resposta do Incident Manager.
17. Em Plano de resposta, escolha um plano de resposta para usar como modelo para os incidentes criados.
18. EventBridge pode criar a função do IAM necessária para que sua regra seja executada.
    - Para criar um perfil do IAM automaticamente, escolha Criar novo perfil para este recurso específico.
    - Para usar um perfil do IAM já existente, escolha Usar perfil existente.
19. (Opcional) Insira uma ou mais tags para a regra.
20. Selecione Next (Próximo).
21. Analise os detalhes da regra e selecione Criar regra.

Agora que você criou essa EventBridge regra, as descobertas de segurança que correspondem aos valores dos atributos que você definiu criarão incidentes no Incident Manager. Você pode fazer a triagem, gerenciar, monitorar e criar análises pós-incidentes a partir desses incidentes.

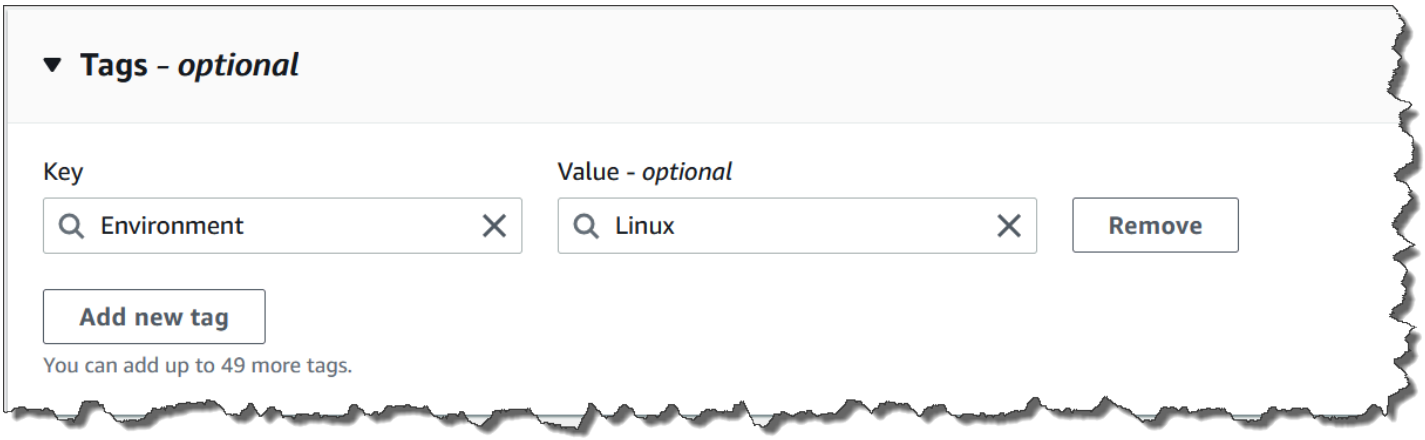
Marcando recursos no Incident Manager

As tags são metadados opcionais que você pode atribuir aos recursos do Incident Manager de acordo com o Regiões da AWS especificado no conjunto de replicação. Você pode atribuir tags a planos de resposta, registros de incidentes e contatos. Você também pode adicionar tags às agendas e rotações de plantão e ao próprio conjunto de replicação. As tags permitem categorizar os recursos e controlar o acesso a eles de maneiras diferentes. Cada tag consiste em uma chave e um valor opcional, ambos definidos por você. Recomendamos que você desenvolva um conjunto de chave de tags que atenda às suas necessidades para cada tipo de recurso. Usar um conjunto consistente de chaves de tags facilita o gerenciamento desses recursos e o acesso a eles. Você pode pesquisar e filtrar recursos com base nessas tags. Para obter mais informações sobre controlar o acesso aos recursos usando as tags, consulte Controlar o acesso a AWS recursos usando tags no Guia do usuário do IAM.

Você pode especificar tags na seção Incidente padrão ao criar um plano de resposta. Essas tags são aplicadas ao registro do incidente quando um incidente é criado usando o plano de resposta.

> **Note**
>
> As tags não têm significado semântico. Tags são interpretadas estritamente como sequências de caracteres.

Você pode adicionar ou remover tags usando o console do Incident Manager. A captura de tela a seguir mostra a seção de tags ao criar um novo plano de resposta.



Para trabalhar com tags de forma programática, use as seguintes ações de API:

- TagResource
- UntagResource
- ListTagsForResource

> **Important**
>
> As etiquetas aplicadas aos planos de resposta, registros de incidentes, contatos, agendas e rotações de plantão e conjuntos de replicação só podem ser visualizados e modificados na conta do proprietário do recurso.

Segurança em AWS Systems Manager Incident Manager

A segurança na nuvem AWS é a maior prioridade. Como AWS cliente, você se beneficia de data centers e arquiteturas de rede criados para atender aos requisitos das organizações mais sensíveis à segurança.

A segurança é uma responsabilidade compartilhada entre você AWS e você. O modelo de responsabilidade compartilhada descreve isso como segurança da nuvem e segurança na nuvem:

- Segurança da nuvem — AWS é responsável por proteger a infraestrutura que é executada Serviços da AWS no Nuvem AWS. AWS também fornece serviços que você pode usar com segurança. Auditores terceirizados testam e verificam regularmente a eficácia de nossa segurança como parte dos Programas de Conformidade Programas de AWS de . Para saber mais sobre os programas de conformidade aplicáveis AWS Systems Manager Incident Manager, consulte AWS Serviços no escopo do programa de conformidade AWS .
- Segurança na nuvem — Sua responsabilidade é determinada pelo AWS serviço que você usa. Você também é responsável por outros fatores, incluindo a confidencialidade de seus dados, os requisitos da empresa e as leis e regulamentos aplicáveis.

Esta documentação o ajuda a entender como aplicar o modelo de responsabilidade compartilhada ao usar o Incident Manager. Os tópicos a seguir mostram como configurar o Incident Manager para atender aos seus objetivos de segurança e conformidade. Você também aprenderá a usar outros Serviços da AWS que o ajudem a monitorar e proteger seus recursos do Incident Manager.

Tópicos

- Proteção de dados no Incident Manager
- Identity and Access Management para AWS Systems Manager Incident Manager
- Usar contatos compartilhados e planos de resposta no Incident Manager
- Validação de conformidade para AWS Systems Manager Incident Manager
- Resiliência em AWS Systems Manager Incident Manager
- Segurança da infraestrutura em AWS Systems Manager Incident Manager
- Trabalhando com endpoints VPC AWS Systems Manager Incident Manager e fazendo interface ()AWS PrivateLink
- Análise de configuração e vulnerabilidade no Incident Manager
- Melhores práticas de segurança em AWS Systems Manager Incident Manager

Proteção de dados no Incident Manager

O modelo de responsabilidade AWS compartilhada modelo se aplica à proteção de dados em AWS Systems Manager Incident Manager. Conforme descrito neste modelo, AWS é responsável por proteger a infraestrutura global que executa todos os Nuvem AWS. Você é responsável por manter o controle sobre seu conteúdo hospedado nessa infraestrutura. Você também é responsável pelas tarefas de configuração e gerenciamento de segurança dos Serviços da AWS que usa. Para obter mais informações sobre a privacidade de dados, consulte as Perguntas Frequentes sobre Privacidade de Dados.. Para obter mais informações sobre a proteção de dados na Europa, consulte a postagem do blog AWS LGPD e Modelo de Responsabilidade Compartilhada no AWS Blog de Segurança.

Para fins de proteção de dados, recomendamos que você proteja Conta da AWS as credenciais e configure usuários individuais com AWS IAM Identity Center ou AWS Identity and Access Management (IAM). Dessa maneira, cada usuário receberá apenas as permissões necessárias para cumprir suas obrigações de trabalho. Recomendamos também que você proteja seus dados das seguintes formas:

- Use uma autenticação multifator (MFA) com cada conta.
- Use SSL/TLS para se comunicar com os recursos. AWS Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Configure a API e o registro de atividades do usuário com AWS CloudTrail.
- Use soluções de AWS criptografia, juntamente com todos os controles de segurança padrão Serviços da AWS.
- Use serviços gerenciados de segurança avançada, como o Amazon Macie, que ajuda a localizar e proteger dados sigilosos armazenados no Amazon S3.
- Se você precisar de módulos criptográficos validados pelo FIPS 140-2 ao acessar AWS por meio de uma interface de linha de comando ou de uma API, use um endpoint FIPS. Para ter mais informações sobre endpoints do FIPS disponíveis, consulte Federal Information Processing Standard (FIPS) 140-2.

É altamente recomendável que nunca sejam colocadas informações de identificação confidenciais, como endereços de e-mail dos seus clientes, em marcações ou campos de formato livre, como um campo Nome. Isso inclui quando você trabalha com o Incident Manager ou outro Serviços da AWS usando o console, a API ou AWS os SDKs. AWS CLI Quaisquer dados inseridos em tags ou campos de texto de formato livre usados para nomes podem ser usados para logs de faturamento ou de

diagnóstico. Se você fornecer um URL para um servidor externo, recomendemos fortemente que não sejam incluídas informações de credenciais no URL para validar a solicitação a esse servidor.

Por padrão, o Incident Manager criptografa os dados em trânsito usando SSL/TLS.

Criptografia de dados

O Incident Manager usa as chaves AWS Key Management Service (AWS KMS) para criptografar seus recursos do Incident Manager. Para obter mais informações sobre AWS KMS, consulte o Guia do AWS KMS desenvolvedor. AWS KMS combina hardware e software seguros e de alta disponibilidade para fornecer um sistema de gerenciamento de chaves dimensionado para a nuvem. O Incident Manager criptografa seus dados usando a chave especificada e criptografa os metadados usando uma AWS chave própria. Para usar o Incident Manager, você deve configurar seu conjunto de replicação, o que inclui a configuração da criptografia. O Incident Manager requer criptografia de dados para uso.

Você pode usar uma chave AWS própria para criptografar seu conjunto de replicação ou pode usar sua própria chave gerenciada pelo cliente que você criou AWS KMS para criptografar as regiões em seu conjunto de replicação. O Incident Manager só oferece suporte a AWS KMS chaves de criptografia simétricas para criptografar seus dados criados nele. AWS KMS O Incident Manager não oferece suporte a AWS KMS chaves com material de chaves importadas, armazenamentos de chaves personalizados, Código de Autenticação de Mensagens (HMAC) baseado em Hash ou outros tipos de chaves. Se você usa chaves gerenciadas pelo cliente, usa o console AWS KMS ou as APIs AWS KMS para criar centralmente as chaves gerenciadas pelo cliente e definir as principais políticas que controlam como o Incident Manager pode usar as chaves gerenciadas pelo cliente. Quando você usa uma chave gerenciada pelo cliente para criptografia com o Incident Manager, a chave gerenciada pelo AWS KMS cliente deve estar na mesma região dos recursos. Para saber mais sobre como configurar a criptografia de dados no Incident Manager, consulte Assistente Prepare-se.

Há cobranças adicionais pelo uso de chaves gerenciadas pelo AWS KMS cliente. Para obter mais informações, consulte Conceitos de AWS KMS - Chaves KMS no Guia do desenvolvedor do AWS Key Management Service e Preços do AWS KMS.

> **Important**
>
> Se você usar uma chave gerenciada pelo cliente (CMK) para criptografar seu conjunto de replicação e os dados do Incident Manager, mas depois decidir excluir o conjunto de

replicação, certifique-se de excluir o conjunto de replicação antes de desativar ou excluir a CMK.

Para permitir que o Incident Manager use sua chave gerenciada pelo cliente para criptografar seus dados, você deve adicionar as seguintes declarações de política à política de chave da sua chave gerenciada pelo cliente. Para saber mais sobre como configurar e alterar a política de chave em sua conta, consulte Como usar políticas de chaves AWS KMS no Guia do desenvolvedor AWS Key Management Service . A política a seguir fornece essas permissões:

- Permite que o Incident Manager execute operações somente leitura para encontrar a CMK para o Incident Manager na sua conta.
- Permite que o Incident Manager use a CMK para criar concessões e descrever a chave, mas somente quando está atuando em nome de entidades principais na conta que tem permissão para usar o Incident Manager. Se as entidades principais especificadas na instrução da política não tiverem permissão para usar as chaves KMS e o Incident Manager, a chamada falhará, mesmo se vier do serviço do Incident Manager.

```
    {
    "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"
        ]
      }
    }
  }
```

Substitua o valor de `Principal` pela entidade principal do IAM que criou seu conjunto de replicação.

O Incident Manager usa um contexto de criptografia em todas as solicitações AWS KMS de operações criptográficas. Você pode usar esse contexto de criptografia para identificar eventos de CloudTrail log nos quais o Incident Manager usa suas chaves KMS. O Incident Manager usa o seguinte contexto de criptografia:

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

Identity and Access Management para AWS Systems Manager Incident Manager

AWS Identity and Access Management (IAM) é uma ferramenta AWS service (Serviço da AWS) que ajuda o administrador a controlar com segurança o acesso aos AWS recursos. Os administradores do IAM controlam quem pode ser autenticado (fazer login) e autorizado (ter permissões) para usar os atributos do Incident Manager. O IAM é um AWS service (Serviço da AWS) que você pode usar sem custo adicional.

Tópicos

- Público
- Autenticando com identidades
- Gerenciando acesso usando políticas
- Como AWS Systems Manager Incident Manager funciona com o IAM
- Exemplos de políticas baseadas em identidade para o AWS Systems Manager Incident Manager
- Exemplos de políticas baseadas em recursos para AWS Systems Manager Incident Manager
- Prevenção do problema do substituto confuso entre serviços do Incident Manager
- Usar perfis vinculados ao serviço do Incident Manager
- AWS políticas gerenciadas para AWS Systems Manager Incident Manager
- Solução de problemas AWS Systems Manager Incident Manager de identidade e acesso

Público

A forma como você usa o AWS Identity and Access Management (IAM) é diferente, dependendo do trabalho que você faz no Incident Manager.

Usuário do serviço: se você usa o serviço Incident Manager para fazer o trabalho, o administrador fornece as credenciais e as permissões necessárias. À medida que você usar mais atributos do Incident Manager para fazer seu trabalho, poderá precisar de permissões adicionais. Entender como o acesso é gerenciado pode ajudar você a solicitar as permissões corretas ao seu administrador. Se não for possível acessar um atributo no Incident Manager, consulte Solução de problemas AWS Systems Manager Incident Manager de identidade e acesso.

Administrador do serviço: se você for o responsável pelos atributos do Incident Manager na empresa, provavelmente terá acesso total ao Incident Manager. Cabe a você determinar quais funcionalidades e atributos do Incident Manager os usuários do serviço devem acessar. Assim, você deve enviar solicitações ao administrador do IAM para alterar as permissões dos usuários de seu serviço. Revise as informações nesta página para entender os Introdução ao IAM. Para saber mais sobre como a empresa pode usar o IAM com o Incident Manager, consulte Como AWS Systems Manager Incident Manager funciona com o IAM.

Administrador do IAM: se você for um administrador do IAM, talvez queira saber detalhes sobre como é possível criar políticas para gerenciar o acesso ao Incident Manager. Para visualizar exemplos de políticas baseadas em identidade do Incident Manager que podem ser usadas no IAM, consulte Exemplos de políticas baseadas em identidade para o AWS Systems Manager Incident Manager.

Autenticando com identidades

A autenticação é a forma como você faz login AWS usando suas credenciais de identidade. Você deve estar autenticado (conectado AWS) como o Usuário raiz da conta da AWS, como usuário do IAM ou assumindo uma função do IAM.

Você pode entrar AWS como uma identidade federada usando credenciais fornecidas por meio de uma fonte de identidade. AWS IAM Identity Center Usuários (IAM Identity Center), a autenticação de login único da sua empresa e suas credenciais do Google ou do Facebook são exemplos de identidades federadas. Quando você faz login como identidade federada, o administrador já configurou anteriormente a federação de identidades usando perfis do IAM. Ao acessar AWS usando a federação, você está assumindo indiretamente uma função.

Dependendo do tipo de usuário que você é, você pode entrar no AWS Management Console ou no portal de AWS acesso. Para obter mais informações sobre como fazer login em AWS, consulte Como fazer login Conta da AWS no Guia do Início de Sessão da AWS usuário.

Se você acessar AWS programaticamente, AWS fornece um kit de desenvolvimento de software (SDK) e uma interface de linha de comando (CLI) para assinar criptograficamente suas solicitações usando suas credenciais. Se você não usa AWS ferramentas, você mesmo deve assinar as solicitações. Para obter mais informações sobre como usar o método recomendado para assinar solicitações por conta própria, consulte Assinatura de solicitações de AWS API no Guia do usuário do IAM.

Independente do método de autenticação usado, também pode ser exigido que você forneça informações adicionais de segurança. Por exemplo, AWS recomenda que você use a autenticação multifator (MFA) para aumentar a segurança da sua conta. Para saber mais, consulte Autenticação multifator no Guia AWS IAM Identity Center do usuário e Utilizar a autenticação multifator (MFA) na AWS no Guia do usuário do IAM.

Conta da AWS usuário root

Ao criar uma Conta da AWS, você começa com uma identidade de login que tem acesso completo a todos Serviços da AWS os recursos da conta. Essa identidade é chamada de usuário Conta da AWS raiz e é acessada fazendo login com o endereço de e-mail e a senha que você usou para criar a conta. É altamente recomendável não usar o usuário raiz para tarefas diárias. Proteja as credenciais do usuário raiz e use-as para executar as tarefas que somente ele puder executar. Para obter a lista completa das tarefas que exigem login como usuário raiz, consulte Tarefas que exigem credenciais de usuário raiz no Guia do Usuário do IAM.

Identidade federada

Como prática recomendada, exija que usuários humanos, incluindo usuários que precisam de acesso de administrador, usem a federação com um provedor de identidade para acessar Serviços da AWS usando credenciais temporárias.

Uma identidade federada é um usuário do seu diretório de usuários corporativo, de um provedor de identidade da web AWS Directory Service, do diretório do Identity Center ou de qualquer usuário que acesse usando credenciais fornecidas Serviços da AWS por meio de uma fonte de identidade. Quando as identidades federadas são acessadas Contas da AWS, elas assumem funções, e as funções fornecem credenciais temporárias.

Para o gerenciamento de acesso centralizado, recomendamos usar o AWS IAM Identity Center. Você pode criar usuários e grupos no IAM Identity Center ou pode se conectar e sincronizar com um conjunto de usuários e grupos em sua própria fonte de identidade para uso em todos os seus Contas da AWS aplicativos. Para obter mais informações sobre o Centro de Identidade do IAM, consulte "O que é o Centro de Identidade do IAM?" no Guia do usuário AWS IAM Identity Center .

Usuários e grupos do IAM

Um usuário do IAM é uma identidade dentro da sua Conta da AWS que tem permissões específicas para uma única pessoa ou aplicativo. Sempre que possível, recomendamos contar com credenciais temporárias em vez de criar usuários do IAM com credenciais de longo prazo, como senhas e chaves de acesso. No entanto, se você tiver casos de uso específicos que exijam credenciais de longo prazo com usuários do IAM, recomendamos alternar as chaves de acesso. Para obter mais informações, consulte Alterne as chaves de acesso regularmente para casos de uso que exijam credenciais de longo prazo no Guia do Usuário do IAM.

Um grupo do IAM é uma identidade que especifica uma coleção de usuários do IAM. Não é possível fazer login como um grupo. É possível usar grupos para especificar permissões para vários usuários de uma vez. Os grupos facilitam o gerenciamento de permissões para grandes conjuntos de usuários. Por exemplo, você pode ter um grupo chamado IAMAdmins e conceder a esse grupo permissões para administrar recursos do IAM.

Usuários são diferentes de perfis. Um usuário é exclusivamente associado a uma pessoa ou a uma aplicação, mas um perfil pode ser assumido por qualquer pessoa que precisar dele. Os usuários têm credenciais permanentes de longo prazo, mas os perfis fornecem credenciais temporárias. Para saber mais, consulte Quando criar um usuário do IAM (em vez de um perfil) no Guia do usuário do IAM.

Perfis do IAM

Uma função do IAM é uma identidade dentro da sua Conta da AWS que tem permissões específicas. Ele é semelhante a um usuário do IAM, mas não está associado a uma pessoa específica. Você pode assumir temporariamente uma função do IAM no AWS Management Console trocando de funções. Você pode assumir uma função chamando uma operação de AWS API AWS CLI ou usando uma URL personalizada. Para obter mais informações sobre métodos para o uso de perfis, consulte Utilizar perfis do IAM no Guia do usuário do IAM.

Funções do IAM com credenciais temporárias são úteis nas seguintes situações:

- Acesso de usuário federado: para atribuir permissões a identidades federadas, você pode criar um perfil e definir permissões para ele. Quando uma identidade federada é autenticada, essa identidade é associada ao perfil e recebe as permissões definidas pelo mesmo. Para obter mais informações sobre perfis para federação, consulte Criar um perfil para um provedor de identidades de terceiros no Guia do Usuário do IAM. Se você usar o Centro de identidade do IAM, configure um conjunto de permissões. Para controlar o que suas identidades podem acessar após a autenticação, o Centro de identidade do IAM correlaciona o conjunto de permissões a um perfil no IAM. Para obter informações sobre conjuntos de permissões, consulte Conjuntos de permissões no Guia do usuário AWS IAM Identity Center .
- Permissões temporárias para usuários do IAM –- um usuário ou um perfil do IAM pode presumir um perfil do IAM para obter temporariamente permissões diferentes para uma tarefa específica.
- Acesso entre contas –- é possível usar um perfil do IAM para permitir que alguém (uma entidade principal confiável) em outra conta acesse recursos em sua conta. Os perfis são a principal forma de conceder acesso entre contas. No entanto, com alguns Serviços da AWS, você pode anexar uma política diretamente a um recurso (em vez de usar uma função como proxy). Para saber a diferença entre funções e políticas baseadas em recursos para acesso entre contas, consulte Acesso a recursos entre contas no IAM no Guia do usuário do IAM.
- Acesso entre serviços — Alguns Serviços da AWS usam recursos em outros Serviços da AWS. Por exemplo, quando você faz uma chamada em um serviço, é comum que esse serviço execute aplicativos no Amazon EC2 ou armazene objetos no Amazon S3. Um serviço pode fazer isso usando as permissões do principal de chamada, usando um perfil de serviço ou um perfil vinculado a serviço.
  - Sessões de acesso direto (FAS) — Quando você usa um usuário ou uma função do IAM para realizar ações AWS, você é considerado o principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O FAS usa as permissões do diretor chamando um AWS service (Serviço da AWS), combinadas com a solicitação AWS service (Serviço da AWS) para fazer solicitações aos serviços posteriores. As solicitações do FAS são feitas somente quando um serviço recebe uma solicitação que requer interações com outros Serviços da AWS ou com recursos para ser concluída. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte Encaminhar sessões de acesso.
  - Função de serviço: um perfil de serviço é um perfil do IAM que um serviço assume para realizar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para obter mais informações, consulte Criar um perfil para delegar permissões a um AWS service (Serviço da AWS) no Guia do Usuário do IAM.

- Função vinculada ao serviço — Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. AWS service (Serviço da AWS) O serviço pode presumir a função de executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não editar as permissões para funções vinculadas ao serviço.
- Aplicativos em execução no Amazon EC2 — Você pode usar uma função do IAM para gerenciar credenciais temporárias para aplicativos que estão sendo executados em uma instância do EC2 e fazendo AWS CLI solicitações de API. AWS É preferível fazer isso a armazenar chaves de acesso na instância do EC2. Para atribuir uma AWS função a uma instância do EC2 e disponibilizá-la para todos os seus aplicativos, você cria um perfil de instância anexado à instância. Um perfil de instância contém o perfil e permite que os programas em execução na instância do EC2 obtenham credenciais temporárias. Para mais informações, consulte Utilizar um perfil do IAM para conceder permissões a aplicações em execução nas instâncias do Amazon EC2 no Guia do usuário do IAM.

Para saber se deseja usar perfis do IAM, consulte Quando criar um perfil do IAM (em vez de um usuário) no Guia do usuário do IAM.

Gerenciando acesso usando políticas

Você controla o acesso AWS criando políticas e anexando-as a AWS identidades ou recursos. Uma política é um objeto AWS que, quando associada a uma identidade ou recurso, define suas permissões. AWS avalia essas políticas quando um principal (usuário, usuário raiz ou sessão de função) faz uma solicitação. As permissões nas políticas determinam se a solicitação será permitida ou negada. A maioria das políticas é armazenada AWS como documentos JSON. Para obter mais informações sobre a estrutura e o conteúdo de documentos de políticas JSON, consulte Visão geral das políticas JSON no Guia do Usuário do IAM.

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

Por padrão, usuários e funções não têm permissões. Para conceder aos usuários permissões para executar ações nos recursos que eles precisam, um administrador do IAM pode criar políticas do IAM. O administrador pode então adicionar as políticas do IAM aos perfis e os usuários podem presumir os perfis.

As políticas do IAM definem permissões para uma ação independente do método usado para executar a operação. Por exemplo, suponha que você tenha uma política que permite a ação

`iam:GetRole`. Um usuário com essa política pode obter informações de função da AWS Management Console AWS CLI, da ou da AWS API.

Políticas baseadas em identidade

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como usuário do IAM, grupo de usuários ou perfil. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte Criando políticas do IAM no Guia do Usuário do IAM.

As políticas baseadas em identidade podem ser categorizadas ainda adicionalmente como políticas em linha ou políticas gerenciadas. As políticas em linha são anexadas diretamente a um único usuário, grupo ou perfil. As políticas gerenciadas são políticas autônomas que você pode associar a vários usuários, grupos e funções em seu Conta da AWS. As políticas AWS gerenciadas incluem políticas gerenciadas e políticas gerenciadas pelo cliente. Para saber como escolher entre uma política gerenciada ou uma política em linha, consulte Escolher entre políticas gerenciadas e políticas em linha no Guia do Usuário do IAM.

Políticas baseadas em recursos

Políticas baseadas em recursos são documentos de políticas JSON que você anexa a um recurso. São exemplos de políticas baseadas em recursos as políticas de confiança de perfil do IAM e as políticas de bucket do Amazon S3. Em serviços que suportem políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o recurso ao qual a política está anexada, a política define quais ações um principal especificado pode executar nesse recurso e em que condições. Você deve especificar uma entidade principal em uma política baseada em recursos. Os diretores podem incluir contas, usuários, funções, usuários federados ou. Serviços da AWS

Políticas baseadas em recursos são políticas em linha localizadas nesse serviço. Você não pode usar políticas AWS gerenciadas do IAM em uma política baseada em recursos.

Listas de controle de acesso (ACLs)

As listas de controle de acesso (ACLs) controlam quais entidades principais (membros, usuários ou perfis da conta) têm permissões para acessar um recurso. As ACLs são semelhantes as políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

O Amazon S3 e o Amazon VPC são exemplos de serviços que oferecem suporte a ACLs. AWS WAF Para saber mais sobre ACLs, consulte Visão geral da lista de controle de acesso (ACL) no Guia do Desenvolvedor do Amazon Simple Storage Service.

Outros tipos de política

AWS oferece suporte a tipos de políticas adicionais menos comuns. Esses tipos de política podem definir o máximo de permissões concedidas a você pelos tipos de política mais comuns.

- Limites de permissões: um limite de permissões é um atributo avançado no qual você define o máximo de permissões que uma política baseada em identidade pode conceder a uma entidade do IAM (usuário ou perfil do IAM). É possível definir um limite de permissões para uma entidade. As permissões resultantes são a interseção das políticas baseadas em identidade de uma entidade com seus limites de permissões. As políticas baseadas em recurso que especificam o usuário ou o perfil no campo `Principal` não são limitadas pelo limite de permissões. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações sobre limites de permissões, consulte Limites de permissões para identidades do IAM no Guia do Usuário do IAM.
- Políticas de controle de serviço (SCPs) — SCPs são políticas JSON que especificam as permissões máximas para uma organização ou unidade organizacional (OU) em. AWS Organizations AWS Organizations é um serviço para agrupar e gerenciar centralmente vários Contas da AWS que sua empresa possui. Se você habilitar todos os atributos em uma organização, poderá aplicar políticas de controle de serviço (SCPs) a qualquer uma ou a todas as contas. O SCP limita as permissões para entidades nas contas dos membros, incluindo cada uma Usuário raiz da conta da AWS. Para obter mais informações sobre o Organizações e SCPs, consulte How SCPs work (Como os SCPs funcionam) no Guia do usuário do AWS Organizations .
- Políticas de sessão: são políticas avançadas que você transmite como um parâmetro quando cria de forma programática uma sessão temporária para um perfil ou um usuário federado. As permissões da sessão resultante são a interseção das políticas baseadas em identidade do usuário ou do perfil e das políticas de sessão. As permissões também podem ser provenientes de uma política baseada em atributo. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações, consulte Políticas de sessão no Guia do Usuário do IAM.

Vários tipos de política

Quando vários tipos de política são aplicáveis a uma solicitação, é mais complicado compreender as permissões resultantes. Para saber como AWS determinar se uma solicitação deve ser permitida quando vários tipos de políticas estão envolvidos, consulte Lógica de avaliação de políticas no Guia do usuário do IAM.

Como AWS Systems Manager Incident Manager funciona com o IAM

Antes de usar o IAM para gerenciar o acesso ao Incident Manager, saiba quais atributos do IAM estão disponíveis para uso com o Incident Manager.

Recursos do IAM que você pode usar com AWS Systems Manager Incident Manager

atributo do IAM	Suporte ao Incident Manager
Políticas baseadas em identidade	Sim
Políticas baseadas em atributos	Sim
Ações das políticas	Sim
Atributos de políticas	Sim
Chaves de condição de políticas	Não
ACLs	Não
ABAC (tags em políticas)	Não
Credenciais temporárias	Sim
Permissões de entidade principal	Sim
Perfis de serviço	Sim
Funções vinculadas a serviço	Sim

Para ter uma visão de alto nível de como o Incident Manager e outros AWS serviços funcionam com a maioria dos recursos do IAM, consulte AWS os serviços que funcionam com o IAM no Guia do usuário do IAM.

O Incident Manager não oferece suporte a políticas que negam acesso ao uso compartilhado de atributos AWS RAM.

Políticas baseadas em identidade para o Incident Manager

Suporta políticas baseadas em identidade	Sim

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como usuário, grupo de usuários ou perfil do IAM. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte Criando políticas do IAM no Guia do Usuário do IAM.

Com as políticas baseadas em identidade do IAM, é possível especificar ações ou recursos permitidos ou negados, assim como as condições sob as quais as ações são permitidas ou negadas. Você não pode especificar a entidade principal em uma política baseada em identidade porque ela se aplica ao usuário ou perfil ao qual ela está anexada. Para saber mais sobre todos os elementos que podem ser usados em uma política JSON, consulte Referência de elementos da política JSON do IAM no Guia do Usuário do IAM.

Exemplos de políticas baseadas em identidade do Incident Manager

Para visualizar exemplos de políticas baseadas em identidade do Incident Manager, consulte Exemplos de políticas baseadas em identidade para o AWS Systems Manager Incident Manager.

Políticas baseadas em atributos no Incident Manager

É compatível com políticas baseadas em atributos	Sim

Políticas baseadas em recursos são documentos de políticas JSON que você anexa a um recurso. São exemplos de políticas baseadas em recursos as políticas de confiança de perfil do IAM e as políticas de bucket do Amazon S3. Em serviços que suportem políticas baseadas em recursos, os

administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o recurso ao qual a política está anexada, a política define quais ações um principal especificado pode executar nesse recurso e em que condições. Você deve especificar uma entidade principal em uma política baseada em recursos. Os diretores podem incluir contas, usuários, funções, usuários federados ou. Serviços da AWS

Para permitir o acesso entre contas, você pode especificar uma conta inteira ou as entidades do IAM em outra conta como a entidade principal em uma política baseada em atributo. Adicionar uma entidade principal entre contas à política baseada em recurso é apenas metade da tarefa de estabelecimento da relação de confiança. Quando o principal e o recurso são diferentes Contas da AWS, um administrador do IAM na conta confiável também deve conceder permissão à entidade principal (usuário ou função) para acessar o recurso. Eles concedem permissão ao anexar uma política baseada em identidade para a entidade. No entanto, se uma política baseada em recurso conceder acesso a uma entidade principal na mesma conta, nenhuma política baseada em identidade adicional será necessária. Para obter mais informações, consulte Acesso a recursos entre contas no IAM no Guia do usuário do IAM.

O serviço Incident Manager suporta somente dois tipos de políticas baseadas em recursos chamadas usando o AWS RAM console ou a PutResourcePolicy ação, que é anexada a um plano de resposta ou contato. Essa política define quais entidades principais podem realizar ações nos planos de resposta, contatos, planos de escalação e incidentes. O Incident Manager usa políticas baseadas em atributos para compartilhar atributos entre contas.

O Incident Manager não oferece suporte a políticas que negam acesso ao uso compartilhado de atributos AWS RAM.

Para saber como anexar uma política baseada em atributos a um plano de reposta ou a um contato, consulte Incident management entre regiões e entre contas no Incident Manager.

Exemplos de políticas baseadas em atributos no Incident Manager

Para visualizar exemplos de políticas baseadas em atributos do Incident Manager, consulte Exemplos de políticas baseadas em recursos para AWS Systems Manager Incident Manager.

Ações da políticas do Incident Manager

Oferece compatibilidade com ações de políticas	Sim

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos, e em que condições.

O elemento `Action` de uma política JSON descreve as ações que você pode usar para permitir ou negar acesso em uma política. As ações de política geralmente têm o mesmo nome da operação de AWS API associada. Existem algumas exceções, como ações somente de permissão, que não têm uma operação de API correspondente. Algumas operações também exigem várias ações em uma política. Essas ações adicionais são chamadas de ações dependentes.

Incluem ações em uma política para conceder permissões para executar a operação associada.

Para ver uma lista das ações do Incident Manager, consulte Ações definidas pelo AWS Systems Manager Incident Manager na Referência de autorização do serviço.

As ações de política no Incident Manager usam os seguintes prefixos antes da ação:

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

Para especificar várias ações em uma única declaração, separe-as por vírgulas.

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

Você também pode especificar várias ações usando caracteres-curinga (*). Por exemplo, para especificar todas as ações que começam com a palavra `Get`, inclua a seguinte ação:

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

Para visualizar exemplos de políticas baseadas em identidade do Incident Manager, consulte Exemplos de políticas baseadas em identidade para o AWS Systems Manager Incident Manager.

O Incident Manager usa ações em dois namespace, ssm-incidents e ssm-contacts diferentes. Ao criar políticas para o Incident Manager, certifique-se de usar o namespace correto para a ação. O SSM-incidents é usado para planos de resposta e ações relacionadas a incidentes. O SSM-Contacts é usado para ações relacionadas a contatos e engajamento de contatos. Por exemplo: .

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

atributos de política para o Incident Manager

Oferece compatibilidade com recursos de políticas	Sim

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos, e em que condições.

O elemento de política JSON `Resource` especifica o objeto ou os objetos aos quais a ação se aplica. As instruções devem incluir um elemento `Resource` ou `NotResource`. Como prática recomendada, especifique um recurso usando seu nome do recurso da Amazon (ARN). Isso pode ser feito para ações que oferecem compatibilidade com um tipo de recurso específico, conhecido como permissões em nível de recurso.

Para ações que não oferecem suporte a permissões em nível de atributo, como operações de listagem, use um curinga (*) para indicar que a instrução se aplica a todos os atributos.

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

Para obter uma lista dos tipos de atributos do Incident Manager e seus ARNs, consulte atributos definidos pelo AWS Systems Manager Incident Manager na Referência de autorização do serviço. Para saber com quais ações é possível especificar o ARN de cada atributo, consulte Ações definidas pelo AWS Systems Manager Incident Manager.

Para visualizar exemplos de políticas baseadas em identidade do Incident Manager, consulte Exemplos de políticas baseadas em identidade para o AWS Systems Manager Incident Manager.

Os atributos do Incident Manager são usados para criar incidentes, colaborar em canais de bate-papo, resolver incidentes e engajar os respondentes. Se um usuário tiver acesso a um plano de resposta, ele terá acesso a todos os incidentes criados a partir dele. Se um usuário tiver acesso a um contato ou plano de escalação, ele poderá envolver o contato ou contatos no plano de escalação.

Chaves de condição de políticas para o Incident Manager

Suporta chaves de condição de política específicas de serviço	Não

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos, e em que condições.

O elemento `Condition` (ou bloco `Condition`) permite que você especifique condições nas quais uma instrução estiver em vigor. O elemento `Condition` é opcional. É possível criar expressões condicionais que usem agentes de condição, como “igual a” ou “menor que”, para fazer a condição da política corresponder aos valores na solicitação.

Se você especificar vários elementos `Condition` em uma instrução ou várias chaves em um único `Condition` elemento, a AWS os avaliará usando uma operação lógica `AND`. Se você especificar vários valores para uma única chave de condição, AWS avalia a condição usando uma `OR` operação lógica. Todas as condições devem ser atendidas antes que as permissões da instrução sejam concedidas.

Você também pode usar variáveis de espaço reservado ao especificar condições. Por exemplo, é possível conceder a um usuário do IAM permissão para acessar um atributo somente se ele estiver marcado com seu nome de usuário do IAM. Para obter mais informações, consulte Elementos da política do IAM: variáveis e tags no Guia do usuário do IAM.

AWS suporta chaves de condição globais e chaves de condição específicas do serviço. Para ver todas as chaves de condição AWS globais, consulte as chaves de contexto de condição AWS global no Guia do usuário do IAM.

Listas de controle de acesso (ACLs) no Incident Manager

Oferece compatibilidade com ACLs	Não

As listas de controle de acesso (ACLs) controlam quais entidades principais (membros, usuários ou perfis da conta) têm permissões para acessar um recurso. As ACLs são semelhantes as políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

Controle de acesso por atributo (ABAC) com o Incident Manager

Oferece compatibilidade com ABAC (tags em políticas)	Não

O controle de acesso por atributo (ABAC) é uma estratégia de autorização que define permissões com base em atributos. Em AWS, esses atributos são chamados de tags. Você pode anexar tags a entidades do IAM (usuários ou funções) e a vários AWS recursos. A marcação de entidades e atributos é a primeira etapa do ABAC. Em seguida, você cria políticas de ABAC para permitir operações quando a tag da entidade principal corresponder à tag do recurso que ela estiver tentando acessar.

O ABAC é útil em ambientes que estão crescendo rapidamente e ajuda em situações onde o gerenciamento de políticas se torna um problema.

Para controlar o acesso baseado em tags, forneça informações sobre as tags no elemento de condição de uma política usando as `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` ou chaves de condição `aws:TagKeys`.

Se um serviço oferecer suporte às três chaves de condição para cada tipo de recurso, o valor será Sim para o serviço. Se um serviço oferecer suporte às três chaves de condição somente para alguns tipos de recursos, o valor será Parcial

Para obter mais informações sobre o ABAC, consulte O que é ABAC? no Guia do Usuário do IAM. Para visualizar um tutorial com etapas para configurar o ABAC, consulte Utilizar controle de acesso baseado em atributos (ABAC) no Guia do usuário do IAM.

Usar credenciais temporárias com o Incident Manager

Oferece compatibilidade com credenciais temporárias	Sim

Alguns Serviços da AWS não funcionam quando você faz login usando credenciais temporárias. Para obter informações adicionais, incluindo quais Serviços da AWS funcionam com credenciais temporárias, consulte Serviços da AWS “Trabalhe com o IAM” no Guia do usuário do IAM.

Você está usando credenciais temporárias se fizer login AWS Management Console usando qualquer método, exceto um nome de usuário e senha. Por exemplo, quando você acessa AWS usando o link de login único (SSO) da sua empresa, esse processo cria automaticamente credenciais temporárias. Você também cria automaticamente credenciais temporárias quando faz login no console como usuário e, em seguida, alterna perfis. Para obter mais informações sobre como alternar funções, consulte Alternar para um perfil (console) no Guia do usuário do IAM.

Você pode criar manualmente credenciais temporárias usando a AWS API AWS CLI ou. Em seguida, você pode usar essas credenciais temporárias para acessar AWS. AWS recomenda que você gere credenciais temporárias dinamicamente em vez de usar chaves de acesso de longo prazo. Para mais informações, consulte Credenciais de segurança temporárias no IAM.

Permissões de entidade principal entre serviços para o Incident Manager

Suporte para o recurso Encaminhamento de sessões de acesso (FAS)	Sim

Quando você usa um usuário ou uma função do IAM para realizar ações em AWS, você é considerado um principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O FAS usa as permissões do diretor chamando um AWS service (Serviço da AWS), combinadas com a solicitação AWS service (Serviço da AWS) para fazer solicitações aos serviços posteriores. As solicitações do FAS são feitas somente quando um serviço recebe uma solicitação que requer interações com outros Serviços da AWS ou com recursos para ser concluída. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte Encaminhar sessões de acesso.

Perfis de serviço para o Incident Manager

Oferece compatibilidade com funções de serviço	Sim

O perfil de serviço é um perfil do IAM que um serviço assume para realizar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para obter mais informações, consulte Criar um perfil para delegar permissões a um AWS service (Serviço da AWS) no Guia do Usuário do IAM.

> **Warning**
>
> Alterar as permissões de um perfil de serviço pode prejudicar a funcionalidade do Incident Manager. Só edite os perfis de serviço quando o Incident Manager orientar você a fazê-lo.

Escolher um perfil do IAM no Incident Manager

Quando você cria um atributo de plano de resposta no Incident Manager, você deve escolher um perfil para permitir que o Incident Manager execute um documento de automação do Systems Manager em seu nome. Caso já tenha criado um perfil de serviço ou perfil vinculado ao serviço, o Incident Manager fornecerá uma lista dos perfis para sua escolha. É importante escolher um perfil que permita o acesso para executar suas instâncias de documentos de automação. Para ter mais informações, consulte Trabalho com runbooks do Automation do Systems Manager no Incident Manager. Ao criar um canal de AWS Chatbot bate-papo para ser usado durante um incidente, você pode selecionar uma função de serviço que permita usar comandos diretamente do chat. Para saber mais sobre como criar canais de bate-papo para colaboração em incidentes, consulte Trabalhando com canais de chat no Incident Manager. Para saber mais sobre as políticas do IAM em AWS Chatbot, consulte Gerenciamento de permissões para execução de comandos AWS Chatbot no Guia AWS Chatbot do administrador.

Perfis vinculados ao serviço do Incident Manager

Oferece suporte a perfis vinculados ao serviço	Sim

Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. AWS service (Serviço da AWS) O serviço pode presumir a função de executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não editar as permissões para funções vinculadas ao serviço.

Para obter informações sobre como criar ou gerenciar perfis vinculados ao serviço do Incident Manager, consulte Usar perfis vinculados ao serviço do Incident Manager.

Exemplos de políticas baseadas em identidade para o AWS Systems Manager Incident Manager

Por padrão, usuários e perfis não têm permissão para criar ou modificar atributos do Incident Manager. Eles também não podem realizar tarefas usando a AWS API AWS Management Console, AWS Command Line Interface (AWS CLI) ou. Para conceder aos usuários permissão para executar ações nos recursos de que precisam, um administrador do IAM pode criar políticas do IAM. O administrador pode então adicionar as políticas do IAM aos perfis e os usuários podem presumir os perfis.

Para saber como criar uma política baseada em identidade do IAM usando esses exemplos de documento de política JSON, consulte Criação de políticas do IAM no Guia do Usuário do IAM.

Para obter detalhes sobre ações e tipos de atributo definidos pelo Incident Manager, incluindo o formato dos ARNs para cada tipo de atributo, consulte Ações, atributos e chaves de condição do AWS Systems Manager Incident Manager na Referência de autorização do serviço.

Tópicos

- Melhores práticas de política
- Usar o console do Incident Manager
- Permitir que usuários visualizem suas próprias permissões
- Acessar um plano de resposta

Melhores práticas de política

As políticas baseadas em identidade determinam se alguém pode criar, acessar ou excluir atributos do Incident Manager em sua conta. Essas ações podem incorrer em custos para seus Conta da AWS. Ao criar ou editar políticas baseadas em identidade, siga estas diretrizes e recomendações:

- Comece com as políticas AWS gerenciadas e avance para as permissões de privilégios mínimos — Para começar a conceder permissões aos seus usuários e cargas de trabalho, use as políticas AWS gerenciadas que concedem permissões para muitos casos de uso comuns. Eles estão disponíveis no seu Conta da AWS. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo AWS cliente que sejam específicas para seus casos de uso. Para obter mais informações, consulte Políticas gerenciadas pela AWS ou Políticas gerenciadas pela AWS para funções de trabalho no Guia do Usuário do IAM.

- Aplique permissões de privilégio mínimo –- ao definir permissões com as políticas do IAM, conceda apenas as permissões necessárias para executar uma tarefa. Você faz isso definindo as ações que podem ser executadas em atributos específicos sob condições específicas, também conhecidas como permissões de privilégio mínimo. Para obter mais informações sobre como usar o IAM para aplicar permissões, consulte Políticas e permissões no IAM no Guia do Usuário do IAM.
- Use condições nas políticas do IAM para restringir ainda mais o acesso –- você pode adicionar uma condição às políticas para limitar o acesso a ações e recursos. Por exemplo, você pode gravar uma condição de política para especificar que todas as solicitações devem ser enviadas usando SSL. Você também pode usar condições para conceder acesso às ações de serviço se elas forem usadas por meio de uma ação específica AWS service (Serviço da AWS), como AWS CloudFormation. Para obter mais informações, consulte Elementos da política JSON do IAM: Condição no Guia do usuário do IAM.
- Use o IAM Access Analyzer para validar suas políticas do IAM a fim de garantir permissões seguras e funcionais –- o IAM Access Analyzer valida as políticas novas e existentes para que elas sigam a linguagem de política do IAM (JSON) e as práticas recomendadas do IAM. O IAM Access Analyzer oferece mais de 100 verificações de política e recomendações acionáveis para ajudá-lo a criar políticas seguras e funcionais. Para obter mais informações, consulte Validação de políticas do IAM Access Analyzer no Guia do Usuário do IAM.
- Exigir autenticação multifator (MFA) — Se você tiver um cenário que exija usuários do IAM ou um usuário root, ative Conta da AWS a MFA para obter segurança adicional. Para exigir MFA quando as operações de API forem chamadas, adicione condições de MFA às suas políticas. Para obter mais informações, consulte Configuração de acesso à API protegido por MFA no Guia do Usuário do IAM.

Para obter mais informações sobre as práticas recomendadas do IAM, consulte Práticas Recomendadas de Segurança no IAM no Guia do Usuário do IAM.

Usar o console do Incident Manager

Para acessar o AWS Systems Manager Incident Manager console, você deve ter um conjunto mínimo de permissões. Essas permissões devem autorizar você a listar e visualizar detalhes sobre os atributos do Incident Manager na sua Conta da AWS. Se você criar uma política baseada em identidade que seja mais restritiva do que as permissões mínimas necessárias, o console não funcionará como pretendido para entidades (usuários ou perfis) com essa política.

Você não precisa permitir permissões mínimas do console para usuários que estão fazendo chamadas somente para a API AWS CLI ou para a AWS API. Em vez disso, permita o acesso somente a ações que correspondam a operação de API que estiverem tentando executar.

Para garantir que usuários e funções possam resolver incidentes usando o console do Incident Manager, anexe também a política `IncidentManagerResolverAccess` AWS gerenciada do Incident Manager às entidades. Para obter mais informações, consulte Adicionando Permissões a um Usuário no Guia do Usuário do IAM.

```
IncidentManagerResolverAccess
```

Permitir que usuários visualizem suas próprias permissões

Este exemplo mostra como criar uma política que permita que os usuários do IAM visualizem as políticas gerenciadas e em linha anexadas a sua identidade de usuário. Essa política inclui permissões para concluir essa ação no console ou programaticamente usando a API AWS CLI ou 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": "*"
        }
    ]
}
```

Acessar um plano de resposta

Neste exemplo, você vai permitir que um usuário do IAM na sua conta da Amazon Web Services acesse um dos seus planos de respostas do Incident Manager, `exampleplan`. Você também deseja permitir que o usuário adicione, atualize e exclua o plano de resposta.

A política concede as permissões `ssm-incidents:ListResponsePlans`, `ssm-incidents:GetResponsePlan`, `ssm-incidents:UpdateResponsePlan`, e `ssm-incident:ListResponsePlan` ao usuário.

```
{
   "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/*"
      }
   ]
}
```

Exemplos de políticas baseadas em recursos para AWS Systems Manager Incident Manager

AWS Systems Manager Incident Manager suporta políticas de permissões baseadas em recursos para planos de resposta e contatos do Incident Manager.

O Incident Manager não oferece suporte a políticas baseadas em recursos que negam acesso aos recursos de uso compartilhado. AWS RAM

Para saber como criar um plano de resposta ou contato, consulte Como trabalhar com planos de resposta no Incident Manager e Como trabalhar com contatos do Incident Manager.

Restringir o acesso ao plano de resposta do Incident Manager por organização

O exemplo a seguir concede permissões aos usuários da organização com o ID da organização: `o-abc123def45` para responder a incidentes criados usando o plano `myplan` de resposta.

O `Condition` bloco usa as `StringEquals` condições e a chave de `aws:PrincipalOrgID` condição, que é uma chave de condição AWS Organizations específica. Para obter mais informações sobre essas chaves de condições, consulte Especificar condições em uma política.

```
{
  "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/*"
      ]
    }
  ]
}
```

Fornecer acesso de contato do Incident Manager a uma entidade principal

O exemplo a seguir concede permissão à entidade principal com o ARN `arn:aws:iam::999988887777:root` para criar compromissos com o contato `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/*"
            ]
```

```
        }
    ]
}
```

Prevenção do problema do substituto confuso entre serviços do Incident Manager

O problema do substituto confuso é um problema de segurança em que uma entidade que não tem permissão para executar uma ação chama uma entidade mais privilegiada a executar a ação. Isso pode permitir que agentes mal-intencionados executem comandos ou modifiquem recursos que, de outra forma, não teriam permissão para executar ou acessar.

Em AWS, a falsificação de identidade entre serviços pode levar a um cenário confuso de delegado. Personificação entre serviços é quando um serviço (o serviço de chamada) chama outro serviço (o serviço chamado). Um agente mal-intencionado pode usar o serviço de chamada para alterar atributos em outro serviço usando permissões que normalmente não teria.

AWS fornece aos diretores de serviços acesso gerenciado aos recursos em sua conta para ajudá-lo a proteger a segurança de seus recursos. Recomendamos usar`aws:SourceArn` e `aws:SourceAccount` as chaves de contexto de condição globais nas políticas de atributos. Essas chaves limitam as permissões que AWS Systems Manager Incident Manager concedem outro serviço a esse recurso. Se você utilizar ambas as chaves de contexto de condição global, o valor `aws:SourceAccount` e a conta referenciada no valor `aws:SourceArn` deverão utilizar o mesmo ID de conta quando utilizados na mesma instrução de política.

O valor de `aws:SourceArn` deve ser o ARN do registro do incidente afetado. Se você não souber o ARN completo do atributo ou estiver especificando vários atributos, use a chave de condição de contexto global `aws:SourceArn` com curingas (`*`) para as partes desconhecidas do ARN. Por exemplo, você pode usar o `aws:SourceArn` para `arn:aws:ssm-incidents::`*`111122223333`*`:*`.

No exemplo de política de confiança de perfil a seguir, você pode usar a chave de condição `aws:SourceArn` para restringir o acesso ao perfil de serviço com base no ARN do registro de incidente. Somente registros de incidentes criados com base no atributo do plano de resposta `myresponseplan` são capazes de usar esse perfil.

```
{
  "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/*"
      }
    }
  }
}
```

Usar perfis vinculados ao serviço do Incident Manager

AWS Systems Manager Incident Manager usa funções vinculadas ao serviço AWS Identity and Access Management (IAM). Um perfil vinculado ao serviço é um tipo exclusivo de perfil do IAM vinculado diretamente ao Incident Manager. As funções vinculadas ao serviço são predefinidas pelo Incident Manager e incluem todas as permissões que o serviço exige para chamar outros AWS serviços em seu nome.

Um perfil vinculado ao serviço facilita a configuração do Incident Manager porque você não precisa adicionar as permissões necessárias manualmente. O Incident Manager define as permissões dos perfis vinculados ao serviço e, exceto se definido de outra forma, somente o Incident Manager pode assumir suas perfis. As permissões definidas incluem a política de confiança e a política de permissões, e essa política não pode ser anexada a nenhuma outra entidade do IAM.

Um perfil vinculado ao serviço poderá ser excluído somente após excluir seus atributos relacionados. Isso protege seus atributos do Incident Manager, pois você não pode remover por engano as permissões para acessar os atributos.

Para obter informações sobre outros serviços compatíveis com perfis vinculados a serviços, consulte Serviços da AWS compatíveis com o IAM e procure os serviços que contenham Sim na coluna Service-Linked Role. Escolha um Sim com um link para visualizar a documentação do perfil vinculado a esse serviço.

Permissões dos perfis vinculados ao serviço do Incident Manager

O Incident Manager usa a função vinculada ao serviço chamada AWSServiceRoleforIncidentManager— permite que o Incident Manager gerencie os registros de incidentes do Incident Manager e os recursos relacionados em seu nome.

A função AWSServiceRoleforIncidentManager vinculada ao serviço confia nos seguintes serviços para assumir a função:

- `ssm-incidents.amazonaws.com`

A política de permissões do perfil `AWSIncidentManagerServiceRolePolicy` permite que o Incident Manager conclua as seguintes ações nos atributos especificados:

- Ação: `ssm-incidents:ListIncidentRecords` em todos os atributos relacionados à ação.
- Ação: `ssm-incidents:CreateTimelineEvent` em todos os atributos relacionados à ação.
- Ação: `ssm:CreateOpsItem` em todos os atributos relacionados à ação.
- Ação: `ssm:AssociateOpsItemRelatedItem` em `all resources related to the action.`
- Ação: `ssm-contacts:StartEngagement` em todos os atributos relacionados à ação.
- Ação: `cloudwatch:PutMetricData` nas CloudWatch métricas dentro do `AWS/IncidentManager` namespace

Você deve configurar permissões para que uma entidade do IAM (por exemplo, um usuário, grupo ou função) crie, edite ou exclua uma função vinculada a serviço. Para obter mais informações, consulte Permissões de perfil vinculado ao serviço no Guia do usuário do IAM.

Criar um perfil vinculado ao serviço no Incident Manager

Não é necessário criar manualmente uma função vinculada ao serviço. Quando você cria um conjunto de replicação na, na ou na AWS API AWS Management Console AWS CLI, o Incident Manager cria a função vinculada ao serviço para você.

Se excluir essa função vinculada ao serviço e precisar criá-la novamente, você poderá usar esse mesmo processo para recriar a função em sua conta. Quando você cria uma configuração de replicação, o Incident Manager cria o perfil vinculado ao serviço para você novamente.

Editar um perfil vinculado a serviço no Incident Manager

O Incident Manager não permite que você edite a função AWSServiceRoleforIncidentManager vinculada ao serviço. Depois que você criar um perfil vinculado ao serviço, não poderá alterar o nome do perfil, pois várias entidades podem fazer referência ao perfil. No entanto, você poderá editar

a descrição do perfil usando o IAM. Para obter mais informações, consulte Editar um perfil vinculado ao serviço no Guia do usuário do IAM.

Excluir um perfil vinculado ao serviço no Incident Manager

Se você não precisar mais usar um atributo ou serviço que requer um perfil vinculado ao serviço, é recomendável excluí-la. Dessa forma, você não terá uma entidade não utilizada que não seja monitorada ativamente ou mantida. No entanto, você deve limpar os atributos de seu perfil vinculado ao serviço antes de excluí-lo manualmente.

Para excluir o perfil vinculado ao serviço, você deve primeiro excluir o conjunto de replicação. A exclusão do conjunto de replicação exclui todos os dados criados e armazenados no Incident Manager, incluindo planos de resposta, contatos e planos de escalação. Você também perderá todos os incidentes criados anteriormente. Todos os alarmes e EventBridge regras que apontem para planos de resposta excluídos não criarão mais um incidente na combinação de alarmes ou regras. Para excluir o conjunto de replicação, você deve excluir todas as regiões do conjunto.

> **Note**
>
> Se o serviço Incident Manager estiver usando o perfil quando você tenta excluir os atributos, a exclusão poderá falhar. Se isso acontecer, espere alguns minutos e tente a operação novamente.

Para excluir as regiões no conjunto de replicação usado pelo AWSServiceRoleforIncidentManager

1. Abra o console do Incident Manager e escolha Configurações no painel de navegação à esquerda.
2. Selecione uma Região no Conjunto de replicação.
3. Escolha Excluir.
4. Para confirmar a exclusão da região, insira o nome da região e escolha Excluir.
5. Repita essas etapas até excluir todas as regiões do seu conjunto de replicação. Ao excluir a região final, o console informa que exclui o conjunto de replicação com ela.

Como excluir manualmente o perfil vinculado ao serviço usando o IAM

Use o console do IAM AWS CLI, o ou a AWS API para excluir a função AWSServiceRoleforIncidentManager vinculada ao serviço. Para obter mais informações, consulte Excluir um perfil vinculado ao serviço no Guia do usuário do IAM.

Regiões com suporte a perfis vinculados ao serviço do Incident Manager

O Incident Manager é compatível com perfis vinculados ao serviço em todas as regiões em que o serviço está disponível. Para mais informações, consulte Regiões e endpoints da AWS.

AWS políticas gerenciadas para AWS Systems Manager Incident Manager

Uma política AWS gerenciada é uma política autônoma criada e administrada por AWS. AWS as políticas gerenciadas são projetadas para fornecer permissões para muitos casos de uso comuns, para que você possa começar a atribuir permissões a usuários, grupos e funções.

Lembre-se de que as políticas AWS gerenciadas podem não conceder permissões de privilégio mínimo para seus casos de uso específicos porque estão disponíveis para uso de todos os AWS clientes. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo cliente da específicas para seus casos de uso.

Você não pode alterar as permissões definidas nas políticas AWS gerenciadas. Se AWS atualizar as permissões definidas em uma política AWS gerenciada, a atualização afetará todas as identidades principais (usuários, grupos e funções) às quais a política está anexada. AWS é mais provável que atualize uma política AWS gerenciada quando uma nova AWS service (Serviço da AWS) é lançada ou novas operações de API são disponibilizadas para serviços existentes.

Para obter mais informações, consulte Políticas gerenciadas pela AWS no Guia do usuário do IAM.

AWS política gerenciada: AWSIncidentManagerIncidentAccessServiceRolePolicy

Você pode anexar `AWSIncidentManagerIncidentAccessServiceRolePolicy` às entidades do IAM. O Incident Manager também atribui essa política a um perfil do Incident Manager que permite que o Incident Manager execute ações em seu nome.

Essa política concede permissões somente de leitura que permitem que o Incident Manager leia recursos em outros Serviços da AWS para identificar descobertas relacionadas a incidentes nesses serviços.

Detalhes das permissões

Esta política inclui as seguintes permissões:

- `cloudformation`— Permite que os diretores descrevam as AWS CloudFormation pilhas. Isso é necessário para que o Incident Manager identifique CloudFormation eventos e recursos relacionados a um incidente.
- `codedeploy`— Permite que os diretores leiam as AWS CodeDeploy implantações. Isso é necessário para que o Incident Manager identifique CodeDeploy implantações e alvos relacionados a um incidente.
- `autoscaling`— Permite que os diretores determinem se uma instância do Amazon Elastic Compute Cloud (EC2) faz parte de um grupo de Auto Scaling. Isso é necessário para que o Incident Manager possa fornecer descobertas para instâncias do EC2 que fazem parte dos grupos do 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": "*"
        }
    ]
}
```

Para visualizar mais detalhes sobre a política, inclusive a versão mais recente do documento de política JSON, consulte AWSIncidentManagerIncidentAccessServiceRolePolicy no AWS Managed Policy Reference Guide.

Política gerenciada da AWS : **`AWSIncidentManagerServiceRolePolicy`**

Não é possível anexar `AWSIncidentManagerServiceRolePolicy` às entidades do IAM. Essa política é anexada a um perfil vinculado ao serviço que permite que o Incident Manager realize ações em seu nome. Para ter mais informações, consulte Usar perfis vinculados ao serviço do Incident Manager.

Essa política concede ao Incident Manager permissões para listar incidentes, criar eventos de cronograma OpsItems, criar, associar itens relacionados OpsItems, iniciar engajamentos e publicar CloudWatch métricas relacionadas a um incidente.

Detalhes das permissões

Esta política inclui as seguintes permissões:

- `ssm-incidents`: permite que as entidades principais listem incidentes e criem eventos do cronograma. Isso é necessário para que os respondentes possam colaborar durante um incidente no painel de incidentes.
- `ssm`— Permite que os diretores criem OpsItems e associem itens relacionados. Isso é necessário para criar um pai OpsItem quando um incidente começa.
- `ssm-contacts`: permite que as entidades principais iniciem contratos. Isso é necessário para que o Incident Manager interaja com contatos durante um incidente.
- `cloudwatch`— Permite que os diretores publiquem CloudWatch métricas. Isso é necessário para que o Incident Manager publique métricas relacionadas a um incidente.

```
{
    "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"
                }
            }
        }
    ]
}
```

Para visualizar mais detalhes sobre a política, inclusive a versão mais recente do documento de política JSON, consulte AWSIncidentManagerServiceRolePolicy no AWS Managed Policy Reference Guide.

AWS política gerenciada: **`AWSIncidentManagerResolverAccess`**

Você pode conectar `AWSIncidentManagerResolverAccess` às suas entidades do IAM para permitir que elas iniciem, visualizem e atualizem incidentes. Você também pode usá-las para criar eventos do cronograma do cliente e itens relacionados no painel de incidentes. Você também pode anexar essa política à função de AWS Chatbot serviço ou diretamente à sua função gerenciada pelo cliente associada a qualquer canal de bate-papo usado para colaboração em incidentes. Para saber mais sobre as políticas do IAM em AWS Chatbot, consulte Gerenciamento de permissões para execução de comandos AWS Chatbot no Guia AWS Chatbot do administrador.

Detalhes das permissões

Esta política inclui as seguintes permissões:

- `ssm-incidents`: permite iniciar incidentes, listar planos de resposta, listar incidentes, atualizar incidentes, listar eventos de cronograma, criar eventos de cronograma personalizados, atualizar eventos de cronograma personalizados, excluir eventos de cronograma personalizados, listar itens relacionados, criar itens relacionados e atualizar itens relacionados.

```
{
    "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": "*"
        }
    ]
}
```

Para visualizar mais detalhes sobre a política, inclusive a versão mais recente do documento de política JSON, consulte AWSIncidentManagerResolverAccess no AWS Managed Policy Reference Guide.

Atualizações do Incident Manager nas políticas AWS gerenciadas

Veja detalhes sobre as atualizações das políticas AWS gerenciadas do Incident Manager desde que esse serviço começou a rastrear essas alterações. Para obter alertas automáticos sobre alterações feitas nesta página, inscreva-se no feed RSS na página de histórico de documentos do Incident Manager.

Alteração	Descrição	Data
AWSIncidentManagerIncidentAccessServiceRolePolicy — Atualização da política	O Incident Manager adicionou uma nova permissão `AWSIncidentManagerIncidentAccessServiceRolePolicy` , em apoio ao recurso Findings, que permite verificar se uma	20 de fevereiro de 2024

Alteração	Descrição	Data
	instância do EC2 faz parte de um grupo de Auto Scaling.	
`AWSIncidentManager IncidentAccessServ iceRolePolicy` – Nova política	O Incident Manager adicionou uma nova política que concede ao Incident Manager permissões para ligar para outras pessoas Serviços da AWS como parte do gerenciamento de um incidente.	17 de novembro de 2023
`AWSIncidentManager ServiceRolePolicy` — Atualização da política	O Incident Manager adicionou uma nova permissão que permite que o Incident Manager publique métricas em sua conta.	16 de dezembro de 2022
`AWSIncidentManager ResolverAccess` – Nova política	O Incident Manager adicionou uma nova política que permite iniciar incidentes, listar planos de resposta, listar incidentes, atualizar incidentes, listar eventos de cronograma, criar eventos de cronograma personali zados, atualizar eventos de cronograma personalizados, excluir eventos de cronogram a personalizados, listar itens relacionados, criar itens relacionados e atualizar itens relacionados.	26 de abril de 2021

Alteração	Descrição	Data
`AWSIncidentManager ServiceRolePolicy` – Nova política	O Incident Manager adicionou uma nova política para conceder ao Incident Manager permissões para listar incidentes, criar eventos de cronograma OpsItems, criar, associar OpsItems itens relacionados e iniciar compromissos relacionados a um incidente.	26 de abril de 2021
O Incident Manager começou a monitorar alterações	O Incident Manager começou a monitorar as mudanças em suas políticas AWS gerenciad as.	26 de abril de 2021

Solução de problemas AWS Systems Manager Incident Manager de identidade e acesso

Use as seguintes informações para ajudar a diagnosticar e corrigir problemas comuns que podem ser encontrados ao trabalhar com o Incident Manager e o IAM.

Tópicos

- Não tenho autorização para executar uma ação no Incident Manager
- Não estou autorizado a realizar iam: PassRole
- Quero permitir que pessoas fora da minha conta Amazon Web Services acessem meus atributos do Incident Manager

Não tenho autorização para executar uma ação no Incident Manager

Se você receber uma mensagem de erro informando que não tem autorização para executar uma ação, suas políticas deverão ser atualizadas para permitir que você realize a ação.

O erro do exemplo a seguir ocorre quando o usuário do IAM `mateojackson` tenta usar o console para visualizar detalhes sobre um atributo *`my-example-widget`* fictício, mas não tem as permissões `ssm-incidents:`*`GetWidget`* fictícias.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform: ssm-
incidents:GetWidget on resource: my-example-widget
```

Nesse caso, a política do usuário `mateojackson` deve ser atualizada para permitir o acesso ao recurso *`my-example-widget`* usando a ação `ssm-incidents:`*`GetWidget`*.

Se precisar de ajuda, entre em contato com seu AWS administrador. Seu administrador é a pessoa que forneceu suas credenciais de login.

Não estou autorizado a realizar iam: PassRole

Se você receber uma mensagem de erro informando que não tem autorização para executar a ação `iam:PassRole`, as suas políticas deverão ser atualizadas para permitir a passagem de um perfil para o Incident Manager.

Alguns Serviços da AWS permitem que você passe uma função existente para esse serviço em vez de criar uma nova função de serviço ou uma função vinculada ao serviço. Para fazer isso, é preciso ter permissões para passar o perfil para o serviço.

O erro de exemplo a seguir ocorre quando uma usuária do IAM chamada `marymajor` tenta usar o console para executar uma ação no Incident Manager. No entanto, a ação exige que o serviço tenha permissões concedidas por um perfil de serviço. Mary não tem permissões para passar o perfil para o serviço.

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

Nesse caso, as políticas de Mary devem ser atualizadas para permitir que ela realize a ação `iam:PassRole`.

Se precisar de ajuda, entre em contato com seu AWS administrador. Seu administrador é a pessoa que forneceu suas credenciais de login.

Quero permitir que pessoas fora da minha conta Amazon Web Services acessem meus atributos do Incident Manager

Você pode criar um perfil que os usuários de outras contas ou pessoas fora da sua organização podem usar para acessar seus atributos. Você pode especificar quem é confiável para assumir o perfil. Para serviços que oferecem compatibilidade com políticas baseadas em recursos ou listas de controle de acesso (ACLs), você pode usar essas políticas para conceder às pessoas acesso aos seus recursos.

Para saber mais, consulte:

- Para saber se o Incident Manager é compatível com esses atributos, consulte Como AWS Systems Manager Incident Manager funciona com o IAM.
- Para saber como fornecer acesso aos seus recursos em todos os Contas da AWS que você possui, consulte Como fornecer acesso a um usuário do IAM em outro Conta da AWS que você possui no Guia do usuário do IAM.
- Para saber como fornecer acesso aos seus recursos a terceiros Contas da AWS, consulte Como fornecer acesso Contas da AWS a terceiros no Guia do usuário do IAM.
- Para saber como conceder acesso por meio da federação de identidades, consulte Conceder acesso a usuários autenticados externamente (federação de identidades) no Guia do usuário do IAM.
- Para saber a diferença entre usar funções e políticas baseadas em recursos para acesso entre contas, consulte Acesso a recursos entre contas no IAM no Guia do usuário do IAM.

Usar contatos compartilhados e planos de resposta no Incident Manager

Com o compartilhamento de contatos, como proprietário do contato, você pode compartilhar informações de contato, planos de escalonamento e compromissos com outras pessoas Contas da AWS ou dentro de uma organização. AWS Você pode criar e gerenciar contatos e planos de escalação centralmente e garantir que outras pessoas possam contratar os contatos corretos durante um incidente.

Com o compartilhamento do plano de resposta, como proprietário do plano de resposta, você pode compartilhar um plano de resposta e os incidentes relacionados com outras pessoas Contas da AWS ou dentro de uma AWS organização. Você pode criar e gerenciar planos de resposta centralmente

para que os respondentes nas contas dos consumidores possam interagir com os incidentes à medida que eles acontecem.

O proprietário de um contato ou plano de resposta pode compartilhar contatos e planos de resposta com:

- Específico Contas da AWS dentro ou fora de sua organização em AWS Organizations
- Uma unidade organizacional dentro de sua organização em AWS Organizations
- Toda a sua organização em AWS Organizations

Conteúdo

- Pré-requisitos para compartilhar contatos e planos de resposta
- Serviços relacionados
- Compartilhar um plano de contato ou resposta
- Interromper um compartilhamento de um contato ou plano de resposta
- Identificar um contato ou um plano de resposta compartilhado
- Permissões compartilhadas de contatos e de planos de resposta
- Faturamento e medição
- Limites de instâncias

Pré-requisitos para compartilhar contatos e planos de resposta

Para compartilhar um plano de contato ou resposta com sua organização ou unidade organizacional em AWS Organizations:

- Você deve possuir o recurso em seu Conta da AWS. Não é possível compartilhar um contato ou plano de resposta que tenha sido compartilhado com você.
- Você deve habilitar o compartilhamento com AWS Organizations. Para obter mais informações, consulte Habilitar o compartilhamento com o AWS Organizations no Guia do usuário do AWS RAM .

Serviços relacionados

O compartilhamento do plano de contato e resposta se integra com AWS Resource Access Manager (AWS RAM). Com AWS RAM, você pode compartilhar seus AWS recursos com qualquer um

Conta da AWS ou por meio de AWS Organizations. Você compartilha atributos que possui criando um compartilhamento de atributos. Um compartilhamento de atributos especifica os atributos a serem compartilhados, e os consumidores com os quais compartilhá-los. Os consumidores podem ser indivíduos Contas da AWS, unidades organizacionais ou uma organização inteira em AWS Organizations.

Para obter mais informações sobre AWS RAM, consulte o Guia AWS RAM do usuário.

Compartilhar um plano de contato ou resposta

Depois de compartilhar um plano de resposta, os consumidores têm acesso a todos os incidentes passados, atuais e futuros criados usando esse plano de resposta.

Depois de compartilhar um contato, os consumidores têm acesso às informações de contato, ao plano de engajamento, aos planos de escalonamento e aos compromissos que ocorrem durante um incidente. Os consumidores também podem contratar um plano de contato ou escalação durante um incidente.

Se você faz parte de uma organização AWS Organizations e o compartilhamento dentro de sua organização está ativado, os consumidores em sua organização recebem automaticamente acesso ao contato compartilhado ou ao plano de resposta. Caso contrário, os consumidores receberão um convite para participar do compartilhamento de atributos e acesso ao contato compartilhado depois de aceitar o convite.

Você pode compartilhar um contato ou um plano de resposta de sua propriedade usando o AWS RAM console ou AWS CLI o.

Para compartilhar um contato ou plano de resposta que você possui usando o AWS RAM console

Consulte Criar um compartilhamento de atributos no Manual do usuário do AWS RAM .

Para compartilhar um plano de contato ou resposta de sua propriedade usando o AWS CLI

Use o comando create-resource-share.

Interromper um compartilhamento de um contato ou plano de resposta

Quando o proprietário de um atributo deixa de compartilhar um contato ou plano de resposta com um consumidor, os contatos, os planos de resposta, os planos de escalação, os engajamentos e os incidentes não aparecem mais no console do consumidor.

> **Note**
>
> O consumidor continua vendo os contatos, planos de resposta, planos de escalação, engajamentos ou incidentes sem atualizações, se estiver visualizando-os no console, até atualizar a página ou sair da página.

Para interromper o compartilhamento de um contato ou plano de resposta compartilhado de sua propriedade, remova-o do compartilhamento de atributos. Você pode fazer isso usando o AWS RAM console ou AWS CLI o.

Para interromper o compartilhamento de um contato ou plano de resposta de sua propriedade usando o console do AWS RAM

Consulte Atualização de um compartilhamento de atributos no Guia do usuário do AWS RAM .

Para interromper o compartilhamento de um contato ou plano de resposta de sua propriedade usando AWS CLI

Use o comando disassociate-resource-share.

Identificar um contato ou um plano de resposta compartilhado

Os proprietários e os consumidores podem identificar contatos e planos de resposta compartilhados usando o console do Incident Manager e a AWS CLI.

Para identificar um contato ou um plano de resposta compartilhado usando o console do Incident Manager

> **Note**
>
> Contatos, planos de resposta, planos de escalação, engajamentos e incidentes geralmente não são identificáveis como um atributo compartilhado no console do Incident Manager. Em locais onde o Nome do atributo da Amazon (ARN) está visível, o ARN contém o ID da conta do proprietário.

Para identificar um contato compartilhado ou um plano de resposta usando o AWS CLI

Use os ListResponsePlanos ou ListContactsos comandos. O comando retorna os contatos e os planos de resposta de sua propriedade e os contatos e planos de resposta compartilhados com você. O ARN mostra a Conta da AWS ID do contato ou do proprietário do plano de resposta.

Permissões compartilhadas de contatos e de planos de resposta

Permissões para proprietários

Os proprietários podem atualizar, visualizar, compartilhar, interromper o compartilhamento e usar contatos e planos de resposta. Os contatos e os planos de resposta incluem compromissos e incidentes relacionados.

Permissões para consumidores

Os consumidores podem usar e visualizar somente planos de resposta e contatos. Os contatos e os planos de resposta incluem compromissos e incidentes relacionados.

Faturamento e medição

O proprietário do atributo é cobrado pelo atributo. Os consumidores não são cobrados pelos atributos compartilhados com eles. Não há custos extras associados ao compartilhamento de um atributo.

Limites de instâncias

Compartilhar um atributo não afeta os limites do atributo na conta do proprietário ou do consumidor. Somente a conta do proprietário é usada para calcular os limites do atributo.

Validação de conformidade para AWS Systems Manager Incident Manager

Auditores terceirizados avaliam a segurança e a conformidade AWS Systems Manager Incident Manager como parte de vários programas de AWS conformidade. Isso inclui SOC, PCI, FedRAMP, HIPAA e outros.

Para saber se um AWS service (Serviço da AWS) está dentro do escopo de programas de conformidade específicos, consulte Serviços da AWS Escopo por Programa de Conformidade Serviços da AWS e escolha o programa de conformidade em que você está interessado. Para obter informações gerais, consulte Programas de AWS conformidade Programas AWS de .

Você pode baixar relatórios de auditoria de terceiros usando AWS Artifact. Para obter mais informações, consulte Baixar relatórios em AWS Artifact .

Sua responsabilidade de conformidade ao usar Serviços da AWS é determinada pela confidencialidade de seus dados, pelos objetivos de conformidade de sua empresa e pelas leis e regulamentações aplicáveis. AWS fornece os seguintes recursos para ajudar na conformidade:

- Guias de início rápido sobre segurança e conformidade — Esses guias de implantação discutem considerações arquitetônicas e fornecem etapas para a implantação de ambientes básicos AWS focados em segurança e conformidade.
- Arquitetura para segurança e conformidade com a HIPAA na Amazon Web Services — Este whitepaper descreve como as empresas podem usar AWS para criar aplicativos qualificados para a HIPAA.

> **Note**
>
> Nem todos Serviços da AWS são elegíveis para a HIPAA. Para mais informações, consulte a Referência dos serviços qualificados pela HIPAA.

- AWS Recursos de https://aws.amazon.com/compliance/resources/ de conformidade — Essa coleção de pastas de trabalho e guias pode ser aplicada ao seu setor e local.
- AWS Guias de conformidade do cliente — Entenda o modelo de responsabilidade compartilhada sob a ótica da conformidade. Os guias resumem as melhores práticas de proteção Serviços da AWS e mapeiam as diretrizes para controles de segurança em várias estruturas (incluindo o Instituto Nacional de Padrões e Tecnologia (NIST), o Conselho de Padrões de Segurança do Setor de Cartões de Pagamento (PCI) e a Organização Internacional de Padronização (ISO)).
- Avaliação de recursos com regras no Guia do AWS Config desenvolvedor — O AWS Config serviço avalia o quão bem suas configurações de recursos estão em conformidade com as práticas internas, as diretrizes e os regulamentos do setor.
- AWS Security Hub— Isso AWS service (Serviço da AWS) fornece uma visão abrangente do seu estado de segurança interno AWS. O Security Hub usa controles de segurança para avaliar os recursos da AWS e verificar a conformidade com os padrões e as práticas recomendadas do setor de segurança. Para obter uma lista dos serviços e controles aceitos, consulte a Referência de controles do Security Hub.
- Amazon GuardDuty — Isso AWS service (Serviço da AWS) detecta possíveis ameaças às suas cargas de trabalho Contas da AWS, contêineres e dados monitorando seu ambiente em busca de atividades suspeitas e maliciosas. GuardDuty pode ajudá-lo a atender a vários requisitos de

conformidade, como o PCI DSS, atendendo aos requisitos de detecção de intrusões exigidos por determinadas estruturas de conformidade.

- AWS Audit Manager— Isso AWS service (Serviço da AWS) ajuda você a auditar continuamente seu AWS uso para simplificar a forma como você gerencia o risco e a conformidade com as regulamentações e os padrões do setor.

Resiliência em AWS Systems Manager Incident Manager

A infraestrutura AWS global é construída em torno de AWS regiões e zonas de disponibilidade. AWS As regiões fornecem várias zonas de disponibilidade fisicamente separadas e isoladas, conectadas a redes de baixa latência, alta taxa de transferência e alta redundância. Com as zonas de disponibilidade, é possível projetar e operar aplicativos e bancos de dados que automaticamente executam o failover entre as zonas sem interrupção. As zonas de disponibilidade são altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de datacenters tradicionais.

Para obter mais informações sobre AWS regiões e zonas de disponibilidade, consulte Infraestrutura AWS global.

O Incident Manager é um serviço regional global e atualmente não oferece suporte às zonas de disponibilidade.

Além da infraestrutura AWS global, o Incident Manager oferece vários recursos para ajudar a suportar suas necessidades de resiliência e backup de dados. Durante o assistente de preparação, você deverá configurar um conjunto de replicação. Esse conjunto de replicação regional garante que seus dados e atributos sejam acessíveis de várias regiões, tornando o gerenciamento de incidentes em uma rede em nuvem mais gerenciável. Essa replicação também garante que seus dados estejam seguros e acessíveis no caso de uma de suas regiões cair.

Para obter mais informações sobre o conjunto de replicação do Incident Manager, consulte Como usar o conjunto de replicação do Incident Manager.

Segurança da infraestrutura em AWS Systems Manager Incident Manager

Como serviço gerenciado, AWS Systems Manager Incident Manager é protegido pela segurança de rede AWS global. Para obter informações sobre serviços AWS de segurança e como AWS proteger

a infraestrutura, consulte AWS Cloud Security. Para projetar seu AWS ambiente usando as melhores práticas de segurança de infraestrutura, consulte Proteção de infraestrutura no Security Pillar AWS Well-Architected Framework.

Você usa chamadas de API AWS publicadas para acessar o Incident Manager pela rede. Os clientes devem oferecer suporte para:

- Transport Layer Security (TLS). Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Conjuntos de criptografia com perfect forward secrecy (PFS) como DHE (Ephemeral Diffie-Hellman) ou ECDHE (Ephemeral Elliptic Curve Diffie-Hellman). A maioria dos sistemas modernos, como Java 7 e versões posteriores, comporta esses modos.

Além disso, as solicitações devem ser assinadas usando um ID da chave de acesso e uma chave de acesso secreta associada a uma entidade principal do IAM. Ou você pode usar o AWS Security Token Service (AWS STS) para gerar credenciais de segurança temporárias para assinar solicitações.

Trabalhando com endpoints VPC AWS Systems Manager Incident Manager e fazendo interface ()AWS PrivateLink

Você pode estabelecer uma conexão privada entre sua VPC e criar uma AWS Systems Manager Incident Manager interface VPC endpoint. Os endpoints de interface são desenvolvidos pelo AWS PrivateLink. Com AWS PrivateLink, você pode acessar de forma privada as operações da API do Incident Manager sem um gateway de internet, dispositivo NAT, conexão VPN ou AWS Direct Connect conexão. As instâncias na VPC não precisam de endereços IP públicos para a comunicação com as operações de API do Incident Manager. O tráfego entre sua VPC e o Incident Manager permanece na rede da Amazon.

Cada endpoint de interface é representado por uma ou mais Interfaces de Rede Elástica nas sub-redes.

Para obter mais informações, consulte Interface VPC endpoints (AWS PrivateLink) no Guia do usuário da Amazon VPC.

Considerações sobre os endpoints da VPC do Incident Manager

Antes de configurar um endpoint da VPC de interface para o Incident Manager, certifique-se de revisar as propriedades e limitações do endpoint de interface e cotas do AWS PrivateLink no Guia do usuário da Amazon VPC.

O Incident Manager é compatível com chamadas para todas as ações de API da sua VPC. Para usar todo o Incident Manager, você deve criar dois endpoints da VPC: um para `ssm-incidents` e outro para `ssm-contacts`.

Criação de um endpoint da VPC de interface para o Incident Manager

É possível criar um endpoint da VPC para o serviço do Incident Manager usando o console do Amazon VPC ou a AWS Command Line Interface (AWS CLI). Para mais informações, consulte Criar um endpoint de interface no Guia do usuário da Amazon VPC.

Crie um endpoint da VPC para o Incident Manager usando os seguintes nomes de serviço:

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

Se você habilitar o DNS privado para o endpoint, poderá fazer solicitações de API para o Incident Manager usando seu nome DNS padrão para a região. Por exemplo, você pode usar os nomes `ssm-incidents.us-east-1.amazonaws.com` ou `ssm-contacts.us-east-1.amazonaws.com`.

Para mais informações, consulte Acessar um serviço por um endpoint de interface no Guia do usuário da Amazon VPC.

Criar uma política de endpoint da VPC do Incident Manager

É possível anexar uma política de endpoint ao endpoint da VPC que controla o acesso ao Incident Manager. Essa política especifica as seguintes informações:

- A entidade principal que pode executar ações.
- As ações que podem ser executadas.
- Os atributos no quais as ações podem ser executadas.

Para obter mais informações, consulte Controlar o acesso a serviços com endpoints da VPC no Guia do usuário da Amazon VPC.

Exemplo: política de endpoints da VPC para ações do Incident Manager

Veja a seguir um exemplo de uma política de endpoint para o Incident Manager. Quando anexada a um endpoint, essa política concede acesso às ações listadas no Incident Manager para todas as entidades principais em todos os atributos.

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

Análise de configuração e vulnerabilidade no Incident Manager

A configuração e os controles de TI são uma responsabilidade compartilhada entre você AWS e você, nosso cliente. Para obter mais informações, consulte o modelo de responsabilidade AWS compartilhada.

Melhores práticas de segurança em AWS Systems Manager Incident Manager

AWS Systems Manager Incident Manager fornece muitos recursos de segurança a serem considerados ao desenvolver e implementar suas próprias políticas de segurança. As melhores práticas a seguir são diretrizes gerais e não representam uma solução completa de segurança. Como essas melhores práticas podem não ser adequadas ou suficientes para o seu ambiente, trate-as como considerações úteis em vez de prescrições.

Tópicos

- Práticas recomendadas de segurança preventiva no Incident Manager
- Práticas recomendadas de segurança preventiva no Incident Manager

Práticas recomendadas de segurança preventiva no Incident Manager

Implemente o acesso de privilégio mínimo

Ao conceder permissões, você decide quem receberá quais permissões para quais atributos do Incident Manager. Você habilita ações específicas que quer permitir nesses atributos. Portanto, você deve conceder apenas as permissões necessárias para executar uma tarefa. A implementação do acesso de privilégio mínimo é fundamental para reduzir o risco de segurança e o impacto que pode resultar de erros ou usuários mal-intencionados.

As ferramentas a seguir estão disponíveis para implementar o acesso de privilégio mínimo:

- Controle do acesso aos AWS recursos usando políticas e limites de permissões para entidades do IAM
- Políticas de controle de serviço

Criação e gerenciamento de contatos

Ao ativar os contatos, o Incident Manager entra em contato com o dispositivo para confirmar a ativação. Verifique se as informações do dispositivo estão corretas antes de ativá-lo. Isso reduz a possibilidade de o Incident Manager entrar em contato com o dispositivo ou a pessoa errada durante a ativação.

Revise regularmente seus contatos e planos de escalação para garantir que somente os contatos que precisam ser contatados durante um incidente sejam contatados. Revise regularmente os contatos para remover informações desatualizadas ou incorretas. Se um contato não precisar mais ser informado quando ocorrer um incidente, remova-o dos planos de escalação relacionados ou remova-o do Incident Manager.

Torne os canais de bate-papo privados

Você pode tornar seus canais de bate-papo sobre incidentes privados para implementar o acesso de privilégios mínimos. Considere usar um canal de bate-papo diferente com uma lista de usuários reduzida para cada modelo de plano de resposta. Isso garante que somente os respondentes corretos sejam direcionados para um canal de bate-papo que pode conter informações confidenciais.

AWS Chatbot os canais habilitados do Slack herdam as permissões da função do IAM usada para configurar. AWS Chatbot Isso permite que os respondentes em um canal AWS Chatbot habilitado do Slack chamem qualquer ação permitida, como APIs do Incident Manager e recuperação de gráficos de métricas.

Mantenha AWS as ferramentas atualizadas

AWS lança regularmente versões atualizadas de ferramentas e plug-ins que você pode usar em suas AWS operações. Manter esses atributos atualizados garante que os usuários e instâncias em sua conta tenham acesso às funcionalidades e atributos de segurança mais recentes nessas ferramentas.

- AWS CLI — O AWS Command Line Interface (AWS CLI) é uma ferramenta de código aberto que permite interagir com AWS serviços usando comandos em seu shell de linha de comando. Para atualizar a AWS CLI, execute o mesmo comando usado para instalar a AWS CLI. Recomendamos criar uma tarefa programada em sua máquina local para executar o comando adequado para o sistema operacional pelo menos uma vez a cada duas semanas. Para obter informações sobre os comandos de instalação, consulte Instalando a interface de linha de AWS comando no Guia do usuário da interface de linha de AWS comando.
- AWS Tools for Windows PowerShell — As Ferramentas para Windows PowerShell são um conjunto de PowerShell módulos que se baseiam na funcionalidade exposta pelo AWS SDK for .NET. As Ferramentas para Windows PowerShell permitem que você crie scripts de operações em seus AWS recursos a partir da linha de PowerShell comando. Periodicamente, à medida que as versões atualizadas das Ferramentas para Windows PowerShell são lançadas, você deve atualizar a versão que está sendo executada localmente. Para obter informações, consulte Atualizando o AWS Tools for Windows PowerShell no Windows ou Atualizando o AWS Tools for Windows PowerShell no Linux ou macOS.

Conteúdo relacionado

Práticas recomendadas de segurança para o Systems Manager

Práticas recomendadas de segurança preventiva no Incident Manager

Identificar e auditar todos os seus atributos do Incident Manager

A identificação de seus ativos de TI é um aspecto essencial de governança e segurança. Identifique todos os seus atributos do Systems Manager para avaliar sua postura de segurança e agir em possíveis áreas de pontos fracos. Crie grupos de atributos para seus atributos do Incident Manager. Para obter mais informações, consulte O que são grupos de atributos? no Guia do usuário do AWS Resource Groups .

Use AWS CloudTrail

AWS CloudTrail fornece um registro das ações realizadas por um usuário, função ou AWS serviço no Incident Manager. Usando as informações coletadas por AWS CloudTrail, você pode determinar a solicitação que foi feita ao Incident Manager, o endereço IP do qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita e detalhes adicionais. Para ter mais informações, consulte Log de chamadas de API do Incident Manager usando o AWS CloudTrail.

Monitore os avisos AWS de segurança

Verifique regularmente os avisos de segurança publicados Trusted Advisor para você. Conta da AWS Você pode fazer isso programaticamente usando describe-trusted-advisor-checks.

Além disso, monitore ativamente o endereço de e-mail principal registrado em cada um de seus Contas da AWS. AWS entraremos em contato com você, usando este endereço de e-mail, sobre problemas de segurança emergentes que possam afetá-lo.

AWS problemas operacionais com amplo impacto são publicados no AWS Service Health Dashboard. Eles também são publicados em contas individuais por meio do AWS Health Dashboard. Para obter mais informações, consulte a documentação do AWS Health.

Conteúdo relacionado

Amazon Web Services: visão geral do processo de segurança (whitepaper)

Introdução: siga as melhores práticas de segurança ao configurar seus AWS recursos (Blog AWS de segurança)

Práticas recomendadas do IAM

Melhores práticas de segurança em AWS CloudTrail

Registro e monitoramento no Incident Manager

O AWS Systems Manager Incident Manager se integra aos seguintes serviços que oferecem recursos de monitoramento e registro:

Métricas do CloudWatch

Use métricas do CloudWatch para recuperar estatísticas sobre pontos de dados para suas operações do AWS Systems Manager Incident Manager como um conjunto ordenado de dados de séries temporais, conhecido como métricas. Você pode usar essas métricas para verificar se o sistema está executando conforme o esperado. Para obter mais informações, consulte Métricas do Amazon CloudWatch no Incident Manager.

Logs do CloudTrail

Use o AWS CloudTrail para capturar informações detalhadas sobre as chamadas feitas para a API da AWS. Você pode armazenar essas chamadas como arquivos de log no Amazon Simple Storage Service. Você pode usar esses logs do CloudTrail para determinar quais chamadas foram feitas, o endereço IP de origem da chamada, quem fez a chamada e quando ela foi feita. Os logs do CloudTrail contêm informações sobre as chamadas para ações de API do Incident Manager. Para obter mais informações, consulte Log de chamadas de API do Incident Manager usando o AWS CloudTrail.

Trusted Advisor

O AWS Trusted Advisor pode ajudar a monitorar os recursos da AWS para melhorar a performance, a confiabilidade, a segurança e a economia. Quatro verificações do Trusted Advisor estão disponíveis a todos os usuários; mais de 50 verificações estão disponíveis para usuários com um plano de suporte Business ou Enterprise. No Incident Manager, o Trusted Advisor verifica se a configuração de um conjunto de replicação usa mais de uma Região da AWS para suportar o failover e a resposta regionais. Para obter mais informações, consulte AWS Trusted Advisor no Guia do usuário do AWS Support.

Métricas do Amazon CloudWatch no Incident Manager

O Incident Manager fornece métricas agregadas que você pode monitorar no Amazon CloudWatch. Use essas métricas para identificar tendências de incidentes e plano de resposta.

Dentre estas métricas:

- Número de incidentes criados em um determinado período de tempo
- O tempo para responder e resolver esses incidentes
- Número de incidentes resolvidos

Você pode monitorar as métricas do Incident Manager para entender melhor sua saúde operacional e tomar medidas significativas para impulsionar a excelência operacional da sua resposta a incidentes. As métricas do Incident Manager estão disponíveis em todas as regiões do Incident Manager. Suas métricas estarão disponíveis para visualização no Amazon CloudWatch para todas as regiões especificadas no conjunto de replicação ao integrar o Incident Manager. Você pode ver as métricas publicadas na região em que foram tomadas as ações para o incidente. Não há cobrança adicional por essas métricas.

No console do CloudWatch, você pode criar painéis com essas métricas para:

- Medir e analisar sua carga de incidentes existente
- Monitorar se a carga de incidentes está aumentando, diminuindo ou permanecendo a mesma
- Use o Incident Manager de forma mais eficaz para reduzir a frequência, a duração e o impacto dos incidentes

Esta página descreve as métricas do Incident Manager disponíveis no console do CloudWatch.

> **Important**
>
> Para um evento gerado pelo cliente, se o valor da fonte em `TriggerDetails` for nomeado usando caracteres não ASCII, as métricas do evento não serão relatadas nas métricas do Amazon CloudWatch, que não aceitam texto não ASCII. A `source` pode ser fornecida somente de forma programática; por exemplo, usando um SDK ou Amazon AWS CLI.

O Incident Manager envia as seguintes métricas ao CloudWatch.

Métrica	Descrição
`NumberOfCreateIncidents`	Número de incidentes criados.

Métrica	Descrição
	Dimensões válidas: [](dimensão vazia), [`ResponsePlan`], [`Impact`], [`Source`], [`ResponsePlan`, `Impact`], [`ResponsePlan`, `Source`] Unidade: Contagem
`NumberOfResolveIncidents`	Número de incidentes resolvidos. Dimensões válidas: [](dimensão vazia), [`ResponsePlan`], [`Impact`], [`Source`], [`ResponsePlan`, `Impact`], [`ResponsePlan`, `Source`] Unidade: Contagem
`TimeToFirstAcknowledgement`	Diferença horária entre a hora de criação do incidente e a hora em que o incidente foi confirmado pela primeira vez. Dimensões válidas: [](dimensão vazia), [`ResponsePlan`], [`Impact`], [`Source`], [`ResponsePlan`, `Impact`], [`ResponsePlan`, `Source`] Unidade: segundos
`TimeToResolveIncident`	Diferença de horário entre o momento da criação e o momento da resolução do incidente. Dimensões válidas: [](dimensão vazia), [`ResponsePlan`], [`Impact`], [`Source`], [`ResponsePlan`, `Impact`], [`ResponsePlan`, `Source`] Unidade: segundos

Como visualizar métricas do Incident Manager no console do CloudWatch

Para visualizar as métricas do Incident Manager no console do CloudWatch

1. Abra o console do CloudWatch em https://console.aws.amazon.com/cloudwatch/.

2. No painel de navegação, selecione Métricas.
3. Selecione o namespace `IncidentManager`.
4. Na guia Métricas, escolha uma dimensão e, em seguida, escolha uma métrica.

Para obter mais informações sobre como trabalhar com as métricas do CloudWatch, consulte os seguintes tópicos no Manual do usuário do Amazon CloudWatch:

- Métricas
- Usar métricas do Amazon CloudWatch

Dimensões para métricas

As métricas do Incident Manager usam o namespace `IncidentManager` e fornecem métricas para as seguintes dimensões:

Dimensão	Descrição
`By Response Plan`	Visualize métricas agregadas por plano de resposta.
`By Impact Level`	Visualize métricas agregadas por nível de severidade.
`By Source`	Visualize métricas de incidentes criados manualmente, criados por alarme do CloudWatch ou por evento do EventBridge.
`Across All Incidents`	Ver métricas agregadas de todos os incidentes na região AWS atual.
`Response Plan name and Source`	Ver métricas agregadas de cada combinação de plano de resposta e origem.
`Response Plan Name and Impact Level`	Ver métricas agregadas de cada combinação de plano de resposta e nível de severidade.

Log de chamadas de API do Incident Manager usando o AWS CloudTrail

O AWS Systems Manager Incident Manager é integrado ao AWS CloudTrail, serviço que fornece um registro de ações que foram executadas no Incident Manager por um usuário, um perfil ou um serviço da AWS . O CloudTrail captura todas as chamadas de API do Incident Manager como eventos. As chamadas capturadas incluem as chamadas do console do Incident Manager e as chamadas de código para as operações de API do Incident Manager. Se você criar uma trilha, poderá ativar a entrega contínua de eventos do CloudTrail para um bucket do Amazon S3, incluindo eventos para o Incident Manager. Se você não configurar uma trilha, ainda poderá visualizar os eventos mais recentes no console do CloudTrail em Event history (Histórico de eventos). Usando as informações coletadas pelo CloudTrail, é possível determinar a solicitação feita para o Incident Manager, o endereço IP do qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita, além de detalhes adicionais.

Para saber mais sobre o CloudTrail, consulte o Guia do usuário do AWS CloudTrail.

Informações sobre o Incident Manager no CloudTrail

O CloudTrail é habilitado em sua Conta da AWS quando ela é criada. Quando ocorre uma atividade no Incident Manager, ela é registrada em um evento do CloudTrail junto com outros eventos de serviços da AWS no Histórico de eventos. Você pode visualizar, pesquisar e baixar eventos recentes em sua Conta da AWS. Para obter mais informações, consulte Como visualizar eventos com o histórico de eventos do CloudTrail.

Para obter um registro de eventos em andamento na sua Conta da AWS, incluindo eventos do Incident Manager, crie uma trilha. Uma trilha permite que o CloudTrail entregue arquivos de log a um bucket do Amazon S3. Por padrão, quando você cria uma trilha no console, ela é aplicada a todas as regiões da AWS. A trilha registra em log eventos de todas as regiões na partição da AWS e entrega os arquivos de log para o bucket do Amazon S3 especificado por você. Além disso, é possível configurar outros serviços da AWS para analisar mais ainda e agir com base nos dados de eventos coletados nos logs do CloudTrail. Para obter mais informações, consulte:

- Visão geral da criação de uma trilha
- Serviços e integrações compatíveis com o CloudTrail
- Configurar notificações do Amazon SNS para o CloudTrail

- Receber arquivos de log do CloudTrail de várias regiões e Receber arquivos de log do CloudTrail de várias contas

O CloudTrail registra todas as ações do Incident Manager e o Incident Manager documenta as ações na Referência de API do AWS Systems Manager Incident Manager. Por exemplo, as chamadas para as APIs `CreateResponsePlan`, `ActivateDevice` e `StartIncident` geram entradas nos arquivos de log do CloudTrail.

Cada entrada de log ou evento contém informações sobre quem gerou a solicitação. As informações de identidade ajudam a determinar:

- Se a solicitação foi feita com credenciais de usuário raiz ou do usuário do IAM.
- Se a solicitação foi feita com credenciais de segurança temporárias de um perfil ou de um usuário federado.
- Se a solicitação foi feita por outro serviço da AWS.

Para obter mais informações, consulte Elemento de identidade do usuário do CloudTrail.

Noções básicas sobre as entradas do arquivo de log do Incident Manager

Uma trilha é uma configuração que permite a entrega de eventos como arquivos de log a um bucket do Amazon S3 especificado. Os arquivos de log do CloudTrail contêm uma ou mais entradas de log. Um evento representa uma única solicitação de qualquer fonte e inclui informações sobre a ação solicitada, a data e a hora da ação, os parâmetros de solicitação e assim por diante. Os arquivos de log do CloudTrail não são um rastreamento de pilha ordenada de chamadas de API pública. Dessa forma, eles não são exibidos em uma ordem específica.

O exemplo a seguir mostra uma entrada de log do CloudTrail que demonstra a ação `StartIncident`.

```
 {
"eventVersion": "1.08",
"userIdentity": {
    "type": "IAMUser",
    "principalId": "1234567890abcdef0",
    "arn": "arn:aws:iam::246873129580111122223333:user/nikki_wolf",
    "accountId": "abcdef01234567890",
    "accessKeyId": "021345abcdef6789",
    "userName": "nikki_wolf"
```

```
    },
    "eventTime": "2021-04-22T23:20:10Z",
    "eventSource": "gamma-ssm-incidents.amazonaws.com",
    "eventName": "StartIncident",
    "awsRegion": "us-west-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"
}
```

O exemplo a seguir mostra uma entrada de log do CloudTrail que demonstra a ação `DeleteContactChannel`.

```
    {
    "eventVersion":"1.08",
    "userIdentity":{
        "type":"IAMUser",
        "principalId":"1234567890abcdef0",
        "arn":"arn:aws:iam::246873129580111122223333:user/nikki_wolf",
        "accountId":"abcdef01234567890",
        "accessKeyId":"021345abcdef6789",
        "userName":"nikki_wolf"
    },
    "eventTime":"2021-04-08T02:27:21Z",
    "eventSource":"ssm-contacts.amazonaws.com",
    "eventName":"DeleteContactChannel",
    "awsRegion":"us-east-1",
```

```
    "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"
}
```

Integrações de produtos e serviços com o Incident Manager

O Incident Manager, um recurso do AWS Systems Manager, se integra aos seguintes produtos, serviços e ferramentas.

Integração com Serviços da AWS

O Incident Manager se integra Serviços da AWS às ferramentas descritas na tabela a seguir.

AWS CDK	AWS CDK É uma estrutura de desenvolv imento para usar código para definir sua infraestrutura de nuvem e usá-lo AWS CloudFormation para provisionamento. O AWS CDK suporta várias linguagens de programaç ão TypeScript, incluindo,, JavaScript PythonJav a, e C#/.Net. Para obter informações sobre como usar o AWS CDK com o Incident Manager, consulte as seções a seguir na Referência da AWS CDK API: • Módulo @aws-cdk/aws-ssmincidents • Módulo @aws-cdk/aws-ssmcontacts
AWS Chatbot	AWS Chatbotpermite que DevOps as equipes de desenvolvimento de software usem salas de bate-papo do programa de mensagens para monitorar e responder aos eventos operacion ais em suas Nuvem AWS. Usando AWS Chatbot o Incident Manager, você pode criar canais de bate-papo que os respondentes podem usar para monitorar e responder aos incidentes. AWS Chatbot s uporta salas de Slack bate-papo, Microsoft

	Teams canais e salas de bate-papo do Amazon Chime como canais de bate-papo. Ao criar um canal de chat, você também cria um tópico no Amazon Simple Notification Service (Amazon SNS). O Amazon SNS é um serviço gerenciado que fornece entrega de mensagens de publicadores para assinante s. Nos planos de resposta a incidentes, ao associar um canal de chat criado ao plano, você também escolhe um ou mais tópicos associados ao canal de chat. Esses tópicos do SNS são usados para enviar notificações sobre um incidente aos respondentes do incidente. Para ter mais informações, consulte Trabalhan do com canais de chat no Incident Manager.
AWS CloudFormation	AWS CloudFormation é um serviço que você pode usar para criar um modelo com todos os recursos necessários para seu aplicativ o e, em seguida, configurar e provisionar os recursos para você. Ele também configurará todas as dependências, para que você possa se concentrar mais no seu aplicativo e menos no gerenciamento de recursos. Para obter informações sobre como usar AWS CloudFormation com o Incident Manager, consulte os seguintes tópicos no Guia AWS CloudFormation do usuário: • Referência do tipo de recurso do Incident Manager • Referência de tipo de recurso de contatos, referência de tipo de recurso

Amazon CloudWatch	CloudWatchmonitora seus AWS recursos e os aplicativos em que você executa AWS em tempo real. Você pode usar CloudWatch para coletar e monitorar métricas, que são variáveis que você pode medir para seus recursos e aplicativos. Você pode configurar CloudWatch alarmes para criar incidentes no Gerenciador de incidentes. CloudWatch trabalha com o Systems Manager e o Incident Manager para criar um incidente a partir de um modelo de plano de resposta quando um alarme entra em estado de alarme. Para ter mais informações, consulte Como configurar criação automática de incidentes com alarmes do CloudWatch.
Amazon Chime	O Amazon Chime é um local de trabalho on-line que combina reuniões, chat e chamadas comerciais. O Amazon Chime permite conhecer, conversar e fazer chamadas de negócios dentro e fora da sua organização. Você pode integrar uma sala do Amazon Chime às suas operações do Incident Manager criando um canal de chat do Amazon Chime no AWS Chatbot e adicionando esse canal a um plano de resposta. Para ter mais informações, consulte Trabalhando com canais de chat no Incident Manager.

Amazon EventBridge	EventBridgeé um serviço sem servidor que usa eventos para conectar componentes do aplicativo, facilitando a criação de aplicativos escaláveis orientados por eventos. Você pode configurar EventBridge regras para observar padrões de eventos em seus AWS recursos e criar um incidente no Gerenciador de incidentes quando um evento corresponder a um padrão definido por você. Suas regras podem monitorar padrões de eventos em dezenas de aplicativos Serviços da AWS e serviços de terceiros. Para ter mais informações, consulte Criação automática de incidentes com eventos do EventBridge.
AWS Secrets Manager	O Secrets Manager ajuda você a gerenciar, recuperar e alternar credenciais do banco de dados, credenciais de aplicativo, tokens OAuth, chaves de API e outros segredos durante os ciclos de vida. Ao integrar o Incident Manager ao PagerDuty serviço, você cria um segredo no Secrets Manager que contém suas PagerDuty credenciais. Para ter mais informações, consulte Armazenando credenciais de PagerDuty acesso em segredo AWS Secrets Manager.

AWS Systems Manager	O Systems Manager é um hub de operações que você pode usar para visualizar e controlar sua infraestrutura de aplicativos e uma solução end-to-end de gerenciamento segura para ambientes em nuvem. Os seguintes recursos do Systems Manager se integram diretamente ao Incident Manager: • Automação: um runbook de automação define as ações que o Systems Manager realizará nos recursos da AWS . No Incident Manager, um runbook define uma série de etapas automatizadas e manuais para uso na resolução dos incidentes. Para obter informações sobre como criar runbooks de automação para uso no Incident Manager, consulte Trabalho com runbooks do Automation do Systems Manager no Incident Manager. • OpsCenter— OpsCenter fornece um local central onde engenheiros de operações e profissionais de TI podem gerenciar itens de trabalho operacionais, chamados de OpsItems, relacionados aos AWS recursos. Você pode criar OpsItems diretamente a partir de uma análise pós-incidente para acompanhar o trabalho relacionado. Para ter mais informações, consulte Como realizar uma análise pós-incidente no Incident Manager.

AWS Trusted Advisor	Trusted Advisoré uma ferramenta disponível para AWS clientes com um plano de suporte básico ou de desenvolvedor. Trusted Advisor inspeciona seu AWS ambiente e, em seguida, faz recomendações quando existem oportunid ades para economizar dinheiro, melhorar a disponibilidade e o desempenho do sistema ou ajudar a fechar lacunas de segurança. Para o Incident Manager, Trusted Advisor verifica se a configuração de um conjunto de replicação usa mais de um Região da AWS para suportar o failover e a resposta regionais.

Integração com outros produtos e serviços

Você pode integrar ou usar o Incident Manager com os serviços de terceiros descritos na tabela a seguir.

Jira Cloud	Usando o AWS Service Management Connector, você pode integrar o Incident Manager com o Jira Cloud (Atlassian), uma plataforma de fluxo de trabalho terceirizada baseada em nuvem. Depois de configurar a integração com o Jira Cloud, ao criar um novo incidente no Incident Manager, a integração também cria o incidente no Jira Cloud. Se você atualizar um incidente no Incident Manager, ele fará essas atualizações no incidente correspondente no Jira Cloud. Se você resolver um incidente no Incident Manager ou no Jira Cloud, a integraçã o resolverá o incidente nos dois serviços com base nas preferências configuradas.

	Para obter mais informações, consulte Integração AWS Systems Manager Incident Manager (Jira Cloud) no Guia do AWS Service Management Connector administrador.
Jira Service Management	Usando o AWS Service Management Connector, você pode integrar o Incident Manager com o Jira Service Management, uma plataforma de fluxo de trabalho terceirizada baseada em nuvem. Depois de configurar a integração com o Jira Service Management, ao criar um novo incidente no Incident Manager, a integraçã o também cria o incidente no Jira Service Management. Se você atualizar um incidente no Incident Manager, ele fará essas atualizaç ões no incidente correspondente no Jira Service Management. Se você resolver um incidente no Incident Manager ou no Jira Service Management, a integração resolverá o incidente nos dois serviços base nas preferênc ias configuradas. Para obter mais informações, consulte Configuri ng Jira Service Management no Guia do administrador do AWS Service Management Connector .

Microsoft Teams	O Microsoft Teams fornece ferramentas colaborativas baseadas em nuvem para mensagens em equipe, conferência de áudio e vídeo e compartilhamento de arquivos. Você pode integrar um canal do Microsoft Teams às suas operações do Incident Manager criando um canal de chat do Microsoft Team no AWS Chatbot, em seguida, adicionar esse canal a um plano de resposta. Para ter mais informações, consulte Trabalhando com canais de chat no Incident Manager.

PagerDuty	PagerDutyé uma ferramenta de resposta a incidentes que oferece suporte a fluxos de trabalho de paginação e políticas de escalonamento. Ao integrar o Incident Manager com PagerDuty, você pode adicionar um PagerDuty serviço ao seu plano de resposta. Depois disso, um incidente correspondente é criado PagerDuty sempre que um incidente é criado no Incident Manager. O incidente em PagerDuty usa o fluxo de trabalho de paginação e as políticas de escalonamento que você definiu lá, além das do Incident Manager. PagerDutyanexa eventos do cronograma do Incident Manager como notas sobre seu incidente. Para integrar o Incident Manager com PagerDuty, você deve primeiro criar um segredo AWS Secrets Manager que contenha suas PagerDuty credenciais. Para obter informações sobre como adicionar uma chave de API PagerDuty REST e outros detalhes necessários a um segredo em AWS Secrets Manager, consulteArmazenando credenciais de PagerDuty acesso em segredo AWS Secrets Manager. Para obter informações sobre como adicionar um PagerDuty serviço da sua PagerDuty conta a um plano de resposta no Gerenciador de incidentes, consulte as etapas para integrar um PagerDuty serviço ao plano de resposta no tópicoCriar um plano de resposta.

ServiceNow	Usando o AWS Service Management Connector, você pode integrar o Incident Manager com ServiceNowuma plataforma de fluxo de trabalho terceirizada baseada em nuvem. Depois de configurar a integração com ServiceNow, ao criar um novo incidente no Incident Manager, a integração ServiceNow também cria o incidente. Se você atualizar um incidente no Gerenciador de incidentes, ele fará essas atualizações no incidente correspon dente em ServiceNow. Se você resolver um incidente no Incident Manager ou ServiceNow, a integração resolverá o incidente em ambos os serviços com base nas preferências que você configura. Para obter mais informações, consulte Integração AWS Systems Manager Incident Manager ServiceNow no Guia do AWS Service Management Connector Administrador.
Slack	O Slack fornece ferramentas colaborativas baseadas em nuvem para mensagens em equipe, conferência de áudio e vídeo e compartilhamento de arquivos. Você pode integrar um canal do Slack às suas operações do Incident Manager criando um canal de chat do Slack no AWS Chatbot, em seguida, adicionar esse canal a um plano de resposta. Para ter mais informações, consulte Trabalhan do com canais de chat no Incident Manager.

Terraform	HashiCorp O Terraform é uma ferramenta de software de infraestrutura como código (IaC) de código aberto que fornece um fluxo de trabalho de interface de linha de comando (CLI) para gerenciar vários serviços em nuvem. No Incident Manager, você pode usar o Terraform para gerenciar ou provisionar o seguinte: Recursos de contatos do SSM Incident Manager • aws_ssmcontacts_contact • aws_ssmcontacts_contact_channel • aws_ssmcontacts_plan • aws_ssmcontacts_rotation Fontes de dados de contatos do SSM • aws_ssmcontacts_contact • aws_ssmcontacts_contact_channel • aws_ssmcontacts_plan • aws_ssmcontacts_rotation Recursos do SSM Incident Manager • aws_ssmincidents_replication_set • aws_ssmincidents_response_plan Fontes de dados do SSM Incident Manager • aws_ssmincidents_replication_set • aws_ssmincidents_response_plan

Armazenando credenciais de PagerDuty acesso em segredo AWS Secrets Manager

Depois de ativar a integração com um plano PagerDuty de resposta, o Incident Manager trabalha com PagerDuty ele das seguintes formas:

- O Incident Manager cria um incidente correspondente PagerDuty quando você cria um novo incidente no Incident Manager.
- O fluxo de trabalho de paginação e as políticas de escalonamento que você criou PagerDuty são usados no PagerDuty ambiente. No entanto, o Incident Manager não importa sua PagerDuty configuração.
- O Incident Manager publica eventos do cronograma como notas sobre o incidente em PagerDuty, até um máximo de 2.000 notas.
- Você pode optar por resolver PagerDuty incidentes automaticamente ao resolver o incidente relacionado no Gerenciador de incidentes.

Para integrar o Incident Manager com PagerDuty, você deve primeiro criar um segredo AWS Secrets Manager que contenha suas PagerDuty credenciais. Isso permite que o Incident Manager se comunique com seu PagerDuty serviço. Em seguida, você pode incluir um PagerDuty serviço nos planos de resposta criados no Incident Manager.

Esse segredo que você cria no Secrets Manager deve conter, no formato JSON adequado, o seguinte:

- Uma chave de API da sua PagerDuty conta. É possível usar uma chave de API REST de acesso geral ou uma chave de API REST de token de usuário.
- Um endereço de e-mail de usuário válido do seu PagerDuty subdomínio.
- A região PagerDuty de serviço em que você implantou seu subdomínio.

> **Note**
>
> Todos os serviços em um PagerDuty subdomínio são implantados na mesma região de serviço.

Pré-requisitos

Antes de criar o segredo no Secrets Manager, verifique se você atende aos seguintes requisitos.

Chave do KMS

Você deve criptografar o segredo criado com uma chave gerenciada pelo cliente que você criou em AWS Key Management Service (AWS KMS). Você especifica essa chave ao criar o segredo que armazena PagerDuty suas credenciais.

> **Important**
>
> O Secrets Manager oferece a opção de criptografar o segredo com um Chave gerenciada pela AWS, mas esse modo de criptografia não é suportado.

A chave gerenciada pelo cliente deve atender aos seguintes requisitos:

- Tipo de chave: escolha Simétrica.
- Uso da chave: escolha Criptografar e descriptografar.
- Regionalidade: se você quiser replicar seu plano de resposta para vários Regiões da AWS, certifique-se de selecionar a chave multirregional.

Política de chave

O usuário que está configurando o plano de resposta deve ter permissão para `kms:GenerateDataKey` e `kms:Decrypt` na política baseada em recursos da chave. O responsável pelo serviço `ssm-incidents.amazonaws.com` deve ter permissão para `kms:GenerateDataKey` e `kms:Decrypt` na política baseada em recursos da chave.

A política a seguir demonstra essas permissões. Substitua cada *`espaço reservado para entrada do usuário`* por suas próprias informações.

```
{
    "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": "*"
        }
    ]
}
```

Para obter mais informações sobre como criar uma chave gerenciada pelo cliente, consulte Criar chaves de criptografia simétrica do KMS no Guia do desenvolvedor do AWS Key Management Service . Para obter mais informações sobre AWS KMS chaves, consulte AWS KMS conceitos.

Se uma chave gerenciada pelo cliente existente atender a todos os requisitos anteriores, você poderá editar sua política para adicionar essas permissões. Para obter informações sobre como modificar uma política de chave, consulte Alterar uma política de chave no Guia do desenvolvedor do AWS Key Management Service .

> **Tip**
>
> Você pode especificar uma chave de condição para limitar ainda mais o acesso. Por exemplo, a política a seguir permite acesso por meio do Secrets Manager somente na região Leste dos EUA (Ohio) (us-east-2):

```
{
    "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"
        }
    }
}
```

Permissão do **`GetSecretValue`**

A identidade do IAM (usuário, função ou grupo) que cria o plano de resposta deve ter a permissão `secretsmanager:GetSecretValue` do IAM.

Para armazenar as credenciais de PagerDuty acesso em segredo AWS Secrets Manager

1. Siga as etapas da Etapa 3a em Criar um AWS Secrets Manager segredo no Guia do AWS Secrets Manager usuário.
2. Na Etapa 3b, para Pares de chave/valor, faça o seguinte:
   - Escolha a guia Texto simples.
   - Substitua o conteúdo padrão da caixa pela seguinte estrutura JSON:

```
{
    "pagerDutyToken": "pagerduty-token",
    "pagerDutyServiceRegion": "pagerduty-region",
    "pagerDutyFromEmail": "pagerduty-email"
```

```
}
```

- Na amostra JSON que você colou, substitua os *valores do espaço reservado* da seguinte forma:

  - *pagerduty-token*: o valor de uma chave de API REST de acesso geral ou de uma chave de API REST de token de usuário da sua conta. PagerDuty

    Para obter informações relacionadas, consulte Chaves de acesso à API na Base de PagerDuty Conhecimento.

  - *pagerduty-region: a região* de serviço do PagerDuty data center que hospeda seu subdomínio. PagerDuty

    Para obter informações relacionadas, consulte Regiões de serviço na Base de PagerDuty Conhecimento.

  - *pagerduty-email*: o endereço de e-mail válido de um usuário que pertence ao seu subdomínio. PagerDuty

    Para obter informações relacionadas, consulte Gerenciar usuários na Base de PagerDuty Conhecimento.

O exemplo a seguir mostra um segredo JSON completo contendo as PagerDuty credenciais necessárias:

```
{
    "pagerDutyToken": "y_NbAkKc66ryYEXAMPLE",
    "pagerDutyServiceRegion": "US",
    "pagerDutyFromEmail": "JohnDoe@example.com"
}
```

3. Na Etapa 3c, em Chave de criptografia, escolha uma chave gerenciada pelo cliente que você criou que atenda aos requisitos listados na seção anterior, Pré-requisitos.
4. Na Etapa 4c, em Permissões de recursos, faça o seguinte:
   - Expanda Permissões de recursos.
   - Escolha Editar permissões.
   - Substitua o conteúdo padrão da caixa de política pela seguinte estrutura JSON:

```
{
```

```
    "Effect": "Allow",
    "Principal": {
        "Service": "ssm-incidents.amazonaws.com"
    },
    "Action": "secretsmanager:GetSecretValue",
    "Resource": "*"
}
```

- Escolha Salvar.

5. Na Etapa 4d, em Replicar segredo, faça o seguinte se você tiver replicado seu plano de resposta para mais de uma Região da AWS:
   - Expanda Replicar segredo.
   - Na Região da AWS, selecione a região para a qual você replicou seu plano de resposta.
   - Em Chave de criptografia, escolha uma chave gerenciada pelo cliente que você criou ou replicou nessa região e que atenda aos requisitos listados na seção Pré-requisitos.
   - Para cada adicional Região da AWS, escolha Adicionar região e selecione o nome da região e a chave gerenciada pelo cliente.
6. Conclua as etapas restantes em Criar um AWS Secrets Manager segredo no Guia AWS Secrets Manager do usuário.

Para obter informações sobre como adicionar um PagerDuty serviço a um fluxo de trabalho de incidentes do Incident Manager, consulte Integrar um PagerDuty serviço ao plano de resposta no tópicoCriar um plano de resposta.

Informações relacionadas

Como automatizar a resposta a incidentes com PagerDuty e AWS Systems Manager Incident Manager (blog de Nuvem AWS operações e migrações)

Criptografia secreta no AWS Secrets Manager no Guia do usuário do AWS Secrets Manager

Solução de problemas do AWS Systems Manager Incident Manager

Se enfrentar problemas ao usar o AWS Systems Manager Incident Manager, você poderá usar as informações a seguir para resolvê-los de acordo com nossas práticas recomendadas. Se os problemas enfrentados estiverem fora do escopo das informações a seguir ou se eles persistem depois que você tiver tentado resolvê-los, entre em contato com AWS Support.

Tópicos

- A mensagem de erro: ValidationException – We were unable to validate the AWS Secrets Manager secret
- Outros casos de solução de problemas

A mensagem de erro: `ValidationException – We were unable to validate the AWS Secrets Manager secret`

Problema 1: a AWS Identity and Access Management identidade (IAM) (usuário, perfil ou grupo) que cria o plano de resposta não tem a `secretsmanager:GetSecretValue` permissão do IAM. As identidades do IAM devem ter essa permissão para validar os segredos do Secrets Manager.

- Solução: adicione a `secretsmanager:GetSecretValue` permissão ausente à política do IAM para a identidade do IAM que cria o plano de resposta. Para obter mais informações sobre como acrescentar uma política a uma entidade do IAM, consulte Adding IAM identity permissions (console) [Adicionar permissões de identidade do IAM (console)] ou Adding IAM policies [Adicionar política do IAM] (AWS CLI) no Guia do usuário do IAM.

Problema 2: o segredo não tem uma política baseada em recursos anexada que permita que a identidade do IAM execute a `GetSecretValue` ação, ou a política baseada em recursos nega permissão à identidade.

- Solução: crie ou adicione uma `Allow` declaração à política baseada em recursos do segredo que conceda permissão `secrets:GetSecretValue` para a identidade do IAM. Ou, se você usar uma `Deny` declaração que inclua a identidade do IAM, atualize a política para que a identidade possa

executar a ação. Para obter informações, consulte Anexar uma política de permissões a um AWS Secrets Manager segredo no Guia AWS Secrets Manager do usuário.

Problema 3: os segredos não têm uma política baseada em recursos anexada que permita o acesso à entidade principal do serviço Incident Manager, `ssm-incidents.amazonaws.com`.

- Solução: crie ou atualize a política baseada em recursos para o segredo e inclua a seguinte permissão:

```
{
    "Effect": "Allow",
    "Principal": {
        "Service": ["ssm-incidents.amazonaws.com"]
    },
    "Action": "secretsmanager:GetSecretValue",
    "Resource": "*"
}
```

Problema 4: a chave AWS KMS key selecionada para criptografar o segredo não é uma chave gerenciada pelo cliente, ou a chave gerenciada pelo cliente selecionada não fornece as permissões do IAM `kms:Decrypt` e `kms:GenerateDataKey*` à entidade principal de serviço do Incident Manager. Como alternativa, a identidade do IAM que cria o plano de resposta pode não ter a permissão do IAM `GetSecretValue`.

- Solução: verifique se você atende aos requisitos descritos em Pré-requisitos no tópico Armazenando credenciais de PagerDuty acesso em segredo AWS Secrets Manager.

Problema 5: o ID do segredo que contém a chave de API REST de acesso geral ou a chave de API REST de token de usuário não são válidos.

- Solução: verifique se você inseriu o ID do segredo do Secrets Manager com precisão, sem espaço no final. Você deve trabalhar da mesma Região da AWS que armazena o segredo que deseja usar. Você não pode usar um segredo excluído.

Problema 6: em casos raros, o serviço Secrets Manager pode ter um problema ou o Incident Manager pode ter problemas para se comunicar com ele.

- Solução: aguarde alguns minutos e tente novamente. Verifique se há problemas que possam afetar qualquer um dos serviços AWS Health Dashboard.

Outros casos de solução de problemas

Se as etapas anteriores não resolveram seu problema, você pode encontrar ajuda adicional nos seguintes recursos:

- Para problemas do IAM específicos do Incident Manager quando você acessa o console do Incident Manager, consulte Solução de problemas AWS Systems Manager Incident Manager de identidade e acesso.
- Para problemas de autenticação e autorização durante o acesso a AWS Management Console, consulte Solução de problemas do IAM no Guia do usuário do IAM

Glossário do AWS

Para obter a terminologia mais recente da AWS, consulte o glossário da AWS na Referência do Glossário da AWS.

Histórico de documentos do Incident Manager

Alteração	Descrição	Data
Atualização da política gerenciada `AWSIncidentManagerIncidentAccessServiceRolePolicy`	O Incident Manager adicionou uma nova permissão `AWSIncidentManagerIncidentAccessServiceRolePolicy`, em apoio ao recurso Findings, que permite verificar se uma instância do EC2 faz parte de um grupo de Auto Scaling. Para obter mais informações, consulte Atualizações do Incident Manager nas políticas AWS gerenciadas.	20 de fevereiro de 2024
Suporte adicional ao HashiCorp Terraform: rotações de plantão	O Terraform adicionou suporte ao Incident Manager. Agora você pode provisionar ou gerenciar recursos de plantão do Incident Manager usando o Terraform. Para obter informações sobre essa e outras integrações de terceiros com o Incident Manager, consulte Integração com outros produtos e serviços.	2 de fevereiro de 2022
Novo recurso: descobertas de outros Serviços da AWS	As descobertas fornecem informações sobre mudanças relacionadas a AWS CloudFormation pilhas e AWS CodeDeploy implantações que ocorreram na mesma época	15 de novembro de 2023

em que um incidente foi criado no Incident Manager. No console do Incident Manager, você pode visualizar informaçõ es resumidas sobre essas alterações e, em muitos casos, acessar links para os CodeDeploy consoles CloudFormation ou para obter detalhes completos sobre a alteração. As descobertas reduzem o tempo necessári o para avaliar as possíveis causas dos incidentes. Elas também reduzem as chances de os responden tes acessarem a conta ou o console incorretos ao investiga r a causa de um incidente . Esse recurso também introduz uma nova política gerenciada`AWSIncide ntManagerIncidentA ccessServiceRolePo licy` , que permite que o Incident Manager leia outros recursos Serviços da AWS para identificar descobert as relacionadas a incidente s. Para obter informações, consulte os tópicos a seguir:

- Como trabalhar com descobertas
- AWS política gerenciad a: AWSIncidentManager

	IncidentAccessServiceRolePolicy	
Listas atualizadas de integrações com o Incident Manager	O tópico Integrações de produtos e serviços com o Incident Manager foi expandido para listar e descrever todas as ferramentas do Serviços da AWS e de terceiros que você pode integrar com o Incident Manager em suas operações de detecção e resposta a incidentes.	9 de junho de 2023

Integração com AWS Trusted Advisor	Trusted Advisor agora verifica se a configuração de um conjunto de replicação usa mais de um Região da AWS para oferecer suporte ao failover e à resposta regionais . Para incidentes criados por CloudWatch alarmes ou EventBridge eventos, o Incident Manager cria um incidente da mesma forma que a Região da AWS regra de alarme ou evento. Se o Incident Manager estiver temporariamente indisponí vel nessa região, o sistema tentará criar um incidente em outra região no conjunto de replicação. Se o conjunto de replicação incluir somente uma região, o sistema não conseguirá criar um registro de incidente enquanto o Incident Manager estiver indisponível. Para ajudar a evitar essa situação, Trusted Advisor relata quando um conjunto de replicação está configurado para somente uma região. Para obter informações sobre como trabalhar com o Trusted Advisor, consulte AWS Trusted Advisor no Guia do usuário do AWS Support .	28 de abril de 2023

Usar o Microsoft Teams como um canal de chat nos planos de resposta	Por meio da integração com o Microsoft Teams e AWS Chatbot, agora você pode usar o Microsoft Teams para o canal de bate-papo em seus planos de resposta. Isso é uma adição, além de suportar os canais de chat do Slack e do Amazon Chime. Durante um incidente, o Incident Manager envia notificaç ões de status diretamente para um canal de chat para manter todos os respondentes informados. Os respondentes também podem se comunicar entre si e com AWS CLI comandos relacionados a incidentes no aplicativo Microsoft Teams para atualizar e interagir com os incidentes. Para obter mais informações, consulte Como trabalhar com canais de chat no Incident Manager.	4 de abril de 2023

Novo atributo: escalas de plantão	Uma escala de plantão no Incident Manager define quem é notificado quando ocorre um incidente que requer intervenção do operador. Uma escala de plantão consiste em uma ou mais rotações que você cria para a escala. Cada rotação pode conter até 30 contatos. Depois de criar, inclua a escala de plantão como escalação no plano de escalação. Quando ocorre um incidente associado a esse plano de escalação, o Incident Manager notifica o operador (ou operadores) que estão de plantão de acordo com a escala. Para obter mais informações, consulte Como trabalhar com escalas de plantão no Incident Manager.	28 de março de 2023

Imprimir análise de incidentes formatada ou salvar como PDF	A página de análise de incidentes agora tem um botão Imprimir para gerar uma versão da análise formatada para impressão. Usando os destinos de impressora configurados no seu dispositivo, você pode salvar a análise de incidentes como PDF ou enviá-la para uma impressora local ou de rede. Para obter mais informações, consulte Imprimir uma análise de incidentes formatada.	17 de janeiro de 2023

PagerDuty integração: o Incident Manager agora copia eventos do cronograma de incidentes para PagerDuty incidentes	Quando você ativa a integração com um plano PagerDuty de resposta, o Incident Manager adiciona eventos do cronograma criados a partir desse plano ao registro de incidentes correspondente em PagerDuty. PagerDuty adiciona eventos da linha do tempo como notas sobre o incidente, até um máximo de 2.000 notas. Para saber mais sobre essas mudanças, consulte os seguintes tópicos: • Armazene as credenciais de PagerDuty acesso em segredo AWS Secrets Manager • Integre um PagerDuty serviço ao plano de resposta	15 de dezembro de 2022
Integração do Incident Manager com CloudWatch métricas.	Agora você pode ter métricas relacionadas a incidentes publicadas em. CloudWatch Para obter mais informações, consulte CloudWatchmétricas . Isso AWSIncidentManagerServiceRolePolicy incluiu uma permissão adicional para permitir que nosso serviço publique métricas em seu nome.	15 de dezembro de 2022

Lançou Notas do incidente e atualizou a tela Detalhes do incidente	Você pode colaborar e se comunicar com outros usuários que trabalham em um incidente usando notas de incidentes. Além disso, você pode ver os runbooks e os status dos engajamentos na tela Detalhes do incidente. Para obter mais informações, consulte Detalhes do incidente .	16 de novembro de 2022

Integre planos PagerDuty de escalonamento e fluxos de trabalho de paginação aos planos de resposta do Incident Manager	Agora você pode integrar o Incident Manager PagerDuty e adicionar um PagerDuty serviço a um plano de resposta. Depois de configura r a integração, o Incident Manager pode criar um incidente correspondente PagerDuty para cada novo incidente criado no Incident Manager. PagerDuty usa o fluxo de trabalho de paginação e as políticas de escalonam ento que você define no PagerDuty ambiente. Para obter informações, consulte os tópicos a seguir: • Integrações de produtos e serviços com o Incident Manager • Armazene as credencia is de PagerDuty acesso em segredo AWS Secrets Manager • Integre um PagerDuty serviço ao plano de resposta do tópico Criar um plano de resposta • Solução de problemas	16 de novembro de 2022

Lançou Notas do incidente e atualizou a tela Detalhes do incidente.	Você pode colaborar e se comunicar com outros usuários que trabalham em um incidente usando Notas de incidentes. Além disso, você pode ver os runbooks e os status dos engajamentos na tela Detalhes do incidente. Para obter mais informações, consulte Detalhes do incidente .	16 de novembro de 2022
Compatibilidade com marcação em conjuntos de replicação	Agora você pode atribuir tags ao seu conjunto de replicação no AWS Systems Manager Incident Manager. Isso aumenta o suporte existente para atribuir tags a planos de resposta, registros de incidentes e contatos no Regiões da AWS especificado em seu conjunto de replicaçã o. Para obter informações, consulte os seguintes tópicos: • Assistente Prepare-se • Marcando recursos no Incident Manager	2 de novembro de 2022

Integração do Incident Manager com o Atlassian Jira Service Management	Você pode integrar o Incident Manager com o Jira Service Management usando o AWS Service Managemen t Connector for Jira Service Management. Depois de configurar a integração, novos incidentes criados no Incident Manager criam um incidente correspondente no Jira. Se você atualizar um incidente no Incident Manager, as atualizaç ões serão adicionadas ao incidente correspondente no Jira. Se você resolver um incidente no Incident Manager ou no Jira, o incidente correspondente também será resolvido, com base nas preferências configuradas. Para obter mais informaçõ es, consulte Como configura r o Jira Service Management no Guia do administrador do AWS Service Management Connector.	6 de outubro de 2022

Suporte aprimorado de marcação	O Incident Manager suporta a atribuição de tags a planos de resposta, registros de incidentes e contatos no Regiões da AWS especificado em seu conjunto de replicaçã o. O Incident Manager também suporta a atribuição automática de tags a incidente s criados nos planos de resposta. Para obter mais informações, consulte Como aplicar tags em recursos do Incident Manager.	28 de junho de 2022

Integração do Incident Manager com ServiceNow	Você pode integrar o Incident Manager ServiceNowusando o AWS Service Managemen t Connector para ServiceNo w. Depois de configurar a integração, novos incidentes criados no Incident Manager criam um incidente correspon dente em ServiceNow. Se você atualizar um incidente no Gerenciador de incidentes, as atualizações serão adicionad as ao incidente correspon dente em ServiceNow. Se você resolver um incidente no Gerenciador de Incidente s ou ServiceNow, o incidente correspondente também será resolvido, com base nas preferências configuradas. Para obter mais informações, consulte Integrando o AWS Systems Manager Incident Manager em ServiceNow.	9 de junho de 2022

Importar detalhes de contato	Quando um incidente é criado, o Incident Manager pode notificar os respondentes por voz ou SMS. Para garantir que os respondentes vejam que a chamada ou a notificaç ão por SMS é do Incident Manager, recomendamos que todos os respondentes baixem o arquivo em formato de cartão virtual (.vcf) do Incident Manager para o catálogo de endereços nos dispositi vos móveis. Para obter mais informações, consulte Importar detalhes de contato para seu catálogo de endereços.	18 de maio de 2022

Várias melhorias de atributos para aprimorar a criação e a remediação de incidentes	O Incident Manager lançou as seguintes melhorias para aprimorar a criação e a remediação de incidentes: • Crie incidentes automatic amente em outros Regiões da AWS: caso o Incident Manager não esteja disponível Região da AWS quando a Amazon CloudWatch ou a Amazon EventBridge criarem um incidente, esses serviços agora criam automatic amente o incidente em uma das regiões disponíve is especificadas em seu conjunto de replicação. Para obter mais informaçõ es, consulte Incident management entre regiões. • Preencha automatic amente os parâmetros do runbook com metadados de incidentes: agora você pode configurar o Incident Manager para coletar informações sobre AWS recursos de incidente s. O Incident Manager pode então preencher os parâmetros do runbook com as informações coletadas. Para obter mais informaçõ es, consulte Tutorial:	17 de maio de 2022

	como usar runbooks da automação do gerenciador de sistemas com o Incident Manager. • Colete automaticamente as informações dos AWS recursos: quando o sistema cria um incidente, o Incident Manager agora coleta automaticamente informaçõ es sobre os AWS recursos envolvidos no incidente. Em seguida, o Incident Manager adiciona essas informações à guia Itens relacionados.	
Suporte para vários runbooks	O Incident Manager agora suporta a execução de vários runbooks durante um incidente na página de detalhes do incidente.	14 de janeiro de 2022
O Incident Manager foi lançado em novo Regiões da AWS	O Incident Manager agora está disponível nas regiões: us-west-1, sa-east-1, ap-northeast-2, ap-south-1, ca-central-1, eu-west-2 e eu-west-3. Para obter mais informações sobre regiões e cotas do Incident Manager, consulte o Guia de referência do Referência geral da AWS.	8 de novembro de 2021
Confirmação do engajamento no console	Agora você pode confirmar engajamentos diretamente no console do Incident Manager.	5 de agosto de 2021

Guia Propriedades	O Incident Manager introduziu uma guia de propriedades na página de detalhes do incidente, fornecendo mais informações sobre os incidentes, o pai OpsItem e a análise pós-incidente relacionada.	3 de agosto de 2021
Lançamento do Incident Manager	O Incident Manager é um console de gerenciamento de incidentes projetado para ajudar os usuários a mitigar e se recuperar de incidentes que afetam seus aplicativos AWS hospedados.	10 de maio de 2021

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.