Guia do Usuário

AWS Audit Manager

AWS Audit Manager: Guia do Usuário

Table of Contents

O que é AWS Audit Manager?

Bem-vindo ao Guia do Usuário AWS Audit Manager.

AWS Audit Manager ajuda a auditar continuamente seu uso da AWS para simplificar a forma como gerencia os riscos e a conformidade com regulamentos e padrões do setor. O Audit Manager automatiza a coleta de evidências para que você possa avaliar mais facilmente se suas políticas, procedimentos e atividades, também conhecidos como controles, estão funcionando de modo eficaz. Quando é hora de uma auditoria, o Audit Manager ajuda você a gerenciar as análises de seus controles pelas partes interessadas. Isso significa que você pode criar relatórios prontos para auditoria com menos esforço manual.

O Audit Manager fornece estruturas pré-compiladas que organizam e automatizam as avaliações de um determinado padrão ou regulamento de conformidade. Esse framework inclui uma coleção pré-compilada de controles com descrições e procedimentos de teste. Esses controles são agrupados de acordo com os requisitos do padrão ou regulamento de conformidade especificado. Você também pode personalizar frameworks e controles para apoiar auditorias internas de acordo com requisitos específicos.

Você pode criar uma avaliação a partir de qualquer framework. Quando você cria uma avaliação, o Audit Manager executa as avaliações de atributos automaticamente. Essas avaliações coletam dados tanto para Conta da AWS quanto para os serviços que você define como escopo de sua auditoria. Os dados coletados são automaticamente transformados em evidências para auditoria. Em seguida, são anexados aos controles pertinentes, para ajudá-lo a demonstrar conformidade em segurança, gerenciamento de mudanças, continuidade de negócios e licenciamento de software. Quando você cria uma avaliação, isso inicia a coleta contínua de evidências. Depois de concluir uma auditoria e não precisar mais do Audit Manager para coletar evidências, você pode interromper a coleta. Para fazer isso, altere o status da sua avaliação para Inativa.

Atributos do Audit Manager

Com AWS Audit Manager, você pode realizar as seguintes tarefas:

- Início ágil — crie sua primeira avaliação selecionando em uma galeria de frameworks pré-construídos que oferecem suporte a uma variedade de padrões e regulamentações de conformidade. Em seguida, inicie a coleta automática de evidências para auditar seu uso da AWS service (Serviço da AWS).

- Carregue e gerencie evidências de ambientes híbridos ou multicloud— além das evidências que o Audit Manager coleta do seu ambiente AWS, você também pode carregar e gerenciar centralmente as evidências do seu ambiente on-premises ou multicloud.
- Suporte a padrões e regulamentações de conformidade comuns — escolha um dos frameworks AWS Audit Manager padrão. Esses frameworks fornecem mapeamentos de controle pré-compilados para padrões e regulamentações de conformidade comuns. Isso inclui o CIS Foundation Benchmark, PCI DSS, LGPD, HIPAA, SOC2, GxP e as práticas operacionais recomendadas AWS.
- Monitore suas avaliações ativas — use o painel do Audit Manager para visualizar os dados analíticos de suas avaliações ativas e identificar rapidamente evidências de não conformidade que precisam ser corrigidas.
- Pesquise evidências — use o atributo de busca de evidências para encontrar rapidamente evidências relevantes para sua consulta de pesquisa. Você pode gerar um relatório de avaliação a partir dos resultados da pesquisa ou exportar os resultados no formato .CSV.
- Crie controles personalizados — crie seu próprio controle do zero ou personalize um controle existente para atender às suas necessidades. Você também pode usar o atributo de controles personalizados para criar perguntas de avaliação de risco e armazenar as respostas a essas perguntas como evidência manual.
- Personalize frameworks — Crie seus próprios frameworks com controles padrão ou personalizados e base em seus requisitos específicos, para auditorias internas.
- Compartilhe frameworks personalizados — Compartilhe seus frameworks personalizados do Audit Manager com outro Conta da AWS, ou replique-os em outro Região da AWS usando sua própria conta.
- Suporte à colaboração entre equipes — Delegue conjuntos de controle a especialistas no assunto, que podem analisar evidências relacionadas, adicionar comentários e atualizar o status de cada controle.
- Crie relatórios para auditores — Gere relatórios de avaliação que resumem as evidências relevantes coletadas para sua auditoria e vinculam-nas a pastas contendo as evidências detalhadas.
- Garanta a integridade das evidências — Armazene as evidências em um local seguro, onde elas permanecerão inalteradas.

> **Note**
>
> AWS Audit Manager auxilia na coleta de evidências relevantes para verificar a conformidade com padrões e regulamentações de conformidade específicos. No entanto, ele não avalia a sua conformidade em si. Portanto, as evidências coletadas por meio do AWS Audit Manager podem não incluir todas as informações sobre seu uso AWS necessário a auditorias. AWS Audit Manager não substitui a assessoria jurídica ou os especialistas em conformidade.

Precificação do Audit Manager

Para obter mais informações sobre precificação, consulte Precificação do AWS Audit Manager.

Você está usando o Audit Manager pela primeira vez?

Se você estiver usando o Audit Manager pela primeira vez, recomendamos que comece pelas seguintes páginas:

1. Conceitos e terminologiaAWS Audit Manager – aprenda sobre os principais conceitos e termos usados no Audit Manager, como avaliações, frameworks e controles.
2. Como AWS Audit Manager coleta evidências – saiba como o Audit Manager coleta evidências para a avaliação de atributos.
3. Configuração – saiba mais sobre os requisitos de configuração do Audit Manager.
4. Introdução – siga um tutorial para criar sua primeira avaliação do Audit Manager.
5. AWS Audit ManagerReferência da API – familiarize-se com as ações e os tipos de dados da API Audit Manager.

Mais atributos do Audit Manager

Explore os atributos a seguir para saber mais sobre o Audit Manager.

- Colete evidências e gerencie dados de auditoria usando AWS Audit Manager
- Configure manualmente uma avaliação personalizada do Audit Manager a partir dos AWSWorkshops
- Integre o modelo de três linhas (parte 2): transforme pacotes de AWS Config conformidade em avaliações de AWS Audit Manager a partir do Blog de gerenciamento e governança da AWS

Conceitos e terminologia AWS Audit Manager

Para ajudá-lo a começar, esta página define termos e explica alguns dos principais conceitos do AWS Audit Manager,

A

A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z

Avaliação

Você pode usar uma avaliação do Audit Manager para coletar automaticamente evidências relevantes a uma auditoria.

Uma avaliação do Audit Manager é baseada em um framework, um agrupamento de controles relacionados à sua auditoria. Dependendo dos requisitos do seu negócio, você pode criar uma avaliação a partir de um framework padrão ou personalizado. Frameworks padrão contêm conjuntos de controle predefinidos que oferecem suporte a um padrão ou regulamento de conformidade específico. Por outro lado, frameworks personalizados contêm controles que você pode personalizar e agrupar de acordo com seus requisitos de auditoria interna. Ao usar um framework como ponto de partida, você pode criar uma avaliação que especifique as Contas da AWS e os serviços que deseja incluir no escopo de sua auditoria.

Ao criar uma avaliação, o Audit Manager começará automaticamente a avaliar os atributos em Contas da AWS e nos serviços com base nos controles definidos no framework. Em seguida, ele coleta as evidências relevantes e as converte em um formato amigável para o auditor. Depois de fazê-lo, ele anexa as evidências aos controles em sua avaliação. Na hora de fazer uma auditoria, você ou um representante de sua escolha pode analisar as evidências coletadas e adicioná-las a um relatório de avaliação. Este relatório de avaliação ajuda a mostrar que seus controles estão funcionando conforme o esperado.

A coleta de evidências é um processo continuo, que começa quando você cria uma avaliação. Você pode interromper a coleta de evidências alterando o status da avaliação para Inativo. Como alternativa, você pode interromper a coleta de evidências no nível de controle. Você pode fazer isso alterando o status de um controle específico na sua avaliação para Inativo.

Para obter instruções sobre como criar e gerenciar avaliações, consulte Avaliações em AWS Audit Manager.

Relatório de avaliação da

Um relatório de avaliação é um documento finalizado gerado a partir de uma avaliação do Audit Manager. Esses relatórios resumem as evidências relevantes coletadas para sua auditoria. Eles são vinculados às pastas de evidências relevantes. As pastas são nomeadas e organizadas de acordo com os controles especificados em sua avaliação. Para cada avaliação, você pode analisar as evidências coletadas pelo Audit Manager e decidir quais deseja incluir no relatório de avaliação.

Para saber mais sobre esses relatórios, consulte Relatórios de avaliação. Para saber como gerar um relatório de avaliação, consulte Como gerar um relatório de avaliação.

Destino do relatório de avaliação

O destino do relatório de avaliação é o bucket padrão do S3 onde o Audit Manager salva seus relatórios de avaliação. Para saber mais, consulte Destino do relatório de avaliação (opcional).

Auditoria

Uma auditoria é um exame independente dos ativos, das operações ou da integridade de negócios de sua organização. Uma auditoria de Tecnologia da Informação (TI) examina especificamente os controles nos sistemas de informação da sua organização. O objetivo de uma auditoria de TI é determinar se os sistemas de informação protegem os ativos, operam de forma eficaz e mantêm a integridade dos dados. Tudo isso é importante para atender aos requisitos regulatórios exigidos por um padrão ou regulamento de conformidade.

Proprietário da auditoria de

O termo proprietário da auditoria tem dois significados diferentes, dependendo do contexto.

No contexto do Audit Manager, o proprietário da auditoria é um usuário ou uma função que gerencia uma avaliação e seus atributos relacionados. As responsabilidades dessa persona do Audit Manager incluem criar avaliações, analisar evidências e gerar relatórios de avaliação. O Audit Manager é um serviço colaborativo, e os proprietários da auditoria se beneficiam quando outras partes interessadas participam de suas avaliações. Por exemplo, você pode adicionar outros proprietário da auditoria à sua avaliação para compartilhar tarefas de gerenciamento. Ou, se você for o proprietário de uma auditoria e precisar de ajuda para interpretar as evidências coletadas para um controle, você pode delegar esse conjunto de controles a uma parte interessada que tenha experiência no assunto nessa área. Essa pessoa é conhecida como persona delegada.

Em termos comerciais, o responsável por uma auditoria é alguém que coordena e supervisiona os esforços de preparação para a auditoria de sua empresa e apresenta evidências a um auditor. Normalmente, é um profissional de governança, risco e conformidade (governance, risk, and compliance, ou GRC), como um Diretor de Conformidade ou um Diretor de Proteção de Dados LGPD. Os profissionais GRC têm a experiência e a autoridade para gerenciar a preparação da auditoria. Mais especificamente, eles entendem os requisitos de conformidade e podem analisar, interpretar e preparar dados de relatórios. No entanto, outras funções do negócio também podem assumir a persona de Gerente de Auditoria de um proprietário da auditoria; não apenas os profissionais de GRC assumem essa função. Por exemplo, você pode optar por ter suas avaliações do Audit Manager configuradas e gerenciadas por um especialista técnico de uma das seguintes equipes:

- SecOps
- TI/DevOps
- Centro de Operações de Segurança/ Resposta a Incidentes
- Equipes semelhantes que possuem, desenvolvem, remediam e implantam ativos de nuvem e entendem a infraestrutura de nuvem de sua organização

Quem você escolhe designar como proprietário da auditoria em sua avaliação do Audit Manager depende muito da sua organização. Também depende de como você estrutura suas operações de segurança e das especificidades da auditoria. No Audit Manager, o mesmo indivíduo pode assumir a personalidade do proprietário da auditoria em uma avaliação e a persona delegada em outra.

Independente de como você decida usar o Audit Manager, você pode gerenciar a separação de tarefas em toda a sua organização usando a persona de proprietário/delegado da auditoria concedendo políticas específicas do IAM para cada usuário. Por meio dessa abordagem em duas etapas, o Audit Manager garante que controle total sobre todas as especificidades de uma avaliação individual. Para obter mais informações, consulte Políticas recomendadas para personas de usuários no AWS Audit Manager.

C

A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z

Changelog

Para cada controle em uma avaliação, o Audit Manager captura changelogs de alterações para rastrear a atividade do usuário nesse controle. Você pode analisar a trilha de auditoria das atividades relacionadas a um controle específico. Para obter mais informações sobre quais atividades do usuário são capturadas nos changelogs de alterações, consulte Guia changelog.

Conformidade da nuvem

A conformidade da nuvem é o princípio geral de que sistemas fornecidos na nuvem devem estar em conformidade com os padrões enfrentados pelos clientes da nuvem.

Regulamentação de conformidade

A regulamentação de conformidade é uma lei, regra ou outra ordem prescrita por uma autoridade, normalmente para regular a conduta. O LGPD é um exemplo.

Padrão de conformidade

Um padrão de conformidade é um conjunto estruturado de diretrizes que detalha os processos da organização para manter a conformidade com os regulamentos, especificações ou legislação estabelecidos. Os exemplos incluem PCI DSS e HIPAA.

Controle

O controle é uma salvaguarda ou contramedida prescrita para um sistema de informação ou uma organização. Os controles são projetados para proteger a confidencialidade, integridade e disponibilidade de suas informações, bem como para atender a um conjunto de requisitos de segurança definidos. Eles fornecem a garantia de que seus atributos estão operando conforme o esperado, que seus dados são confiáveis e que sua organização está em conformidade com as leis e regulamentações aplicáveis.

No Audit Manager, um controle também pode representar uma pergunta em um questionário de avaliação de risco do fornecedor. Nesse caso, um controle é uma pergunta específica que solicita informações sobre a postura de segurança e conformidade de uma organização.

Os controles coletam evidências continuamente quando estão ativos durante as avaliações do Audit Manager. Você também pode adicionar evidências manualmente a qualquer controle. Cada evidência se torna um registro que ajuda a demonstrar conformidade com os requisitos do controle.

Existem dois tipos de controle no Audit Manager:

- Controles padrão — esses são controles pré-construídos associados a um framework específico no Audit Manager. Use controles padrão para ajudá-lo na preparação da auditoria para vários padrões e regulamentações de conformidade.
- Controles personalizados — esses controles personalizados que você define como usuário do Audit Manager. Use controles personalizados para ajudá-lo a atender aos requisitos específicos de conformidade para auditorias internas ou avaliações de risco de fornecedores.

Para obter mais informações, consulte Exemplos de controles do AWS Audit Manager. Para obter instruções sobre como criar e configurar um controle, consulte Biblioteca de controle.

Domínios de controle

Você pode pensar em um domínio de controle como uma categoria geral de controles não específica a nenhum framework. Os agrupamentos de domínios de controle são alguns dos atributos mais poderosos do painel do Audit Manager. O Audit Manager destaca os controles em suas avaliações que tenham evidências de não conformidade e os agrupa por domínio de controle. Isso permite que você concentre seus esforços de remediação em domínios específicos, enquanto se prepara para uma auditoria.

> **Note**
>
> Um domínio de controle é diferente de um conjunto de controles. Um conjunto de controles é um agrupamento de controles específico do framework que normalmente é definido por um órgão regulador. Por exemplo, o framework do PCI DSS tem um conjunto de controles chamado Requisito 8: identificar e autenticar o acesso aos componentes do sistema. Esse conjunto de controles está sob o domínio do Gerenciamento de identidade e acesso.

O Audit Manager categoriza os controles nos seguintes domínios.

Nome do domínio de controle	Descrição do que cada controle governa
Continuidade de negócios e planejamento de contingência	Como estabelecer processos que protejam as operações comerciais críticas dos efeitos de grandes interrupções no sistema e na rede.

Nome do domínio de controle	Descrição do que cada controle governa
Gerenciamento de alterações	Como você testa, aprova, implementa e documenta as mudanças em sua infraestrutura de nuvem.
Segurança e privacidade de dados	Como você protege a privacidade, a disponibilidade e a integridade de seus dados.
Gerenciamento de desenvolvimento e configuração	Como você mantém sua infraestrutura de nuvem em um estado desejado e consistente.
Governança e supervisão	Como você alinha o uso da computação em nuvem às suas obrigações legais, regulatórias e éticas.
Gerenciamento de identidade e acesso	Como garantir que os usuários certos tenham o acesso adequado aos seus atributos de tecnologia.
Gerenciamento de incidentes	Como você estabelece responsabilidades e procedimentos que garantam uma resposta rápida e eficaz aos incidentes de segurança.
Logging e monitoramento	Como analisar a atividade do usuário em busca de indicações de que uma atividade não autorizada foi tentada ou realizada.
Gerenciamento de rede	Como administrar e operar sua rede de dados usando um sistema de gerenciamento de rede.
Gestão de pessoal	Como avaliar e gerenciar os riscos de segurança do pessoal em nível organizacional.
Segurança física	Como detectar e evitar problemas de segurança física em suas instalações.
Gestão de riscos	Como avaliar possíveis riscos, perdas e como reduzir ou eliminar essas ameaças.

Nome do domínio de controle	Descrição do que cada controle governa
Gestão da cadeia de suprimentos	Como identificar, avaliar e mitigar os riscos associados a produtos de TI, fornecedores e cadeias de suprimentos.
Gerenciamento de dispositivos de usuários	Como reduzir o risco de perda, dano ou comprometimento do hardware de TI de seus funcionários.
Gerenciamento de vulnerabilidade	Como definir, avaliar e corrigir todas as vulnerabilidades conhecidas dos ativos em sua infraestrutura de nuvem.

D

A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z

Fonte de dados

O Audit Manager usa uma fonte de dados para coletar evidências para um controle. A terminologia a seguir descreve uma fonte de dados e como ela funciona.

- Um Tipo de fonte de dados define onde o Audit Manager coleta evidências para um controle. Se você carregar sua própria evidência, o tipo de fonte de dados será Manual. Se o Audit Manager coletar as evidências em seu nome, o tipo de fonte de dados será um dos seguintes: AWS Security Hub, AWS Config, AWS CloudTrail, ou chamadas de API AWS. A API Audit Manager se refere a um tipo de fonte de dados, como SourceType (singular) ou ControlSources (plural).
- Um Mapeamento é uma palavra-chave específica relacionada a um tipo de fonte de dados. Por exemplo, pode ser um nome de evento do CloudTrail ou um nome AWS Config. A API Audit Manager se refere a um tipo de fonte de dados como sourceKeyword (singular) ou controlMappingSources (plural).
- O nome da fonte de dados é um nome dado a uma fonte de dados. Em outras palavras, o nome da fonte de dados rotula a combinação do tipo de fonte e mapeamento de dados. Para controles padrão, o Audit Manager fornece o nome da fonte de dados padrão (como Fonte de dados 1 e Fonte de dados 2). Para controles personalizados, você pode fornecer seu próprio nome da fonte de dados. Isso pode ajudar a distinguir entre vários mapeamentos que se

enquadrem no mesmo tipo de fonte de dados. A API Audit Manager se refere a um nome de fonte de dados como SourceName.

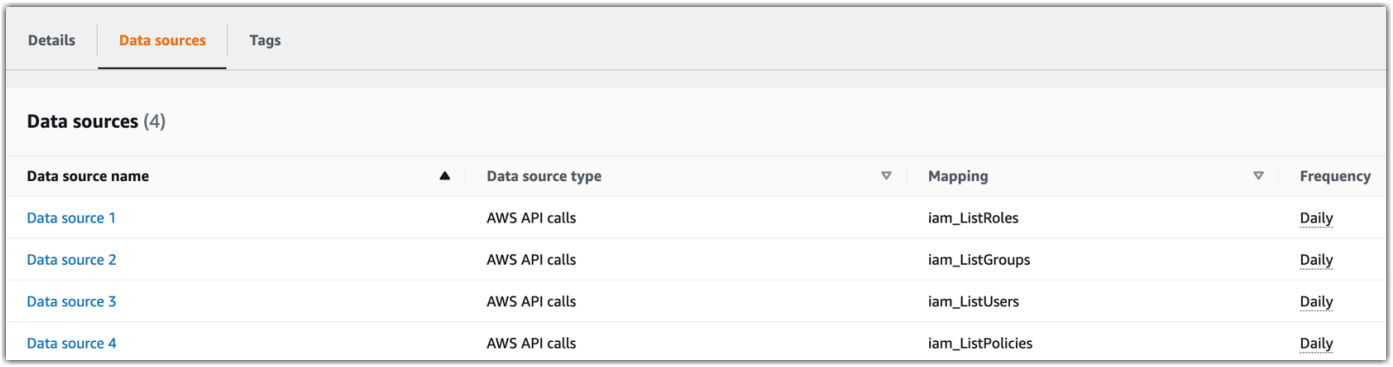
Um único controle pode ter vários tipos de fonte de dados e vários mapeamentos. Por exemplo, um controle pode coletar evidências de uma combinação de tipos de fonte de dados (como AWS Config e o Security Hub). Outro controle pode ter AWS Config como único tipo de fonte de dados, com várias regras AWS Config como mapeamentos.

A tabela a seguir lista os tipos de fonte de dados automatizados e exemplos de alguns mapeamentos correspondentes.

Tipo de fonte de dados	Descrição	Exemplo de mapeamento
AWS Security Hub	Use esse tipo de fonte de dados para captura de tela da sua postura de segurança de atributos. O Audit Manager usa o nome de um controle do Security Hub como a palavra-chave de mapeamento e relata o resultado dessa verificação de segurança diretamente do Security Hub.	`1.1 – Avoid the use of the "root" account`
AWS Config	Use esse tipo de fonte de dados para captura de tela da sua postura de segurança de atributos . O Audit Manager usa o nome de uma regra AWS Config como palavra-chave de mapeamento e relata o resultado dessa verificaç ão de regra diretamente de AWS Config.	`EC2_INSTANCE_MANAG ED_BY_SSM`

Tipo de fonte de dados	Descrição	Exemplo de mapeamento
AWS CloudTrail	Use esse tipo de fonte de dados para rastrear uma atividade específica do usuário necessária à sua auditoria. O Audit Manager usa o nome de um evento do CloudTrail como a palavra-chave de mapeamento e coleta a atividade relacionada do usuário dos seus logs do CloudTrail.	`CreateAccessKey`
Chamadas de API da AWS	Use esse tipo de fonte de dados para captura de tela da configuração do seu atributo por meio de uma chamada de API para uma fonte específica AWS service (Serviço da AWS). O Audit Manager usa o nome da chamada de API como palavra-chave de mapeamento e coleta a resposta da API.	`ec2_DescribeSecurityGroups`

A imagem a seguir mostra exemplos de diferentes fontes de dados, conforme visto no console do Audit Manager.



> **Note**
>
> Embora alguns tipos de fonte de dados sejam Serviços da AWS, o tipo de fonte de dados é diferente do serviço no escopo. Para obter mais informações, consulte Qual é a diferença entre um serviço no escopo e um tipo de fonte de dados? na seção Solução de problemas deste guia.

Delegado

O delegado é um usuário AWS Audit Manager com permissões limitadas. Os delegados geralmente têm conhecimento técnico ou de negócios especializado. Por exemplo, esses conhecimentos podem estar em políticas de retenção de dados, planos de treinamento, infraestrutura de rede ou gerenciamento de identidades. Os delegados ajudam os proprietários da auditoria a analisarem as evidências coletadas para os controles que se enquadrem na sua área de especialização. Os delegados podem analisar conjuntos de controles e suas evidências relacionadas, adicionar comentários, carregar evidências adicionais e atualizar o status de um controle.

Os responsáveis pela auditoria atribuem conjuntos de controle específicos aos delegados, não avaliações completas. Como resultado, os delegados têm acesso limitado às avaliações. Para obter instruções sobre como delegar um conjunto de controles, consulte Delegações em AWS Audit Manager.

E

A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z

Evidências

A evidência é um registro que contém as informações necessárias para demonstrar a conformidade com os requisitos de um controle. Exemplos de evidências incluem uma atividade de alteração invocada por um usuário e uma captura de tela da configuração do sistema.

Existem dois tipos principais de evidência no Audit Manager — evidência automatizada e evidência manual.

- Evidência automatizada — evidência que o Audit Manager coleta automaticamente. Inclui as três categorias de evidências automatizadas a seguir:
  - Verificação de conformidade — o resultado de uma verificação de conformidade capturado de AWS Security Hub, AWS Config ou de ambos. Exemplos de verificações de conformidade incluem um resultado de verificação de segurança do Security Hub para um controle PCI DSS e uma avaliação de regras AWS Config para um controle HIPAA. Para obter mais informações, consulte Regras AWS Config suportadas por AWS Audit Manager e controles AWS Security Hub suportados por AWS Audit Manager.
  - Atividade do usuário — a atividade do usuário que altera a configuração de um atributo é capturada dos logs do CloudTrail à medida que essa atividade ocorre. Exemplos de atividades do usuário incluem uma atualização da tabela de rotas, uma alteração na configuração de backup da instância do Amazon RDS e uma alteração na política de criptografia do bucket do S3. Para obter mais informações, consulte Nomes de eventos do AWS CloudTrail suportados pelo AWS Audit Manager.
  - Dados de configuração — captura de tela da configuração do atributo capturada diretamente do AWS service (Serviço da AWS), em base diária, semanal ou mensal. Exemplos de capturas de tela de configuração incluem uma lista de rotas para uma tabela de rotas VPC, uma configuração de backup da instância do Amazon RDS e uma política de criptografia de bucket do S3. Para obter mais informações, consulte Controles de chamadas de API suportados pelo AWS Audit Manager.
- Evidência manual — essa é a evidência que você mesmo adiciona ao Audit Manager. Há três maneiras de adicionar sua própria evidência:
  - Importar um arquivo do Amazon S3
  - Carregar um arquivo do seu navegador
  - Inserir uma resposta de texto para uma pergunta de avaliação de risco

  Para obter mais informações, consulte Como adicionar evidências manuais em AWS Audit Manager.

Quando você cria uma avaliação, também inicia a coleta contínua automatizada de evidências. Esse é um processo contínuo, e o Audit Manager coleta evidências em diferentes frequências, de acordo com o tipo de evidência e fonte de dados subjacente. Para obter mais informações sobre coleta de evidências, consulte Como AWS Audit Manager coleta evidências. Para obter instruções sobre como analisar evidências em uma avaliação, consulte Analisando a evidência em uma avaliação.

Método de coleta de evidências

Há duas maneiras pelas quais um controle pode coletar evidências.

- Controles automatizados coletam evidências das fontes de dados AWS de forma automática. Essa evidência automatizada pode ajudá-lo a demonstrar a conformidade total ou parcial com o controle.
- Controles manuais exigem que você carregue suas próprias evidências para demonstrar a conformidade com o controle.

> **Note**
>
> Você pode anexar evidências manuais a qualquer controle automatizado. Em muitos casos, é necessária uma combinação de evidências automatizadas e manuais para demonstrar total conformidade com um controle. Embora o Audit Manager possa fornecer evidências automatizadas úteis e relevantes, algumas evidências automatizadas podem demonstrar apenas conformidade parcial. Nesse caso, você pode complementar a evidência automatizada fornecida pelo Audit Manager com sua própria evidência.
> Por exemplo:
>
> - O framework de práticas recomendadas de IA generativa da AWS contém um controle chamado `Error analysis`. Esse controle exige que você identifique imprecisões detectadas no uso do modelo. Também exige que você realize uma análise completa dos erros para entender as causas raiz e tomar medidas corretivas.
> - Para apoiar esse controle, o Audit Manager coleta evidências automatizadas que mostram se os alarmes do CloudWatch estão habilitados para o local da Conta da AWS em que sua avaliação está sendo executada. Você pode usar essa evidência para demonstrar a conformidade parcial com o controle, provando que seus alarmes e verificações estão configurados corretamente.
> - Para demonstrar total conformidade, você pode complementar a evidência automatizada com evidência manual. Por exemplo, você pode carregar uma política ou um procedimento que mostre seu processo de análise de erros, seus limites para

escalonamentos e relatórios, bem como resultados de sua análise de causa raiz. Você pode usar essa evidência manual para demonstrar que as políticas estabelecidas estão em vigor e que a ação corretiva foi tomada quando solicitada.

Para um exemplo mais detalhado, consulte Controles com fontes de dados mistas.

Destinos de exportação

O destino de exportação é o bucket padrão do S3 em que o Audit Manager salva os arquivos que você exporta do localizador de evidências. Para saber mais, consulte Destino de exportação (opcional).

F

A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z

Framework

Um framework do Audit Manager é um arquivo usado para estruturar e automatizar avaliações de um padrão específico ou princípio de governança de risco. Esses frameworks ajudam a mapear seus atributos AWS, de acordo com os requisitos em um controle. Eles incluem uma coleção de controles pré-compilados ou definidos pelo cliente. A coleção tem descrições e procedimentos de teste para cada controle. Esses controles são organizados e agrupados de acordo com os requisitos de conformidade padrão ou regulamento especificados. Os exemplos incluem PCI DSS e LGPD.

Existem dois tipos de framework no Audit Manager:

- Frameworks padrão — frameworks pré-compilados baseados nas práticas recomendadas AWS para vários padrões e regulamentações de conformidade. Você pode usar esses frameworks na preparação da sua auditoria.
- Frameworks personalizados — frameworks personalizados que você define como usuário do Audit Manager. Você pode usar esses frameworks para auxiliar na preparação da auditoria de acordo com seus requisitos específicos de conformidade ou governança de risco.

Para obter instruções sobre como criar e configurar frameworks, consulte Biblioteca framework.

> **Note**
>
> AWS Audit Manager auxilia na coleta de evidências relevantes para verificar a conformidade com padrões e regulamentações de conformidade específicos. No entanto, ele não avalia a sua conformidade em si. Portanto, as evidências coletadas por meio do AWS Audit Manager podem não incluir todas as informações sobre seu uso AWS necessário a auditorias. AWS Audit Manager não substitui a assessoria jurídica ou os especialistas em conformidade.

Compartilhamento de framework

Você pode usar o atributo de compartilhamento de framework personalizado do Audit Manager para compartilhar rapidamente seus frameworks personalizados entre Contas da AWS e Regiões. Para compartilhar um framework personalizado, crie uma solicitação de compartilhamento. O destinatário da solicitação de compartilhamento tem 120 dias para aceitar ou recusar a solicitação. Ao aceitar, o Audit Manager replica o framework personalizado compartilhado em sua biblioteca de frameworks. Além de replicar framework personalizado, o Audit Manager também replica todos os conjuntos de controles e controles personalizados que fazem parte desse framework. Esses controles personalizados são adicionados à biblioteca de controle do destinatário. O Audit Manager não replica frameworks ou controles padrão. Isso ocorre porque esses atributos já estão disponíveis por padrão em cada conta e Região.

R

A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z

Atributo

Um atributo é um ativo físico ou informação avaliada em uma auditoria. Exemplos de atributos AWS incluem instâncias do Amazon EC2, instâncias do Amazon RDS, buckets do Amazon S3 e sub-redes Amazon VPC.

Avaliação de atributos

Uma avaliação de atributos é o processo de avaliar um atributo individual. Essa avaliação é baseada no atributo de um controle. Enquanto uma avaliação está ativa, o Audit Manager executa avaliações de atributos para cada atributo individual no escopo da avaliação. Uma avaliação de atributos executa o seguinte conjunto de tarefas:

1. Coleta evidências, incluindo configurações de atributos, logs de eventos e descobertas
2. Traduz e mapeia evidências para controles
3. Armazena e rastreia a linhagem de evidências para habilitar integridade

Conformidade de atributos

A conformidade do atributo se refere ao status de avaliação de um atributo avaliado ao coletar evidências de verificação de conformidade.

O Audit Manager coleta evidências de verificação de conformidade para controles que utilizam AWS Config e Security Hub como um tipo de fonte de dados. Vários atributos podem ser avaliados durante essa coleta de evidências. Como resultado, uma única evidência de verificação de conformidade pode incluir um ou mais atributos.

Você pode usar o filtro conformidade de atributos no localizador de evidências para explorar o status de conformidade no nível do atributo. Depois que sua pesquisa for concluída, você poderá visualizar os atributos que corresponderem à sua consulta de pesquisa.

No localizador de evidências, há três valores possíveis para a conformidade do atributo:

- Não conformidade: se refere a atributos com problemas de verificação de conformidade. Isso acontece se o Security Hub relatar um resultado de Falha para o atributo ou se AWS Config relatar um resultado de Não conformidade.
- Em conformidade – se refere a atributos com problemas de verificação de conformidade. Isso acontece se o Security Hub relatar um resultado de Êxito para o atributo, ou se AWS Config relatar um resultado Em conformidade.
- Inconclusivo – se refere a atributos para os quais uma verificação de conformidade não está disponível ou não é aplicável. Isso acontece se AWS Config ou o Security Hub forem o tipo de fonte de dados subjacente mas não estiverem habilitados. Isso também acontece se o tipo de fonte de dados subjacente não oferecer suporte a verificações de conformidade (como evidências manuais, chamadas de API AWS ou CloudTrail).

S

A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z

Serviço em escopo

Um AWS service (Serviço da AWS) incluído no escopo da sua avaliação. Quando você especifica um serviço como incluído no escopo de sua avaliação, o Audit Manager avalia os atributos desse

serviço. O Audit Manager pode avaliar uma grande variedade de atributos de um serviço no escopo. Alguns exemplos de atributos incluem:

- Uma instância do Amazon EC2
- Um bucket do S3
- Usuário ou perfil
- Uma tabela do DynamoDB
- Um componente de rede, como uma nuvem privada virtual (VPC), um grupo de segurança ou uma tabela de lista de controle de acesso à rede (ACL)

Quando você usa o console do Audit Manager para criar ou atualizar uma avaliação a partir de um framework padrão, a lista de Serviços da AWS no escopo é selecionada por padrão. Essa lista não pode ser editada. Isso ocorre porque o Audit Manager mapeia e seleciona automaticamente as fontes de dados e os serviços para você. Essa seleção é feita de acordo com os requisitos do framework padrão. Se o framework padrão que você selecionou contiver somente controles manuais, nenhum Serviços da AWS estará no escopo de sua avaliação e você não poderá adicionar nenhum serviço à sua avaliação.

Se você precisar editar a lista de serviços em escopo de um framework padrão, poderá fazê-lo usando as operações da API CreateAssessment ou UpdateAssessment. Como alternativa, você pode personalizar o framework padrão e, em seguida, criar uma avaliação a partir do framework personalizado.

> **Note**
>
> Lembre-se de que um serviço no escopo é diferente de um tipo de fonte de dados, que também pode ser um AWS service (Serviço da AWS) ou outra coisa. Para obter mais informações, consulte Qual é a diferença entre um serviço no escopo e um tipo de fonte de dados? na seção Solução de problemas deste guia.

Como AWS Audit Manager coleta evidências

Cada avaliação ativa no AWS Audit Manager coleta automaticamente evidências de uma variedade de fontes de dados. Cada avaliação tem um escopo definido que especifica as Serviços da AWS e contas das quais o Audit Manager coleta dados. Cada um desses serviços e contas definidos no escopo contém vários atributos, e cada atributo é um inventário de ativos do sistema que você

possui. A coleta de evidências no Audit Manager envolve a avaliação de cada atributo dentro do escopo. Isso é chamado de avaliação de atributos.

As etapas a seguir descrevem como o Audit Manager coleta evidências para cada avaliação de atributo:

1. Avaliação de um atributo a partir de fonte de dados

Para iniciar a coleta de evidências, o Audit Manager avalia um atributo dentro do escopo a partir de uma fonte de dados. Ele faz isso capturando a tela da configuração, um resultado de verificação de conformidade relacionado e qualquer atividade do usuário. Em seguida, ele executa uma análise para determinar qual controle esses dados suportam. O resultado da avaliação dos atributos é salvo e convertido em evidências. Para obter mais informações sobre os diferentes tipos de evidência, consulte Evidências na seção Conceitos e terminologia do AWS Audit Manager deste guia.

2. Convertendo os resultados da avaliação em evidência

O resultado da avaliação do atributo contém os dados originais capturados desse atributo e os metadados, que indicam quais controles são suportados pelos dados. AWS Audit Manager converte os dados originais em formato amigável ao auditor. Os dados e metadados convertidos são então salvos como evidência do Audit Manager, antes de serem anexados a um controle.

3. Anexando evidências ao controle relacionado

O Audit Manager lê os metadados da evidência. Em seguida, ele anexa a evidência salva a um controle relacionado na avaliação. A evidência anexada fica visível no Audit Manager. Isso completa o ciclo de uma avaliação de atributos.

> **Note**
>
> De acordo com as configurações de controle, a mesma evidência pode, em alguns casos, ser anexada a vários controles de várias avaliações do Audit Manager. Quando a mesma evidência é anexada a vários controles, o Audit Manager mede a avaliação do atributo apenas uma vez. Isso ocorre porque a mesma evidência é coletada apenas uma vez. No entanto, um controle em uma avaliação do Audit Manager pode ter várias evidências, de várias fontes de dados.

Frequência das coletas de evidências

A coleta de evidências é um processo contínuo, que começa quando você cria sua avaliação. AWS Audit Manager coleta evidências de várias fontes de dados em frequências variadas. Como resultado, não há uma resposta única para a frequência com que as evidências são coletadas. A frequência da coleta de evidências é baseada no tipo de evidência e em sua fonte de dados, conforme descrito abaixo.

- Verificações de conformidade — o Audit Manager coleta esse tipo de evidência de AWS Security Hub e AWS Config.
  - Para AWS Security Hub, a frequência da coleta de evidências segue o cronograma de suas verificações do Security Hub. Para obter mais informações sobre o agendamento das verificações do Security Hub, consulte Programação para execução de verificações de segurança no Guia do Usuário AWS Security Hub. Para obter mais informações sobre as verificações do Security Hub suportadas pelo Audit Manager, consulte AWS Security Hub controles suportados por AWS Audit Manager.
  - Para AWS Config, a frequência da coleta de evidências segue os gatilhos definidos em suas regras AWS Config. Para obter mais informações sobre os acionadores das regras AWS Config, consulte Tipos de gatilhos no Guia do Usuário do AWS Config. Para obter mais informações sobre as Regras do AWS Config com suporte pelo Audit Manager, consulte Regras do AWS Config apoiado por AWS Audit Manager.
- Atividade do usuário — o Audit Manager coleta esse tipo de evidência de AWS CloudTrail de forma contínua. Essa frequência é contínua porque a atividade do usuário pode acontecer a qualquer hora do dia. Para obter mais informações, consulte AWS CloudTrail nomes de eventos suportados por AWS Audit Manager.
- Dados de configuração: o Audit Manager coleta esse tipo de evidência usando uma chamada de API de descrição para outro AWS service (Serviço da AWS), como Amazon EC2, Amazon S3 ou IAM. Você pode escolher quais ações de API quer chamar. Você também configura a frequência como diária, semanal ou mensal no Audit Manager. Você pode especificar essa frequência ao criar ou editar um controle na biblioteca de controle. Para obter instruções sobre como editar ou criar um controle, consulte Biblioteca de controle. Para obter mais informações sobre como o Audit Manager usa chamadas de API para criar evidências, consulte Chamadas de API suportadas por AWS Audit Manager.

Independente da frequência da coleta de evidências, novas evidências são coletadas automaticamente enquanto a avaliação está ativa.

Novos exemplos de controles AWS Audit Manager

Você pode analisar os exemplos nesta página para saber mais sobre como os controles funcionam em AWS Audit Manager. Esses exemplos descrevem a aparência de um controle, como o Audit Manager gera evidências desse controle e as próximas etapas para demonstrar conformidade.

> **Tip**
>
> Recomendamos que você ative AWS Config e AWS Security Hub para obter uma experiência ideal no Audit Manager. Quando você ativa esses serviços, eles podem ser usados como um tipo de fonte de dados para os controles em suas avaliações do Audit Manager. Em outras palavras, o Audit Manager pode usar as descobertas do Security Hub e Regras do AWS Config para gerar evidências automatizadas.
>
> - Depois de habilitar AWS Security Hub, certifique-se de habilitar também todos os padrões de segurança e ativar a configuração de descobertas de controle consolidadas. Essa etapa garante que o Audit Manager possa importar descobertas para todos os padrões de conformidade suportados.
> - Depois de habilitar AWS Config, certifique-se de também habilitar o Regras do AWS Config pertinente ou implantar um pacote de conformidade para o padrão de conformidade relacionado à sua auditoria. Essa etapa garante que o Audit Manager possa importar descobertas para todos os Regras do AWS Config compatíveis que você ativou.

Os exemplos estão disponíveis para cada um dos seguintes tipos de controles:

Tópicos

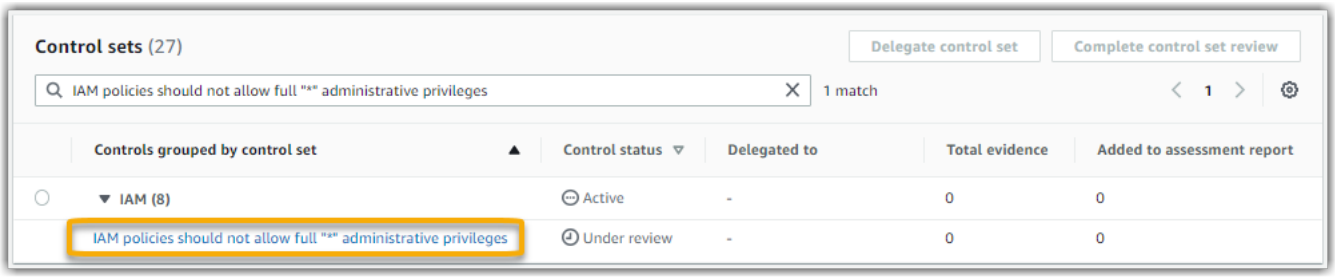
Controles automatizados que usam AWS Security Hub como tipo de fonte de dados

Este exemplo mostra um controle que usa AWS Security Hub como tipo de fonte de dados. Esse é um controle padrão retirado do Framework de Práticas Recomendadas de Segurança Básica (Foundational Security Best Practices, ou FSBP) AWS. O Audit Manager usa esse controle para gerar evidências que podem ajudar a alinhar o ambiente da AWS aos requisitos do FSBP.

Exemplo de detalhes de controle

- Nome do controle — `IAM policies should not allow full "*" administrative privileges`
- Conjunto de controles — esse controle pertence ao conjunto de controles `IAM`. Esse é um agrupamento de controles relacionado ao gerenciamento de identidade e acesso.
- Tipo de fonte de dadoss: AWS Security Hub
- Tipo de evidência — verificação de conformidade

No exemplo a seguir, esse controle está dentro de uma avaliação do Audit Manager criada a partir do framework do FSBP.



A avaliação mostra o status do controle. Também mostra o volume evidência coletado para esse controle até o momento e volume de evidência incluso em seu relatório de avaliação. A partir daqui, você pode delegar a análise do conjunto de controles ou conclui-la você mesmo. A escolha do nome do controle abre uma página de detalhes com mais informações, incluindo as evidências desse controle.

O que esse controle faz

O Audit Manager pode usar esse controle para verificar se suas políticas do IAM são amplas demais para atender aos requisitos do FSBP. Mais especificamente, ele pode verificar se suas políticas do

IAM gerenciadas pelo cliente têm acesso de administrador incluindo a seguinte declaração curinga: `"Effect": "Allow"` com `"Action": "*"` sobre `"Resource": "*"`.

Como o Audit Manager coleta evidências para esse controle

O Audit Manager executa as seguintes etapas para coletar evidências para esse controle:

1. Para cada controle, o Audit Manager avalia seus atributos dentro do escopo. Ele faz isso usando a fonte de dados especificada nas configurações de controle. Neste exemplo, suas políticas do IAM são o atributo e o Security Hub AWS Config, o tipo de fonte de dados. O Audit Manager procura o resultado de uma verificação específica do Security Hub ([IAM.1]), que, por sua vez, usa uma regra AWS Config para avaliar suas políticas do IAM (iam-policy-no-statements-with-admin-access).
2. O resultado da avaliação dos atributos é salvo e convertido em evidências amigáveis ao auditor. O Audit Manager gera evidências de verificação de conformidade para controles que usam o Security Hub como um tipo de fonte de dados. Essa evidência contém o resultado da verificação de conformidade relatada diretamente do Security Hub.
3. O Audit Manager anexa a evidência salva ao controle denominado `IAM policies should not allow full "*" administrative privileges` em sua avaliação.

Como você pode usar o Audit Manager para demonstrar conformidade com esse controle

Depois que a evidência é anexada ao controle, você ou um representante de sua escolha podem analisar a evidência para checar se é necessária alguma remediação.

Neste exemplo, o Audit Manager pode exibir uma decisão de Falha do Security Hub. Isso pode acontecer se suas políticas do IAM contiverem curingas (*) e forem demasiado amplas para atender o controle. Nesse caso, você pode atualizar suas políticas do IAM para que elas não permitam privilégios administrativos completos. Para fazer isto, você pode determinar o que os usuários precisam fazer e, em seguida, criar políticas para eles que permitam que os usuários executem apenas aquelas tarefas. Essa ação corretiva ajuda a alinhar seu ambiente AWS aos requisitos do FSBP.

Quando suas políticas do IAM estiverem alinhadas com o controle, marque o controle como Analisado e adicione as evidências ao seu relatório de avaliação. Em seguida, você pode compartilhar esse relatório com os auditores para demonstrar que o controle está funcionando conforme o esperado.

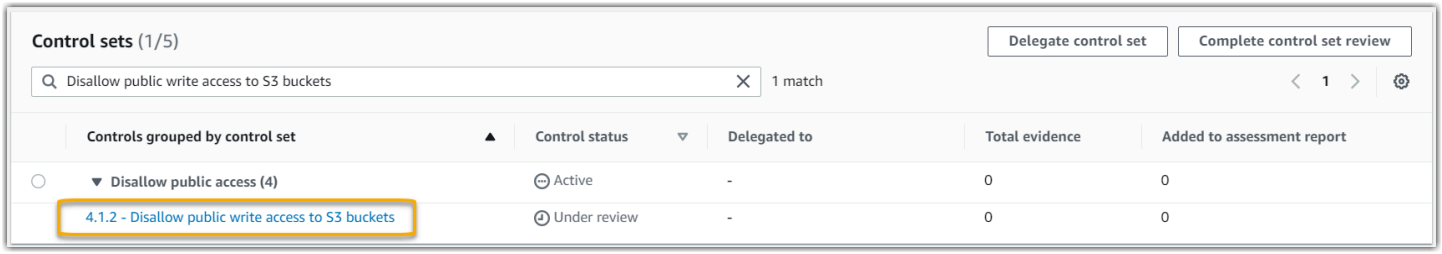
Controles automatizados que usam AWS Config como tipo de fonte de dados

Este exemplo mostra um controle que usa AWS Config como tipo de fonte de dados. Esse é um controle padrão retirado do Framework de Proteção do AWS Control Tower. O Audit Manager usa esse controle para gerar evidências que podem ajudar a alinhar o ambiente da AWS à proteção do AWS Control Tower.

Exemplo de detalhes de controle

- Nome do controle — `4.1.2 - Disallow public write access to S3 buckets`
- Conjunto de controles — esse controle pertence ao conjunto de controles `Disallow public access`. Esse é um agrupamento de controles relacionado ao gerenciamento de identidade e acesso.
- Tipo de fonte de dados: AWS Config
- Tipo de evidência — verificação de conformidade

No exemplo a seguir, esse controle está dentro de uma avaliação do Audit Manager criada a partir do Framework de Proteção AWS Control Tower.



A avaliação mostra o status do controle, quanta evidência foi coletada para esse controle até o momento e quanta evidência está incluída em seu relatório de avaliação. A partir daqui, você pode delegar a análise do conjunto de controles ou conclui-la você mesmo. A escolha do nome do controle abre uma página de detalhes com mais informações, incluindo as evidências desse controle.

O que esse controle faz

O Audit Manager pode usar esse controle para verificar se os níveis de acesso de suas políticas de bucket do S3 são muito tolerantes para atender aos requisitos AWS Control Tower. Mais especificamente, ele pode verificar as configurações do Block Public Access, as políticas do bucket e as listas de controle de acesso (ACL) do bucket, para confirmar se seus buckets não permitem acesso público de gravação.

Como o Audit Manager coleta evidências para esse controle

O Audit Manager executa as seguintes etapas para coletar evidências para esse controle:

1. Para cada controle, o Audit Manager avalia seus atributos dentro do escopo usando a fonte de dados especificada nas configurações de controle. Nesse caso, seus buckets do S3 serão os atributos e AWS Config será o tipo de fonte de dados. O Audit Manager procura o resultado de uma regra AWS Config específica (s3-bucket-public-write-prohibited) para avaliar as configurações, a política e a ACL de cada um dos buckets do S3 no escopo de sua avaliação.
2. O resultado da avaliação dos atributos é salvo e convertido em evidências amigáveis ao auditor. O Audit Manager gera evidências de verificação de conformidade para controles que usam AWS Config como um tipo de fonte de dados. Essa evidência contém o resultado da verificação de conformidade relatada diretamente do AWS Config.
3. O Audit Manager anexa a evidência salva ao controle denominado `4.1.2 - Disallow public write access to S3 buckets` em sua avaliação.

Como você pode usar o Audit Manager para demonstrar conformidade com esse controle

Depois que a evidência é anexada ao controle, você ou um representante de sua escolha podem analisar a evidência para checar se é necessária alguma remediação.

Neste exemplo, o Audit Manager pode exibir uma regra de AWS Config declarando que um bucket do S3 não está em conformidade. Isso pode acontecer se um de seus buckets do S3 tiver uma configuração de Block Public Access que não restrinja políticas públicas, e a política em uso permita acesso público de gravação. Para corrigir isso, você pode atualizar a configuração de Block Public Access para restringir políticas públicas. Ou você pode usar uma política de bucket diferente que não permita acesso público de gravação. Essa ação corretiva ajuda a alinhar seu ambiente AWS aos requisitos do AWS Control Tower.

Quando estiver satisfeito com o fato de que seus níveis de acesso ao bucket do S3 estarem alinhados com o controle, você poderá marcar o controle como Analisado e adicionar as evidências ao seu relatório de avaliação. Em seguida, você pode compartilhar esse relatório com os auditores para demonstrar que o controle está funcionando conforme o esperado.

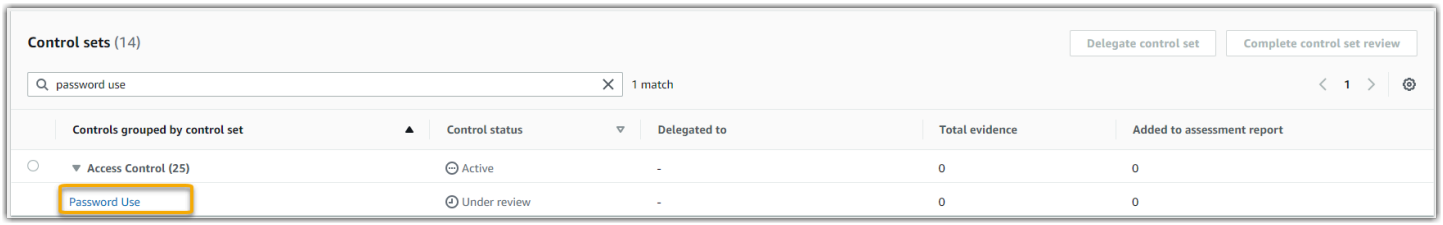
Controles automatizados que usam chamadas de API AWS como tipo de fonte de dados

Este exemplo mostra um controle que usa chamadas de API AWS como tipo de fonte de dados. O Audit Manager usa esse controle para gerar evidências que podem ajudar a alinhar o ambiente da AWS aos seus requisitos específicos.

Exemplo de detalhes de controle

- Nome do controle — `Password Use`
- Conjunto de controles: esse controle pertence ao conjunto de controles chamado `Access Control`. Esse é um agrupamento de controles relacionado ao gerenciamento de identidade e acesso.
- Tipo de fonte de dados – chamadas de API AWS
- Tipo de evidência – dados de configuração

No exemplo a seguir, o controle está dentro de uma avaliação do Audit Manager criada a partir de um framework personalizado.



A avaliação mostra o status do controle. Também mostra o volume evidência coletado para esse controle até o momento e volume de evidência incluso em seu relatório de avaliação. A partir daqui, você pode delegar a análise do conjunto de controles ou conclui-la você mesmo. A escolha do nome do controle abre uma página de detalhes com mais informações, incluindo as evidências desse controle.

O que esse controle faz

O Audit Manager pode usar esse controle personalizado para ajudá-lo a garantir acesso suficiente a políticas de controle de acesso. Esse controle exige que você siga práticas recomendadas de segurança na seleção e uso de senhas. O Audit Manager pode ajudá-lo a validar isso recuperando uma lista de todas as políticas de senha das entidades principais do IAM que estão no escopo de sua avaliação.

Como o Audit Manager coleta evidências para esse controle

O Audit Manager executa as seguintes etapas para coletar evidências para esse controle personalizado:

1. Para cada controle, o Audit Manager avalia seus atributos dentro do escopo usando a fonte de dados especificada nas configurações de controle. Nesse caso, seus diretores do IAM são os atributos e as chamadas de API AWS são o tipo de fonte de dados. O Audit Manager procura o resultado de uma chamada específica da API do IAM (getAccountPasswordPolicy). Em seguida, ele retorna as políticas de senha para as Contas da AWS no escopo de sua avaliação.
2. O resultado da avaliação dos atributos é salvo e convertido em evidências amigáveis ao auditor. O Audit Manager gera evidências de dados de configuração para controles que usam chamadas de API como fonte de dados. Essa evidência contém os dados originais capturados das respostas da API e metadados adicionais, que indicam quais controles os dados suportam.
3. O Audit Manager anexa a evidência salva ao controle denominado `Password Use` em sua avaliação.

Como você pode usar o Audit Manager para demonstrar conformidade com esse controle

Depois que a evidência é anexada ao controle, você ou um representante de sua escolha podem analisar a evidência para checar se é necessária alguma remediação.

Neste exemplo, você pode analisar as evidências para ver as respostas da chamada de API. A resposta getAccountPasswordPolicy descreve os requisitos de complexidade e os períodos de rotação obrigatórios para as senhas de usuário em sua conta. Você pode usar esta resposta de API como evidência para mostrar que você tem políticas de controle de acesso a senhas suficientes para aqueles Contas da AWS no escopo de sua avaliação. Se quiser, você também pode fornecer comentários adicionais sobre essas políticas adicionando um comentário ao controle.

Quando estiver satisfeito com o fato de que as políticas de senhas das entidades principais do AIM estão alinhadas com o controle personalizado, você poderá marcar o controle como Analisado e adicionar as evidências ao seu relatório de avaliação. Em seguida, você pode compartilhar esse relatório com os auditores para demonstrar que o controle está funcionando conforme o esperado.

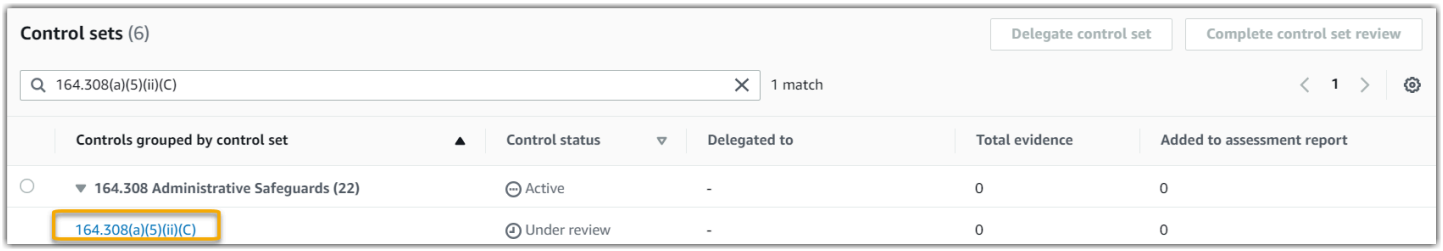
Controles automatizados que usam AWS CloudTrail como tipo de fonte de dados

Este exemplo mostra um controle que usa AWS CloudTrail como tipo de fonte de dados. Esse é um controle padrão retirado do Framework da HIPPA. O Audit Manager usa esse controle para gerar evidências que podem ajudar a alinhar o ambiente da AWS aos requisitos da HIPPA.

Exemplo de detalhes de controle

- Nome do controle — `164.308(a)(5)(ii)(C)`
- Conjunto de controles: esse controle pertence ao conjunto de controles chamado`164.308 Administrative Safeguards`.
- Tipo de fonte de dados:AWS CloudTrail
- Tipo de evidência: atividade do usuário

Aqui esse controle é mostrado em uma avaliação do Audit Manager criada a partir do framework HIPAA:



A avaliação mostra o status do controle. Também mostra o volume evidência coletado para esse controle até o momento e volume de evidência incluso em seu relatório de avaliação. A partir daqui, você pode delegar a análise do conjunto de controles ou conclui-la você mesmo. A escolha do nome do controle abre uma página de detalhes com mais informações, incluindo as evidências desse controle.

O que esse controle faz

Esse controle requer um procedimento de monitoramento para detectar logins inadequados. Um exemplo de login inadequado ocorre quando alguém insere várias combinações de nomes de usuário ou senhas para tentar acessar um sistema de informações. O Audit Manager ajuda você a validar esse controle fornecendo uma lista de todas as tentativas de login detectadas para os atributos no escopo de sua avaliação.

Como o Audit Manager coleta evidências para esse controle

O Audit Manager executa as seguintes etapas para coletar evidências para esse controle:

1. Para cada controle, o Audit Manager avalia seus atributos dentro do escopo usando a fonte de dados especificada nas configurações de controle. Nesse caso, seus usuários são o atributo e o CloudTrail é o tipo de fonte de dados. O Audit Manager procura o resultado de todos os eventos de login do AWS Management Console que são registrados pelo CloudTrail. Em seguida, ele retorna um log dos eventos relevantes que estão dentro do escopo de sua avaliação.
2. O resultado da avaliação dos atributos é salvo e convertido em evidências amigáveis ao auditor. O Audit Manager gera evidências da atividade do usuário para controles que usam o CloudTrail como um tipo de fonte de dados. Essa evidência contém os dados originais que são capturados dos usuários e metadados adicionais que indicam quais controles os dados suportam.
3. O Audit Manager anexa a evidência salva ao controle denominado `164.308(a)(5)(ii)(C)` em sua avaliação.

Como você pode usar o Audit Manager para demonstrar conformidade com esse controle

Depois que a evidência é anexada ao controle, você ou um representante de sua escolha podem analisar a evidência para checar se é necessária alguma remediação.

Neste exemplo, você pode analisar as evidências para ver os eventos de login que foram logados pelo CloudTrail. Esse log descreve a atividade de login do console para seus usuários, que inclui as seguintes informações:

- Cada login bem-sucedido
- Cada tentativa de login sem êxito
- Verificação de autenticação multifator (MFA) aplicada
- O endereço IP de cada evento de login

Você pode usar esse log como evidência para mostrar que você tem procedimentos de monitoramento suficientes para aqueles Contas da AWS que estão no escopo de sua avaliação. Se quiser, você também pode fornecer comentários adicionais sobre essas políticas adicionando um comentário ao controle. Por exemplo, se o log mostrar alguma discrepância, como várias tentativas malsucedidas de login, você pode adicionar um comentário que descreva como você corrigiu o problema. O monitoramento regular dos logins do console ajuda a evitar problemas de segurança

que podem surgir a partir de discrepâncias e tentativas inadequadas de login. Por sua vez, essa prática recomendada ajuda a alinhar seu ambiente AWS aos requisitos da HIPAA.

Quando estiver satisfeito com o fato de que seu procedimento de monitoramento está alinhado com o controle, você poderá marcar o controle como Analisado e adicionar as evidências ao seu relatório de avaliação. Em seguida, você pode compartilhar esse relatório com os auditores para demonstrar que o controle está funcionando conforme o esperado.

Controles manuais

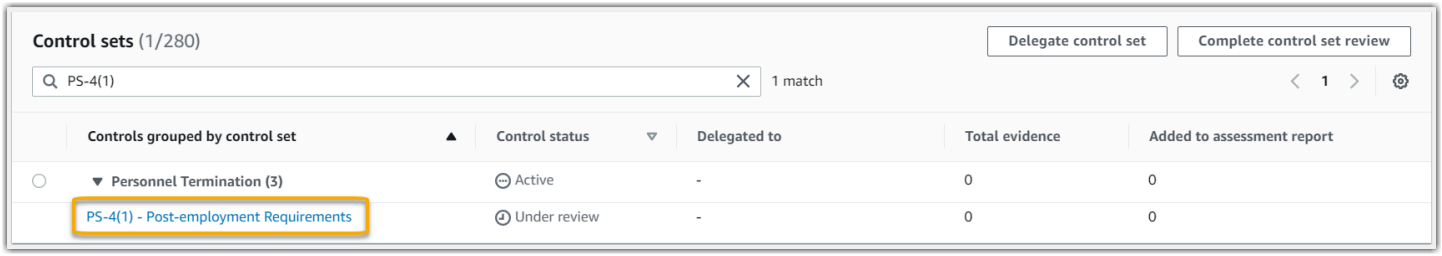
Alguns controles não oferecem suporte à coleta automatizada de evidências. Isso inclui controles que dependem do fornecimento de registros físicos e assinaturas, além de observações, entrevistas e outros eventos não gerados na nuvem. Nesses casos, você pode carregar manualmente evidências para demonstrar que está satisfazendo os requisitos do controle.

Este exemplo mostra um controle manual para o qual o Audit Manager não coleta evidências automatizadas. Esse é um controle padrão retirado do Framework NIST 800-53 (Rev. 5). Você pode usar o Audit Manager para carregar e armazenar evidências que demonstrem a conformidade com esse controle.

Exemplo de detalhes de controle

- Nome do controle — `PS-4(1) - Post-employment Requirements`
- Conjunto de controles — esse controle pertence ao conjunto de controles `Personnel Termination`. Esse é um agrupamento de controles relacionado à segurança da informação, no contexto dos procedimentos de rescisão do contrato de trabalho.
- Tipo de fonte de dados – Manual
- Tipo de evidência – Manual

Aqui, o controle mostrado em uma avaliação do Audit Manager criada a partir do framework NIST 800-53 (Rev. 5) Baixo-Moderado-Alto:



A avaliação mostra o status do controle. Também mostra o volume evidência coletado para esse controle até o momento e volume de evidência incluso em seu relatório de avaliação. A partir daqui, você pode delegar a análise do conjunto de controles ou conclui-la você mesmo. A escolha do nome do controle abre uma página de detalhes com mais informações, incluindo as evidências desse controle.

O que esse controle faz

Você pode usar esse controle para confirmar que está protegendo as informações organizacionais caso um funcionário seja demitido. Especificamente, você pode demonstrar que notifica consistentemente os indivíduos demitidos sobre os requisitos pós-emprego aplicáveis e juridicamente vinculativos para a proteção das informações organizacionais. Além disso, você pode demonstrar que todos os indivíduos demitidos assinaram uma confirmação dos requisitos pós-emprego como parte do processo de rescisão de sua organização.

Como você pode carregar manualmente evidências para esse controle

Você pode adotar as seguintes etapas para carregar manualmente evidências que suportem esse controle:

1. Coloque a evidência manual que deseja carregar em um bucket do Amazon Simple Storage Service (S3) e anote o URI do S3.
2. Em sua avaliação do Audit Manager, abra o controle, vá até a guia de pastas de evidências e carregue as evidências inserindo o URI do S3. Para obter instruções, consulte Carregando evidências manuais em AWS Audit Manager.
3. O Audit Manager criará uma pasta de evidências com o nome da data na qual você carregou a evidência. O Audit Manager anexa a evidência carregada ao controle denominado `PS-4(1) - Post-employment Requirements` em sua avaliação.

Como você pode usar o Audit Manager para demonstrar conformidade com esse controle

Se você tiver documentação que suporte esse controle, poderá carregá-la como evidência manual. Por exemplo, você pode carregar a cópia mais recente dos requisitos pós-emprego juridicamente vinculativos que seu departamento de Recursos Humanos emitiu aos funcionários demitidos. Se alguma pessoa foi demitida durante o período de auditoria, você também pode carregar cópias datadas endereçadas a essas pessoas demitidas.

Assim como nos controles automatizados, você pode delegar controles manuais às partes interessadas para ajudá-lo a analisar as evidências (ou, nesse caso, fornecê-las). Por exemplo, ao

analisar esse controle, você percebe que ele atende apenas parcialmente aos requisitos. Esse pode ser o caso se você não tiver uma carta de confirmação assinada por uma pessoa demitida. Você pode delegar o controle a uma parte interessada do RH, que pode, então, carregar uma cópia da carta assinada. Ou, se nenhum funcionário foi demitido durante o período de auditoria, você pode deixar um comentário informando por que nenhuma carta assinada foi anexada ao controle.

Quando estiver satisfeito com o fato de que você está alinhado com o controle, você poderá marcar o controle como Analisado e adicionar as evidências ao seu relatório de avaliação. Em seguida, você pode compartilhar esse relatório com os auditores para demonstrar que o controle está funcionando conforme o esperado.

Controles com tipos de fonte de dados mistos (automatizados e manuais)

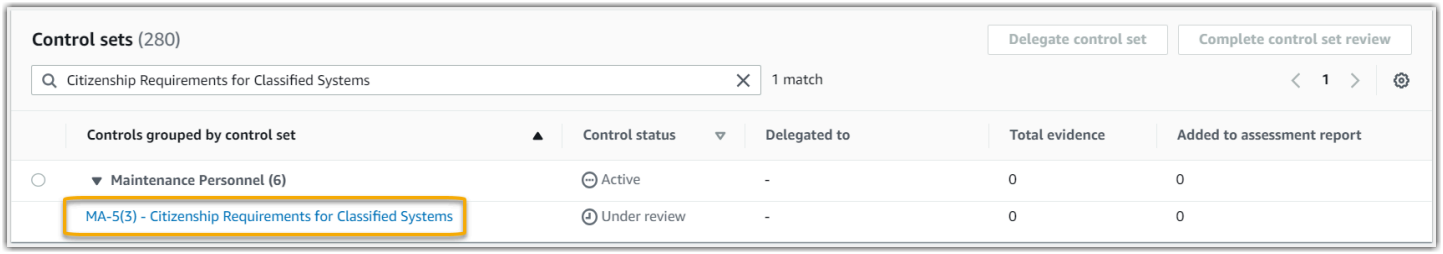
Em muitos casos, é necessária uma combinação de evidências automatizadas e manuais para satisfazer um controle. Embora o Audit Manager possa fornecer evidências automatizadas relevantes para o controle, talvez seja necessário complementar esses dados com evidências manuais que você mesmo identifique e carregue.

Este exemplo mostra um controle que usa uma combinação de evidências manuais e automatizadas provenientes de chamadas de API da AWS. Esse é um controle padrão retirado do Framework NIST 800-53 (Rev. 5). O Audit Manager usa esse controle para gerar evidências que podem ajudar a alinhar o ambiente da AWS aos requisitos NIST.

Exemplo de detalhes de controle

- Nome do controle — `MA-5(3) - Citizenship Requirements for Classified Systems`
- Conjunto de controles — esse controle pertence ao conjunto de controles `Maintenance Personnel`. Esse é um agrupamento de controles relacionados aos indivíduos que realizam manutenção de hardware ou software em sistemas organizacionais.
- Tipo de fonte de dados: chamadas de API AWS, além de evidências manuais complementares
- Tipo de evidência – dados de configuração

Aqui, esse controle mostrado em uma avaliação do Audit Manager foi criado a partir do framework Baixa-Moderada-Alta do NIST 800-53 (Rev. 5):



A avaliação mostra o status do controle. Também mostra o volume evidência coletado para esse controle até o momento e volume de evidência incluso em seu relatório de avaliação. A partir daqui, você pode delegar a análise do conjunto de controles ou conclui-la você mesmo. A escolha do nome do controle abre uma página de detalhes com mais informações, incluindo as evidências desse controle.

O que esse controle faz

O Audit Manager pode usar esse controle para ajudá-lo a garantir que o pessoal que realiza suas atividades de manutenção e diagnóstico tenha o status de cidadania exigido. Se seu sistema processa, armazena ou transmite informações confidenciais, você deve demonstrar que sua equipe de manutenção é cidadã dos EUA. O Audit Manager ajuda você a validar isso. Ele faz isso retornando uma lista completa de todas as políticas do IAM e princípios no escopo de sua avaliação. Em seguida, você pode verificar e demonstrar que essa lista de usuários tem os requisitos de cidadania necessários. Você pode fazer isso carregando manualmente evidências complementares de seus status de cidadania.

Como o Audit Manager coleta evidências para esse controle

O Audit Manager executa as seguintes etapas para coletar evidências para esse controle:

1. Para cada controle, o Audit Manager avalia seus atributos dentro do escopo usando a fonte de dados especificada nas configurações de controle. Nesse caso, suas políticas e diretores do IAM são os atributos e as chamadas de API AWS são o tipo de fonte de dados. O Audit Manager procura o resultado de quatro chamadas específicas da API do IAM (ListUsers/ListRoles/ListGroups/ListPolicies) e retorna uma lista das políticas e princípios do IAM que estiverem no escopo da sua avaliação.
2. O resultado da avaliação dos atributos é salvo e convertido em evidências amigáveis ao auditor. O Audit Manager gera evidências de dados de configuração para controles que usem chamadas de API como fonte de dados. Essa evidência contém os dados originais capturados das respostas da API e metadados adicionais, que indicam quais controles os dados suportam.

3. O Audit Manager anexa a evidência salva ao controle denominado `MA-5(3) - Citizenship Requirements for Classified Systems` em sua avaliação.

Como você pode carregar manualmente evidências para esse controle

Você pode adotar as seguintes etapas para carregar evidências manuais que suplementem as evidências automatizadas:

1. Coloque a documentação da cidadania em um bucket do Amazon Simple Storage Service (Amazon S3) e anote o URI do S3.
2. Em sua avaliação do Audit Manager, abra o controle, vá até a guia de pastas de evidências e carregue as evidências. Você faz isso inserindo o URI do S3. Para obter instruções, consulte Adicionando evidências manuais em AWS Audit Manager.
3. O Audit Manager anexa a evidência carregada ao controle denominado `MA-5(3) - Citizenship Requirements for Classified Systems` em sua avaliação.

Como você pode usar o Audit Manager para demonstrar conformidade com esse controle

Depois que a evidência é anexada ao controle, você ou um representante de sua escolha podem analisar a evidência para checar se é necessária alguma remediação.

Neste exemplo, você pode analisar as evidências e ver uma lista de 20 usuários. Se você não tiver certeza de como identificar quais usuários são funcionários de manutenção ou a cidadania desses usuários, pode delegar o controle a um especialista no assunto para validação. O delegado pode confirmar a lista do pessoal de manutenção e carregar evidências suplementares manualmente como documentação de seus status de cidadania. Confirmar a cidadania de todos os usuários relevantes listados ajuda a alinhar seu ambiente da AWS aos requisitos do NIST. Como alternativa, se seu sistema não processar, armazenar ou transmitir informações confidenciais, você pode deixar um comentário informando porque esse controle não é aplicável.

Quando estiver satisfeito com seu alinhamento com o controle, você poderá marcar o controle como Analisado e adicionar as evidências ao seu relatório de avaliação. Em seguida, você pode compartilhar esse relatório com os auditores para demonstrar que o controle está funcionando conforme o esperado.

Integrações com serviços relacionados Serviços da AWS

AWS Audit Manager se integra a vários Serviços da AWS para coletar automaticamente evidências que você pode incluir em seus relatórios de avaliação.

AWS Security Hub

AWS Security Hub monitora seu ambiente usando verificações de segurança automatizadas baseadas nas práticas recomendadas da AWS e nos padrões do setor. O Audit Manager captura telas de sua postura de segurança de atributos relatando os resultados das verificações de segurança diretamente do Security Hub. Para obter mais informações sobre o Security Hub, consulte O que é AWS Security Hub? no Guia do Usuário do AWS Security Hub.

AWS CloudTrail

AWS CloudTrail ajuda você a monitorar as chamadas feitas para atributos AWS da sua conta. Estas incluem chamadas feitas pelo Management Console do AWS, pela CLI do AWS e outros Serviços da AWS. O Audit Manager coleta dados de log diretamente do CloudTrail e converte os logs processados em evidências de atividades do usuário. Para obter mais informações sobre o CloudTrail, consulte O que é AWS CloudTrail? no Guia do Usuário do AWS CloudTrail.

AWS Config

AWS Config fornece uma visão detalhada da configuração dos atributos da AWS em sua Conta da AWS. Isto inclui informações sobre como os atributos estão relacionados entre si e como eles foram configurados no passado. O Audit Manager captura telas da sua postura de segurança de atributos relatando as descobertas do AWS Config. Para obter mais informações sobre o AWS Config, consulte O que é AWS Config? no AWS Config Guia do Usuário.

AWS License Manager

O AWS License Manager simplifica o processo de transferir as licenças de fornecedor de software para a nuvem. À medida que você desenvolve a infraestrutura da nuvem em AWS, é possível reduzir custos redefinindo o inventário de sua licença existente para uso com atributos de nuvem. O Audit Manager fornece um framework no License Manager para ajudá-lo na preparação da sua auditoria. Este framework é integrado ao License Manager para agregar informações de uso da licença com base nas regras de licenciamento definidas pelo cliente. Para obter mais informações sobre o License Manager, consulte O que é AWS License Manager? no Guia do Usuário do AWS License Manager.

AWS Control Tower

AWS Control Tower impõe proteções investigativas preventivas e de detecção para a infraestrutura em nuvem. O Audit Manager fornece um framework de proteção AWS Control Tower para ajudá-lo na preparação da auditoria. Este framework contém todas as regras de AWS Config baseadas nas proteções do AWS Control Tower. Para obter mais informações sobre o AWS Control Tower, consulte O que é AWS Control Tower? no Guia do Usuário doAWS Control Tower.

AWS Artifact

AWS Artifact é um portal de recuperação de artefatos de auditoria de autoatendimento que fornece acesso sob demanda à documentação de conformidade e às certificações da infraestrutura AWS. AWS Artifact oferece evidências para provar que a infraestrutura de nuvem AWS atende aos requisitos de conformidade. Por outro lado, AWS Audit Manager ajuda você a coletar, analisar e gerenciar evidências, para demonstrar que seu uso do Serviços da AWS está em conformidade. Para obter mais informações sobre o AWS Artifact, consulte O que é AWS Artifact? no Guia do Usuário doAWS Artifact. Você pode baixar uma lista de relatórios da AWS no AWS Management Console.

Para obter uma lista dos Serviços da AWS no escopo de programas de conformidade específicos, consulte Serviços da AWS no Escopo por programa de conformidade. Para obter informações gerais, consulte Programas de conformidade da AWS.

Integrações com produtos GRC de terceiros.

AWS Audit Manager oferece suporte a integrações com os produtos GRC de parceiros terceirizados listados nesta página.

Se sua empresa usa um modelo de nuvem híbrida ou multicloud, é provável que você use um produto GRC para gerenciar evidências desses ambientes. Quando esse produto for integrado ao Audit Manager, você poderá obter evidências sobre seu uso da AWS diretamente em seu ambiente GRC. Isso simplifica a forma como você gerencia a conformidade fornecendo um local centralizado para analisar e corrigir evidências, enquanto prepara para as auditorias.

Leia esta página para obter uma visão geral dos produtos GRC de terceiros que podem consumir evidências do Audit Manager. Você também pode ver uma referência de quais ações da API do Audit Manager você pode realizar diretamente nesses produtos.

Tópicos

- Saiba como como as integrações de terceiros funcionam com o Audit Manager

- Produtos parceiros de GRC de terceiros que se integram ao Audit Manager

Saiba como como as integrações de terceiros funcionam com o Audit Manager

Os parceiros GRC podem usar as APIs públicas para integrar seus produtos ao Audit Manager. Com essa integração implementada, você pode mapear os controles corporativos em seu ambiente GRC de acordo com os controles fornecidos pelo Audit Manager.

Depois de concluir esse exercício único de mapeamento de controle, você pode criar avaliações do Audit Manager diretamente no produto GRC. Essa ação inicia a coleta de evidências sobre seu uso da AWS. Você pode então ver essa evidência da AWS junto com as outras evidências coletadas de seu ambiente híbrido, tudo dentro do mesmo contexto dos controles corporativos.

Ao usar uma integração do Audit Manager com um produto de GRC de terceiros, lembre-se dos seguintes pontos:

- As integrações estão disponíveis para todas as Regiões da AWS onde o Audit Manager for suportado.
- Todos os atributos que você criar no produto parceiro GRC também serão refletidos no Audit Manager.
- Você está sujeito à precificação da AWS Audit Manager, além doa precificação do produto GRC de terceiros.
- As evidências que o Audit Manager coleta são imutáveis. As evidências são apresentadas exatamente da mesma forma em produtos GRC de terceiros e no console do Audit Manager. No entanto, se você usar uma integração de terceiros, poderá aprimorar essas evidências fornecendo contexto adicional em seus relatórios.
- As mesmas cotas que se aplicam ao Audit Manager também se aplicam ao produto GRC de terceiros. Por exemplo, cada Conta da AWS pode ter até 100 avaliações ativas do Audit Manager. Essa cota em nível de conta se aplica caso você crie as avaliações no console do Audit Manager ou no produto GRC de terceiros. Grande parte das cotas do Audit Manager, mas não todas, estão listadas no AWS Audit Manager namespace do console do Service Quotas. Para saber mais sobre como solicitar um aumento da cota, consulte Gerenciando suas cotas Audit Manager.

Se você tem uma solução de conformidade e está interessado em integrá-la com o Audit Manager, envie um e-mail para `auditmanager-partners@amazon.com`.

Produtos parceiros de GRC de terceiros que se integram ao Audit Manager

Os seguintes produtos GRC de terceiros podem consumir evidências do Audit Manager.

MetricStream

Para usar essa integração, entre em contato com a MetricStream para acessar e comprar o software MetricStream GRC.

Construída na plataforma MetricStream, a solução MetricStream Enterprise GRC permite uma abordagem abrangente e colaborativa das atividades e processos de GRC em toda a empresa. Ao ingerir evidências do Audit Manager no MetricStream, você pode identificar proativamente as evidências em não conformidade do seu ambiente da AWS e analisá-las junto com as evidências de suas fontes de dados on-premises ou de outros parceiros de nuvem. Isso fornece uma maneira conveniente e centralizada de analisar e melhorar sua segurança da nuvem e postura de conformidade ao se preparar para as auditorias.

Com a integração do MetricStream e do Audit Manager, você pode realizar as seguintes operações de API.

Tarefa	Operação de API
Configurando a integração do Audit Manager	• GetAccountStatus • GetOrganizationAdminAccount • GetSettings
Analisando os atributos do Audit Manager	• GetAssessment • GetAssessmentFramework • GetControl • ListAssessmentFrameworks • ListControls
Criando atributos do Audit Manager	• CreateAssessment • CreateAssessmentFramework
Atualizando atributos do Audit Manager	• UpdateAssessment • UpdateAssessmentControl

Tarefa	Operação de API
	• UpdateAssessmentStatus
Gerenciando evidências	• StartQuery (API AWS CloudTrail) • GetQueryResults (API AWS CloudTrail)
Excluindo atributos do Audit Manager	• DeleteAssessmentFramework

Links relacionados ao MetricStream

- AWS Marketplace link
- Link do produto
- Precificação do produto

Usando o Audit Manager com um SDK AWS

Os kits de desenvolvimento de software (software development kits, ou SDKs) AWS estão disponíveis em muitas linguagens de programação populares. Cada SDK fornece uma API, exemplos de código e documentação que os desenvolvedores podem usar para construir aplicativos em seu idioma preferido.

Documentação do SDK	Documentação específica do Audit Manager	Exemplos de código	
AWS SDK for C++	Referência de API AWS SDK for C++ para Audit Manager	Exemplos de código do AWS SDK for C++	
AWS SDK for Go	Referência de API AWS SDK for Go para Audit Manager	Exemplos de código do AWS SDK for Go	
AWS SDK for Java	Referência de API AWS SDK for Java 2.x para Audit Manager	Exemplos de código do AWS SDK for Java	

Documentação do SDK	Documentação específica do Audit Manager	Exemplos de código
AWS SDK for JavaScript	Referência de API AWS SDK for JavaScript para Audit Manager	Exemplos de código do AWS SDK for JavaScript
AWS SDK for .NET	Referência de API AWS SDK for .NET para Audit Manager	Exemplos de código do AWS SDK for .NET
AWS SDK for PHP	Referência de API AWS SDK for PHP para Audit Manager	Exemplos de código do AWS SDK for PHP
AWS SDK for Python (Boto3)	Referência de API AWS SDK for Python (Boto) para Audit Manager	Exemplos de código do AWS SDK for Python (Boto3)
AWS SDK for Ruby	Referência de API AWS SDK for Ruby para Audit Manager	Exemplos de código do AWS SDK for Ruby

Para exemplos específicos do Audit Manager, consulte Exemplos de código para AWS Audit Manager.

> **Note**
>
> O Audit Manager está disponível no botocore versão 1.19.32 e posterior para o AWS SDK for Python (Boto3). Antes de começar a usar o SDK, certifique-se de usar a versão adequada do botocore.

Configurar o AWS Audit Manager

Antes de começar a usar o Audit Manager, certifique-se de ter concluído as seguintes tarefas de configuração.

Tópicos

- Pré-requisitos: criar um Conta da AWS e configurar permissões
- Habilitar o Audit Manager: usar o console, o AWS CLI, ou a API para habilitar o Audit Manager
- Recomendações: configurar integrações recomendadas com outros Serviços da AWS

Pré-requisitos

Siga estas etapas para criar um Conta da AWS e um usuário administrativo com privilégios de configuração do Audit Manager.

Etapas

- Inscrever-se para uma Conta da AWS
- Crie um usuário administrador
- Adicionar as permissões necessárias para acessar e habilitar o Audit Manager

> **Important**
>
> Se você já estiver configurado com AWS e IAM, você poderá ignorar as etapas 1 e 2. No entanto, você deve concluir a etapa 3 para garantir que possui as permissões necessárias para configurar o Audit Manager.

Inscrever-se para uma Conta da AWS

Se você ainda não tem uma Conta da AWS, siga as etapas a seguir para criar uma.

Para se cadastrar em uma 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 cadastra em uma Conta da AWS, um Usuário raiz da conta da AWS é criado. O usuário raiz tem acesso a todos os Serviços da AWS e recursos na conta. Como prática recomendada de segurança, atribua acesso administrativo a um usuário administrativo e use somente o usuário raiz para realizar as tarefas que exigem acesso do usuário raiz.

A AWS envia um e-mail de confirmação depois que o processo de cadastramento é concluído. A qualquer momento, é possível visualizar as atividades da conta atual e gerenciar sua conta acessando https://aws.amazon.com/ e selecionando Minha conta.

Crie um usuário administrador

Depois de se cadastrar em uma Conta da AWS, proteja seu Usuário raiz da conta da AWS, habilite o AWS IAM Identity Center e crie um usuário administrativo para não usar o usuário raiz em tarefas cotidianas.

Proteger seu Usuário raiz da conta da AWS

1. Faça login no AWS Management Console como o proprietário da conta ao escolher a opção Usuário raiz e inserir o endereço de e-mail da Conta da AWS. Na próxima página, digite sua senha.

   Para obter ajuda ao fazer login usando o usuário raiz, consulte Fazer login como usuário raiz no Guia do usuário do Início de Sessão da AWS.
2. Ative a autenticação multifator (MFA) para o usuário raiz.c

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

Criar um usuário administrativo

1. Habilitar o IAM Identity Center.

   Para obter instruções, consulte Enabling AWS IAM Identity Center no AWS IAM Identity Center User Guide.
2. No Centro de Identidade do IAM, atribua acesso administrativo a um usuário administrativo.

Para obter um tutorial sobre como usar o Diretório do Centro de Identidade do IAM como fonte de identidade, consulte Configure user access with the default Diretório do Centro de Identidade do IAM no AWS IAM Identity Center User Guide.

Login como usuário 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 com o login utilizando um usuário do Centro de Identidade do IAM, consulte Fazer login no portal de acesso da AWS, no Guia do usuário do Início de Sessão da AWS.

Adicionar as permissões necessárias para acessar e habilitar o Audit Manager

É necessário conceder aos usuários as permissões necessárias para habilitar o Audit Manager. Para usuários que precisam de acesso total ao Audit Manager, use a política gerenciada AWSauditManagerAdministratorAccess. Essa é uma política gerenciadaAWS que está disponível no seu Conta da AWS, e é a política recomendada para administradores do Audit Manager.

> **Tip**
>
> Como uma prática recomendada de segurança, recomendamos que você comece com políticas gerenciadas AWS e depois passe para as permissões de privilégios mínimos. Políticas gerenciadas AWS concedem permissões para vários casos de uso comuns. Lembre-se de que, como as políticas gerenciadas AWS estão disponíveis para uso por todos os clientes AWS, elas podem não conceder permissões de privilégio mínimo para seus casos de uso específicos. Como resultado, recomendamos que você reduza ainda mais as permissões definindo as políticas gerenciadas pelo cliente específicas para seus casos de uso. Para obter mais informações, consulte políticas gerenciadas AWS no Guia do Usuário AWS Identity and Access Management.

Para fornecer acesso, adicione as permissões aos seus usuários, grupos ou perfis:

- Usuários e grupos no AWS IAM Identity Center:

Crie um conjunto de permissões. Siga as instruções em Create a permission set (Criação de um conjunto de permissões) no Guia do usuário do AWS IAM Identity Center.

- Usuários gerenciados no IAM com provedor de identidades:

  Crie um perfil para a federação de identidades. Siga as instruções em Criar um perfil para um provedor de identidades de terceiros (federação) no Guia do usuário do IAM.

- Usuários do IAM:
  - Crie um perfil que seu usuário possa assumir. Siga as instruções em Creating a role for an IAM user (Criação de um perfil para um usuário do IAM) no Guia do usuário do IAM.
  - (Não recomendado) Vincule uma política diretamente a um usuário ou adicione um usuário a um grupo de usuários. Siga as instruções em Adicionando permissões a um usuário (console) no Guia do Usuário do IAM.

Habilitar AWS Audit Manager

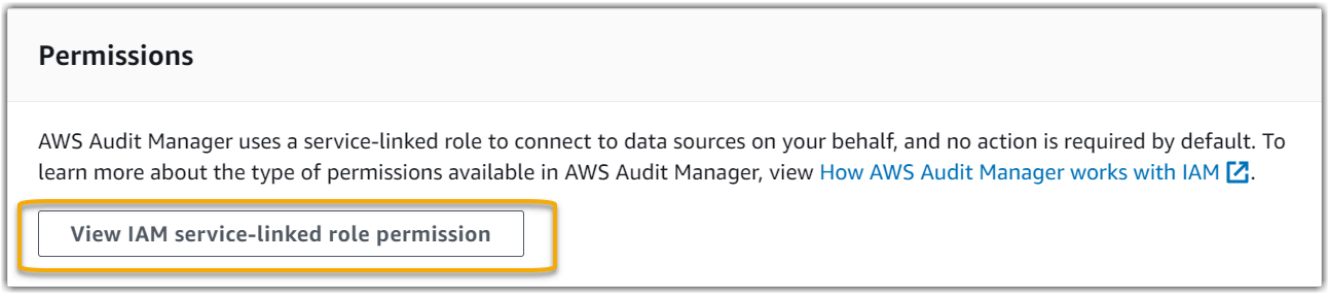
Você pode habilitar o Audit Manager usando o AWS Management Console, a API do Audit Manager ou o AWS Command Line Interface (AWS CLI).

Audit Manager console

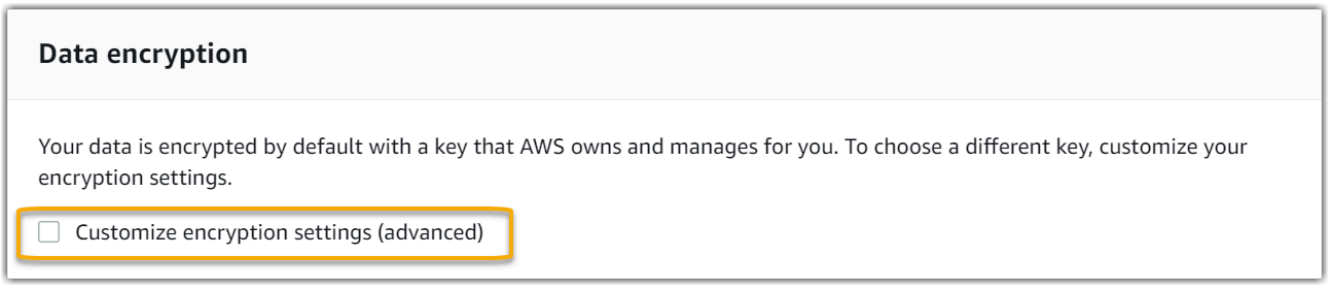
Para habilitar o Audit Manager usando o console

1. Abra o console do AWS Audit Manager em https://console.aws.amazon.com/auditmanager/home.
2. Use as credenciais da sua identidade do IAM para fazer login.
3. Escolha Configurar AWS Audit Manager.

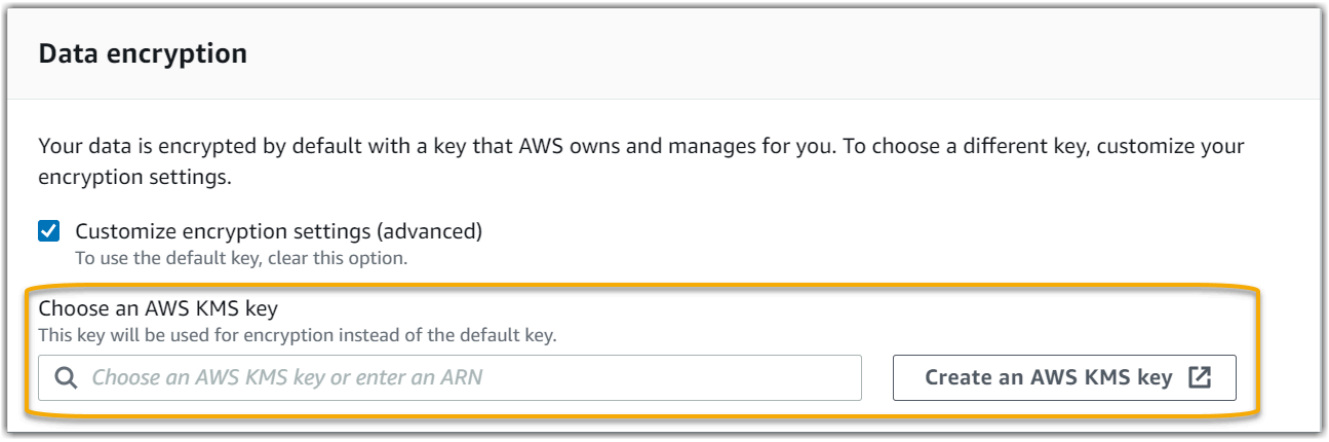
4. Em Permissões, nenhuma ação é necessária. Isso ocorre porque o Audit Manager usa uma função vinculada a serviço para se conectar às fontes de dados em seu nome. Você pode analisar a função vinculada a serviço escolhendo a permissão Exibir perfil vinculado ao serviço do IAM.



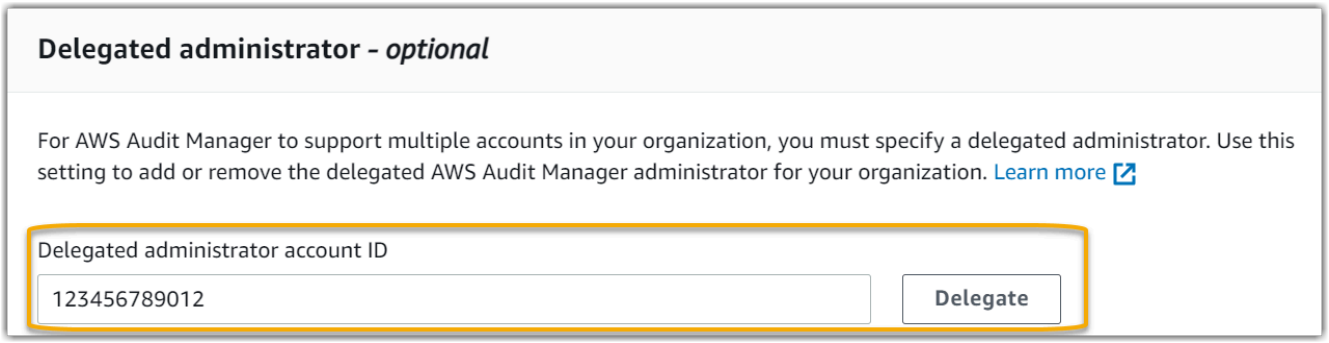
5. Em Criptografia de dados, a opção padrão é para o Audit Manager criar e gerenciar um AWS KMS key para armazenar seus dados com segurança.



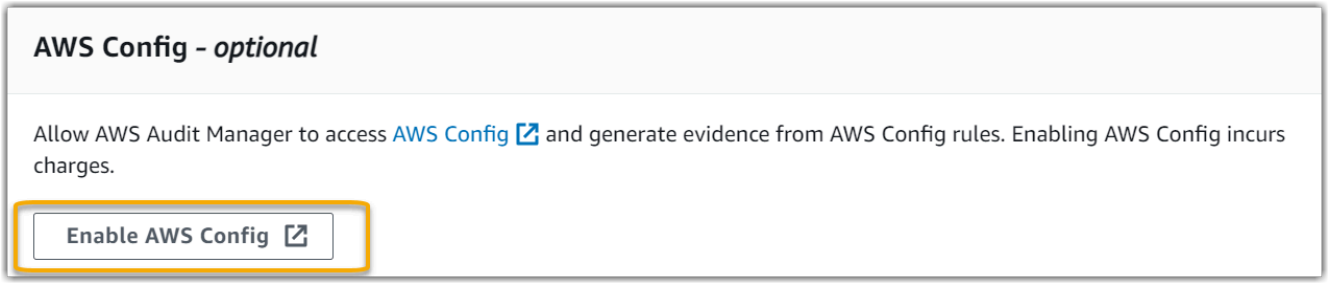
Se você quiser usar sua própria chave gerenciada pelo cliente para criptografar dados no Audit Manager, marque a caixa de seleção ao lado de Personalizar configurações de criptografia (avançado). É possível escolher uma chave KMS existente ou criar uma nova.



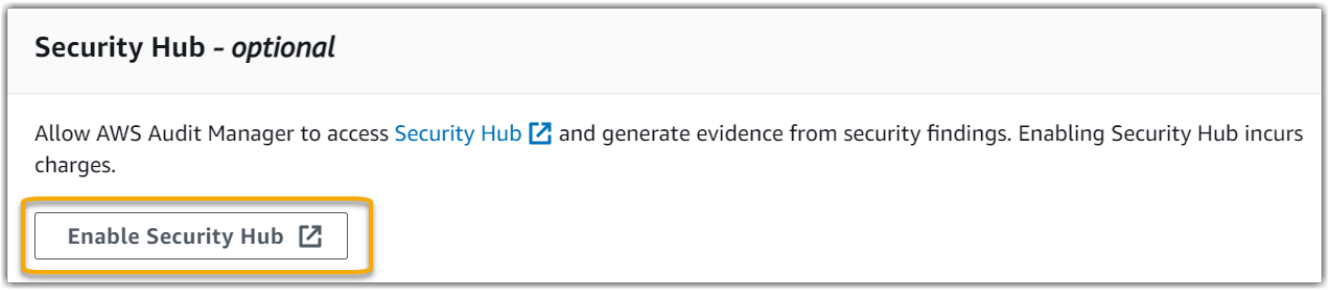
6. (Opcional) Em Administrador delegado - opcional, você pode especificar uma conta de administrador delegado se quiser que o Audit Manager execute avaliações para várias contas. Para obter mais informações e recomendações, consulte Habilitar e configurar AWS Organizations para uso com o Audit Manager.



7. (Opcional) Em AWS Config— opcional, recomendamos que você habilite AWS Config para uma experiência ideal. Isso permite que o Audit Manager gere evidências usando regras AWS Config. Para obter instruções e configurações recomendadas, consulte Habilitar e configurar AWS Config para uso com o Audit Manager.



8. (Opcional) Em Security Hub — opcional, recomendamos que você habilite o Security Hub para uma experiência ideal. Isso permite que o Audit Manager gere evidências usando as verificações do Security Hub. Para obter instruções e configurações recomendadas, consulte Habilitar e configurar AWS Security Hub para uso com o Audit Manager.



9. Escolha Concluir configuração para concluir o processo de configuração.

AWS CLI

Para habilitar o Audit Manager usando o AWS CLI

Na linha de comando, execute o comando register-account usando os seguintes parâmetros de configuração:

- `--kms-key` (opcional) — Use esse parâmetro para criptografar os dados do Audit Manager usando sua própria chave gerenciada pelo cliente. Se você não especificar uma opção aqui, o Audit Manager criará e gerenciará uma AWS KMS key em seu nome para o armazenamento seguro de seus dados.
- `--delegated-admin-account` (opcional) — Use esse parâmetro para designar a conta de administrador delegado da sua organização para o Audit Manager. Se você não especificar uma opção aqui, nenhum administrador delegado será registrado.

Exemplo de entrada (substitua o *texto do espaço reservado* por suas próprias informações):

```
aws auditmanager register-account \
--kms-key arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab \
--delegated-admin-account 111122224444
```

Exemplo de saída:

```
{
    "status": "ACTIVE"
}
```

Para obter mais informações sobre a AWS CLI e instruções sobre como instalar as ferramentas AWS CLI, consulte a seção abaixo no Guia do usuário AWS Command Line Interface.

- Guia do Usuário da Interface de Linha de Comando AWS
- Começando com AWS Command Line Interface

Audit Manager API

Para habilitar o Audit Manager usando a API do Audit Manager

Use a operação RegisterAccount com os seguintes parâmetros de configuração:

- kmsKey (opcional) — Use esse parâmetro para criptografar os dados do Audit Manager usando sua própria chave gerenciada pelo cliente. Se você não especificar uma opção aqui, o Audit Manager criará e gerenciará uma AWS KMS key em seu nome para o armazenamento seguro de seus dados.
- delegatedAdminAccount (opcional) — Use esse parâmetro para especificar a conta de administrador delegado da sua organização para o Audit Manager. Se você não especificar um, nenhum administrador delegado será registrado.

Exemplo de entrada (substitua o *texto do espaço reservado* por suas próprias informações):

```
{
    "kmsKey":"arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "delegatedAdminAccount":"111122224444"
}
```

Exemplo de saída:

```
{
  "status": "ACTIVE"
}
```

Recomendações

Para uma experiência ideal no Audit Manager, recomendamos que você configure os seguintes atributos e habilite o seguinte Serviços da AWS.

Tópicos

- Configurar os atributos recomendados do Audit Manager
- Configure integrações recomendadas com outro Serviços da AWS

Configurar os atributos recomendados do Audit Manager

Depois de habilitar o Audit Manager, recomendamos que você habilite o atributo de localização de evidências.

Localizador de evidências fornece uma maneira poderosa de pesquisar evidências no Audit Manager. Em vez de navegar em pastas de evidências profundamente aninhadas para encontrar o que está procurando, você pode usar o localizador de evidências para consultar rapidamente suas evidências. Se usar o localizador de evidências como administrador delegado, poderá pesquisar evidências em todas as contas membros da sua organização. Ao usar uma combinação de filtros e agrupamentos, você pode restringir progressivamente o escopo da sua consulta de pesquisa. Por exemplo, se quiser uma visão de alto nível da integridade do sistema, faça uma pesquisa ampla e filtre por avaliação, intervalo de datas e conformidade de atributos. Se sua meta for remediar um atributo específico, você pode realizar uma pesquisa restrita para direcionar evidências de um controle ou ID de atributo específico. Depois de definir seus filtros, você pode agrupar e visualizar os resultados da correspondentes antes de criar um relatório de avaliação.

Para usar o localizador de evidências, você deve habilitar esse atributo nas configurações do Audit Manager. Para obter instruções, consulte Configurações do localizador de evidências.

Configure integrações recomendadas com outro Serviços da AWS

Para uma experiência ideal no Audit Manager, recomendamos fortemenete que habilite o seguinte Serviços da AWS:

- AWS Organizations — Você pode usar o Organizations para executar avaliações do Audit Manager em várias contas e consolidar evidências em uma conta de administrador delegado.
- AWS Security Hub e AWS Config — Quando você os ativa esses Serviços da AWS, eles podem ser usados como um tipo de fonte de dados para os controles em suas avaliações do Audit Manager. O Audit Manager pode então relatar os resultados das verificações de conformidade diretamente desses serviços.

Tópicos

Habilitar e configurar AWS Config (opcional)

Muitos controles no Audit Manager usam AWS Config como um tipo de fonte de dados. Para oferecer suporte a esses controles, você deve habilitar AWS Config em todas as contas em cada Região da AWS em que o Audit Manager estiver ativado. Se o Audit Manager tentar coletar evidências para controles que usam AWS Config como tipo de fonte de dados e as regras AWS Config relacionadas não estiverem habilitadas, nenhuma evidência será coletada para esses controles.

O Audit Manager não gerencia AWS Config para você. Você pode seguir estas etapas para habilitar AWS Config e definir suas configurações.

Tarefas para integrar AWS Config ao Audit Manager

- Etapa 1: habilitar AWS Config
- Etapa 2: Defina suas configurações AWS Config para uso com o Audit Manager

Etapa 1: habilitar AWS Config

É possível habilitar AWS Config usando o console AWS Config ou a API. Para obter instruções, consulte Conceitos básicos de AWS Config no Guia do Desenvolvedor do AWS Config.

Etapa 2: Defina suas configurações AWS Config para uso com o Audit Manager

> **Important**
>
> Habilitar AWS Config é uma recomendação opcional. No entanto, se você habilitar AWS Config, as seguintes configurações serão necessárias.

Depois de habilitar AWS Config, certifique-se de também habilitar as regras AWS Config ou implantar um pacote de conformidade para o padrão de conformidade relacionado à sua auditoria. Essa etapa garante que o Audit Manager possa importar descobertas para as regras AWS Config que você habilitou.

Depois de habilitar uma regra AWS Config, recomendamos analisar os parâmetros dessa regra. Em seguida, você deve validar esses parâmetros em relação aos requisitos do framework de conformidade escolhido. Se necessário, você pode atualizar os parâmetros de uma regra AWS

Config para garantir que ela esteja alinhada aos requisitos do framework. Isso ajudará a garantir que suas avaliações coletem as evidências corretas de verificação de conformidade para um determinado framework.

Por exemplo, suponha que você esteja criando uma avaliação para o CIS v1.2.0. Esse framework tem um controle chamado 1.4 — Garanta que as chaves de acesso sejam alternadas a cada 90 dias ou menos. Em AWS Config, a regra de alternância da chave de acesso tem um parâmetro `maxAccessKeyAge` com um valor padrão de 90 dias. Como resultado, a regra se alinha aos requisitos de controle. Se você não estiver usando o valor padrão, verifique se o valor que está usando é igual ou maior que o requisito de 90 dias do CIS v1.2.0.

Você pode encontrar os detalhes do parâmetro padrão para cada regra gerenciada na documentação AWS Config. Para obter instruções sobre como configurar uma regra, consulte Como trabalhar com regras gerenciadas AWS Config.

Habilitar e configurar AWS Security Hub (opcional)

Muitos controles no Audit Manager usam o Security Hub como um tipo de fonte de dados. Para oferecer suporte a esses controles, você deve habilitar o Security Hub em todas as contas em cada região onde o Audit Manager estiver habilitado. Se o Audit Manager tentar coletar evidências para controles que usem o Security Hub como um tipo de fonte de dados e os padrões relacionados não estiverem habilitados, nenhuma evidência será coletada para esses controles.

O Audit Manager não gerencia o Security Hub para você. Você pode seguir estas etapas para habilitar o Security Hub e definir suas configurações.

Tarefas para integrar AWS Security Hub ao Audit Manager

- Etapa 1: habilitar AWS Security Hub
- Etapa 2: Definir as configurações do Security Hub para uso com o Audit Manager

Etapa 1: habilitar AWS Security Hub

É possível habilitar o Security Hub usando o console ou a API. Para obter instruções, consulte Configurando AWS Security Hub no Guia do Usuário AWS Security Hub.

Etapa 2: Definir as configurações do Security Hub para uso com o Audit Manager

> **Important**
>
> Habilitar o Security Hub é uma recomendação opcional. No entanto, se habilitar o Security Hub, as seguintes configurações serão necessárias.

Depois de habilitar o Security Hub, certifique-se de também fazer o seguinte:

- Habilitar AWS Config e configurar a gravação de atributos - O Security Hub usa regras AWS Config vinculadas a serviços para realizar a maioria das verificações de segurança dos controles. Para oferecer suporte a esses controles, AWS Config deve estar habilitado e configurado para registrar os atributos necessários aos controles ativados em cada padrão habilitado.
- Habilitar todos os padrões de segurança - Essa etapa garante que o Audit Manager possa importar descobertas para todos os padrões de conformidade compatíveis.
- Ativar a configuração de descobertas de controle consolidadas no Security Hub - Essa configuração será ativada por padrão se você habilitar o Security Hub em ou após 23 de fevereiro de 2023.

  > **Note**
  >
  > Quando você habilita descobertas consolidadas, o Security Hub produz uma única descoberta para cada verificação de segurança (mesmo que a mesma verificação seja usada em vários padrões). Cada descoberta do Security Hub é coletada como uma avaliação de recurso exclusiva no Audit Manager. Como resultado, as descobertas consolidadas resultam em uma diminuição do total de avaliações exclusivas de atributos que o Audit Manager desempenha para as descobertas do Security Hub. Por esse motivo, o uso de descobertas consolidadas geralmente pode resultar em uma redução nos custos de uso do Audit Manager. Para obter mais informações sobre como usar o Security Hub como um tipo de fonte de dados, consulte AWS Security Hub controles suportados por AWS Audit Manager. Para obter mais informações sobre precificação do Audit Manager, consulte Precificação AWS Audit Manager.

Se você usa AWS Organizations e deseja coletar evidências do Security Hub de suas contas membro, você também deve executar as seguintes etapas no Security Hub.

Para definir as configurações do Security Hub

1. Faça login no AWS Management Console e abra o console do AWS Security Hub em https://console.aws.amazon.com/securityhub/.
2. Usando sua conta de gerenciamento AWS Organizations, designe uma conta como administrador delegado do Security Hub. Para obter mais informações, consulte Designando uma conta de administrador do Security Hub no Guia do Usuário AWS Security Hub.

   > **Note**
   >
   > Certifique-se de que a conta de administrador delegado designada no Security Hub é a mesma que você usa no Audit Manager.

3. Usando sua conta de administrador delegado do Organizations, acesse Configurações, Contas, selecione todas as contas e adicione-as como membros selecionando Inscrição automática. Para obter mais informações, consulte Como habilitar contas de membro na sua organização no Guia do usuário AWS Security Hub.
4. Habilite AWS Config para cada conta membro da organização. Para obter mais informações, consulte Como habilitar contas de membro na sua organização no Guia do usuário AWS Security Hub.
5. Habilitar o padrão de segurança PCI DSS para cada conta de membro da organização. Os padrões AWS CIS Foundations Benchmark e AWS Foundational Best Practices já vem habilitados. Para obter mais informações, consulte Habilitando um padrão de segurança no Guia do Usuário AWS Security Hub.

Habilitar AWS Organizations (opcional)

O Audit Manager é compatível com várias contas por meio da integração com AWS Organizations. O Audit Manager pode executar avaliações em várias contas e consolidar evidências em uma conta de administrador delegado. O administrador delegado tem permissões para criar e gerenciar atributos do Audit Manager com a organização como zona de confiança. Somente a conta de gerenciamento pode designar um administrador delegado.

Tarefas para integrar AWS Organizations ao Audit Manager

- Etapa 1: criar ou participar de uma organização
- Etapa 2: habilitar todos os recursos na sua organização

- Etapa 3: especificar um administrador delegado para o Audit Manager

Etapa 1: criar ou participar de uma organização

Se seu Conta da AWS não faz parte de uma organização, você pode criar ou participar de uma organização. Para obter instruções, consulte Criando e gerenciando uma organização no Guia do Usuário AWS Organizations.

Etapa 2: habilitar todos os recursos na sua organização

Em seguida, você deve habilitar todos os recursos da sua organização. Para obter instruções, consulte Habilitando todos os recursos da sua organização no Guia do Usuário AWS Organizations.

Etapa 3: especificar um administrador delegado para o Audit Manager

Recomendamos que habilite o Audit Manager usando uma conta de gerenciamento do Organizations e, em seguida, especifique um administrador delegado. Depois disso, você pode usar a conta de administrador delegado para fazer login e executar avaliações. É uma prática recomendada criar avaliações usando apenas a conta de administrador delegado em vez da conta de gerenciamento.

> ⚠ Warning
>
> Depois de especificar um administrador delegado usando uma conta de gerenciamento do Organizations, sua conta de gerenciamento não poderá mais criar avaliações adicionais no Audit Manager. Além disso, a coleta de evidências é interrompida para todas as avaliações existentes criadas pela conta de gerenciamento. Em vez disso, o Audit Manager coleta e anexa evidências ao administrador delegado, que é a conta principal para gerenciar as avaliações da sua organização.

Para adicionar ou alterar um administrador delegado depois de habilitar o Audit Manager, consulte Configurações AWS Audit Manager, Administrador delegado.

Questões a serem consideradas:

- Você não pode usar sua conta de gerenciamento como administrador delegado no Audit Manager.
- Se você quiser habilitar o Audit Manager em mais de uma Região da AWS, deverá designar uma conta de administrador delegada separadamente em cada região. Nas configurações do Audit Manager, você deve designar a mesma conta de administrador delegado em todas as Regiões.

- Se você forneceu uma chave gerenciada pelo cliente ao habilitar o Audit Manager, certifique-se de que a conta do administrador delegado possui acesso a essa chave KMS. Para analisar e alterar as configurações de criptografia do Audit Manager, consulte Criptografia de dados.
- Para soluções para problemas comuns do Organizations e administradores delegados no Audit Manager, consulte Solução de problemas de administradores delegados e do AWS Organizations.

O que faço agora?

Agora que você configurou o Audit Manager, está pronto para começar a usar o serviço. Você também pode visitar a página de configurações do console para atualizar qualquer uma das configurações escolhidas ao definir o Audit Manager.

Conceitos básicos do Audit Manager

Você pode começar no Audit Manager seguindo um tutorial que explica como criar sua primeira avaliação. Para obter mais informações, consulte Tutorial para proprietários de auditoria: Criar uma avaliação.

Atualizar suas configurações do Audit Manager

É possível atualizá-las quando quiser. Para obter mais informações, consulte configurações AWS Audit Manager.

Conceitos básicos do AWS Audit Manager

Use os tutoriais passo a passo nesta seção para saber como executar tarefas usando o AWS Audit Manager.

Tip

Os tutoriais a seguir são categorizados por público. Escolha o tutorial adequado para você com base em sua função como proprietário da auditoria ou delegado.

- Os proprietários da auditoria são usuários do Audit Manager que são responsáveis por criar e gerenciar avaliações. No mundo dos negócios, os proprietários de auditoria geralmente são profissionais de governança, gerenciamento de riscos e conformidade (governance, risk management, and compliance, ou GRC). No contexto do Audit Manager, no entanto, indivíduos das equipes de SecOps ou DevOps também podem assumir a personalidade de usuário de um proprietário de auditoria. Os proprietários da auditoria podem solicitar assistência de um especialista no assunto, também conhecido como delegado, para analisar controles específicos e validar evidências. Os proprietários de auditoria devem ter as permissões necessárias para gerenciar uma avaliação.
- Delegados são especialistas no assunto, com conhecimento técnico ou comercial especializado. Embora não possuam nem gerenciem as avaliações do Audit Manager, eles ainda podem contribuir com elas. Os delegados auxiliam os proprietários de auditoria em tarefas como validar evidências para os controles que se enquadrem em sua área de especialização. Os delegados têm permissões limitadas no Audit Manager. Isso ocorre porque os proprietários da auditoria delegam conjuntos de controles específicos para análise, não avaliações completas.

Para obter mais informações sobre essas personas e outros conceitos do Audit Manager, consulte Proprietários de auditoria e Delegados na seção Conceitos e terminologia AWS Audit Manager deste guia. Para obter mais informações sobre as permissões do IAM recomendadas para cada persona, consulte Políticas recomendadas para personas de usuários em AWS Audit Manager.

Tutoriais Audit Manager

Como criar uma avaliação

Público:Proprietários de auditoria

Visão geral:Seguem as instruções passo a passo para criar sua primeira avaliação e começar a trabalhar rapidamente. Este tutorial explica como você pode usar uma framework padrão para criar uma avaliação e iniciar a coleta automatizada de evidências.

Analisando um conjunto de controles

Público: Delegados

Visão geral: Auxilia o proprietário de uma auditoria analisando as evidências dos controles que se enquadram na sua área de especialização. Aprende a analisar conjuntos de controles e evidências relacionadas, adicionar comentários, carregar evidências adicionais e atualizar o status de um controle.

Tutorial para proprietários de auditoria: criando uma avaliação

Este tutorial fornece uma introdução ao AWS Audit Manager. Neste tutorial, você cria uma avaliação usando o AWS Audit Manager Sample Framework. Ao criar uma avaliação, você inicia o processo contínuo de coleta automatizada de evidências para os controles nessa framework.

Este tutorial mostra como fazer o seguinte:

- Selecione uma framework padrão a partir da qual criar uma avaliação
- Especifique as contas da AWS a serem incluídas em sua avaliação
- Especifique os serviços da AWS a serem incluídas em sua avaliação
- Especifique os proprietários da auditoria para sua avaliação
- Analise e crie sua avaliação

Antes de começar este tutorial, certifique-se de atender às seguintes condições:

- Você completou todos os pré-requisitos descritos em Configurar o AWS Audit Manager. Você deve usar sua conta da AWS e o console do AWS Audit Manager para concluir este tutorial.

- Sua identidade do IAM recebe as permissões apropriadas para criar e gerenciar uma avaliação em AWS Audit Manager. Duas políticas sugeridas que concedem essas permissões são Exemplo 2: permitir acesso total do administrador e Exemplo 3: permitir acesso de gerenciamento.
- Você está familiarizado com a terminologia e a funcionalidade do Audit Manager. Para obter uma visão geral, consulte O que é AWS Audit Manager? e Conceitos e terminologia AWS Audit Manager.

> **Note**
>
> AWS Audit Manager auxilia na coleta de evidências relevantes para verificar a conformidade com frameworks e regulamentações de conformidade específicos. No entanto, ele não avalia a sua conformidade em si. Portanto, as evidências coletadas por meio do AWS Audit Manager podem não incluir todas as informações sobre seu uso AWS necessário a auditorias. AWS Audit Manager não substitui a assessoria jurídica ou os especialistas em conformidade.

Etapa 1: especificar detalhes da avaliação

Para a primeira etapa, selecione uma framework e forneça informações básicas para sua avaliação.

Para especificar detalhes da avaliação

1. Abra o console do AWS Audit Manager em https://console.aws.amazon.com/auditmanager/home.
2. Escolha IniciarAWS Audit Manager.
3. No painel de navegação, escolha Conceitos básicos e Começar com uma framework.
4. Selecione a framework que você deseja e, em seguida, selecione Criar avaliação a partir da framework. Este exemplo usa o AWS Audit Manager Sample Framework.
5. Em Nome da avaliação, insira um nome para sua avaliação.
6. (Opcional) Em Descrição da avaliação, insira uma descrição para a sua avaliação.
7. Em Destino dos relatórios de avaliação, selecione o bucket do Amazon S3 onde deseja salvar seus relatórios de avaliação.
8. Em frameworks, confirme se AWS Audit Manager Sample Framework (ou framework de sua escolha) está selecionada.

9. Em Tags, selecione Adicionar nova tag para associar uma tag à sua avaliação. Você pode especificar uma chave e um valor para cada tag. A chave da tag é obrigatória, e pode ser usada como critério de pesquisa ao buscar essa avaliação. Para obter mais informações sobre tags no AWS Audit Manager, consulte Marcando atributos AWS Audit Manager.
10. Escolha Avançar.

Etapa 2: especificar contas da AWS no escopo

Em seguida, especifique as contas da AWS que você deseja incluir no escopo da sua avaliação.

AWS Audit Manager se integra com AWS Organizations, para que você possa executar uma avaliação do Audit Manager em várias contas e consolidar evidências em uma conta de administrador delegado. Para habilitar Organizações no Audit Manager (se ainda não o fez), consulte Habilitar AWS Organizations (opcional) na página Configuração deste guia.

> **Note**
>
> O Audit Manager pode suportar até aproximadamente 150 contas no escopo de uma avaliação. Se tentar incluir mais de 150 contas, a criação da avaliação poderá falhar.

Para especificar contas no escopo

1. Em Contas da AWS, selecione as contas da AWS que você deseja incluir no escopo da sua avaliação.
   - Se você habilitou Organizações no AWS Audit Manager, várias contas serão listadas.
   - Se você não habilitou Organizações no Audit Manager, somente sua conta atual será listada.
2. Escolha Avançar.

Etapa 3: especificar serviços da AWS no escopo

A framework que você selecionou anteriormente define os serviços da AWS que o Audit Manager monitora e coleta evidências.

Quando você usa o console do Audit Manager para criar uma avaliação a partir de uma framework padrão, a lista de serviços no escopo é pré-selecionada e não pode ser editada. Isso ocorre porque

o Audit Manager mapeia e seleciona automaticamente as fontes de dados e os serviços para você. Essa seleção é feita de acordo com os requisitos do framework padrão. Se um serviço da AWS listado não for selecionado, o Audit Manager não coletará evidências de atributos relacionados a esse serviço. Esse também é o caso se estiver selecionado, mas você não tiver se inscrito nele em seu ambiente.

Nesta etapa do tutorial, você pode analisar quais serviços da AWS estão no escopo da avaliação com base na definição da framework. Para saber mais sobre frameworks, como acessá-las e analisá-las, consulte a seção Biblioteca framework deste guia.

Para especificar serviços da AWS no escopo

1. Em Serviços da AWS, analise a lista de serviços que estão no escopo dessa avaliação.
2. Escolha Avançar.

> **Tip**
>
> Se precisar editar a lista de serviços no escopo, pode fazê-lo isso usando a API CreateAssessment fornecida pelo Audit Manager.
> Como alternativa, você pode personalizar uma framework padrão e, em seguida, criar uma avaliação a partir da framework personalizada.

Etapa 4: especificar proprietários de auditoria

Nesta etapa, especifique os proprietários da auditoria para sua avaliação. Os proprietários da auditoria são as pessoas em seu local de trabalho, geralmente das equipes de GRC, SecOps ou DevOps, responsáveis por gerenciar a avaliação do Audit Manager. Recomendamos que usem a política AWSauditManagerAdministratorAccess.

Para especificar proprietários de auditoria

1. Em Proprietários da auditoria, selecione os proprietários da auditoria para sua avaliação. Para encontrar outros proprietários de auditoria, use a barra de pesquisa para pesquisar por nome ou conta da AWS.
2. Escolha Avançar.

Etapa 5: analisar e criar

Analise as informações para a sua avaliação. Para alterar as informações de uma etapa, selecione Editar. Ao terminar, selecione Criar avaliação para iniciar sua primeira avaliação e iniciar a coleta contínua de evidências.

Depois de criar uma avaliação, a coleta de evidências continuará até que você altere o status da avaliação para Inativo. Como alternativa, você pode interromper a coleta de evidências para um controle específico alterando o status do controle para Inativo.

> **Note**
>
> As evidências automatizadas estão disponíveis 24 horas após a criação da avaliação. O AWS Audit Manager coleta automaticamente evidências de várias fontes de dados, e a frequência dessa coleta de evidências é baseada no tipo de evidência. Para obter mais informações, consulte Frequência das coletas de evidências neste guia.

O que faço agora?

Recomendamos que continue aprendendo sobre os conceitos e as ferramentas apresentadas neste tutorial. Para fazê-lo, consulte os seguintes atributos:

- Como analisar uma avaliação — Apresenta a página de avaliação, onde você pode explorar os diferentes componentes de sua avaliação.
- Avaliações em AWS Audit Manager — Baseia-se neste tutorial e fornece informações detalhadas sobre os conceitos e as tarefas de gerenciamento de uma avaliação. Neste documento, recomendamos em especial que você confira os seguintes tópicos:
  - Como criar uma avaliação a partir de uma framework diferente
  - Como analisar as evidências em uma avaliação e gerar um relatório de avaliação
  - Como alterar o status de uma avaliação ou excluir uma avaliação
- Biblioteca framework—Apresenta a biblioteca de frameworks e explica como criar uma framework personalizada para suas necessidades específicas de conformidade.
- Biblioteca de controle—Apresenta a biblioteca de controle e explica como criar um controle personalizado para uso em sua framework personalizada.

- Conceitos e terminologia AWS Audit Manager—Fornece definições para os conceitos e a terminologia usados no Audit Manager.
- [Vídeo] Colete evidências e gerencie dados de auditoria usando o AWS Audit Manager — mostra o processo de criação da avaliação descrito neste tutorial e outras tarefas, como revisar um controle e gerar um relatório de avaliação.

Tutorial para delegados: analisando um conjunto de controles

Este tutorial descreve como analisar um conjunto de controles que foi compartilhado com você por um proprietário de auditoria no AWS Audit Manager.

Os proprietários da auditoria usam o Audit Manager para criar avaliações e coletar evidências para os controles listados nessa avaliação. Às vezes, os proprietários da auditoria podem ter dúvidas ou precisar de ajuda ao validar as evidências de um conjunto de controles. Nessa situação, o proprietário da auditoria pode delegar um conjunto de controles a um especialista no assunto para análise.

Como delegado, você ajuda os proprietários da auditoria a analisarem as evidências coletadas para os controles que se enquadrem na sua área de especialização.

Este tutorial mostra como fazer o seguinte:

- Acesse as notificações enviadas a você pelo proprietário da auditoria
- Analise um conjunto de controles e suas evidências relacionadas
- Carregue evidências manuais para suportar um controle
- Adicione um comentário para um controle que estiver analisando
- Atualize o status de um controle
- Envie o conjunto de controles revisado ao proprietário da auditoria quando sua análise for concluída

Antes de começar este tutorial, certifique-se de atender às seguintes condições:

- Sua conta da AWS está configurada. Você deve usar sua conta da AWS e o console do AWS Audit Manager para concluir este tutorial. Para obter mais informações, consulte Configurar o AWS Audit Manager.

- Você está familiarizado com a terminologia e a funcionalidade do Audit Manager. Para obter uma visão geral do Audit Manager, consulte O que é AWS Audit Manager? e Conceitos e terminologia AWS Audit Manager.

Etapa 1: Acessar as notificações

Comece fazendo login no AWS Audit Manager, onde você pode acessar suas notificações para ver os conjuntos de controle que foram delegados a você para análise.

Para acessar suas notificações

1. Abra o console do AWS Audit Manager em https://console.aws.amazon.com/auditmanager/home.
2. No painel de navegação à esquerda, escolha Notificações. Ou, na barra azul na parte superior da página, selecione Exibir notificação para abrir a página de notificações.
3. Na página Notificações, você analisa a lista de conjuntos de controle delegados. A tabela de notificações inclui as seguintes informações:
   - Data — data na qual o conjunto de controles foi delegado.
   - Avaliação — o nome da avaliação associada ao conjunto de controles. Você pode escolher um nome de avaliação para abrir a página de detalhes.
   - Conjunto de controles — o nome do conjunto de controles que foi delegado a você para análise.
   - Fonte — o usuário ou função que delegou o conjunto de controles a você.
   - Descrição — as instruções de análise fornecidas pelo proprietário da auditoria.

> **Tip**
>
> Você também pode se inscrever em um tópico do SNS para receber alertas por e-mail quando um conjunto de controles for atribuído a você para análise. Para obter mais informações, consulte Notificações no AWS Audit Manager.

Etapa 2: analisar um conjunto de controles e evidências relacionadas

A próxima etapa é analisar os conjuntos de controle que o proprietário da auditoria delegou a você. Ao examinar os controles e suas evidências, você pode determinar se alguma ação adicional é necessária a um controle. Ações adicionais podem incluir o carregamento manual de evidências adicionais para demonstrar conformidade, ou deixar um comentário sobre esse controle.

Para analisar um conjunto de controles

1. Na página Notificações, analise a lista de conjuntos de controle que foram delegados a você. Em seguida, identifique qual delas você deseja revisar e selecione o nome da avaliação relacionada.
2. Na guia Controles da página de detalhes da avaliação, role para baixo até a tabela Conjuntos de controles.
3. Na coluna Controles agrupados por conjunto de controles, expanda o nome de um conjunto de controles para mostrar seus controles. Em seguida, selecione o nome de um controle para abrir a página de detalhes do controle.
4. (Opcional) Selecione Atualizar status do controle para alterar o status do controle. Enquanto sua análise estiver em andamento, você pode marcar o status como Em análise.
5. Analise as informações sobre o controle nas Pastas de evidências, Fontes de dados, Comentários e guias Changelog. Para obter mais informações sobre cada uma dessas guias e como interpretar os dados nelas contidos, consulte Analisar os controles em uma avaliação.

Para analisar as evidências de um controle

1. Na página de detalhes do controle, selecione a guia Pastas de evidências.
2. Navegue até a tabela de Pastas de evidências, onde uma lista de pastas que contém evidências desse controle é exibida. Essas pastas são organizadas e nomeadas com base na data em que as evidências dentro dessa pasta foram coletadas.
3. Selecione o nome de uma pasta de evidências para abri-la. A partir daqui, você pode analisar um resumo de todas as evidências coletadas naquela data. Esse resumo também inclui o número total de problemas de verificação de conformidade que foram relatados diretamente de AWS Security Hub, AWS Config, ou de ambos. Para obter instruções sobre como interpretar os dados nesta página, consulte Análise de pastas de evidências.
4. Na página de resumo da pasta de evidências, navegue até a tabela de Evidências. Na coluna Hora, selecione um item de linha para abrir e analisar os detalhes da evidência coletada naquele

momento. Para obter instruções sobre como interpretar os dados nesta página de detalhes das evidência, consulte Análise de evidência individual.

Etapa 3. Carregar evidências manualmente (opcional)

Embora o AWS Audit Manager colete automaticamente evidências para muitos controles, em alguns casos, talvez seja necessário fornecer evidências adicionais. Nesses casos, você pode carregar manualmente evidências que ajudem a demonstrar conformidade com esse controle.

Antes de carregar manualmente evidências para sua avaliação, você deve colocar as evidências em um bucket do S3. Para obter instruções, consulte Criando de um bucket e Carregando objetos no Guia do usuário do Amazon Simple Storage Service.

> **Important**
>
> Cada conta da AWS só pode carregar manualmente até 100 arquivos de evidências para um controle por dia. Exceder essa cota diária faz com que qualquer carregamento manual adicional falhe nesse controle. Se você precisar carregar uma grande quantidade de evidências manuais em um único controle, carregue as evidências em lotes ao longo de vários dias.

Para carregar evidências manualmente para um controle

1. Abra o console do AWS Audit Manager em https://console.aws.amazon.com/auditmanager/home.
2. Na página Notificações, você pode ver a lista de conjuntos de controle que foram delegados a você. Identifique para qual conjunto de controles você deseja adicionar evidências e selecione o nome da avaliação relacionada para abrir a página de detalhes da avaliação.
3. Escolha a guia Controles, role para baixo até Conjuntos de controles e selecione o nome de um controle para abri-lo.
4. Escolha a guia Pastas de evidências e, em seguida, escolha Carregar manualmente evidência.
5. Na próxima página, insira o URI do S3 da evidência. Você pode encontrar o URI do S3 navegando até o objeto no console do Amazon S3 e escolhendo Copiar URI do S3.
6. Escolha Carregar para carregar manualmente a evidência.

> **Note**
>
> Quando um controle estiver no status Inativo, você não poderá carregar manualmente evidências desse controle. Para carregar evidências manualmente, primeiro você deve alterar o status do controle para Em análise ou Analisado. Para obter instruções sobre como alterar um status de controle, consulte Etapa 5: marcar um controle como analisado (opcional).

Etapa 4. Adicione um comentário para um controle (opcional)

Você pode adicionar comentários a qualquer controle analisado. Esses comentários estarão visíveis para o proprietário da auditoria. Por exemplo, você pode deixar um comentário para fornecer uma atualização de status e confirmar que corrigiu quaisquer problemas com esse controle.

Para adicionar um comentário a um controle

1. Na página Notificações, analise a lista de conjuntos de controle que foram delegados a você. Encontre o conjunto de controles para o qual você deseja deixar um comentário e selecione o nome da avaliação relacionada.
2. Escolha a guia Controles, role para baixo até a tabela Conjuntos de controles e selecione o nome de um controle para abri-lo.
3. Selecione a guia Comentários.
4. Em Enviar comentários, insira seu comentário na caixa de texto.
5. Selecione Enviar comentário para adicionar seu comentário. Seu comentário agora aparece na seção Comentários anteriores da página, junto a qualquer outro comentário relacionado a esse controle.

Etapa 5: marcar um controle como analisado (opcional)

Alterar o status de um controle é opcional. No entanto, recomendamos que você altere o status de cada controle para Analisado ao concluir a análise desse controle. Independente do status de cada controle individual, você ainda pode enviar os controles ao proprietário da auditoria.

Para marcar um controle como analisado

1. Na página Notificações, analise a lista de conjuntos de controle que foram delegados a você. Encontre o conjunto de controles contendo o controle que deseja marcar como analisado. Em seguida, selecione o nome da avaliação relacionada para abrir a página de detalhes da avaliação.
2. Na guia Controles da página de detalhes da avaliação, role para baixo até a tabela Conjuntos de controles.
3. Na coluna Controles agrupados por conjunto de controles, expanda o nome de um conjunto de controles para mostrar seus controles. Escolha o nome de um controle para abrir a página de detalhes do controle.
4. Selecione Atualizar status do controle e altere o status para Analisado.
5. Na janela exibida, selecione Atualizar status do controle para confirmar que você concluiu a análise do controle.

Etapa 6. Envie o conjunto de controles analisado de volta ao proprietário da auditoria

Quando terminar de analisar todos os controles, envie o conjunto de controles de volta ao proprietário da auditoria para que ele saiba que você concluiu sua análise.

Para enviar um conjunto de controles analisado de volta ao proprietário

1. Na página Notificações, analise a lista de conjuntos de controle atribuídos a você. Encontre o conjunto de controles que você deseja enviar para o proprietário da auditoria e escolha o nome da avaliação relacionada.
2. Role para baixo até a tabela Conjuntos de controles, selecione o conjunto de controles que você deseja enviar de volta ao proprietário da auditoria e escolha Enviar para análise.
3. Na janela exibida, você pode adicionar qualquer comentário de alto nível sobre esse conjunto de controles antes de escolher Enviar para análise.

Depois de enviar o controle ao proprietário da auditoria, ele poderá ver os comentários deixados deixou.

O que faço agora?

Você pode continuar aprendendo mais sobre os conceitos apresentados neste tutorial. Veja a seguir alguns atributos recomendados:

- Como analisar uma avaliação - Apresenta a página de avaliação, onde você pode explorar os diferentes componentes de uma avaliação no AWS Audit Manager.
- Análise dos controles em uma avaliação e Análise das evidências em uma avaliação - Fornece definições de dados para ajudá-lo a interpretar os controles e as evidências de cada avaliação.
- Conceitos e terminologia AWS Audit Manager - Fornece definições para os conceitos e a terminologia usados no Audit Manager.

Usando o painel Audit Manager

Com o painel do Audit Manager, você pode visualizar evidências de não conformidade em suas avaliações ativas. É uma maneira conveniente e rápida de monitorar suas avaliações, manter-se informado e corrigir problemas de forma proativa. Por padrão, o painel fornece uma visão agregada de cima para baixo de todas as suas avaliações ativas. Ao usar essa visualização, você pode identificar visualmente os problemas em suas avaliações sem precisar primeiro examinar grandes quantidades de evidências individuais.

O painel é a primeira tela que você vê ao entrar no console Audit Manager. Ele contém dois widgets que mostram os dados e os principais indicadores de desempenho (KPIs) mais relevantes para você. Ao usar um filtro de avaliação, você pode refinar esses dados para se concentrar nos KPIs de uma avaliação específica. A partir daí, você pode analisar os agrupamentos de domínios de controle para identificar quais possuem evidências em menor nível de não conformidade. Em seguida, você pode explorar os controles subjacentes para examinar e corrigir problemas.

> **Note**
>
> Se for um usuário iniciante do Audit Manager ou não tiver nenhuma avaliação ativa, nenhum dado será exibido no painel. Para começar, crie uma avaliação. Isso inicia a coleta contínua de evidências. Após um período de 24 horas, os dados agregados de evidências começarão a aparecer no painel. Você pode ler as seções a seguir para aprender a entender e interpretar esses dados.

Esta página cobre os seguintes tópicos:

Tópicos

Conceitos e terminologia do painel

Esta seção aborda coisas importantes que você deve saber sobre o painel Audit Manager antes de começar a usá-lo.

Permissões e visibilidade

Tanto os proprietários quanto os delegados da auditoria têm acesso ao painel. Isso significa que essas personas podem ver as métricas e os agregados de todas as avaliações ativas em sua conta AWS. Ter acesso às mesmas informações permite que toda a sua equipe se concentre nos mesmos KPIs e metas.

Filtros

O Audit Manager fornece um nível de página the section called “Filtro de avaliação” que você pode aplicar em todos os widgets do seu painel.

Evidência de não conformidade

O painel destaca os controles em suas avaliações que possuem evidências de verificação de conformidade com uma conclusão de não conformidade. As evidências de verificação de conformidade estão relacionadas a controles que usam AWS Config ou AWS Security Hub como tipo de fonte de dados. Para esse tipo de evidência, o Audit Manager relata o resultado de uma verificação de conformidade diretamente desses serviços. Se o Security Hub relatar um resultado de Falha ou se AWS Config relatar um resultado de não conformidade, o Audit Manager classificará a evidência como em não conformidade.

Evidência inconclusiva

Uma evidência é Inconclusiva se uma verificação de conformidade não estiver disponível ou não for aplicável. Como resultado, nenhuma avaliação de conformidade poderá ser feita. Esse é o caso quando um controle usa AWS Config ou AWS Security Hub como tipo de fonte de dados sem você ter habilitado esses serviços. Esse também é o caso se o controle usar um tipo de fonte de dados que não ofereça suporte a verificações de conformidade, como evidências manuais, chamadas de API AWS ou AWS CloudTrail.

Se a evidência tiver um status de verificação de conformidade não aplicável no console, ela será classificada como inconclusiva no painel.

Evidência em conformidade

A evidência está em conformidade se uma verificação de conformidade não relatar problemas. Será o caso se o Security Hub reportar um resultado de Êxito ou AWS Config um resultado Em conformidade.

Domínios de controle

O painel apresenta o conceito de domínio de controle. Você pode pensar em um domínio de controle como uma categoria geral de controles não específica a nenhum framework. Os agrupamentos de domínios de controle são alguns dos recursos mais poderosos do painel. O Audit Manager destaca os controles em suas avaliações que tenham evidências de não conformidade e os agrupa por domínio de controle. Ao usar esse atributo, você pode concentrar seus esforços de remediação em domínios específicos enquanto se prepara para uma auditoria.

> **Note**
>
> Um domínio de controle é diferente de um conjunto de controles. Um conjunto de controles é um agrupamento de controles específico do framework que normalmente é definido por um órgão regulador. Por exemplo, o framework do PCI DSS tem um conjunto de controles chamado Requisito 8: identificar e autenticar o acesso aos componentes do sistema. Esse conjunto de controles está sob o domínio do Gerenciamento de identidade e acesso.

O Audit Manager categoriza os controles nos seguintes domínios.

Nome do domínio de controle	Descrição do que cada controle governa
Continuidade de negócios e planejamento de contingência	Como estabelecer processos que protejam as operações comerciais críticas dos efeitos de grandes interrupções no sistema e na rede.
Gerenciamento de alterações	Como você testa, aprova, implementa e documenta as mudanças em sua infraestrutura de nuvem.

Nome do domínio de controle	Descrição do que cada controle governa
Segurança e privacidade de dados	Como você protege a privacidade, a disponibilidade e a integridade de seus dados.
Gerenciamento de desenvolvimento e configuração	Como você mantém sua infraestrutura de nuvem em um estado desejado e consistente.
Governança e supervisão	Como você alinha o uso da computação em nuvem às suas obrigações legais, regulatórias e éticas.
Gerenciamento de identidade e acesso	Como garantir que os usuários certos tenham o acesso adequado aos seus atributos de tecnologia.
Gerenciamento de incidentes	Como você estabelece responsabilidades e procedimentos que garantam uma resposta rápida e eficaz aos incidentes de segurança.
Logging e monitoramento	Como analisar a atividade do usuário em busca de indicações de que uma atividade não autorizada foi tentada ou realizada.
Gerenciamento de rede	Como administrar e operar sua rede de dados usando um sistema de gerenciamento de rede.
Gestão de pessoal	Como avaliar e gerenciar os riscos de segurança do pessoal em nível organizacional.
Segurança física	Como detectar e evitar problemas de segurança física em suas instalações.
Gestão de riscos	Como avaliar possíveis riscos, perdas e como reduzir ou eliminar essas ameaças.
Gestão da cadeia de suprimentos	Como identificar, avaliar e mitigar os riscos associados a produtos de TI, fornecedores e cadeias de suprimentos.

Nome do domínio de controle	Descrição do que cada controle governa
Gerenciamento de dispositivos de usuários	Como reduzir o risco de perda, dano ou comprometimento do hardware de TI de seus funcionários.
Gerenciamento de vulnerabilidade	Como definir, avaliar e corrigir todas as vulnerabilidades conhecidas dos ativos em sua infraestrutura de nuvem.

Consistência eventual dos dados

Os dados do painel são eventualmente consistentes. Isso significa que, quando você lê dados do painel, eles podem não refletir instantaneamente os resultados de uma operação de gravação ou atualização recém-concluída. Se verificar novamente em algumas horas, o painel deverá refletir os dados mais recentes.

Dados de avaliações excluídas e inativas

O painel exibe dados de avaliações ativas. Se excluir uma avaliação ou alterar seu status para inativo no mesmo dia que visualizar o painel, os dados dessa avaliação serão incluídos da seguinte forma.

- Avaliações inativas — se o Audit Manager tiver coletado evidências para sua avaliação antes de você alterá-la para inativa, esses dados de evidência serão incluídos no painel de controle para esse dia.
- Avaliações excluídas — se o Audit Manager tiver coletado evidências para sua avaliação antes de você excluí-la, esses dados de evidência não serão incluídos no painel de controle para esse dia.

Elementos do painel

As seções a seguir abordam os diferentes componentes do painel.

Tópicos

- Controles com evidências de não conformidade agrupados por domínio de controle

Filtro de avaliação

Você pode usar o filtro de avaliação para concentrar em uma avaliação ativa específica.

Por padrão, o painel exibe dados agregados de todas as suas avaliações ativas. Se quiser visualizar os dados de uma avaliação específica, aplique um filtro de avaliação. Esse é um filtro em nível de página que se aplica a todos os widgets no painel.

Para aplicar o filtro de avaliação, selecione uma avaliação na lista suspensa na parte superior do painel. Essa lista mostra até 10 de avaliações ativas. As avaliações criadas recentemente aparecem primeiro. Se tiver muitas avaliações ativas, poderá começar a digitar o nome de uma avaliação para encontrá-la rapidamente. Depois de selecionar uma avaliação, o painel exibirá dados somente dessa avaliação.

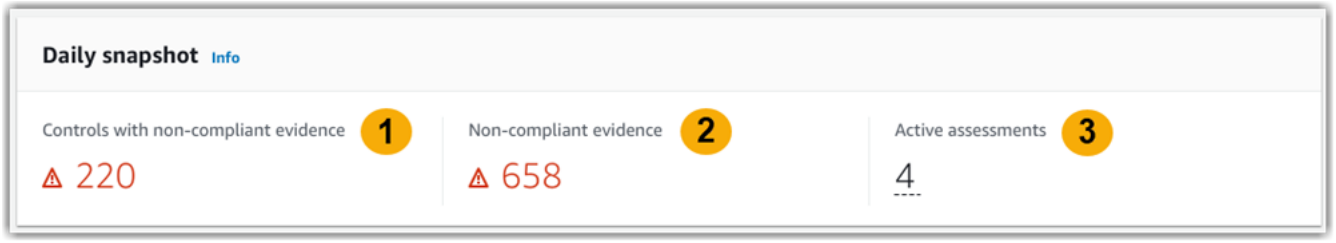
Captura de tela diária

Esse widget mostra uma captura de tela do status atual de conformidade de suas avaliações ativas.

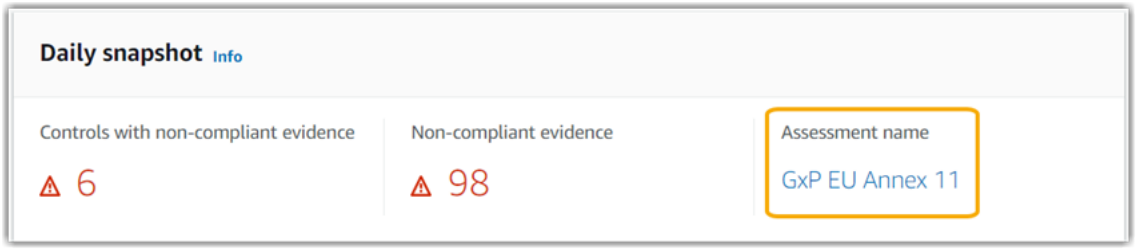
A captura de tela diária reflete os dados mais recentes coletados na data na parte superior do painel. A data e a hora no painel são representadas no Tempo Universal Coordenado (UTC). É importante entender que esses números são contagens diárias com base nesse registro de data e hora. Eles não são uma soma total até o momento.

Por padrão, a captura de tela diária mostra os seguintes dados de todas as suas avaliações ativas:

1. Controles com evidências de não conformidade - número total de controles associados a evidências de não conformidade.
2. Evidência de não conformidade - quantidade total de evidências de verificação de conformidade com uma conclusão de não conformidade.
3. Avaliações ativas - número total de avaliações ativas. Escolha esse número para ver os links para essas avaliações.



Os dados diários da captura de tela são alterados com base no the section called “Filtro de avaliação” que você aplica. Quando você especifica uma avaliação, os dados refletem somente as contagens diárias dessa avaliação. Nesse caso, a captura de tela diária mostra o nome da avaliação que você especificou. Você pode escolher o nome da avaliação para abri-la.

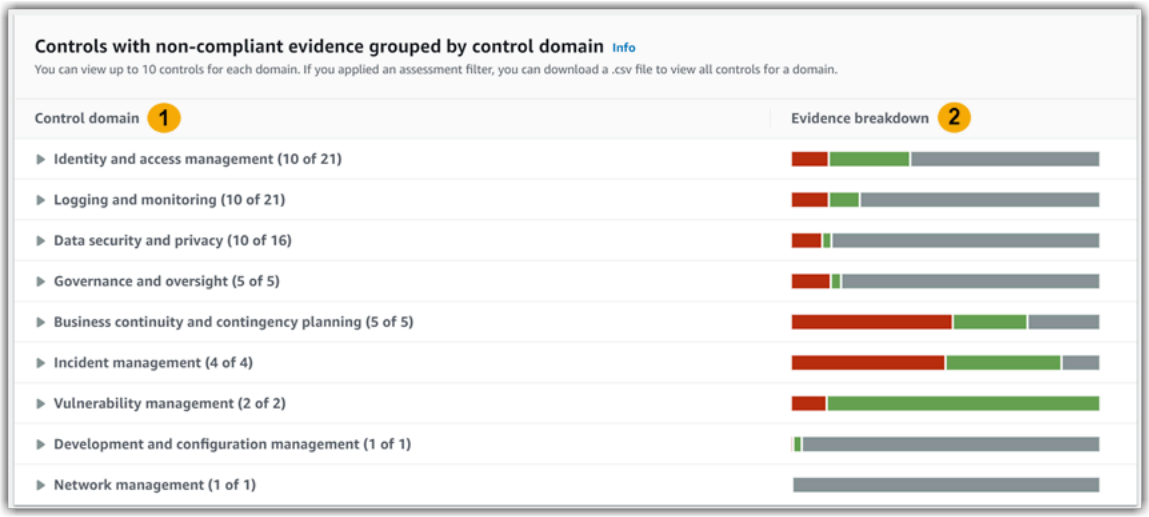


Controles com evidências de não conformidade agrupados por domínio de controle

Você pode usar esse widget para identificar quais controles possuem evidências de não conformidade.

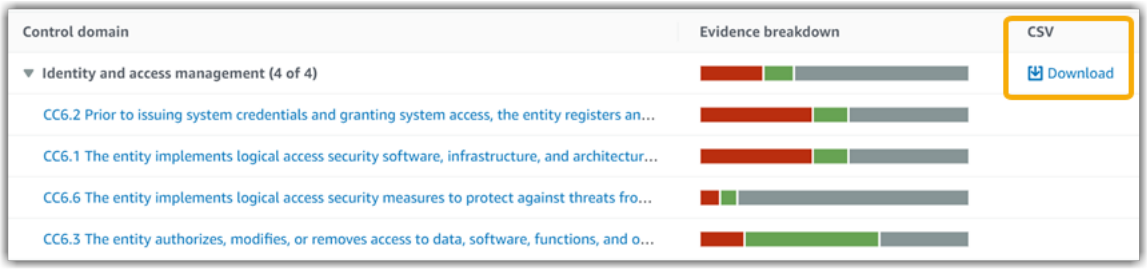
Por padrão, o widget mostra os seguintes dados para todas as suas avaliações ativas:

1. Domínio de controle — lista dos control domains associados às suas avaliações ativas.
2. Detalhamento das evidências — gráfico de barras que mostra um detalhamento do status de conformidade das evidências.



Para expandir um domínio de controle, escolha a seta ao lado do nome. Quando expandido, o console mostra até 10 controles para cada domínio. Esses controles são classificados de acordo com a maior contagem total de evidências de não conformidade.

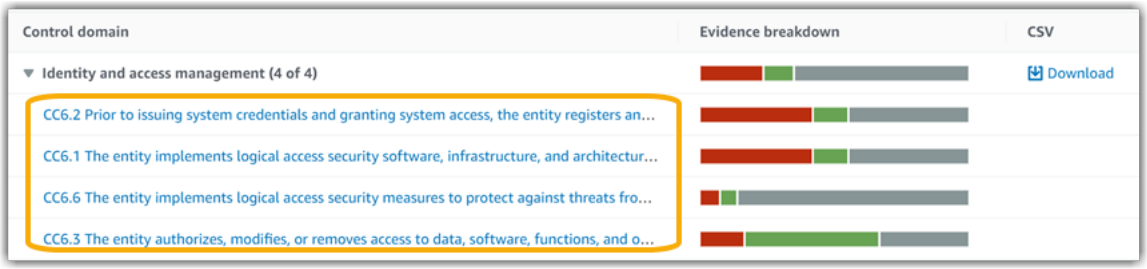
Os dados nesse widget mudam com base no the section called “Filtro de avaliação” que você aplica. Quando você especifica uma avaliação, vê os dados somente dessa avaliação. Além disso, você também pode baixar um arquivo .csv para cada domínio de controle disponível na avaliação.



O arquivo .csv inclui a lista completa de controles no domínio associados a evidências de não conformidade. O exemplo a seguir mostra as colunas de dados. csv com valores fictícios.

	A	B	C	D	E	F	G
1	Date and Time	AssessmentID	AsessmentName	ControlId	ControlName	ControlDescription	DataSource
2	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	abcdefgh-1234-bcde-5678-cdefghijklmn	Control 1	Description of control 1	Manual
3	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	12345678-abcd-9012-bcde-345678901234	Control 2	Description of control 2	Manual
4	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	bcdefghi-2345-cdef-3456-defghijklmno	Control 3	Description of control 3	AWS Config, AWS Security Hub
5	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	23456789-bcde-0123-cdef-456789012345	Control 4	Description of control 4	Manual
6	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	cdefghij-3456-defg-4567-efghijklmnop	Control 5	Description of control 5	AWS Config
7	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	34567890-cdef-1234-defg-567890123456	Control 6	Description of control 6	Manual
8	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	defghijk-4567-efgh-5678-fghijklmnopq	Control 7	Description of control 7	AWS Config
9	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	45678901-defg-2345-efgh-678901234567	Control 8	Description of control 8	AWS Security Hub
10	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	efghijkl-5678-fghi-6789-ghijklmnopqr	Control 9	Description of control 9	Manual
11	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	56789012-efgh-3456-fghi-789012345678	Control 10	Description of control 10	Manual
12	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	fghijklm-6789-ghij-7890-hijklmnopqrs	Control 11	Description of control 11	Manual
13	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	67890123-fghi-4567-ghij-890123456789	Control 12	Description of control 12	Manual
14	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	ghijklmn-7890-hijk-8901-ijklmnopqrst	Control 13	Description of control 13	AWS Config, AWS Security Hub
15	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	78901234-ghij-5678-hijk-901234567890	Control 14	Description of control 14	Manual
16							

Por fim, quando você aplica um filtro de avaliação, os nomes de controle em cada domínio são hiperlinkados. Escolha qualquer controle para abrir a página de detalhes do controle na avaliação especificada.



> **Tip**
>
> Ao usar a página de detalhes do controle como ponto de partida, você pode passar de um nível de detalhe para o próximo.
>
> 1. Página de detalhes do controle - nessa página, a guia de pastas de evidência lista as pastas diárias de evidência que o Audit Manager coletou para esse controle. Para mais detalhes, escolha uma pasta.
> 2. Pasta de evidências - em seguida, você pode analisar um resumo da pasta e uma lista das evidências nessa pasta. Para mais detalhes, escolha um item de evidência individual.
> 3. Evidência individual - por fim, você pode explorar detalhes de evidências individuais. Isso inclui quaisquer atributos aplicáveis e dados de recursos para a evidência. Esse é o nível mais granular de dados de evidência.

O que faço agora?

Aqui estão algumas das próximas etapas que você pode seguir depois de analisar o painel.

- Baixar um arquivo. csv — encontre o domínio de avaliação e controle no qual você deseja se concentrar e baixe a lista completa de controles relacionados com evidências de não conformidade.
- Analisar um controle — depois de identificar um controle que precisa ser corrigido, você pode analisar o controle.
- Delegar um controle para análise — se precisar de ajuda para analisar um controle, você pode delegar um conjunto de controles para análise.

- Editar sua avaliação — se quiser alterar o escopo de uma avaliação ativa, você pode editar a avaliação.
- Atualizar o status de sua avaliação — se quiser parar de coletar evidências para uma avaliação, você poderá alterar a avaliação para inativa.

Solução de problemas

Para encontrar respostas para perguntas e problemas comuns, consulte Solucionar problemas no painel na seção Solução de problemas deste guia.

Avaliações em AWS Audit Manager

Uma avaliação do Audit Manager é baseada em um framework, que é um agrupamento de controles. Usando um framework como ponto de partida, você pode criar uma avaliação que colete evidências dos controles nesse framework. Na avaliação, você também pode definir o escopo de sua auditoria. Isso inclui especificar os serviços Contas da AWS cujas evidências você deseja coletar.

Você pode criar uma avaliação a partir de qualquer framework. Você pode usar umframework padrão fornecido pelo Audit Manager. Ou pode criar uma avaliação a partir de umframework personalizado criado por você mesmo. Frameworks padrão contêm conjuntos de controle predefinidos que oferecem suporte a um padrão ou regulamento de conformidade específico. Por outro lado, frameworks personalizados contêm controles que você pode personalizar e agrupar de acordo com seus requisitos de auditoria interna. Para obter mais informações sobre as diferenças entre frameworks padrão e personalizados, consulte Frameworks na seção Conceitos e terminologia deste guia.

Ao criar uma avaliação, você inicia a coleta contínua de evidências. Na hora de fazer uma auditoria, você, ou um delegado, pode analisar as evidências coletadas e adicioná-las a um relatório de avaliação.

> **Note**
>
> AWS Audit Manager auxilia na coleta de evidências relevantes para verificar a conformidade com padrões e regulamentações de conformidade específicos. No entanto, ele não avalia a sua conformidade em si. Portanto, as evidências coletadas por meio do AWS Audit Manager podem não incluir todas as informações sobre seu uso AWS necessário a auditorias. AWS Audit Manager não substitui a assessoria jurídica ou os especialistas em conformidade.

Tópicos

- Como adicionar evidências manuais em AWS Audit Manager
- Como gerar um relatório de avaliação
- Como alterar o status de uma avaliação para inativo
- Como excluir uma avaliação

Como criar uma avaliação

Este tópico se baseia no tutorial Introdução: Como criar uma avaliação. Contém instruções detalhadas sobre como criar uma avaliação a partir de uma estrutura. Siga estas etapas para criar uma avaliação e iniciar a coleta contínua de evidências.

Tarefas

- Etapa 1: especificar detalhes da avaliação
- Etapa 2: especificar Contas da AWS no escopo
- Etapa 3: especificar Serviços da AWS no escopo
- Etapa 4: especificar proprietários de auditoria
- Etapa 5: analisar e criar
- O que faço agora?

Etapa 1: especificar detalhes da avaliação

Comece selecionando um framework e fornecendo informações básicas para sua avaliação.

Para especificar detalhes da avaliação

1. Abra o console do AWS Audit Manager em https://console.aws.amazon.com/auditmanager/home.
2. No painel de navegação, escolha Avaliações e depois, Criar avaliação.
   - Como alternativa, no painel de navegação, escolha Introdução e depois, Criar avaliação.
3. Em Nome da avaliação, insira um nome para sua avaliação.
4. (Opcional) Em Descrição da avaliação, insira uma descrição para a sua avaliação.
5. Em Destino dos relatórios de avaliação, selecione o bucket Amazon S3 existente onde deseja salvar seus relatórios de avaliação.

> **Tip**
>
> O destino padrão do relatório de avaliação é baseado nas suas configurações do Audit Manager. Para obter mais informações, consulte Configurações AWS Audit Manager, destino do relatório de avaliação. Se preferir, você pode criar e usar vários buckets S3 para ajudá-lo a organizar seus relatórios de avaliação.

6. Em Frameworks, selecione o framework a partir do qual deseja criar sua avaliação. Você também pode usar a barra de pesquisa para pesquisar um framework por nome ou por padrão ou regulamento de conformidade.

> **Tip**
>
> Para saber mais, escolha o nome do framework. Isso abre a página de detalhes do framework. Nessa página, você pode analisar o conteúdo desse framework. Isso inclui seus controles e fontes de dados.

7. Em Tags, selecione Adicionar nova tag para associar uma tag à sua avaliação. Você pode especificar uma chave e um valor para cada tag. A chave da tag é obrigatória, e pode ser usada como critério de pesquisa ao buscar essa avaliação. Para obter mais informações sobre tags no Audit Manager, consulte Marcando atributos AWS Audit Manager.
8. Escolha Next (Próximo).

> **Note**
>
> É importante garantir que sua avaliação colete as evidências corretas para um determinado framework. Antes de iniciar a coleta de evidências, recomendamos que você analise os requisitos do framework escolhido. Em seguida, valide esses requisitos em relação aos parâmetros atuais da regra AWS Config. Para garantir que seus parâmetros de regra estejam alinhados com os requisitos do framework, você pode atualizar a regra em AWS Config.
> Por exemplo, suponha que você esteja criando uma avaliação para o CIS v1.2.0. Esse framework tem um controle chamado 1.9 – Certifique-se de que a política de senha do IAM exija um comprimento mínimo de 14 ou mais. Em AWS Config, a regra iam-password-policy tem um parâmetro `MinimumPasswordLength` que verifica o tamanho da senha. O valor padrão desse parâmetro é de 14 caracteres. Como resultado, a regra se alinha aos requisitos de controle. Se não estiver usando o valor do parâmetro padrão, verifique se o valor que

está usando é igual ou maior que o requisito de 14 caracteres do CIS v1.2.0. Você pode encontrar os detalhes do parâmetro padrão para cada regra gerenciada na documentação AWS Config.

Etapa 2: especificar Contas da AWS no escopo

Você pode especificar múltiplos Contas da AWS para o escopo de uma avaliação. O Audit Manager oferece suporte a várias contas, por meio da integração com o AWS Organizations. Isso significa que as avaliações do Audit Manager podem ser executadas em várias contas, com as evidências coletadas consolidadas em uma conta de administrador delegado. Para habilitar Organizações no Audit Manager, consulte Habilitar AWS Organizations (opcional).

> **Note**
>
> O Audit Manager pode suportar até aproximadamente 150 contas no escopo de uma avaliação. Se tentar incluir mais de 150 contas, a criação da avaliação poderá falhar.

Para especificar Contas da AWS no escopo

1. Em Contas da AWS, selecione a Contas da AWS que deseja incluir no escopo da sua avaliação.
   - Se você habilitou Organizações no Audit Manager, várias contas serão listadas. Você pode escolher uma ou mais contas da lista. Como alternativa, você também pode pesquisar uma conta pelo nome, ID ou e-mail.
   - Se você não habilitou Organizações no Audit Manager, somente sua conta atual Conta da AWS estará listada.
2. Escolha Next (Próximo).

> **Note**
>
> Quando uma conta do escopo é removida da sua organização, o Audit Manager não coleta mais evidências dessa conta. No entanto, a conta continua sendo exibida em sua avaliação na guia Contas da AWS. Para remover a conta da lista de contas no escopo, você pode editar a avaliação. A conta removida não aparece mais na lista durante a edição e você pode salvar suas alterações sem que essa conta esteja no escopo.

Etapa 3: especificar Serviços da AWS no escopo

O framework que você selecionou anteriormente define a Serviços da AWS que o Audit Manager irá monitorar e para a qual coletará evidências. Se uma AWS service (Serviço da AWS) listada não estiver selecionada, ou estiver selecionada, mas você não a habilitou em seu ambiente, o Audit Manager não coleta evidências de recursos relacionados a esse serviço.

Você pode especificar o escopo Serviços da AWS da seguinte forma.

Para avaliações criadas a partir de frameworks padrão

Quando você usa o console do Audit Manager para criar uma avaliação a partir de um framework padrão, a lista de Serviços da AWS no escopo é selecionada por padrão. Essa lista não pode ser editada. Isso ocorre porque o Audit Manager mapeia e seleciona automaticamente as fontes de dados e os serviços para você. Essa seleção é feita de acordo com os requisitos do framework padrão. Se a estrutura padrão que você selecionou contiver somente controles manuais, nenhum Serviços da AWS estará no escopo da sua avaliação e não será possível adicionar nenhum serviço à sua avaliação.

Para prosseguir, analise a lista e escolha Avançar.

> **Tip**
>
> Se você precisar editar a lista de serviços no escopo, pode fazê-lo usando a API CreateAssessment fornecida pelo Audit Manager.
> Como alternativa, você pode personalizar o framework padrão e, em seguida, criar uma avaliação a partir do framework personalizado.

Para avaliações criadas a partir de frameworks personalizados

Se você selecionou um framework personalizado na etapa 1, poderá analisar e modificar a lista de Serviços da AWS no escopo de sua avaliação. Se o framework personalizado selecionado tiver somente controles manuais, todos os Serviços da AWS serão exibidos, mas nenhum será selecionado. Você pode selecionar zero ou mais serviços para fazerem parte do escopo de sua avaliação.

Para especificar o escopo Serviços da AWS (somente para avaliações criadas a partir de frameworks personalizados)

1. Em Serviços da AWS, selecione os serviços que deseja incluir na sua avaliação. Você encontra serviços adicionais usando a barra de pesquisa para buscar por serviço, categoria ou descrição. Para adicionar um serviço, marque a caixa de seleção ao lado do nome do serviço. Para remover um serviço, desmarque a caixa de seleção.
2. Quando terminar de selecionar Serviços da AWS, escolha Avançar.

Etapa 4: especificar proprietários de auditoria

Nesta etapa, especifique os proprietários da auditoria para sua avaliação. Os proprietários da auditoria são as pessoas em seu local de trabalho, geralmente das equipes de GRC, SecOps ou DevOps, responsáveis por gerenciar a avaliação do Audit Manager. Recomendamos que usem a política AWSauditManagerAdministratorAccess.

Para especificar proprietários de auditoria

1. Em Proprietários de auditoria, analise a lista atual de proprietários de auditoria. A coluna Proprietário de auditoria exibe IDs e funções do usuário. A coluna Conta da AWS exibe os associados Conta da AWS desse proprietário de auditoria.
2. Os proprietários de auditoria com uma caixa de seleção marcada serão incluídos na sua avaliação. Desmarque a caixa de seleção de qualquer proprietário de auditoria para removê-lo da avaliação. Você encontra outros proprietários de auditoria usando a barra de pesquisa para buscar por nome ou Conta da AWS.
3. Quando terminar, escolha Próximo.

Etapa 5: analisar e criar

Analise as informações para a sua avaliação. Para alterar as informações de uma etapa, selecione Editar. Quando terminar, escolha Criar avaliação.

Quando inicia a coleta contínua de evidências para a sua avaliação. Depois de criar uma avaliação, a coleta de evidências continuará até que você altere o status da avaliação para Inativo. Como alternativa, você pode interromper a coleta de evidências para um controle específico alterando o status do controle para Inativo.

> **Note**
>
> As evidências automatizadas ficam disponíveis 24 horas após a criação da sua avaliação. O Audit Manager coleta automaticamente evidências de várias fontes de dados. A frequência dessa coleta é baseada no tipo de evidência. Para saber mais, consulte Frequência das coletas de evidências neste guia.

O que faço agora?

Depois de criar sua avaliação, você pode saber mais sobre:

- Como acessar uma avaliação
- Como analisar uma avaliação
- Como editar uma avaliação
- Analisando os controles em uma avaliação
- Analisando a evidência em uma avaliação
- Como carregar evidências manuais para uma avaliação
- Delegações em AWS Audit Manager
- Como gerar um relatório de avaliação
- Como alterar o status de uma avaliação
- Como excluir uma avaliação
- Solução de problemas de avaliação e coleta de evidências

Como acessar as suas avaliações em AWS Audit Manager

Você pode visualizar todas as suas avaliações na página Avaliações, no console do Audit Manager. A partir daqui, você também pode editar uma avaliação, excluir uma avaliação, ou criar uma avaliação.

Você também pode visualizar as suas avaliações usando a API Audit Manager ou o AWS Command Line Interface (AWS CLI).

Audit Manager console

Para visualizar as suas avaliações (console)

1. Abra o console do AWS Audit Manager em https://console.aws.amazon.com/auditmanager/home.
2. No painel de navegação à esquerda, escolha Avaliações para visualizar uma lista de avaliações ativas e anteriores. Você também pode usar a barra de pesquisa para buscar uma avaliação.
3. Escolha qualquer nome de avaliação para abrir uma página de resumo na verá os detalhes dessa avaliação.

AWS CLI

Para visualizar as suas avaliações (CLI)

Para visualizar as avaliações no Audit Manager, execute o comando list-assessments. Você pode usar o subcomando `--status` para visualizar avaliações ativas ou inativas.

```
aws auditmanager list-assessments --status ACTIVE
```

```
aws auditmanager list-assessments --status INACTIVE
```

Audit Manager API

Para visualizar as suas avaliações (API)

Para visualizar avaliações no Audit Manager, use a operação list-assessments. Você pode usar o atributo status para visualizar avaliações que estão ativas ou inativas.

Para obter mais informações, escolha um dos links anteriores para ler mais na Referência de API AWS Audit Manager. Isso inclui informações sobre como usar a operação `ListAssessments` e os parâmetros em um dos SDKs AWS específicos do idioma.

Como editar uma avaliação

É possível editar as configurações de suas avaliações ativas no Audit Manager, como modificar a descrição, o escopo, os proprietários da auditoria e o destino do relatório.

Tarefas

- Etapa 1: editar detalhes da avaliação
- Etapa 2: como editar Contas da AWS no escopo
- Etapa 3: como editar Serviços da AWS no escopo
- Etapa 4: como editar proprietários de auditoria
- Etapa 5: analisar e salvar

Etapa 1: editar detalhes da avaliação

Siga estas etapas para editar os detalhes da sua avaliação.

Para editar uma avaliação

1. Abra o console do AWS Audit Manager em https://console.aws.amazon.com/auditmanager/home.
2. No painel de navegação, escolha Avaliações para exibir sua lista atual de avaliações.
3. Selecione uma avaliação e escolha Editar.
   - Como alternativa, você pode abrir a avaliação e escolher Editar no canto superior direito da página.
4. Em Editar detalhes da avaliação, edite o nome, a descrição e o destino do relatório de avaliação.
5. Escolha Next (Próximo).

> **Tip**
>
> Para editar as tags de uma avaliação, abra a avaliação e escolha o Guia Tags. Lá você pode visualizar e editar as tags associadas à avaliação.

Etapa 2: como editar Contas da AWS no escopo

Nesta etapa, é possível alterar a lista de contas incluídas no escopo da avaliação.

O Audit Manager oferece suporte a várias contas, por meio da integração com o AWS Organizations. Isso significa que as avaliações do Audit Manager podem ser executadas em várias contas, com as evidências coletadas consolidadas em uma conta de administrador delegado. Para adicionar ou

alterar o administrador delegado do Audit Manager, consulte Configurações AWS Audit Manager, administrador delegado.

> **Note**
>
> O Audit Manager pode suportar até aproximadamente 150 contas no escopo de uma avaliação. Se tentar incluir mais de 150 contas, a criação da avaliação poderá falhar.

Para editar Contas da AWS no escopo

1. Em Editar Contas da AWS no escopo, selecione contas adicionais AWS. Você também pode remover contas limpando-as da lista.
2. Escolha Next (Próximo).

Etapa 3: como editar Serviços da AWS no escopo

Essa etapa especifica para qual o Audit Manager Serviços da AWS monitora e coleta evidências. Se uma AWS service (Serviço da AWS) listada não estiver selecionada, ou estiver selecionada, mas você não a habilitou em seu ambiente, o Audit Manager não coleta evidências de recursos relacionados a esse serviço.

Você pode analisar e editar o Serviços da AWS no escopo da seguinte maneira.

Para avaliações criadas a partir de frameworks padrão

Ao usar o console do Audit Manager para editar uma avaliação criada a partir de um framework padrão, você pode analisar a lista de Serviços da AWS no escopo, mas não pode editar essa lista. Isso ocorre porque o Audit Manager mapeia e seleciona automaticamente as fontes de dados e os serviços para você de acordo com o projeto do framework padrão. Se a avaliação foi criada usando um framework contendo apenas controles manuais, nenhum Serviços da AWS estará no escopo para sua avaliação e você não poderá adicionar nenhum serviço.

Para prosseguir, analise a lista e escolha Avançar.

> **Tip**
>
> Se precisar editar a lista de serviços no escopo para uma avaliação existente, você pode fazê-lo usando a API CreateAssessment fornecida pelo Audit Manager.

Para avaliações criadas a partir de frameworks personalizados

Se você criou a avaliação a partir de um framework personalizado, poderá editar as Serviços da AWS no escopo de sua avaliação. Você pode selecionar zero ou mais serviços para fazerem parte do escopo de sua avaliação.

Para editar Serviços da AWS no escopo (somente para avaliações criadas a partir de frameworks personalizados)

1. Em Editar Serviços da AWS no escopo, selecione contas adicionais Serviços da AWS, conforme necessário. Você também pode remover serviços apagando-os da lista.
2. Escolha Next (Próximo).

Etapa 4: como editar proprietários de auditoria

Você também pode alterar os proprietários da auditoria para a sua avaliação. Os proprietários da auditoria são as pessoas em seu local de trabalho, geralmente das equipes de GRC, SecOps ou DevOps, responsáveis por gerenciar a avaliação do Audit Manager. Suas funções incluem delegar conjuntos de controle para análise e gerar relatórios de avaliação. Recomendamos o uso da política AWSauditManagerAdministratorAccess.

Para editar os proprietários da auditoria

1. Selecione novos proprietários de auditoria para adicionar à avaliação. Para remover proprietários de auditoria, apague-os da lista.
2. Escolha Next (Próximo).

Etapa 5: analisar e salvar

Analise as informações para a sua avaliação. Para alterar as informações de uma etapa, selecione Editar. Quando terminar de editar, escolha Salvar alterações para salvar suas edições.

> **Note**
>
> Depois de concluir suas edições, as alterações na avaliação entrarão em vigor 00:00 UTC do dia seguinte.

Como analisar uma avaliação

Depois de criar avaliações no Audit Manager, você pode abrir e analisar suas avaliações a qualquer momento.

Para abrir e analisar uma avaliação

1. Abra o console do AWS Audit Manager em https://console.aws.amazon.com/auditmanager/home.
2. No painel de navegação à esquerda, escolha Avaliações para visualizar uma lista de suas avaliações.
3. Escolha o nome da avaliação para abri-la.

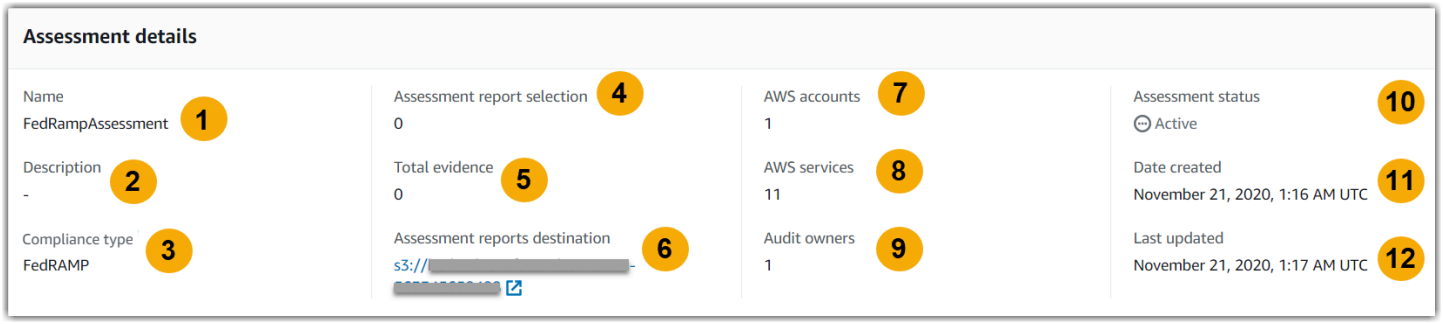
Ao abrir uma avaliação, você verá uma página de resumo contendo várias seções. As seções desta página e seu conteúdo são descritos a seguir.

Seções da página de avaliação

- Detalhes da avaliação
- Guia Controles
- Guia de seleção do relatório de avaliação
- Guia Contas da AWS
- Guia Serviços da AWS
- Guia proprietários da auditoria
- Guia Tags
- Guia changelog

Detalhes da avaliação

A seção Detalhes da avaliação fornece uma visão geral da avaliação.



Isso inclui as informações a seguir:

1. Nome – O nome que você forneceu para a avaliação.
2. Descrição – A descrição opcional que você forneceu para a avaliação.
3. Tipo de conformidade – O padrão ou regulamento de conformidade que a avaliação suporta.
4. Seleção do relatório de avaliação – O número de itens de evidência que você escolheu para incluir no relatório de avaliação.
5. Evidência total – O número total de itens de evidência que são coletados para essa avaliação.
6. Destino dos relatórios de avaliação – O bucket do Amazon S3 no qual o Audit Manager salva o relatório de avaliação.
7. Contas da AWS – O número das Contas da AWS que estão no escopo desta avaliação.
8. Serviços da AWS – O número das Serviços da AWS que estão no escopo desta avaliação.
9. Proprietários da auditoria – O número de proprietários da auditoria dessa avaliação.
10. Estado da avaliação – O status da avaliação.
    - Ativo – Indica que a avaliação está atualmente coletando evidências. As avaliações recém-criadas têm esse status.
    - Ativo – Indica que a avaliação não está mais coletando evidências. Para obter mais informações sobre o avaliações inativas, consulte Como alterar o status de uma avaliação para inativo.
11. Data de criação – A data na qual a avaliação foi criada.
12. Última atualização – Data na qual a avaliação foi atualizada pela última vez.

Guia Controles

A guia Controles exibe um resumo dos controles na avaliação, junto a uma lista completa dos mesmos. Cada avaliação pode conter vários conjuntos de controle; cada conjunto de controles, vários controles. Os controles e conjuntos de controle são organizados para corresponder ao layout definido no padrão ou regulamento de conformidade associado.

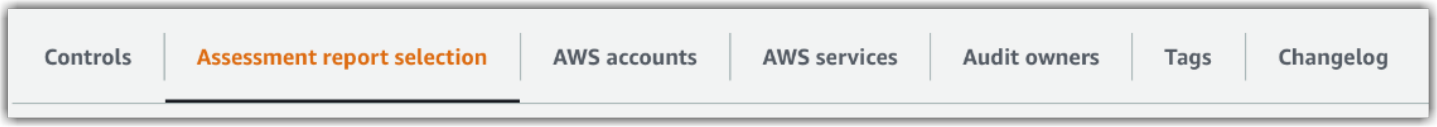
Em Resumo do status do controle, você pode analisar um resumo dos controles dessa avaliação. O resumo inclui as seguintes informações:

- Total de controles – O número total de controles nessa avaliação.
- Revisado – O número de controles que foram revisados por um proprietário ou delegado de auditoria.
- Em análise – O número de controles atualmente em análise.
- Inativo – O número de controles que não estão mais coletando evidências ativamente.

Na tabela Conjuntos de controle, uma lista de controles é exibida e agrupada por conjunto de controles. Você pode expandir ou recolher os controles em cada conjunto de controles. Você também pode pesquisar pelo nome do controle se quiser procurar um controle específico. As seguintes colunas de dados aparecem na tabela Controles agrupados por conjuntos de controles:

- Controles agrupados por conjuntos de controle – O nome do conjunto de controles.
- Status do controle – O status do controle.
  - Sob revisão – indica que esse controle ainda não foi revisado. As evidências ainda estão sendo coletadas para esse controle e você pode carregar evidências manuais. Esse é o status padrão.
  - Analisando indica que as evidências desse controle foram analisadas. No entanto, as evidências ainda estão sendo coletadas para esse controle e você pode carregar evidências manuais.
  - Inativo indica que a coleta automatizada de evidências foi interrompida para esse controle. Não é mais possível carregar evidências manuais.
- Delegado para – O revisor desse controle, se ele tiver sido atribuído a um delegado para revisão.
- Evidências totais – O número total de itens de evidência que foram coletados para essa avaliação.

Guia de seleção do relatório de avaliação



Essa guia exibe a lista de evidências a serem incluídas no relatório de avaliação agrupadas por pastas de evidências. Essas pastas de evidências são organizadas e nomeadas com base na data em que foram criadas. Você pode navegar por essas pastas e selecionar quais evidências deseja incluir em seu relatório de avaliação. Você também pode usar a barra de pesquisa para buscar pelo nome da pasta de evidências ou nome do controle. O número total de itens de evidência adicionados ao relatório de avaliação está resumido na seção Detalhes da avaliação, na parte superior da página.

A tabela Seleção do relatório de avaliação mostra uma lista de pastas de evidências com os seguintes dados:

- Pasta de evidências – O nome da pasta de evidências. O nome da pasta é baseado na data em que as evidências foram coletadas.
- Evidência selecionada – O número de itens de evidência na pasta que estão incluídos no relatório de avaliação.
- Nome do controle – O nome do controle associado a essa pasta de evidências.

Para obter informações sobre como adicionar evidências a um relatório de avaliação, consulte Como gerar um relatório de avaliação.

Guia Contas da AWS

Essa guia exibe a lista de Contas da AWS que estão no escopo da avaliação. O número total de contas está resumido na seção Detalhes da avaliação, na parte superior da página.

A tabela Contas da AWS mostra uma lista de contas com os seguintes dados:

- ID da conta – ID da Conta da AWS.
- Nome da conta – O nome da Conta da AWS.
- Email – o endereço de email que é associado com a Conta da AWS.

Guia Serviços da AWS

Essa guia exibe a lista de Serviços da AWS que estão no escopo da avaliação. Em outras palavras, é sobre esses Serviços da AWS que a sua avaliação coleta evidências.

O número total de serviços está resumido na seção Detalhes da avaliação na parte superior da página.

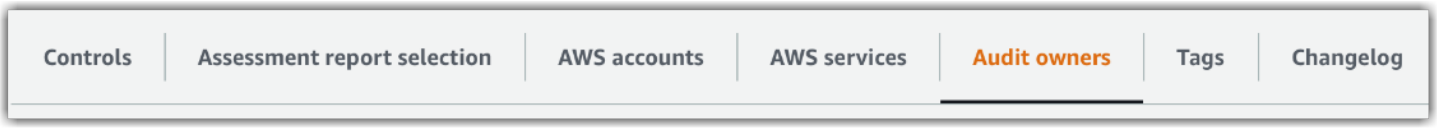
A tabela Serviços da AWS mostra uma lista de serviços com os seguintes dados:

- AWS service (Serviço da AWS) – O nome da AWS service (Serviço da AWS).
- Categoria – A categoria de serviço, como computação ou banco de dados.

O Audit Manager realiza avaliações de recursos para os serviços desta tabela. Por exemplo, se o Amazon S3 estiver listado, o Audit Manager poderá coletar evidências sobre seus buckets S3. A evidência exata que é coletada é determinada pela fonte de dados de um controle. Por exemplo, se o tipo da fonte de dados for AWS Config e o mapeamento da fonte for uma regra AWS Config (como `s3-bucket-public-write-prohibited`), o Audit Manager coletará o resultado dessa avaliação de regra como evidência. Para obter mais informações, consulte Qual é a diferença entre um serviço no escopo e um tipo de fonte de dados? neste manual.

> **Note**
>
> Se sua avaliação foi criada no console a partir de um framework padrão, o Audit Manager selecionou os serviços para você e mapeou suas fontes de dados de acordo com os requisitos da framework. Se o framework padrão contiver somente controles manuais, nenhum dos Serviços da AWS estará no escopo. Se você precisar editar a lista de serviços no escopo, pode usar a API UpdateAssessment.

Guia proprietários da auditoria

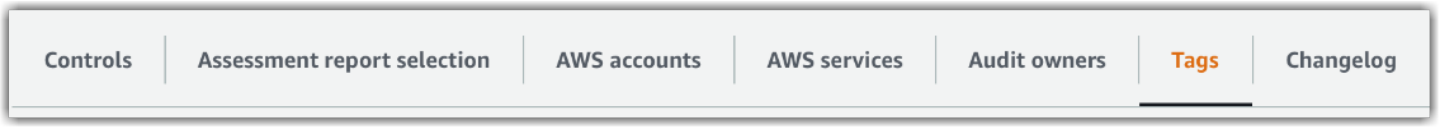


Essa guia exibe os proprietários da auditoria da avaliação. O número total de proprietários de auditoria está resumido na seção Detalhes da avaliação na parte superior da página.

A tabela Proprietários de auditoria mostra uma lista de contas com os seguintes dados:

- Proprietário da auditoria – O nome do proprietário da auditoria.
- Conta da AWS – O endereço de email que está associado com o proprietário da auditoria.

Guia Tags



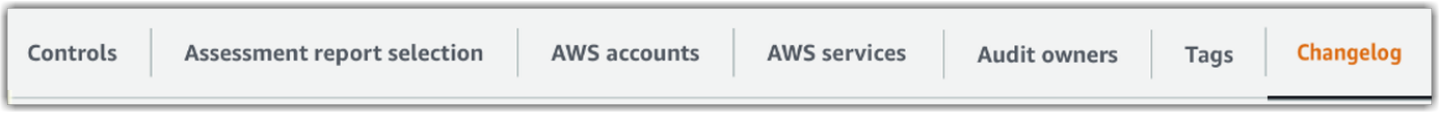
Essa guia exibe a lista de tags herdadas do framework que são usadas para criar essa avaliação. O número total de tags está resumido na seção Detalhes da avaliação na parte superior da página.

A tabela Tags mostra uma lista de contas com os seguintes dados:

- Chave - A chave da tag, como por exemplo, um padrão de conformidade, um regulamento ou uma categoria.
- Valor - O valor da tag.

Para obter mais informações sobre tags no Audit Manager, consulte Marcando atributos AWS Audit Manager.

Guia changelog



Essa guia exibe uma lista das atividades do usuário relacionadas à avaliação.

A tabela Changelog mostra uma lista de contas com os seguintes dados:

- Data – A data da atividade.
- Usuário – O usuário que executou a ação.
- Ação – A ação que ocorreu, como a criação de uma avaliação.
- Tipo – O tipo de objeto que foi alterado, como uma avaliação.
- Recurso – O recurso que foi afetado pela mudança, como o framework a partir do qual a avaliação foi criada.

Analisando os controles em uma avaliação

Os controles do Audit Manager ajudam a atender aos padrões e regulamentações de conformidade comuns exclusivos em suas auditorias. Você pode abrir e analisar os controles em sua avaliação do Audit Manager a qualquer momento.

Para abrir uma página de resumo de controle

1. Abra o console do AWS Audit Manager em https://console.aws.amazon.com/auditmanager/home.
2. No painel de navegação, escolha Avaliações e, em seguida, o nome de avaliação, para abri-la.
3. Da guia Avaliação, escolha a guia Controles, role para baixo até a tabela Conjuntos de controles e selecione o nome de um controle para abri-lo.

Quando você abre uma avaliação, você vê uma página de resumo que contém várias seções. As seções desta página e seu conteúdo são descritos nas seções a seguir.

Seções da página de controle

- Detalhes do controle
- Como atualizar o status do controle
- Guia de pastas de evidências
- Guia fonte de dados
- Guia de comentários
- Guia changelog

Detalhes do controle

A seção Detalhes do controle apresenta uma visão geral do controle.

Isso inclui as informações a seguir:

1. Nome do controle – O nome que é dado a esse controle.
2. Descrição do controle – A descrição fornecida para esse controle.
3. Informações de teste — Os procedimentos de teste recomendados para esse controle.
4. Plano de ação – As ações recomendadas a serem executadas se o controle não for cumprido.

Como atualizar o status do controle

Na seção Atualizar status do controle da página, você pode analisar e atualizar o status do controle de avaliação.

Os seguintes status estão disponíveis:

- Sob revisão – Indica que esse controle ainda não foi revisado. As evidências ainda estão sendo coletadas para esse controle e você pode carregar evidências manuais. Esse é o status padrão.
- Revisado – indica que as evidências desse controle foram analisadas. As evidências ainda estão sendo coletadas, e você pode carregar evidências manuais.
- Inativo – indica que a coleta automatizada de evidências foi interrompida para esse controle. Não é mais possível carregar evidências manuais.

> **Note**
>
> Alterar o status de ucontrole para Analisado é definitivo. Depois de definir o status de um controle como Analisado, você não poderá mais alterar o status desse controle nem reverter para um status anterior.

Guia de pastas de evidências

A guia Pastas de evidências lista as evidências coletadas automaticamente para esse controle. Ela é organizada em pastas diariamente.

A tabela de Pastas de evidências mostra uma lista de pastas com os seguintes dados:

- Pasta de evidências – O nome da pasta de evidências. O nome da pasta é baseado na data em que as evidências foram coletadas ou adicionadas manualmente.
- Verificação de conformidade – O número de problemas encontrados na pasta de evidências. Esse número representa o número total de problemas de segurança que foram relatados diretamente de AWS Security Hub, AWS Config, ou ambos. Se você vir Não aplicável, isso indica que você não tem AWS Security Hub ou AWS Config habilitado, ou que a evidência vem de um tipo de fonte de dados diferente.
- Evidência total – O número total de itens de evidência dentro da pasta.

- Seleção do relatório de avaliação – O número de itens de evidência na pasta incluídos no relatório de avaliação.

A partir da guia Pastas de evidências, você pode realizar as seguintes ações:

- Analisar as evidências individuais – Escolha uma pasta de evidências para abrir. Na página de resumo da pasta de evidências, você pode escolher a evidência individual que deseja analisar.
- Adicionar evidência manual – Para obter mais informações, consulte Como adicionar evidências manuais em AWS Audit Manager.
- Adicionar evidência a um relatório de evidência – Para obter informações, consulte Como gerar um relatório de avaliação.

Guia fonte de dados

Essa guia exibe informações sobre as fontes de dados do controle. Isso inclui as informações a seguir:

- Nome da fonte de dados — Isso se aplica somente aos controles personalizados. Refere-se ao nome descritivo que você deu a cada fonte de dados. Você pode usar esse nome para distinguir entre várias fontes de dados que se enquadram no mesmo tipo de fonte de dados
- Tipo de fonte de dados — Especifica de onde vêm os dados de evidência.
  - Se o Audit Manager coletar as evidências, a fonte de dados poderá ser de um dos quatro tipos: AWS Security Hub, AWS Config, AWS CloudTrail ou AWS chamadas de API.
  - Se você carregar sua própria evidência, o tipo de fonte de dados será Manual. Uma descrição indica se a evidência manual necessária é um carregamento de arquivo ou uma resposta em texto.
- Mapeamento – Esse é o atributo de mapeamento usado para identificar e recuperar dados de uma fonte de dados automatizada.
  - Se o tipo de fonte de dado for AWS Config, o mapeamento será o nome de uma regra AWS Config específica (por exemplo, `EC2_INSTANCE_MANAGED_BY_SSM`). O Audit Manager usa esse mapeamento para relatar o resultado dessa verificação de regras diretamente de AWS Config.
  - Se o tipo de fonte de dados for AWS Security Hub, o mapeamento será o nome de um controle específico do Security Hub (por exemplo, `1.1 – Avoid the use of the "root"`

`account`). O Audit Manager usa esse mapeamento para relatar o resultado dessa verificação de segurança diretamente do Hub de Segurança.

- Se o tipo da fonte de dados for chamadas de API AWS, o mapeamento será o nome de uma chamada de API específica (por exemplo, `ec2_DescribeSecurityGroups`). O Audit Manager usa esse mapeamento para coletar a resposta da API.
- Se o tipo da fonte da dados for AWS CloudTrail, o mapeamento será o nome de uma regra específica `CreateAccessKey` (por exemplo,). O Audit Manager usa esse mapeamento para coletar a atividade relacionada do usuário a partir dos seus logs do CloudTrail.

- Frequência – A frequência da coleta de evidências dessa fonte de dados. A frequência varia de acordo com a fonte de dados. Para obter mais informações, escolha o valor na coluna ou consulte Frequência das coletas de evidências.

Guia de comentários

Na guia Comentários, você pode adicionar um comentário sobre o controle e suas evidências. Ele também exibe uma lista de comentários anteriores.

Em Enviar comentários, você pode adicionar comentários para um controle inserindo texto e escolhendo Enviar comentários.

Em Comentários anteriores, você pode ver uma lista de comentários anteriores junto com a data na qual o comentário foi feito e a ID de usuário associada.

Guia changelog

A guia Changelog exibe uma lista das atividades do usuário relacionadas ao controle. As mesmas informações estão disponíveis nos logs da trilha de auditoria em AWS CloudTrail. Com a atividade do usuário capturada diretamente no Audit Manager, você pode analisar facilmente uma trilha de auditoria da atividade de um determinado controle.

Em Changelog, uma tabela exibe as seguintes colunas de dados:

- Data – A data e a hora da atividade, representadas no formato Tempo Universal Coordenado (UTC).
- Usuário – O usuário ou função que realizou a atividade.
- Ação – Uma descrição da atividade.
- Tipo – O atributo associado que descreve melhor a atividade.

- Recurso – O recurso relacionado, se aplicável.

O Audit Manager rastreia as seguintes atividades do usuário nos changelogs:

- Como criar uma avaliação
- Como editar uma avaliação
- Concluindo uma avaliação
- Como excluir uma avaliação
- Delegando um conjunto de controles para análise
- Enviando um conjunto de controles analisado de volta ao proprietário da auditoria
- Carregando uma evidência manual
- Atualizando um status de controle
- Gerando relatórios de avaliação

Analisando a evidência em uma avaliação

Uma avaliação ativa no Audit Manager coleta automaticamente evidências de uma variedade de fontes de dados. Para obter mais informações, consulte Como AWS Audit Manager coleta evidências. Você pode abrir e analisar evidências para os controles em suas avaliações a qualquer momento.

Para abrir uma evidência para um controle

1. Abra o console do AWS Audit Manager em https://console.aws.amazon.com/auditmanager/home.
2. No painel de navegação, escolha Avaliações e o nome da avaliação para abri-la.
3. A partir da guia de avaliação, escolha Controles, role para baixo até a tabela Conjuntos de controles e então, selecione o nome de um controle para abri-lo.
4. Na página de controle, selecione a guia Pastas de evidências. Na tabela Pastas de evidências, uma lista de pastas contendo evidências desse controle é exibida. Essas pastas são organizadas e nomeadas com base na data na qual as evidências dentro dessa pasta foram coletadas.
5. Selecione o nome de uma pasta de evidências para abri-la.

A partir daqui, você pode analisar as pastas de evidências desse controle e detalhar ainda mais para analisar as evidências individuais, conforme necessário.

Tópicos

- Analisando pastas de evidências
- Analisando evidências individuais

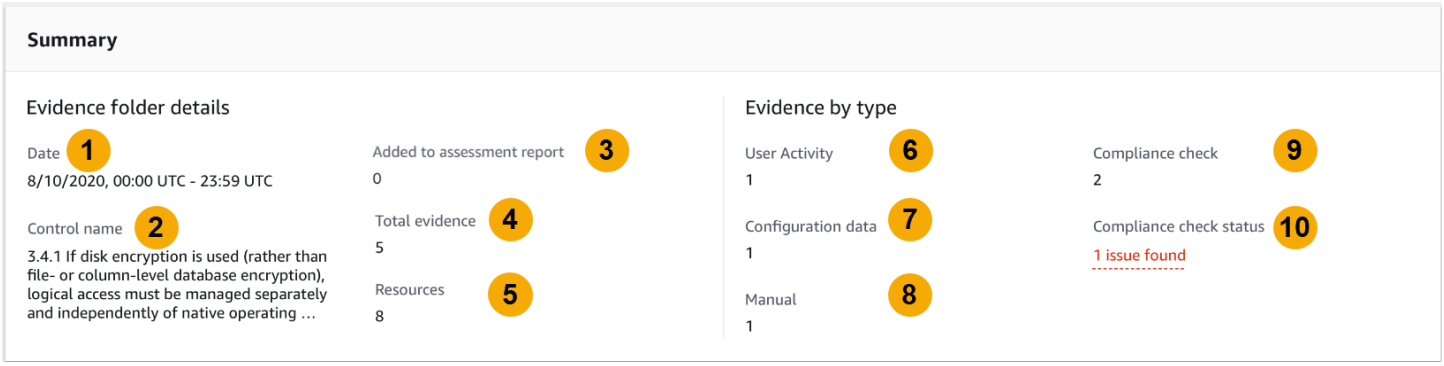
Analisando pastas de evidências

Ao abrir uma pasta de evidências, você vê uma página de resumo da pasta de evidências que contém duas seções: uma seção de Resumo e uma tabela de Evidências. Essas seções e seu conteúdo são descritos a seguir.

- Resumo da pasta de evidências
- Tabela evidências

Resumo da pasta de evidências

A seção Resumo da página fornece uma visão geral de alto nível das evidências na pasta.



Isso inclui as informações a seguir:

1. Data – A hora e a data na qual a pasta de evidências foi criada, representada em Tempo Universal Coordenado (UTC).
2. Nome do controle – O nome do controle associado à pasta de evidências.
3. Seleção do relatório de avaliação – O número de itens de evidência escolhidos manualmente para incluir no relatório de avaliação.
4. Evidência total – O número total de itens de evidência dentro da pasta de evidências.

5. Recursos – O número total de recursos AWS avaliados ao gerar as evidências nesta pasta.
6. Atividade do usuário – O número de itens de evidência que se enquadra na categoria de Atividade do usuário. Essas evidências são coletadas a partir de logs AWS CloudTrail.
7. Dados de configuração – O número de itens de evidência que se enquadra na categoria de Dados de configuração. Essa evidência é coletada a partir de capturas de tela de configuração de outros Serviços da AWS, como o Amazon EC2, o Amazon S3 ou o IAM.
8. Manual – O número de itens de evidência que se enquadram na categoria Manual. Essa evidência é carregada manualmente.
9. Verificação de conformidade – O número de itens de evidência que se enquadram na categoria de Verificação de conformidade. Essas evidências são coletadas de AWS Config ou AWS Security Hub.
10. Status da verificação de conformidade – O número total de problemas relatados diretamente de AWS Security Hub, AWS Config, ou ambos.

> **Tip**
>
> Para obter mais informações sobre diferentes tipos de evidências (atividade do usuário, dados de configuração, verificação de conformidade e manual), consulte Evidências.

Tabela evidências

A tabela Evidências lista as evidências individuais contidas na pasta de evidências.

Isso inclui as informações a seguir:

1. Horário – Especifica quando a evidência foi coletada e também serve como nome da mesma. A hora é representada no formato Tempo Universal Coordenado (UTC). A escolha de um horário nessa coluna abre uma Página de detalhes da evidência. Essa página é descrita nas seções a seguir.
2. Evidência por tipo – A categoria da evidência.
   - As evidências de Verificação de conformidade são coletadas a partir de AWS Config ou AWS Security Hub.
   - A evidência Atividade do usuário é coletada dos logs AWS CloudTrail.
   - A evidência de Dados de configuração é coletada de capturas de tela de outros serviços, como Amazon EC2, Amazon S3 ou IAM.

- A evidência Manual é a evidência que você carrega manualmente.

3. Verificação de conformidade – O status da avaliação das evidências que se enquadram na categoria de Verificação de conformidade.
   - Para evidências coletadas de AWS Security Hub, um resultado de Aprovado ou Falha é relatado diretamente de AWS Security Hub.
   - Para evidências coletadas de AWS Config, um resultado de Em confirmidade ou Não Confirmidade é relatado diretamente de AWS Config.
   - Se Não aplicável for exibido, isso indica que você não tem AWS Security Hub ou AWS Config habilitados, ou que a evidência vem de um tipo de fonte de dados diferente.
4. Fonte de dados – A fonte de dados da qual as evidências são coletadas.
5. Nome do evento — O nome do evento incluso na evidência.
6. Recursos – O número de recursos avaliados para gerar a evidência.
7. Seleção do relatório de avaliação – Indica se essa evidência foi selecionada manualmente para inclusão no relatório de avaliação.
   - Para incluir evidências, selecione-as e escolha Adicionar ao relatório de avaliação.
   - Para excluir evidências, selecione-as e escolha Remover do relatório de avaliação.

Para carregar evidências manuais para a pasta de evidências, escolha Carregar evidência manual, insira o URI S3 da evidência e escolha Carregar. Para obter mais informações, consulte Como carregar evidências manuais em AWS Audit Manager.

Para ver detalhes de qualquer evidência individual, escolha o nome da evidência com hiperlink na coluna Hora. Isso abre uma página de detalhes da evidência, descrita na seção a seguir.

Analisando evidências individuais

Ao abrir uma evidência individual, você vê uma página de detalhes da evidência contendo três seções: a seção de Detalhes da evidência, a tabela de Atributos e a tabela Atributos incluídos. Essas seções e seu conteúdo são descritos a seguir.

- Detalhe da evidência
- Atributos
- Recursos incluídos

Detalhe da evidência

A seção de Detalhes da evidência da página exibe uma visão geral das evidências.

Isso inclui as informações a seguir:

1. Data – A hora e a data na qual a evidência foi coletada, representada no Tempo Universal Coordenado (UTC).
2. Nome da pasta de evidências – O nome da pasta de evidências contendo as mesmas.
3. Nome do controle – O nome do controle associado à evidência.
4. Fonte do evento – O nome do recurso que criou o evento de evidência.
5. Nome do evento — O nome do evento de evidência.
6. Fonte de dados – A fonte de dados da qual a evidência foi coletada.
7. Evidência por tipo – O tipo da evidência.
   - As evidências de Verificação de conformidade são coletadas a partir de AWS Config ou AWS Security Hub.
   - A evidência Atividade do usuário é coletada dos logs AWS CloudTrail.
   - A evidência de Dados de configuração é coletada de capturas de tela de outros Serviços da AWS, como Amazon EC2, Amazon S3 ou IAM.
   - A evidência Manual é a evidência que você carrega manualmente.
8. Verificação de conformidade – O status da avaliação das evidências que se enquadram na categoria de Verificação de conformidade.
   - Para evidências coletadas de AWS Security Hub, um resultado de Aprovado ou Falha é relatado diretamente de AWS Security Hub.
   - Para evidências coletadas de AWS Config, um resultado de Em confirmidade ou Não Confirmidade é relatado diretamente de AWS Config.

- Se Não aplicável for exibido, isso indica que você não tem AWS Security Hub ou AWS Config habilitados, ou ainda que a evidência vem de um tipo diferente de fonte de dados.

9. Atributos incluídos – O número de atributos avaliados para gerar a evidência.
10. Atributos – O número total de atributos que são usados pelo evento na evidência.
11. AWS conta – O Conta da AWS de onde as evidências foram coletadas.
12. JD do IAM – O usuário ou função relevante, se aplicável.
13. Adicionado ao relatório de avaliação – Indica se você optou por incluir a evidência no relatório de avaliação.

Atributos

A tabela de Atributos exibe os nomes e valores que são usados pelo evento nessa evidência. Isso inclui as informações a seguir:

- Nome do atributo – O requisito para a evidência, como allowUsersToChangePassword.
- Valor – O valor do atributo, como verdadeiro ou falso.

Recursos incluídos

A tabela Recursos incluídos exibe a lista de recursos avaliados para gerar essa evidência. Ele inclui um mais campos a seguir:

- ARN – O nome do recurso da Amazon (ARN) do atributo. Um ARN pode não estar disponível para todos os tipos de evidências.
- Valor – O valor desse recurso, se aplicável.
- JSON – O link para visualizar o arquivo JSON desse recurso.

Como adicionar evidências manuais em AWS Audit Manager

O Audit Manager pode coletar automaticamente evidências para vários controles. No entanto, alguns controles exigem que você adicione manualmente suas próprias evidências.

Considere os seguintes exemplos:

- Alguns controles estão relacionados ao fornecimento de registros físicos, (como assinaturas) ou eventos que não são gerados na nuvem (como observações e entrevistas). Nesses casos,

você pode carregar manualmente arquivos como evidência. Por exemplo, se um controle exigir informações sobre seu framework organizacional, você pode carregá-las a partir de uma cópia do organograma da sua empresa como evidência manual.

- Alguns controles representam uma questão de avaliação de risco do fornecedor. Uma pergunta de avaliação de risco pode exigir documentação como evidência (como um organograma). Ou talvez precise apenas de uma resposta de texto simples (como uma lista de cargos). No caso deste último, você pode responder a pergunta e salvar sua resposta como evidência manual.

Você também pode usar o atributo de carregamento manual para gerenciar evidências de vários ambientes. Se sua empresa usa um modelo de nuvem híbrida ou multicloud, você pode carregar evidências do seu ambiente on-premises, de um ambiente hospedado na nuvem ou de seus aplicativos SaaS. Isso permite que você organize suas evidências (independentemente de onde elas vieram) armazenando-as no framework de uma avaliação do Audit Manager, onde cada evidência é mapeada para um controle específico.

Para saber mais sobre os diferentes tipos de evidência no Audit Manager, consulte Evidências na seção Conceitos e terminologia deste guia.

Como adicionar evidências manuais

Você pode usar qualquer um dos métodos a seguir para adicionar sua própria evidência manual a um controle de avaliação.

Lembre-se do seguinte:

- Só é possível usar um método de cada vez para adicionar evidências manuais.
- O tamanho máximo suportado para um único arquivo de evidência manual é 100 MB.
- Os Formatos de arquivo compatíveis para evidências manuais estão listados abaixo nesta página.
- Cada Conta da AWS só pode carregar manualmente até 100 arquivos de evidências para um controle por dia. Exceder essa cota diária faz com que qualquer carregamento manual adicional falhe nesse controle. Se você precisar carregar uma grande quantidade de evidências manuais em um único controle, carregue as evidências em lotes ao longo de vários dias.
- Quando um controle está no status Inativo, você não pode adicionar evidências manuais para o controle. Para carregar manual de evidências, primeiro você deve alterar o status do controle para Em análise ou Revisado. Para obter instruções, consulte Como atualizar o status do controle.

Importar um arquivo do Amazon S3

Siga estas etapas para exportar evidências manuais de um bucket S3.

AWS console

Para importar um arquivo do S3 (console)

1. Abra o console do AWS Audit Manager em https://console.aws.amazon.com/auditmanager/home.
2. No painel de navegação à esquerda, escolha Avaliações e o nome de avaliação para abri-la.
3. Escolha a guia Controles, role para baixo até Conjuntos de controles e selecione o nome de um controle para abri-lo.
4. Na guia Pastas de evidências, escolha Adicionar evidência manual e, em seguida, Importar arquivo S3.
   - Como alternativa, escolha um nome de pasta de evidências na guia Pastas de evidências para analisar o resumo da pasta de evidências e, em seguida, escolha Adicionar evidência manual, Importar arquivo do S3.
5. Na próxima página, insira o URI do S3 da evidência. Você pode encontrar o URI do S3 navegando até o objeto no Console do Amazon S3 e escolhendo Copiar URI do S3.
6. Escolha Carregar.

AWS CLI

No procedimento a seguir, substitua cada *texto do espaço reservado* por suas próprias informações.

Para importar um arquivo do S3 (CLI)

1. Execute o comando `list-assessments` para ver uma lista com as suas avaliações.

   ```
   aws auditmanager list-assessments
   ```

   Na resposta, encontre a avaliação para a qual deseja enviar evidências e anote ID da avaliação.
2. Execute o comando `get-assessment` e especifique ID da avaliação na primeira etapa.

```
aws auditmanager get-assessment --assessment-
id 1a2b3c4d-5e6f-7g8h-9i0j-0k1l2m3n4o5p
```

Na resposta, encontre o conjunto de controles e o controle para o qual deseja enviar evidências e anote seus IDs.

3. Execute o comando batch-import-evidence-to-assessment-control com os seguintes parâmetros:

   - `--assessment-id` – Use o ID da avaliação da primeira etapa.
   - `--control-set-id` – Use o ID do conjunto de controles da etapa dois.
   - `--control-id` – Use o ID do controle da etapa dois.
   - `--manual-evidence` – Use `s3ResourcePath` como tipo de evidência manual e especifique o URI S3 da evidência. Você pode encontrar o URI do S3 navegando até o objeto no console do Amazon S3 e escolhendo Copiar URI do S3.

```
aws auditmanager batch-import-evidence-to-assessment-control --assessment-
id 1a2b3c4d-5e6f-7g8h-9i0j-0k1l2m3n4o5p --control-set-id ControlSet --control-
id a1b2c3d4-e5f6-g7h8-i9j0-k1l2m3n4o5p6 --manual-evidence s3ResourcePath=s3://
example-bucket/example-file.extension
```

Audit Manager API

Para importar um arquivo do S3 (API)

1. Chame a operação ListAssessments para ver uma lista de suas avaliações. Na resposta, encontre a avaliação para a qual deseja enviar evidências e anote ID da avaliação.
2. Chame a operação GetAssessment e especifique ID da avaliação na primeira etapa. Na resposta, encontre o conjunto de controles e o controle para o qual deseja enviar evidências e anote seus IDs.
3. Chame a operação BatchImportEvidenceToAssessmentControl com os seguintes parâmetros:

   - assessmentId – Use o ID da avaliação da primeira etapa.
   - controlSetId – Use o ID do conjunto de controles da etapa dois.

- `controlId` – Use o ID do controle da etapa dois.
- `manualEvidence` – Use `s3ResourcePath` como tipo de evidência manual e especifique o URI S3 da evidência. Você pode encontrar o URI do S3 navegando até o objeto no console do Amazon S3 e escolhendo Copiar URI do S3.

Para obter mais informações, escolha um dos links anteriores para ler mais na Referência de API AWS Audit Manager. Isso inclui informações sobre como usar essas operações e os parâmetros em um dos SDKs da AWS específicos do idioma.

Carregar um arquivo do seu navegador

Siga estas etapas para carregar evidências manuais do seu navegador.

AWS console

Carregar um arquivo do seu navegador (console)

1. Abra o console do AWS Audit Manager em https://console.aws.amazon.com/auditmanager/home.
2. No painel de navegação à esquerda, escolha Avaliações e o nome de avaliação para abri-la.
3. Escolha a guia Controles, role para baixo até Conjuntos de controle e então, selecione o nome de um controle para abri-lo.

   A partir daqui, há três maneiras de carregar um arquivo:

   - (Opção 1) No banner de notificação azul, escolha Carregar evidência manual.
   - (Opção 2) Na guia Pastas de evidências, escolha Adicionar evidência manual e, em seguida, Carregar arquivo do navegador.
   - (Opção 3) Escolha um nome de pasta de evidências para analisar um resumo, escolha Adicionar evidência manual e, em seguida, Carregar arquivo do navegador.
4. Escolha o arquivo que deseja carregar.
5. Escolha Carregar.

AWS CLI

No procedimento a seguir, substitua cada *texto do espaço reservado* por suas próprias informações.

Para carregar um arquivo do seu navegador (CLI)

1. Execute o comando `list-assessments` para ver uma lista com as suas avaliações.

   ```
   aws auditmanager list-assessments
   ```

   Na resposta, encontre a avaliação para a qual deseja enviar evidências e anote ID da avaliação.
2. Execute o comando `get-assessment` e especifique ID da avaliação na primeira etapa.

   ```
   aws auditmanager get-assessment --assessment-
   id 1a2b3c4d-5e6f-7g8h-9i0j-0k1l2m3n4o5p
   ```

   Na resposta, encontre o conjunto de controles e o controle para o qual deseja enviar evidências e anote seus IDs.
3. Execute o comando `get-evidence-file-upload-url` e especifique o arquivo que deseja carregar.

   ```
   aws auditmanager get-evidence-file-upload-url --file-name fileName.extension
   ```

   Na resposta, anote a URL pré-assinada e o `evidenceFileName`.
4. Use a URL pré-assinada da etapa três para carregar o arquivo do seu navegador. Essa ação carrega seu arquivo para o Amazon S3, onde ele é salvo como um objeto, que pode ser anexado a um controle de avaliação. Na etapa a seguir, você referenciará o objeto recém-criado usando o parâmetro `evidenceFileName`.

   > **Note**
   >
   > Quando você carrega um arquivo usando uma URL pré-assinada, o Audit Manager protege e armazena seus dados usando criptografia do lado do servidor com AWS Key Management Service. Para suporte, você deve usar o cabeçalho `x-amz-server-side-encryption` em sua solicitação ao usar a URL pré-assinada para carregar seu arquivo.

Se estiver usando um cliente gerenciado AWS KMS key nas configurações Criptografia de dados do Audit Manager, certifique-se de incluir também o cabeçalho `x-amz-server-side-encryption-aws-kms-key-id` na sua solicitação. Se o cabeçalho `x-amz-server-side-encryption-aws-kms-key-id` não estiver presente na solicitação, o Amazon S3 presumirá que você quer usar a Chave gerenciada pela AWS.
Para obter mais informações, consulte Como proteger os dados usando criptografia do lado do servidor com AWS Key Management Service chaves (SSE-KMS) do Guia do Usuário do Amazon Simple Storage Service.

5. Execute o comando `batch-import-evidence-to-assessment-control` com os seguintes parâmetros:

   - `--assessment-id` – Use o ID da avaliação da primeira etapa.
   - `--control-set-id` – Use o ID do conjunto de controles da etapa dois.
   - `--control-id` – Use o ID do controle da etapa dois.
   - `--manual-evidence` – Use `evidenceFileName` como tipo de evidência manual e especifique o nome do arquivo de evidência na etapa três.

```
aws auditmanager batch-import-evidence-to-assessment-control --assessment-
id 1a2b3c4d-5e6f-7g8h-9i0j-0k1l2m3n4o5p --control-set-id ControlSet
 --control-id a1b2c3d4-e5f6-g7h8-i9j0-k1l2m3n4o5p6 --manual-evidence
 evidenceFileName=fileName.extension
```

Audit Manager API

Para carregar um arquivo do seu navegador (API)

1. Chame a operação `ListAssessments`. Na resposta, encontre a avaliação para a qual deseja enviar evidências e anote ID da avaliação.
2. Chame a operação `GetAssessment` e especifique a `assessmentId` partir da primeira etapa. Na resposta, encontre o conjunto de controles e o controle para o qual deseja enviar evidências e anote seus IDs.
3. Chame a operação `GetEvidenceFileUploadUrl` e especifique a `fileName` que você deseja carregar. Na resposta, anote a URL pré-assinada e o `evidenceFileName`.

4. Use a URL pré-assinada da etapa três para carregar o arquivo do seu navegador. Essa ação carrega seu arquivo para o Amazon S3, onde ele é salvo como um objeto, que pode ser anexado a um controle de avaliação. Na etapa a seguir, você referenciará o objeto recém-criado usando o parâmetro `evidenceFileName`.

   > **Note**
   >
   > Quando você carrega um arquivo usando uma URL pré-assinada, o Audit Manager protege e armazena seus dados usando criptografia do lado do servidor com AWS Key Management Service. Para suporte, você deve usar o cabeçalho `x-amz-server-side-encryption` em sua solicitação ao usar a URL pré-assinada para carregar seu arquivo.
   >
   > Se estiver usando um cliente gerenciado AWS KMS key nas configurações Criptografia de dados do Audit Manager, certifique-se de incluir também o cabeçalho `x-amz-server-side-encryption-aws-kms-key-id` na sua solicitação. Se o cabeçalho `x-amz-server-side-encryption-aws-kms-key-id` não estiver presente na solicitação, o Amazon S3 presumirá que você quer usar a Chave gerenciada pela AWS.
   >
   > Para obter mais informações, consulte Como proteger os dados usando criptografia do lado do servidor com AWS Key Management Service chaves (SSE-KMS) do Guia do Usuário do Amazon Simple Storage Service.

5. Chame a operação `BatchImportEvidenceToAssessmentControl` com os seguintes parâmetros:

   - `assessmentId` – Use o ID da avaliação da primeira etapa.
   - `controlSetId` – Use o ID do conjunto de controles da etapa dois.
   - `controlId` – Use o ID do controle da etapa dois.
   - `manualEvidence` – Use `evidenceFileName` como tipo de evidência manual e especifique o nome do arquivo de evidência na etapa três.

Para obter mais informações, escolha um dos links anteriores para ler mais na Referência de API AWS Audit Manager. Isso inclui informações sobre como usar essas operações e os parâmetros em um dos SDKs da AWS específicos do idioma.

Insira uma resposta de texto

Siga estas etapas para inserir uma resposta a uma pergunta de avaliação de risco e salvar sua resposta como evidência manual.

AWS console

Para inserir uma resposta de texto (console)

1. Abra o console do AWS Audit Manager em https://console.aws.amazon.com/auditmanager/home.
2. No painel de navegação à esquerda, escolha Avaliações e o nome de avaliação para abri-la.
3. Escolha a guia Controles, role para baixo até Conjuntos de controles e selecione o nome de um controle para abri-lo.

   A partir daqui, há três maneiras de inserir uma resposta de texto:

   - (Opção 1) No banner de notificação azul, escolha Inserir resposta.
   - (Opção 2) Na guia Pastas de evidências, escolha Adicionar evidência manual e, em seguida, escolha Inserir resposta de texto.
   - (Opção 3) Escolha um nome de pasta de evidências para analisar um resumo dessa pasta, escolha Adicionar evidência manual e, em seguida, escolha Inserir resposta de texto.
4. Na janela exibida, insira a sua resposta de texto sem formatação.
5. Selecione a opção Confirmar.

AWS CLI

No procedimento a seguir, substitua cada *texto do espaço reservado* por suas próprias informações.

Para inserir uma resposta de texto (CLI)

1. Execute o comando `list-assessments`.

   ```
   aws auditmanager list-assessments
   ```

   Na resposta, encontre a avaliação para a qual deseja enviar evidências e anote ID da avaliação.

2. Execute o comando `get-assessment` e especifique ID da avaliação na primeira etapa.

```
aws auditmanager get-assessment --assessment-
id 1a2b3c4d-5e6f-7g8h-9i0j-0k1l2m3n4o5p
```

   Na resposta, encontre o conjunto de controles e o controle para o qual deseja enviar evidências e anote seus IDs.

3. Execute o comando `batch-import-evidence-to-assessment-control` com os seguintes parâmetros:

   - `--assessment-id` – Use o ID da avaliação da primeira etapa.
   - `--control-set-id` – Use o ID do conjunto de controles da etapa dois.
   - `--control-id` – Use o ID do controle da etapa dois.
   - `--manual-evidence` – Use `textResponse` como tipo de evidência manual e insira o texto que você deseja salvar como evidência manual.

```
aws auditmanager batch-import-evidence-to-assessment-control --assessment-
id 1a2b3c4d-5e6f-7g8h-9i0j-0k1l2m3n4o5p --control-set-id ControlSet --control-
id a1b2c3d4-e5f6-g7h8-i9j0-k1l2m3n4o5p6 --manual-evidence textResponse="enter
 text here"
```

Audit Manager API

Para inserir uma resposta de texto (API)

1. Chame a operação `ListAssessments`. Na resposta, encontre a avaliação para a qual deseja enviar evidências e anote ID da avaliação.
2. Chame a operação `GetAssessment` e especifique a `assessmentId` partir da primeira etapa. Na resposta, encontre o conjunto de controles e o controle para o qual deseja enviar evidências e anote seus IDs.
3. Chame a operação `BatchImportEvidenceToAssessmentControl` com os seguintes parâmetros:

   - `assessmentId` – Use o ID da avaliação da primeira etapa.
   - `controlSetId` – Use o ID do conjunto de controles da etapa dois.

- `controlId` – Use o ID do controle da etapa dois.
- `manualEvidence` – Use `textResponse` como tipo de evidência manual e insira o texto que você deseja salvar como evidência manual.

Para obter mais informações, escolha um dos links anteriores para ler mais na Referência de API AWS Audit Manager. Isso inclui informações sobre como usar essas operações e os parâmetros em um dos SDKs da AWS específicos do idioma.

Formatos de arquivo compatíveis para evidências manuais

A tabela a seguir lista e descreve os tipos de arquivo que você pode carregar como evidência manual. Para cada tipo de arquivo, a tabela também lista as extensões de arquivo suportadas.

Tipo de arquivo	Descrição	Extensões de arquivo compatíveis
Compressão ou arquivamento	Arquivos compactados GNU .zip e arquivos compactados .zip	`.gz`, `.zip`
Documento	Arquivos de documentos comuns, como PDFs e arquivos do Microsoft Office	`.doc`, `.docx`, `.pdf`, `.ppt`, `.pptx`, `.xls`, `.xlsx`
Imagem	Arquivos de imagem e gráficos	`.jpeg`, `.jpg`, `.png`, `.svg`
Texto	Outros arquivos de texto não binários, como documentos de texto sem formatação e arquivos de linguagem de marcação	`.cer`, `.csv`, `.html`, `.jmx`, `.json`, `.md`, `.out`, `.rtf`, `.txt`, `.xml`, `.yaml`, `.yml`

Como gerar um relatório de avaliação

Um relatório de avaliação resume sua avaliação e fornece links para um conjunto organizado de pastas contendo evidências relacionadas. Para obter mais informações, consulte Relatórios de avaliação.

Você pode escolher quais evidências deseja incluir em seu relatório de avaliação antes de gerá-lo. As evidências recém-coletadas não são incluídas automaticamente em um relatório de avaliação.

Tarefas

- Como adicionar evidências a um relatório de avaliação
- Como remover evidências de um relatório de avaliação
- Como gerar um relatório de avaliação
- O que faço agora?

Como adicionar evidências a um relatório de avaliação

Antes de gerar um relatório de avaliação, você deve adicionar pelo menos uma evidência. Você pode adicionar uma pasta de evidências inteira ou itens de evidências individuais de dentro de uma pasta.

Como adicionar evidências a um relatório de avaliação

1. Abra o console do AWS Audit Manager em https://console.aws.amazon.com/auditmanager/home.
2. No painel de navegação, escolha Avaliações e escolha o nome da avaliação para abri-la.
3. Na guia Controles, role para baixo até Conjuntos de controles e então, selecione o nome de um controle para abri-lo.
4. Escolha como deseja adicionar evidências ao seu relatório de avaliação.

    a. Para adicionar uma pasta de evidências inteira, role para baixo até Pastas de evidências, selecione a pasta que deseja adicionar e escolha Adicionar ao relatório de avaliação.

    - Se não conseguir visualizar a pasta que está procurando, altere o filtro suspenso para Sempre. Caso contrário, você verá os últimos sete dias de pastas por padrão.
    - Se a opção Adicionar ao relatório de avaliação estiver cinza, a pasta de evidências já foi adicionada ao relatório de avaliação.

b. Para adicionar evidências específicas, escolha uma pasta para abrir seu conteúdo. Selecione um ou mais itens da lista e escolha Adicionar ao relatório de avaliação.

   - Se Adicionar ao relatório de avaliação estiver em cinza, certifique-se de marcar a caixa de seleção ao lado da evidência e tente novamente.

5. Depois de adicionar a evidência ao relatório de avaliação, um banner verde de êxito será exibido. Escolha Exibir evidências no relatório de avaliação para visualizar as evidências incluídas em seu relatório de avaliação.

   - Como alternativa, você pode ver as evidências incluídas em seu relatório navegando de volta até sua avaliação e escolhendo a guia Seleção do relatório de avaliação.

Como remover evidências de um relatório de avaliação

Se você precisar remover evidências de um relatório de avaliação, siga estas etapas. Você pode adicionar uma pasta de evidências inteira ou adicionar itens de evidências individuais específicas de dentro de uma pasta.

Como remover evidências de um relatório de avaliação

1. Abra o console do AWS Audit Manager em https://console.aws.amazon.com/auditmanager/home.
2. No painel de navegação, escolha Avaliações e escolha o nome da avaliação para abri-la.
3. Na guia Controles, role para baixo até Conjuntos de controles e então, selecione o nome de um controle para abri-lo.
4. Escolha como você deseja remover evidências de seu relatório de avaliação.

   a. Para remover uma pasta de evidências inteira, role para baixo até Pastas de evidências, selecione a pasta que você deseja remover e escolha Remover do relatório de avaliação.

      - Se não conseguir visualizar a pasta que está procurando, altere o filtro suspenso para Sempre. Caso contrário, você verá os últimos sete dias de pastas por padrão.
      - Se a opção Remover ao relatório de avaliação estiver em cinza, a pasta de evidências já foi removida adicionada ao relatório de avaliação.

   b. Para remover evidências específicas, escolha uma pasta de evidências para abrir seu conteúdo. Selecione um ou mais itens da lista e escolha Remover do relatório de avaliação.

- Se Remover do relatório de avaliação estiver em cinza, certifique-se de marcar a caixa de seleção ao lado da evidência e tente novamente.

5. Depois de adicionar a evidência ao relatório de avaliação, um banner verde de êxito será exibido. Escolha Exibir evidências no relatório de avaliação para visualizar as evidências incluídas em seu relatório de avaliação.
   - Como alternativa, você pode ver as evidências incluídas em seu relatório navegando de volta até sua avaliação e escolhendo a guia Seleção do relatório de avaliação.

Como gerar um relatório de avaliação

Depois de adicionar evidências ao seu relatório de avaliação, você pode gerar o relatório final para compartilhar com seus auditores. Quando você gera um relatório de avaliação, ele é colocado no bucket S3 que você escolheu como destino para seu relatório de avaliação.

> **Tip**
>
> Para garantir que seu relatório de avaliação seja gerado com sucesso, revise nosso Dicas de configuração para o destino do seu relatório de avaliação.

Para gerar um relatório de avaliação

1. Abra o console do AWS Audit Manager em https://console.aws.amazon.com/auditmanager/home.
2. No painel de navegação à esquerda, escolha Avaliações.
3. Escolha o nome da avaliação cujo relatório deseja gerar.
4. Escolha a guia Seleção do relatório de avaliação e, em seguida, Gerar relatório de avaliação.
   - Se a opção Gerar relatório de avaliação estiver acinzentada, isso significa que nenhuma evidência foi adicionada ao relatório de avaliação ainda.
5. Na janela, forneça um nome e uma descrição para o relatório de avaliação e analise os detalhes do relatório de avaliação.
6. Escolha Gerar relatório de avaliação e aguarde alguns minutos enquanto seu relatório é gerado.
7. Você pode verificar o status dos seus relatórios de avaliação na página Central de downloads no console do Audit Manager.

- Como alternativa, você pode acessar o bucket S3 de destino do relatório de avaliação e baixá-lo de lá.

O relatório de avaliação tem uma soma de verificação em arquivo para garantir sua integridade. Você pode validar isso com a operação de API ValidateAssessmentReportIntegrity fornecida pelo Audit Manager.

O que faço agora?

Depois de gerar a sua avaliação, você poderá saber mais sobre o seguinte:

- Encontre e baixe seu relatório de avaliação – Saiba como baixar seu relatório de avaliação do Centro de downloads ou Amazon S3.
- Explore o seu relatório de avaliação – Saiba como navegar em um relatório de avaliação e explorar seu conteúdo.
- Valide o seu relatório de avaliação – Saiba como usar a operação da API ValidateAssessmentReportIntegrity para validar o seu relatório de avaliação.
- Excluir um relatório de avaliação indesejado – Saiba como excluir um relatório indesejado do centro de downloads ou do Amazon S3.

Como alterar o status de uma avaliação para inativo

Quando você não quiser mais coletar evidências para uma avaliação, poderá alterar o status da avaliação para Inativa. Quando o status de uma avaliação muda para inativa, a avaliação para de coletar evidências. Como resultado, você não receberá mais nenhuma cobrança por essa avaliação.

Além de interromper a coleta de evidências, o Audit Manager faz as seguintes alterações nos controles dentro da avaliação inativa:

- Todos os conjuntos de controle mudam para o status Analisado.
- Todos os controles Sob análise mudam para o status Analisado.
- Os delegados da avaliação inativa não poderão mais visualizar ou editar seus controles e conjuntos de controles.

> **Warning**
>
> Essa ação é irreversível. Recomendamos que você proceda com cuidado e certifique-se de que deseja marcar a sua avaliação como inativa. Quando uma avaliação está inativa, você tem acesso somentede leitura ao seu conteúdo. Isso significa que você ainda pode visualizar evidências coletadas anteriormente e gerar relatórios de avaliação. No entanto, você não pode editar a avaliação inativa, adicionar comentários ou carregar qualquer evidência manual.

Audit Manager console

Para alterar o status de uma avaliação para inativa (console)

1. Abra o console do AWS Audit Manager em https://console.aws.amazon.com/auditmanager/home.
2. No painel de navegação, escolha Avaliações.
3. Escolha o nome da avaliação para abri-la.
4. No canto superior direito da página, escolha Atualizar status de avaliação e, em seguida, Inativo.
5. Escolha Atualizar status na janela para confirmar que deseja alterar o status para inativo.

As alterações na avaliação e seus controles entrarão em vigor após aproximadamente um minuto.

AWS CLI

Para alterar o status de uma avaliação para inativo (AWS CLI)

1. Primeiro, identifique a avaliação que deseja atualizar. Para fazê-lo, execute o comando list-assessments.

```
aws auditmanager list-assessments
```

A resposta retorna uma lista de avaliações. Encontre a avaliação que deseja desativar e anote a ID.

2. Em seguida, execute o comando update-assessment-status e especifique os seguintes parâmetros:

   - `--assessment-id` – Use esse parâmetro para especificar a avaliação que você deseja desativar.
   - `--status` – defina este valor como `INACTIVE`.

   No exemplo a seguir, substitua o *`texto do espaço reservado`* por suas próprias informações.

   ```
   aws auditmanager update-assessment-status --assessment-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 --status INACTIVE
   ```

As alterações na avaliação e seus controles entrarão em vigor após aproximadamente um minuto.

Audit Manager API

Para alterar o status de uma avaliação para inativo (API)

1. Use a operação ListAssessments para encontrar a avaliação que você deseja desativar e anote a ID da avaliação.
2. Use a operação update-assessment-status e especifique os seguintes parâmetros:

   - assessmentId – Use esse parâmetro para especificar a avaliação que você deseja desativar.
   - Status – Defina esse valor para `INACTIVE`.

As alterações na avaliação e seus controles entrarão em vigor após aproximadamente um minuto.

Para obter mais informações sobre essas operações de API, escolha qualquer um dos links anteriores para ler mais na Referência de API AWS Audit Manager. Isso inclui informações sobre como usar essas operações e os parâmetros em um dos SDKs da AWS específicos do idioma.

Como excluir uma avaliação

Você pode excluir qualquer avaliação do Audit Manager de que não necessite mais. Você pode excluir avaliações usando o console do Audit Manager, a API do Audit Manager ou o AWS Command Line Interface (AWS CLI).

> **Warning**
>
> Essa ação exclui permanentemente sua avaliação e todas as evidências coletadas por ela. Não é possível recuperar esses dados. Como resultado, recomendamos que você proceda com cuidado e que tenha certeza de que deseja excluir a avaliação.

Audit Manager console

Para excluir uma avaliação (console)

1. Abra o console do AWS Audit Manager em https://console.aws.amazon.com/auditmanager/home.
2. No painel de navegação, escolha Avaliações.
3. Selecione a avaliação que deseja excluir e escolha Excluir.
   - Como alternativa, você pode abrir a avaliação e escolher Excluir no canto superior direito da página.

AWS CLI

Para excluir uma avaliação (AWS CLI)

1. Primeiro, identifique a avaliação que você deseja excluir. Para fazê-lo, execute o comando list-assessments.

   ```
   aws auditmanager list-assessments
   ```

   A resposta retorna uma lista de avaliações. Encontre a avaliação que você deseja excluir e anote o ID da avaliação.
2. Em seguida, use o comando delete-assessment e especifique o `--assessment-id` da avaliação que você deseja excluir.

No exemplo a seguir, substitua o *texto do espaço reservado* por suas próprias informações.

```
aws auditmanager delete-assessment --assessment-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Audit Manager API

Para excluir uma avaliação (API)

1. Use a operação ListAssessments para localizar a avaliação que deseja excluir.

   Na resposta, anote a ID da avaliação.
2. Em seguida, use o comando delete-assessment e especifique assessmentId da avaliação que você deseja excluir.

Para obter mais informações sobre essas operações de API, escolha qualquer um dos links anteriores para ler mais na Referência de API AWS Audit Manager. Isso inclui informações sobre como usar essas operações e os parâmetros em um dos SDKs da AWS específicos do idioma.

> **Tip**
>
> Se sua meta é reduzir custos, altere o status da avaliação para inativa em vez de excluí-la. Essa ação interrompe a coleta de evidências e coloca sua avaliação em um estado somente leitura, no qual você pode analisar as evidências coletadas anteriormente. Avaliações inativas não geram cobranças.

Delegações em AWS Audit Manager

Os proprietários de auditoria usam o AWS Audit Manager para criar avaliações e coletar evidências para os controles listados nessa avaliação. Às vezes, os proprietários da auditoria podem ter dúvidas ou precisar de ajuda ao validar as evidências de um conjunto de controles. Nessa situação, o proprietário da auditoria pode delegar um conjunto de controles a um especialista no assunto para análise.

Em alto nível, o processo de delegação é o seguinte.

1. O proprietário da auditoria escolhe um conjunto de controles em sua avaliação e o delega para análise.
2. O delegado revisa esses controles e suas evidências e envia o conjunto de controles ao proprietário da auditoria quando concluído.
3. O proprietário da auditoria é notificado de que a análise foi concluída e verifica se há comentários do delegado nos controles analisados.

Use as seções a seguir deste guia para saber mais sobre como gerenciar tarefas de delegação no AWS Audit Manager.

Tópicos

> **Note**
>
> Uma conta pode ser proprietária de uma auditoria ou delegada em regiões diferentes da AWS.

Tarefas de delegação para proprietários de auditoria

Como proprietário de uma auditoria no AWS Audit Manager, você pode precisar da ajuda de um especialista no assunto para ajudá-lo a analisar os controles e as evidências. Nessa situação, você pode delegar um conjunto de controles para análise.

Os tópicos a seguir descrevem como gerenciar delegações no AWS Audit Manager.

Delegando tarefas

- Delegando um conjunto de controles para análise
- Acessando suas delegações ativas e concluídas
- Excluindo suas delegações ativas e concluídas

Delegando um conjunto de controles para análise

Quando precisar da ajuda de um especialista no assunto, você pode escolher a conta da AWS que deseja ajudá-lo e, em seguida, delegar um conjunto de controles a ele para análise.

Você pode usar um dos seguintes procedimentos para delegar um conjunto de controles.

Delegando um conjunto de controles de uma página de avaliação

Para delegar um conjunto de controles de uma página de avaliação

1. Abra o console do AWS Audit Manager em https://console.aws.amazon.com/auditmanager/home.
2. No painel de navegação, escolha Avaliações.
3. Selecione o nome da avaliação contendo o conjunto de controles a ser delegado.
4. Na página de avaliação, selecione a guia Controles. Isso exibe o resumo do status do controle e a lista de controles na avaliação.
5. Selecione um conjunto de controles e selecione Delegar conjunto de controles.
6. Em Seleção de delegados, uma lista de usuários e funções é exibida. Escolha um usuário ou função ou use a barra de pesquisa para procurar por um.
7. Em Detalhes da delegação, Analise o nome do conjunto de controles e o nome da avaliação.
8. (Opcional) Em Comentários, adicione um comentário com instruções para ajudar o delegado a cumprir sua tarefa de análise. Não inclua nenhuma informação confidencial no seu comentário.
9. Selecione Delegar conjunto de controles.
10. Um banner verde de sucesso confirma a delegação bem-sucedida do conjunto de controles. Selecione Exibir delegação para ver a solicitação de delegação. Você também pode visualizar suas delegações a qualquer momento escolhendo Delegações no painel de navegação esquerdo do console do AWS Audit Manager.

Delegando um conjunto de controles na página de delegações

Para delegar um conjunto de controles da página de delegações

1. Abra o console do AWS Audit Manager em https://console.aws.amazon.com/auditmanager/home.
2. No painel de navegação, selecione Delegações.
3. Na página de delegações, selecione Criar delegação.
4. Em Escolher conjunto de avaliação e controle, especifique a avaliação e o conjunto de controles que você deseja delegar.
5. Em Seleção de delegados, uma lista de usuários e funções é exibida. Escolha um usuário ou função ou use a barra de pesquisa para procurar por um.
6. (Opcional) Em Comentários, adicione um comentário com instruções para ajudar o delegado a cumprir sua tarefa de análise. Não inclua nenhuma informação confidencial no seu comentário.
7. Selecione Criar delegação.
8. Um banner verde de sucesso confirma a delegação bem-sucedida do conjunto de controles. Selecione Exibir delegação para ver a solicitação de delegação. Você também pode visualizar suas delegações a qualquer momento escolhendo Delegações no painel de navegação esquerdo do console do AWS Audit Manager.

Quando você delega um conjunto de controles para análise, o delegado recebe uma notificação e pode então começar a analisar o conjunto de controles. Esse processo que os delegados seguem é descrito em Tarefas de delegação para delegados.

> **Tip**
>
> Os representantes podem se inscrever em um tópico do SNS para receber alertas por e-mail quando uma tarefa de análise for delegada a eles. Para obter mais informações sobre como identificar e assinar o tópico do SNS associado ao AWS Audit Manager, consulte Notificações no AWS Audit Manager.

Acessando suas delegações ativas e concluídas

Você pode acessar uma lista das suas delegações a qualquer momento escolhendo Delegações no painel de navegação esquerdo do AWS Audit Manager. A página de delegações contém uma lista de delegações ativas e concluídas, com os seguintes detalhes para cada uma:

- Delegado a — a conta da AWS a qual você delegou o conjunto de controles.
- Data — a data em que o conjunto de controles foi delegado.
- Status — o status atual da delegação.
- Avaliação — o nome da avaliação com um link para a página de detalhes da avaliação.
- Conjunto de controles — o nome do conjunto de controles que foi delegado para análise.

Quando uma delegação é concluída, você recebe uma notificação no AWS Audit Manager. Você também pode receber comentários com observações do delegado. O procedimento a seguir explica como verificar suas notificações no Audit Manager após a conclusão de uma delegação e como visualizar quaisquer comentários que o delegado possa ter deixado para você.

Para visualizar uma delegação completa e verificar se há comentários

1. Abra o console do AWS Audit Manager em https://console.aws.amazon.com/auditmanager/home.
2. No painel de navegação, selecione Notificações. Ou escolha Notificações na barra azul na parte superior da página para abrir a página de notificações.
3. Analise a página Notificações, que inclui uma tabela com as seguintes informações:
    - Data — a data da notificação.
    - Avaliação — o nome da avaliação associada ao conjunto de controles.
    - Conjunto de controles — o nome do conjunto de controles.
    - Fonte — o usuário ou a função do delegado que enviou o conjunto de controles completo de volta para você.
    - Descrição — comentários de alto nível fornecidos pelo delegado.
4. Encontre o conjunto de avaliação e controle que o delegado analisou e enviou a você e selecione o nome da avaliação para abri-la.
5. Na guia Controles da página de detalhes da avaliação, role para baixo até a tabela Conjuntos de controles. Na coluna Controles agrupados por conjunto de controles, expanda o nome de

um conjunto de controles para mostrar seus controles. Em seguida, selecione o nome de um controle para abrir a página de detalhes do controle.

6. Selecione a guia Comentários para ver quaisquer comentários adicionados pelo delegado para esse controle específico.
7. Quando estiver convencido de que a análise foi concluída para um conjunto de controles, selecione o conjunto de controles e selecione análise completa do conjunto de controles.

> **Important**
>
> O Audit Manager coleta evidências continuamente. Como resultado, novas evidências adicionais podem ser coletadas após o delegado concluir a análise de um controle.
> Se quiser usar apenas evidências analisadas em seus relatórios de avaliação, consulte o registro de data e hora da análise de controle para determinar quando as evidências foram analisadas. Esse registro de data e hora pode ser encontrado na guia Changelog da página de detalhes do controle. Em seguida, você pode usar esse registro de data e hora para identificar quais evidências adicionar aos relatórios de avaliação.

Excluindo suas delegações ativas e concluídas

Pode haver circunstâncias em que você crie uma delegação, mas depois não precise mais de ajuda para analisar esse conjunto de controles. Quando isso acontecer, você poderá excluir uma delegação ativa em AWS Audit Manager. Você também pode excluir delegações concluídas que não deseje mais ver na página de delegações.

Para excluir uma delegação

1. Abra o console do AWS Audit Manager em https://console.aws.amazon.com/auditmanager/home.
2. No painel de navegação, selecione Delegações.
3. Na página Delegações, selecione a delegação que deseja cancelar e selecione Remover delegação.
4. Na janela exibida, selecione Excluir para confirmar sua seleção.

Tarefas de delegação para delegados

Os delegados geralmente têm conhecimento técnico ou comercial especializado em várias áreas diferentes. Isso inclui políticas de retenção de dados, planos de treinamento, infraestrutura de rede e gerenciamento de identidade. Eles podem ajudar os responsáveis pela auditoria a analisar evidências coletadas para controles que se enquadrem na sua área de especialização.

Como delegado, você pode receber solicitações dos proprietários da auditoria para analisar as evidências associadas a um conjunto de controles. Essa solicitação indica que o proprietário da auditoria precisa de sua ajuda para validar essa evidência. Você pode ajudar os proprietários da auditoria por meio de análise de conjuntos de controles e suas evidências relacionadas, adição de comentários, carregamento de evidências adicionais e atualização de status de cada controle analisado.

Os tópicos a seguir descrevem como gerenciar delegações no AWS Audit Manager.

> **Note**
>
> Os proprietários de auditoria delegam conjuntos de controle específicos para análise, não avaliações inteiras. Como resultado, os delegados têm acesso limitado às avaliações. Os delegados podem analisar evidências, adicionar comentários, carregar evidências manuais e atualizar status de cada um dos controles no conjunto. Para obter mais informações sobre funções e permissões no Audit Manager, consulte Políticas recomendadas para personas de usuários em AWS Audit Manager.

Delegando tarefas

- Visualizando notificações para solicitações de delegação recebidas
- analisar um conjunto de controles delegado e as evidências relacionadas
- Adicionar um comentário a um controle
- Marcar um controle como analisado
- Enviar o conjunto de controles analisado de volta ao proprietário da auditoria

Visualizando notificações para solicitações de delegação recebidas

Quando um proprietário de auditoria solicita sua ajuda na análise de um conjunto de controles, você recebe uma notificação informando sobre o conjunto de controles que ele delegou a você.

> **Tip**
>
> Você também pode se inscrever em um tópico do SNS para receber alertas por e-mail quando um conjunto de controles for delegado a você para análise. Para obter mais informações, consulte Notificações no AWS Audit Manager.

Para visualizar suas notificações

1. Abra o console do AWS Audit Manager em https://console.aws.amazon.com/auditmanager/home.
2. Escolha Notificações no painel de navegação à esquerda. Ou, na barra azul na parte superior da página, escolha Exibir notificação para abrir a página de notificações.
3. Na página Notificações, Analise a lista de conjuntos de controle que foram delegados a você para análise. A tabela inclui as seguintes informações:
   - Data — data na qual o conjunto de controles foi delegado.
   - Avaliação — o nome da avaliação associada ao conjunto de controles.
   - Conjunto de controles — O nome do conjunto de controles.
   - Fonte — o usuário ou função que delegou o conjunto de controles a você.
   - Descrição — Instruções de análise fornecidas pelo proprietário da auditoria.

analisar um conjunto de controles delegado e as evidências relacionadas

Você pode ajudar os proprietários de auditoria analisando os conjuntos de controle delegados a você. Você pode examinar esses controles e suas evidências relacionadas para determinar se alguma ação adicional é necessária. Essa ação adicional pode incluir o carregamento manual de evidências adicionais para demonstrar a conformidade ou deixar um comentário detalhando as etapas de remediação seguidas.

Para analisar um conjunto de controles

1. Abra o console do AWS Audit Manager em https://console.aws.amazon.com/auditmanager/home.
2. No painel de navegação, selecione Notificações. Ou, na barra azul, escolha Exibir notificação para abrir a página de notificações.

3. Na página Notificações, uma lista de conjuntos de controle que foram delegados a você é exibida. Identifique qual conjunto de controles você deseja analisar e escolha o nome da avaliação relacionada para abrir a página de detalhes da avaliação.
4. Na guia Controles da página de detalhes da avaliação, role para baixo até a tabela Conjuntos de controles.
5. Na coluna Controles agrupados por conjunto de controles, expanda o nome de um conjunto para mostrar seus controles, e escolha o nome de um controle para abrir a página de detalhes.
6. (Opcional) Selecione Atualizar status do controle para alterar o status do controle. Enquanto sua análise estiver em andamento, você pode marcar o status como Em análise.
7. Analise as informações sobre o controle nas Pastas de evidências, Fontes de dados, Comentários e guias Changelog. Para obter mais informações sobre cada uma dessas guias e como interpretar os dados que elas contêm, consulte analisar os controles em uma avaliação.

Para analisar as evidências de um controle

1. Na página de detalhes do controle, selecione a guia Pastas de evidências.
2. Navegue até a tabela de Pastas de evidências, onde uma lista de pastas que contém evidências desse controle é exibida. Essas pastas são organizadas e nomeadas com base na data em que as evidências foram coletadas.
3. Selecione o nome de uma pasta de evidências para abri-la. Em seguida, analise um resumo de todas as evidências coletadas naquela data. Esse resumo inclui o número total de problemas de verificação de conformidade relatados diretamente do AWS Security Hub, AWS Config ou ambos. Para obter instruções sobre como interpretar os dados nesta página, consulte análise de pastas de evidências.
4. Na página de resumo da pasta de evidências, navegue até a tabela de Evidências. Na coluna Hora, selecione um item de linha para abrir. Em seguida, Analise os detalhes sobre a evidência que foi coletada naquele momento. Para obter instruções sobre como interpretar os dados nesta página de detalhes das evidência, consulte Análise de evidência individual.

> **Tip**
>
> Embora o AWS Audit Manager colete automaticamente evidências para muitos controles, em alguns casos, talvez seja necessário fornecer evidências adicionais para demonstrar

conformidade. Nesses casos, você pode carregar manualmente as evidências. Para obter instruções, consulte Carregar evidências manualmente.

Adicionar um comentário a um controle

Você pode adicionar comentários a qualquer controle analisado. Esses comentários estarão visíveis para o proprietário da auditoria.

Para adicionar um comentário a um controle

1. Abra o console do AWS Audit Manager em https://console.aws.amazon.com/auditmanager/home.
2. Escolha Notificações no painel de navegação à esquerda. Ou, na barra azul na parte superior da página, escolha Exibir notificação para abrir a página de notificações.
3. Na página Notificações, Analise a lista de conjuntos de controle que foram delegados a você. Encontre o conjunto de controles contendo o controle para o qual você deseja deixar um comentário e escolha o nome da avaliação relacionada.
4. Escolha a guia Controles, role para baixo até a tabela Conjuntos de controles e selecione o nome de um controle para abri-lo.
5. Selecione a guia Comentários.
6. Em Enviar comentários, insira seu comentário na caixa de texto.
7. Selecione Enviar comentário para adicionar seu comentário. Em seguida, seu comentário aparecerá na seção Comentários anteriores da página, junto com qualquer outro comentário relacionado a esse controle.

Marcar um controle como analisado

Você pode indicar o progresso da análise atualizando o status dos controles individuais em um conjunto de controles. Alterar o status do controle é opcional. No entanto, recomendamos que você altere o status de cada controle para analisado ao concluir a análise desse controle. Independentemente do status de cada controle individual, você ainda pode enviar os controles de volta ao proprietário da auditoria.

Para marcar um controle como analisado

1. Abra o console do AWS Audit Manager em https://console.aws.amazon.com/auditmanager/home.
2. Escolha Notificações no painel de navegação à esquerda. Ou, na barra azul na parte superior da página, escolha Exibir notificação para abrir a página de notificações.
3. Na página Notificações, Analise a lista de conjuntos de controle que foram delegados a você. Encontre o conjunto de controles que deseja marcar como analisado e escolha o nome da avaliação relacionada.
4. Na guia Controles da página de detalhes da avaliação, role para baixo até a tabela Conjuntos de controles.
5. Na coluna Controles agrupados por conjunto de controles, expanda o nome de um conjunto de controles para mostrar seus controles. Em seguida, escolha o nome de um controle para abrir a página de detalhes do controle.
6. Selecione Atualizar status do controle e altere o status para analisado.
7. Na janela exibida, selecione Atualizar status do controle para confirmar que você concluiu a análise do controle.

Enviar o conjunto de controles analisado de volta ao proprietário da auditoria

Quando terminar de analisar os controles que foram delegados a você, envie o conjunto de controles ao proprietário da auditoria. Isso conclui o processo de delegação.

Para enviar um conjunto de controles analisado de volta ao proprietário da auditoria

1. Abra o console do AWS Audit Manager em https://console.aws.amazon.com/auditmanager/home.
2. Escolha Notificações no painel de navegação à esquerda.
3. Analise a lista de conjuntos de controle que foram delegados a você. Encontre o conjunto de controles que você deseja enviar de volta ao proprietário da auditoria e escolha o nome da avaliação relacionada.
4. Role para baixo até a tabela Conjuntos de controles, selecione o conjunto de controles que você deseja enviar ao proprietário da auditoria e escolha Enviar para análise.

5. Na janela exibida, você pode adicionar comentários antes de escolher Enviar para análise. Depois de enviar o controle ao proprietário da auditoria, ele poderá visualizar quaisquer comentários que você tenha deixado para ele.

Relatórios de avaliação

Um relatório de avaliação resume as evidências selecionadas coletadas para uma avaliação. Ele também contém links para arquivos PDF com detalhes sobre cada evidência. Os conteúdos específicos, a organização e a convenção de nomenclatura de um relatório de avaliação dependem dos parâmetros escolhidos ao gerar o relatório.

Os relatórios de avaliação ajudam a selecionar e compilar as evidências relevantes para sua auditoria. No entanto, eles não avaliam a conformidade da evidência em si. Em vez disso, o Audit Manager simplesmente fornece os detalhes da evidência selecionada como um resultado que você pode compartilhar com seu auditor.

Estrutura de pastas do relatório de avaliação

Quando você baixa um relatório de avaliação, o Audit Manager produz uma pasta compactada. Ela contém seu relatório de avaliação e arquivos de evidências, relacionados em subpastas aninhadas.

A pasta compactada é estruturada da seguinte forma:

- Pasta de avaliação (exemplo: `myAssessmentName-a1b2c3d4`) — A pasta raiz.
  - Pasta do relatório de avaliação (exemplo: `reportName-a1b2c3d4e5f6g7`) — Uma subpasta na qual você pode encontrar os arquivos AssessmentReportSummary.pdf, digest.txt e README.txt.
    - Evidências por pasta de controle (exemplo: `controlName-a1b2c3d4e5f6g`) — Uma subpasta que agrupa arquivos de evidências pelo controle relacionado.
      - Evidências por pasta de fonte de dados (exemplo: `CloudTrail`, `Security Hub`) — Uma subpasta que agrupa arquivos de evidências por tipo de fonte de dados.
        - Pasta de evidências por data (exemplo: `2022-07-01`) – Uma subpasta que agrupa os arquivos de evidências pela data da coleta de evidências.
          - Arquivos de evidências — Arquivos contendo detalhes sobre evidências individuais.

Como navegar por um relatório de avaliação

Comece abrindo a pasta compactada .zip e navegue um nível abaixo, até a pasta do relatório de avaliação. Aqui, você encontra o relatório de avaliação em PDF e o arquivo README.txt.

Você pode analisar o arquivo README.txt para entender a estrutura e o conteúdo da pasta compactada .zip. Ela também fornece informações de referência sobre as convenções de nomenclatura de cada arquivo. Essas informações podem ajudá-lo a navegar diretamente para uma subpasta ou arquivo de evidências, caso esteja procurando por um item específico.

Do contrário, para procurar evidências e localizar as informações de que precisa, abra o PDF do relatório de avaliação. Isso fornece uma visão geral de alto nível do relatório, além de um resumo da avaliação a partir do qual o relatório foi criado.

Em seguida, use o índice (Table Of Contents, ou TOC) para explorar o relatório. Você pode escolher qualquer controle com hiperlink no índice para ir diretamente para um resumo desse controle.

Quando estiver pronto para analisar os detalhes da evidência para um controle, você pode fazê-lo escolhendo o nome da evidência com hiperlink. Para evidências automatizadas, o hiperlink abre um novo arquivo PDF com detalhes sobre as mesmas. Para evidências manuais, o hiperlink leva você ao bucket S3 contendo essas evidências.

> **Tip**
>
> A navegação com rastro na parte superior de cada página mostra sua localização atual no relatório de avaliação enquanto você navega por controles e evidências. Selecione o índice com hiperlink para voltar ao TOC a qualquer momento.

Seções do relatório de avaliação

Use as informações a seguir para saber mais sobre cada seção de um relatório de avaliação.

> **Note**
>
> Um hífen (-) ao lado de qualquer um dos atributos nas seções a seguir indica que o valor desse atributo é nulo ou não existe.

- Capa
- Página de visão geral
- Página de índice

- Página de controle
- Página de resumo de evidências
- Página de detalhes da evidência

Capa

A capa inclui o nome do relatório de avaliação. Ela também exibe a data e a hora em que o relatório foi gerado, junto à ID da conta do usuário que gerou o relatório.

A página de rosto é formatada conforme a seguir. O Audit Manager substitui *espaços reservados* pelas informações relevantes para seu relatório.

```
Assessment report name
Report generated on MM/DD/YYYY at HH:MM:SS AM/PM UCT by AccountID
```

Página de visão geral

A página de visão geral é composta por duas partes: um resumo do relatório em si e outro da avaliação sendo relatada.

Resumo do relatório

Esta seção resume o relatório de avaliação.

- Nome do relatório – O nome do relatório.
- Descrição — A descrição inserida pelo proprietário da auditoria ao gerar o relatório.
- Data de geração — Data na qual o relatório foi gerado. A hora é representada no formato Tempo Universal Coordenado (UTC).
- Total de controles incluídos — Número de controles incluídos no relatório que coletaram evidências. Esse é um subconjunto do número total de controles na avaliação.
- Contas da AWS Incluídos – Número de Contas da AWS inclusos no relatório que coletaram evidências. Este é um subconjunto do número total de Contas da AWS na avaliação.
- Seleção do relatório de avaliação — O número de itens de evidência selecionados para inclusão no relatório. Isso inclui o total de problemas de verificação de conformidade encontrados no relatório.

Resumo da avaliação

Esta seção resume a avaliação a qual o relatório se refere.

- Nome da avaliação — Nome da avaliação a partir da qual o relatório foi gerado.
- Status — Status da avaliação no momento em que o relatório foi gerado.
- Região de avaliação — Região da AWS onde a avaliação foi criada.
- Contas da AWS em escopo — A lista completa de Contas da AWS no escopo da avaliação.
- Serviços da AWS em escopo — A lista completa de Serviços da AWS no escopo da avaliação.
- Nome do framework — O nome do framework a partir do qual a avaliação foi criada.
- Proprietários da auditoria — Usuário ou função dos proprietários da auditoria da avaliação.
- Última atualização — Data na qual a avaliação foi atualizada pela última vez. A hora é representada em UTC.

Página de índice

O TOC exibe o conteúdo completo do relatório de avaliação. Os conteúdos são agrupados e organizados com base nos conjuntos de controle inclusos na avaliação. Os controles estão listados abaixo do respectivo conjunto de controles.

Selecione qualquer item no índice para navegar diretamente até essa seção do relatório. Você pode escolher um conjunto de controles ou ir diretamente para um controle.

Página de controle

A página de controle tem duas partes: um resumo do controle em si e um resumo das evidências coletadas para o mesmo.

Resumo do controle

Esta seção inclui as seguintes informações:

- Nome do controle — O nome do controle.
- Descrição — A descrição do controle.
- Conjunto de controles — O nome do conjunto de controles ao qual o controle pertence.
- Informações de teste — Os procedimentos de teste recomendados para esse controle.
- Plano de ação — As ações recomendadas a serem executadas se o controle não for cumprido.

- Seleção do relatório de avaliação — O número de itens de evidência relacionados a esse controle incluídos no relatório de avaliação. Isso inclui o número de problemas de verificação de conformidade encontrados para as evidências desse controle.

Evidências coletadas

Esta seção mostra as evidências coletadas para o controle. As evidências são agrupadas por pastas, organizadas e nomeadas de acordo com a data de coleta das evidências. Ao lado do nome de cada pasta de evidências está o número total de problemas de verificação de conformidade dessa pasta.

Abaixo do nome de cada pasta de evidências, há uma lista de nomes de evidências com hiperlinks.

- Os nomes automatizados de evidências começam com um registro de data e hora da coleta de evidências, seguido pelo código do serviço, nome do evento (até 20 caracteres), ID da conta e ID exclusiva de 12 caracteres.

  Por exemplo: `21-30-24_IAM_CreateUser_111122223333_a1b2c3d4e5f6`

  Para evidências automatizadas, o nome com hiperlink abre um novo arquivo PDF, com um resumo e mais detalhes.
- Os nomes das evidências manuais começam com um registro de data e hora do carregamento das evidências, seguido pelo rótulo `manual`, ID da conta e ID exclusivo de 12 caracteres. Eles também incluem os primeiros 10 caracteres do nome do arquivo e a extensão (até 10 caracteres).

  Por exemplo: `00-00-00_manual_111122223333_a1b2c3d4e5f6_myimage.png`

  Para evidências manuais, o nome com hiperlink leva ao bucket S3 que contém essa evidência.

Ao lado do nome de cada evidência está o resultado da verificação de conformidade desse item.

- Para evidências automatizadas coletadas de AWS Security Hub ou AWS Config, um resultado Em confirmidade, Não conformidade, ou Inconclusivo é relatado.
- Para evidências automatizadas coletadas a partir de AWS CloudTrail e de chamadas de API, bem como para todas as evidências manuais, um resultado Inconclusivo é exibido.

Página de resumo de evidências

A página de resumo de evidências inclui as seguintes informações:

- ID — Identificador exclusivo da evidência.
- Data da coleta — A data na qual a evidência foi criada ou enviada.
- Descrição — Uma descrição da evidência, incluindo ID da conta e tipo de fonte de dados.
- Nome da avaliação — Nome da avaliação a partir da qual o relatório foi gerado.
- Nome do framework — O nome do framework a partir do qual a avaliação foi criada.
- Nome do controle — O nome do controle que a evidência suporta.
- Nome do conjunto de controles – O nome do conjunto de controles ao qual o controle relacionado pertence.
- Descrição do controle — A descrição do controle que a evidência suporta.
- Informações de teste — Os procedimentos de teste recomendados para o controle.
- Plano de ação — As ações recomendadas a serem executadas se o controle não for cumprido.
- Região da AWS – O nome da região associada à evidência.
- ID do IAM — ARN do usuário ou função associada à evidência.
- Conta da AWS – ID Conta da AWS associado à evidência.
- AWS service (Serviço da AWS) – O nome do AWS service (Serviço da AWS) associado à evidência.
- Recursos incluídos — Os aributos AWS avaliados para gerar as evidências. Esse atributo não é aplicável às evidências de verificação de conformidade do AWS Config. Para esse tipo de evidência, você pode encontrar todos os atributos tabulados em Página de detalhes da evidência no PDF da evidência.
- Nome do evento — O nome do evento de evidência.
- Horário do evento – O horário no qual o evento de evidência ocorreu.
- Fonte de dados — De onde a evidência foi coletada ou enviada. O tipo de fonte de dados pode ser AWS Config, Security Hub, chamadas de API AWS, CloudTrail ou Manual.
- Evidência por tipo — A categoria da evidência.
  - As evidências de Verificação de conformidade são coletadas do AWS Config ou do Security Hub.
  - A evidência Atividade do usuário é coletada a partir dos logs do CloudTrail.
  - A evidência Dados de configuração é coletada a partir de capturas de tela de outros Serviços da AWS.
  - A evidência Manual é a evidência que você carrega manualmente.

- Status da verificação de conformidade – O status da avaliação das evidências que se enquadram na categoria de Verificação de conformidade.
  - Para evidências automatizadas coletadas de AWS Security Hub ou AWS Config, um resultado Em confirmidade, Não conformidade, ou Inconclusivo é relatado.
  - Para evidências automatizadas coletadas a partir de AWS CloudTrail e de chamadas de API, bem como para todas as evidências manuais, um resultado Inconclusivo é exibido.

Página de detalhes da evidência

A página de detalhes da evidência mostra o nome da evidência e uma tabela de detalhes da mesma. Essa tabela fornece uma análise detalhada de cada elemento da evidência, para que você possa entender os dados e validar se estão corretos. A depender da fonte de dados da evidência, o conteúdo da página de detalhes da evidência varia.

> **Tip**
>
> A trilha de navegação na parte superior de cada página mostra sua localização atual enquanto você navega pelos detalhes das evidências. Selecione Resumo da evidência para navegar de volta ao resumo da evidência a qualquer momento.

Verificação da integridade do relatório de avaliação

Quando você gera um relatório de avaliação, o Audit Manager produz uma soma de verificação do arquivo de relatório chamado `digest.txt`. Você pode usar esse arquivo para validar a integridade do relatório e garantir que nenhuma evidência tenha sido modificada após a criação do mesmo. Ele contém um objeto JSON com assinaturas e tabelas hash, invalidados caso alguma parte do arquivo do relatório for alterada.

Para validar a integridade de um relatório de avaliação, use a API ValidateAssessmentReportIntegrity fornecida pelo Audit Manager.

Solução de problemas de relatórios de avaliação

Para encontrar respostas a perguntas e problemas comuns, consulte Solução de problemas do relatório de avaliação na seção Solução de problemas deste guia.

Localizador de evidências

O localizador de evidências fornece uma maneira poderosa de pesquisar evidências no Audit Manager. Em vez de navegar em pastas de evidências profundamente aninhadas para encontrar o que está procurando, agora, você pode usar o localizador para consultar rapidamente suas evidências. Se usar o localizador de evidências como administrador delegado, poderá pesquisar evidências em todas as contas membros da sua organização.

Ao usar uma combinação de filtros e agrupamentos, você pode restringir progressivamente o escopo da sua consulta de pesquisa. Por exemplo, se quiser uma visão de alto nível da integridade do sistema, faça uma pesquisa ampla e filtre por avaliação, intervalo de datas e conformidade de atributos. Se sua meta for remediar um atributo específico, você pode realizar uma pesquisa restrita para direcionar evidências de um controle ou ID de atributo específico. Depois de definir seus filtros, você pode agrupar e visualizar os resultados da correspondentes antes de criar um relatório de avaliação.

Para usar o localizador de evidências, você deve habilitar esse atributo nas configurações do Audit Manager.

No exemplo a seguir, substitua o texto do espaço reservado por ou .

Entendendo como o localizador de evidências funciona com o CloudTrail Lake

O localizador de evidências usa a capacidade de consulta e armazenamento do AWS CloudTrail Lake. Antes de começar a usar o localizador de evidências, é útil entender um pouco mais sobre como o CloudTrail Lake funciona.

O CloudTrail Lake agrega dados em um único armazenamento pesquisável de dados de eventos, que oferece suporte a consultas SQL poderosas. Isso significa que você pode pesquisar dados em toda a sua organização e dentro de intervalos de tempo personalizados. Com o localizador de evidências, você pode usar essa funcionalidade de pesquisa diretamente no console do Audit Manager.

Quando você solicita a ativação do localizador de evidências, o Audit Manager cria um armazenamento de dados de eventos em seu nome. Depois que o localizador de evidências é ativado, todas as evidências futuras do Audit Manager são ingeridas no armazenamento de dados do evento, onde ficam disponíveis para consultas de pesquisa do localizador de evidências. Depois de ativar o localizador de evidências, também preenchemos o repositório de dados de eventos recém-criado com os dados de evidências dos últimos dois anos. Se habilitar o localizador de evidências como administrador delegado, forneceremos dados de todas as contas membros da sua organização.

Todos os seus dados de evidências, preenchidos ou novos, são retidos no armazenamento de dados do evento por dois anos. Você pode fazer alterações no período de retenção padrão a qualquer momento. Para obter instruções, consulte Atualizar um armazenamento de dados de eventos no Guia do usuário AWS CloudTrail. É possível manter dados do evento em um armazenamento de dados de eventos por até 7 anos, ou 2.555 dias.

> **Note**
>
> O processo de preenchimento de dados, quando esse atributo está ativado, é gratuito se concluído até novembro de 2023.
> Quando novos dados de evidências forem adicionados ao armazenamento de dados do evento no futuro, as cobranças do CloudTrail Lake serão cobradas pelo armazenamento e ingestão de dados.
> Para consultas do CloudTrail Lake, você paga conforme o uso. Isso significa que, para cada consulta de pesquisa que você executa no localizador de evidências, você será cobrado pelos dados digitalizados.
> Para obter mais informações sobre precificação do CloudTrail, consulte precificaçãoAWS CloudTrail.

Habilitando o localizador de evidências

Você pode habilitar o localizador de evidências nas configurações do Audit Manager. Para obter instruções, consulte Localizador de evidências na página de configurações AWS Audit Manager deste guia.

Solução de problemas do localizador de evidências

Para encontrar respostas para perguntas e problemas comuns, consulte Solução de problemas no capítulo Solução de problemas deste guia.

Procurando evidências

Siga estas etapas para pesquisar evidências no console do Audit Manager.

> **Note**
>
> Você também pode usar a API do CloudTrail para consultar seus dados de evidência. Para saber mais, consulte StartQuery na Referência de API AWS CloudTrail . Se você preferir usar o AWS CLI, consulte Iniciar uma consulta no Guia do usuário AWS CloudTrail.

Nesta página

Executando uma consulta de pesquisa

Siga estas etapas para realizar uma consulta de pesquisa no localizador de evidências.

Procurando evidências

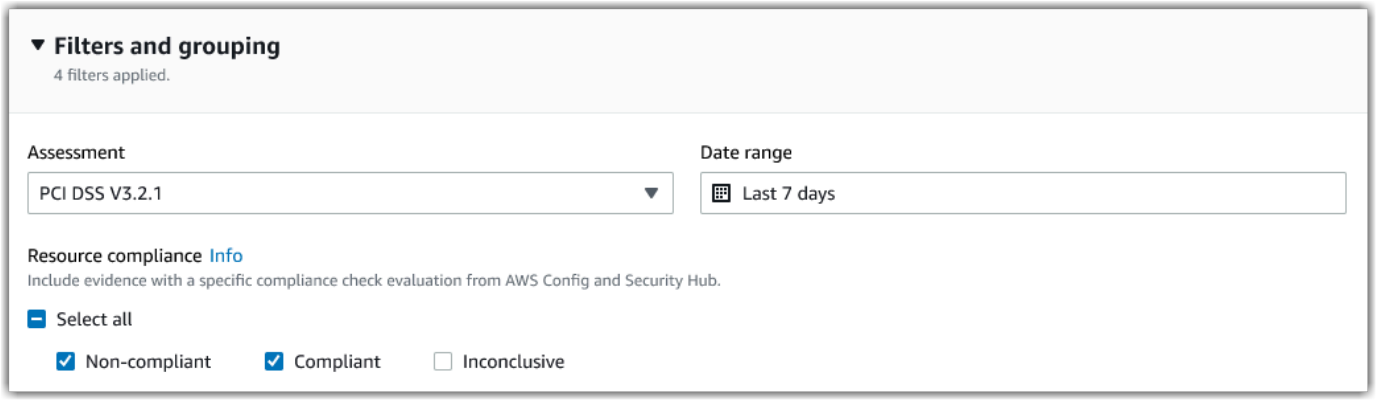
1. Abra o console do AWS Audit Manager em https://console.aws.amazon.com/auditmanager/home.

2. No painel de navegação, selecione a opção Localizador de evidências.
3. Em seguida, aplique filtros para restringir o escopo da sua pesquisa.

   a. Em Avaliação, selecione uma avaliação.

   b. Em Intervalo de datas, selecione um intervalo.

   c. Para Conformidade de atributo, selecione um status de avaliação.

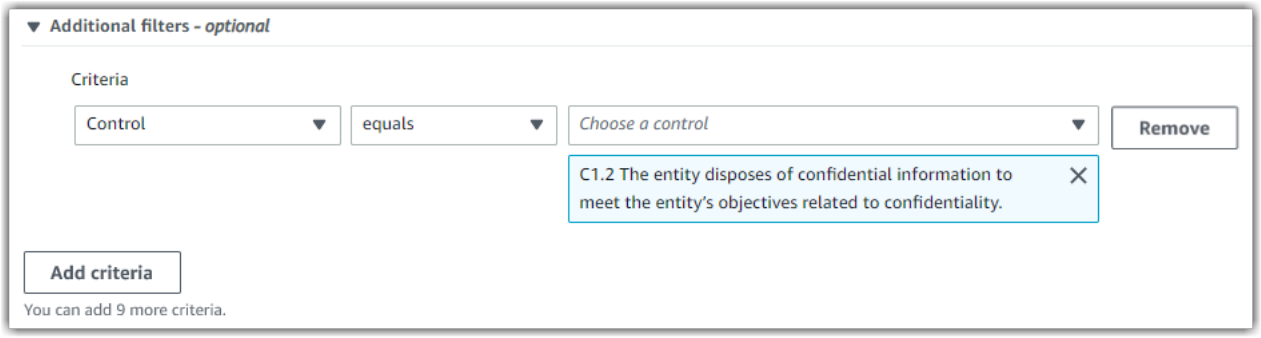


4. (Opcional) Selecione a opção Filtros adicionais: opcional para restringir ainda mais a pesquisa.

   a. Selecione a opção Adicionar critérios, selecione um critério e, em seguida, selecione um ou mais valores para esse critério.

   b. Continue a criar mais filtros da mesma maneira.

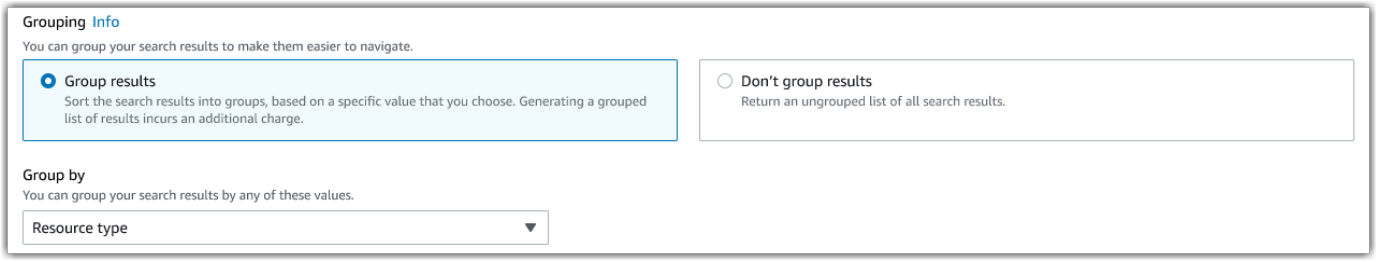
   c. Para remover um filtro indesejável, selecione a opção Remover.



5. Em Agrupamento, especifique se deseja agrupar os resultados da pesquisa.

   a. Se quiser agrupar os resultados, selecione um valor pelo qual agrupar os resultados.

   b. Se não deseja agrupar os resultados, vá para a etapa 6.



6. Selecione a opção Pesquisar.

Sua pesquisa pode levar alguns minutos, de acordo com a quantidade de dados de evidência. Sinta-se à vontade para sair do localizador de evidências enquanto a pesquisa estiver em andamento. Uma barra de flash notifica quando os resultados da pesquisa estiverem prontos.

> **Tip**
>
> Para obter mais informações sobre os filtros e agrupamentos que você pode usar nesse procedimento, consulte Opções de filtro e agrupamento.

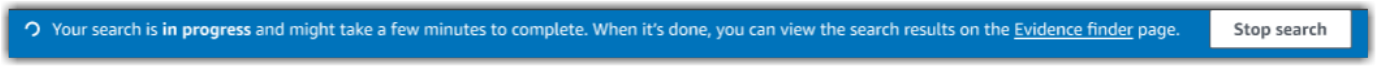
Interrompendo uma consulta de pesquisa

Se pretende interromper uma consulta de pesquisa por qualquer motivo, siga estas etapas.

> **Note**
>
> A interrupção de uma consulta de pesquisa ainda pode resultar em cobranças. Você é cobrado pela quantidade de dados de evidência examinados antes de interromper a consulta de pesquisa. Depois que ela for interrompida, você poderá ver os resultados parciais que retornados.

Para interromper uma consulta de pesquisa em andamento

1. Na barra de progresso de flash azul na parte superior da tela, selecione a opção Interromper a pesquisa.



2. (Opcional) Analise os resultados parciais retornados antes de interromper a consulta de pesquisa.

   a. Se estiver na página do localizador de evidência, os resultados parciais serão exibidos na tela.

   b. Se você saiu do localizador de evidências, selecione a opção Exibir resultados parciais na barra de confirmação de flash verde.

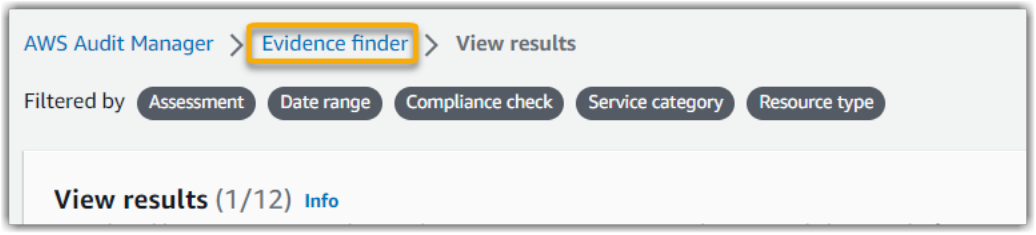
Editar filtros de pesquisa

Você pode retornar à sua consulta de pesquisa mais recente e alterar os filtros conforme necessário.

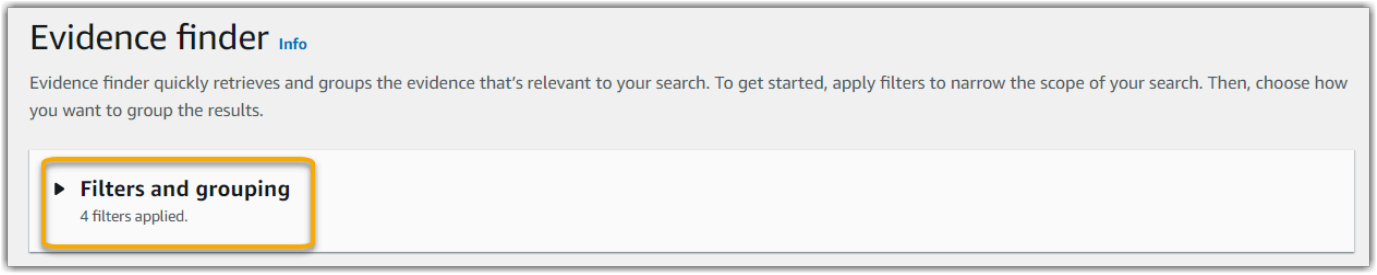
> **Note**
>
> Quando edita seus filtros e seleciona a opção Pesquisar, isso inicia uma nova consulta de pesquisa.

Para editar uma consulta de pesquisa recente

1. Na página Visualizar resultados, aselecione a opçãoLocalizador de evidências no menu de rastro de navegação.



2. Selecione a opção Filtros e agrupamento para expandir a seleção de filtros.



3. Em seguida, edite seus filtros ou inicie uma nova pesquisa.

   a. Para editar filtros, ajuste ou remova os filtros atuais e a seleção de agrupamento.

   b. Para recomeçar, selecione a opção Limpar filtros, aplique os filtros e a seleção de agrupamento de sua escolha.

4. Quando concluir, selecione a opção Pesquisar.

Visualizando resultados no localizador de evidências

Depois que sua pesquisa for concluída, você poderá ver os resultados que corresponderem aos seus critérios de pesquisa.

Lembre-se que vários atributos podem ser avaliados durante a coleta de evidências. Como resultado, as evidências podem incluir um ou mais atributos relacionados. No localizador de evidências, os resultados são mostrados no nível do atributo, com uma linha para cada um. Você pode visualizar um resumo de cada atributo sem sair da página.

Depois de analisar os resultados da pesquisa, você pode gerar um relatório de avaliação que inclua essa evidência. Você pode exportar os resultados de uma consulta de pesquisa de atributo para um arquivo de valores separados por vírgulas (CSV).

> **Important**
>
> Recomendamos que mantenha o localizador de evidências aberto até terminar de explorar os resultados da pesquisa. Os resultados da pesquisa são descartados quando você sai da

tabela Visualizar resultados. Se necessário, você pode visualizar seus resultados recentes no console do CloudTrail em https://console.aws.amazon.com/cloudtrail/. Aqui, os resultados de suas consultas de pesquisa são preservados por 7 dias. No entanto, lembre-se de que não pode gerar um relatório de avaliação a partir dos resultados da pesquisa no console do CloudTrail.

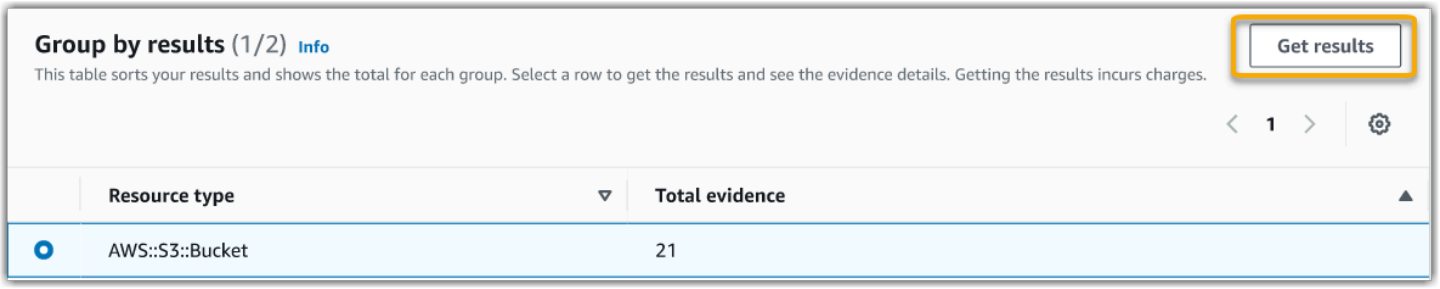
Nesta página

Como visualizar os resultados agrupados

Se agrupou seus resultados, poderá analisar os agrupamentos antes de se aprofundar nas evidências.

> **Note**
>
> Se não agrupou os resultados, o localizador de evidências não exibirá a tabela Agrupar por resultados. Em vez disso, você será levado diretamente para a tabela Visualizar resultados.

Use a tabela Agrupar por resultados para saber sobre a amplitude da evidência correspondente e como ela é distribuída em uma dimensão específica. Os resultados são agrupados pelo valor selecionado. Por exemplo, se você agrupou por Tipo de atributo, a tabela mostra uma lista de tipos de atributos AWS. A coluna Evidência total mostra o número de resultados correspondentes para cada tipo de atributo.



Para obter resultados de um grupo

1. Na tabela Agrupar por resultados, selecione a linha para obter resultados que deseja.
2. Selecione a opção Obter resultados. Isso inicia uma nova consulta de pesquisa e redireciona para a tabela Visualizar resultados, onde você pode ver os resultados desse grupo.

Visualizando resultados de pesquisa

A tabela Visualizar resultados exibe os resultados da pesquisa. No painel, você pode utilizar as seguintes ações:

- Gerencie suas preferências de visualização
- Visualização de resumos de atributos
- Gere um relatório de avaliação a partir dos resultados da sua pesquisa
- Exportar seus resultados da pesquisa

Gerencie suas preferências de visualização

Suas preferências de visualização controlam o que você vê na página de resultados.

Gerencie preferências de visualização

1. Selecione o ícone de configurações (#) na parte superior da tabela Visualizar resultados.
2. Analise e altere as seguintes configurações conforme necessário:

    a. Selecionar colunas visíveis da tabela: use a opção de alternância para trocar quais colunas são exibidas.

    b. Tamanho da página – selecione um botão de opção de seleção para especificar quantos resultados serão exibidos em cada página.

c. Quebrar texto – marque a caixa de seleção para quebrar linhas longas de texto para melhor legibilidade.

3. Selecione Confirmar para salvar suas preferências.

Visualização de resumos de atributos

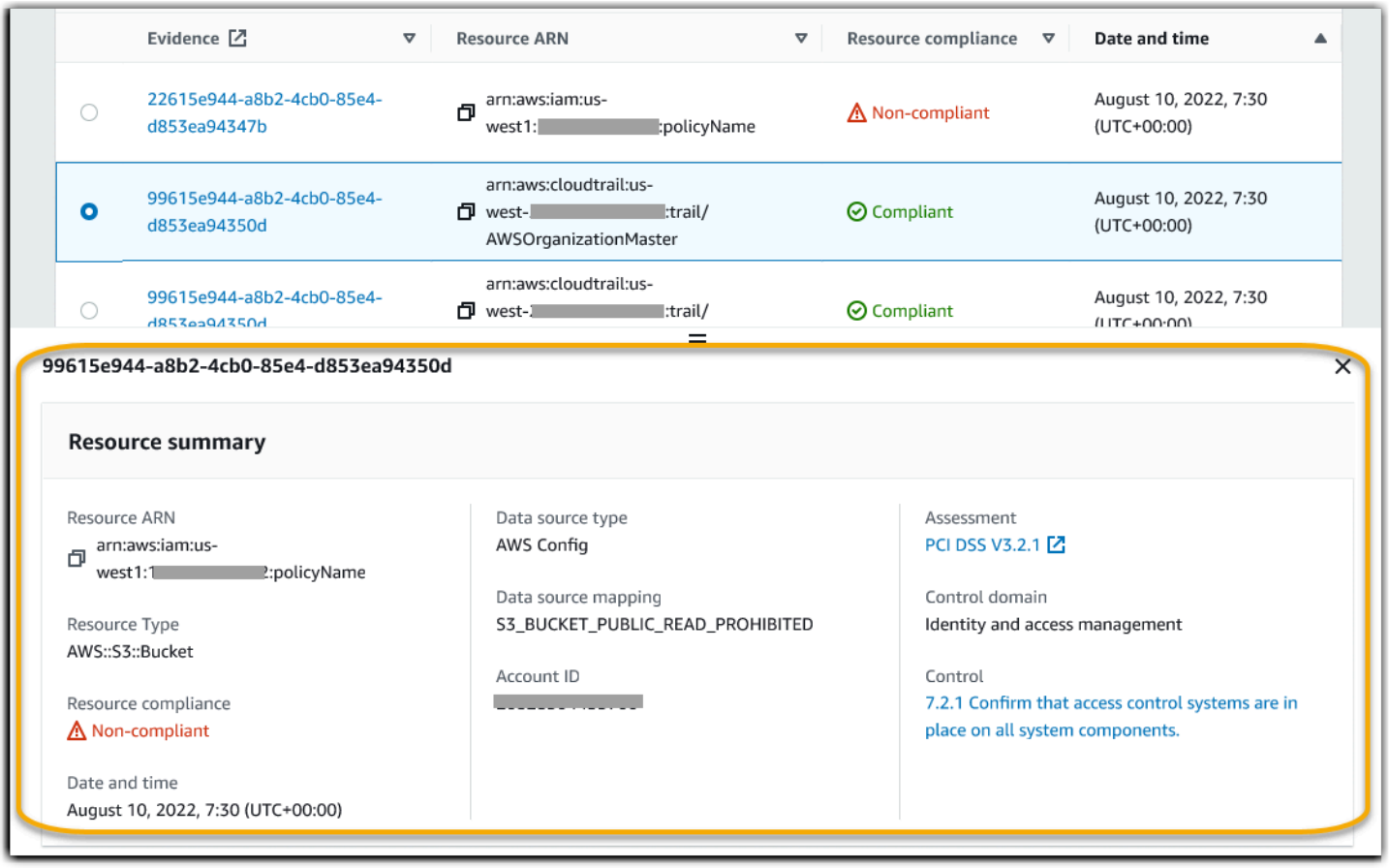
Você pode visualizar os atributos relacionados à evidências que corresponderem à sua consulta de pesquisa. Isso ajuda a determinar se a consulta de pesquisa retornou os resultados pretendidos, ou se você precisa ajustar seus filtros e executar novamente a consulta.

Lembre-se de que as evidências podem ter um ou mais atributos relacionados. No localizador de evidências, resultados são exibidos no nível do atributo, com uma linha para cada.

> **Note**
>
> O localizador retorna resultados para evidências automatizadas e manuais. No entanto, você só pode visualizar resumos de atributos para evidências automatizadas. Isso ocorre porque o Audit Manager não realiza avaliações de atributos para evidências manuais e, como resultado, nenhum resumo de atributo estará disponível.
> Para visualizar detalhes sobre evidências manuais, selecione o nome da evidência para abrir a página de detalhes da mesma. Se gerar um relatório de avaliação a partir dos resultados do localizador de evidências, os detalhes da evidência manual serão incluídos no relatório de avaliação.

Visualização de resumos de atributos

1. Selecione o botão de opção de seleção ao lado de um resultado. Isso abre um painel de resumo do atributo na página atual.
2. (Opcional) Para ver os detalhes completos das evidências relacionadas, selecione a opção o nome da evidência.
3. (Opcional) Use as linhas horizontais (=) para arrastar e redimensionar o painel de resumo do atributo.
4. Selecione a opção (x) para fechar o painel de resumo do atributo.



Gere um relatório de avaliação a partir dos resultados da sua pesquisa

Quando estiver satisfeito com os resultados da pesquisa, gere um relatório de avaliação.

Para gerar um relatório de avaliação a partir dos resultados da sua pesquisa

1. Na parte superior da tabela Visualizar resultados, selecione a opção Gerar relatório de avaliação.
2. Insira um nome e uma descrição para seu relatório de avaliação e analise os detalhes do relatório de avaliação.
3. Selecione a opção Gerar um relatório de avaliação.

Serão necessários alguns minutos para que o relatório de avaliação seja gerado. Você pode sair do localizador de evidências enquanto isso acontece; uma notificação verde de sucesso confirmará quando o relatório estiver pronto. Em seguida, você pode acessar o centro de download do Audit Manager e baixar seu relatório de avaliação.

> **Note**
>
> O Audit Manager gera um relatório único usando apenas as evidências dos resultados da pesquisa. Esse relatório não inclui nenhuma evidência adicionada manualmente a um relatório a partir da página de avaliação.
> Os limites se aplicam à quantidade de evidências que podem ser incluídas em um relatório de avaliação. Para obter mais informações, consulte Localizador de solução de problemas.

Exportar seus resultados da pesquisa

Talvez você precise de uma versão portátil dos resultados da pesquisa do localizador de evidência. Se for o caso, você pode exportar os resultados da pesquisa para um arquivo CSV.

Depois de exportar os resultados da pesquisa, o arquivo CSV ficará disponível na central de downloads do Audit Manager por 7 dias. Uma cópia do arquivo CSV também será entregue ao bucket S3 de sua preferência, conhecido como destino de exportação. Seu arquivo CSV permanecerá disponível nesse bucket até que você exclua esse arquivo.

O Audit Manager usa a funcionalidade CloudTrail Lake para exportar e entregar arquivos CSV do localizador de evidências. Os fatores a seguir definem como o processo de exportação de CSV funciona:

- Todos os resultados da sua pesquisa estão incluídos no relatório de avaliação. Se quiser incluir apenas resultados de pesquisa específicos no relatório de avaliação, recomendamos editar seus filtros de pesquisa atuais. Dessa forma, você pode restringir seus resultados para direcionar apenas as evidências que desejar incluir no relatório.
- Os arquivos CSV são exportados no formato GZIP. O nome padrão do arquivo CSV é `queryID/result.csv.gz`, onde `queryID` é o ID da sua consulta de pesquisa.
- O tamanho máximo de arquivo para uma exportação de CSV é 1 TB. Se estiver exportando mais de 1 TB de dados, seus resultados serão divididos em mais de um arquivo. Cada arquivo CSV chama-se `result_`*`number`*`.csv.gz`. O número de arquivos CSV obtidos depende do tamanho total dos resultados da pesquisa. Por exemplo, a exportação de 2 TB de dados fornece dois arquivos de resultados de consulta: `result_1.csv.gz` e `result_2.csv.gz`.
- Além do arquivo CSV, um arquivo de sinal JSON é entregue ao seu bucket S3. Esse arquivo funciona como uma soma de verificação, atestando que as informações contidas no arquivo CSV são precisas. Para saber mais, consulte a estrutura de arquivos de assinatura CloudTrail no AWS CloudTrail Guia do Desenvolvedor. Para determinar se os resultados de consulta foram

modificados, excluídos ou permaneceram inalterados depois de entregues, você pode usar a validação de integridade de resultados de consulta do CloudTrail. Para obter instruções, consulte Validar resultados de consultas salvos no Guia do DesenvolvedorAWS CloudTrail.

> **Note**
>
> Atualmente, respostas em texto de evidência manual não estão inclusas nas prévias do localizador de evidências nem nas exportações de CSV. Para visualizar dados da resposta em texto, selecione o nome da evidência manual nos resultados do localizador de evidências para abrir a página de detalhes. Se precisar visualizar dados de resposta de texto fora do console do Audit Manager, recomendamos que gere um relatório de avaliação a partir dos resultados do localizador de evidência. Todos os detalhes de evidências manuais, inclusive respostas em texto, estão inclusos nos relatórios de avaliação.

Como exportar seus resultados pela primeira vez

Siga estas etapas para exportar seus resultados de pesquisa pela primeira vez. Esse procedimento oferece a opção de especificar um destino de exportação padrão para todas as suas exportações futuras. Se não quiser salvar um destino de exportação padrão no momento, poderá fazê-lo posteriormente atualizando suas configurações de destino de exportação.

> **Important**
>
> Antes de começar, verifique se possui um bucket S3 disponível para uso como destino de exportação. Você pode usar um dos seus buckets S3 existentes ou criar um novo bucket no Amazon S3. Além disso, seu bucket do S3 deve ter a política de permissões exigida para permitir que o CloudTrail grave os arquivos de exportação nele. Mais especificamente, a política do bucket deve incluir uma ação `s3:PutObject` e o ARN do bucket, além de listar o CloudTrail como entidade principal do serviço. Fornecemos um exemplo de política de permissão que você pode usar. Para obter instruções sobre como anexar essa política ao seu bucket do S3, consulte Adicionando uma política de bucket usando o console do Amazon S3.
>
> Para mais dicas, consulte dicas de configuração para seu destino de exportação. Se encontrar algum problema ao exportar um arquivo CSV, consulte Solução de problemas de exportações de CSV do localizador de evidência.

Para exportar seus resultados de pesquisa (primeira experiência)

1. Na parte superior da tabela Visualizar resultados, selecione a opção Exportar CSV.
2. Especifique o bucket S3 no qual deseja armazenar seus arquivos exportados.
   - Selecione a opção Navegar por S3 para selecionar na sua lista de buckets.
   - Como alternativa, você pode inserir o URI do bucket nesse formato: **`s3://bucketname/prefix`**

   > **Tip**
   >
   > Para manter seu bucket de destino organizado, você pode criar uma pasta opcional para suas exportações de CSV. Para fazer isso, acrescente uma barra (**`/`**) e um prefixo ao valor na caixa URI de Atributo (por exemplo, **`/evidenceFinderExports`**). Em seguida, o Audit Manager incluirá esse prefixo ao adicionar o arquivo CSV ao bucket e o Amazon S3 irá gerar o caminho especificado pelo prefixo. Para obter mais informações sobre prefixos de objeto e pastas no Amazon S3, consulte Organizando objetos no console do Amazon S3 no Guia do Usuário Amazon Simple Storage Service.
3. (Opcional) Se não quiser salvar esse intervalo como destino de exportação padrão, desmarque a caixa de seleção que diz Salvar este bucket como destino de exportação padrão nas configurações do meu localizador de evidência.
4. Selecione a opção Exportar.

Exportando seus resultados depois de salvar um destino de exportação

Depois de salvar um bucket padrão S3 como destino de exportação padrão, você pode seguir estas etapas.

Para exportar os resultados da pesquisa (depois de salvar um destino de exportação padrão)

1. Na parte superior da tabela Visualizar resultados, selecione a opção Exportar CSV.
2. No prompt exibido, analise o bucket padrão do S3 onde o arquivo exportado será salvo.
   a. (Opcional) Para continuar usando esse bucket e ocultar essa mensagem daqui para frente, marque a caixa Não me lembre novamente.

b. (Opcional) Para alterar esse bucket, siga o procedimento para atualizar suas configurações de destino de exportação.

3. Selecione a opção Confirmar.

De acordo com a quantidade de dados que estiver exportando, o processo de exportação pode levar alguns minutos. Sinta-se à vontade para sair do localizador de evidências enquanto a exportação estiver em andamento. Ao sair do localizador de evidências, sua pesquisa será interrompida e os resultados serão descartados no console. No entanto, o processo de exportação de CSV continuará em segundo plano. O arquivo CSV incluirá o conjunto completo de resultados de pesquisa correspondentes à sua consulta.

Visualizando seus resultados depois de exportá-los

Para encontrar seu arquivo CSV e verificar seu status, acesse o centro de download do Audit Manager. Quando o arquivo exportado estiver pronto, você poderá fazer o download do arquivo CSV no centro de download.

Você também pode encontrar e baixar o arquivo CSV do bucket do S3 de destino de exportação.

Para localizar seu arquivo CSV e assinar no console do Amazon S3

1. Abra o console Amazon S3.
2. Selecione o bucket de destino de exportação que você especificou ao exportar seu arquivo CSV.
3. Navegue pela hierarquia de objetos até encontrar o arquivo CSV e o arquivo de assinatura. O arquivo CSV possui uma extensão `.csv.gz`, e o arquivo de assinatura, uma extensão `.json`.

Você irá navegar por uma hierarquia de objetos semelhante ao exemplo a seguir, mas com nome de bucket de destino de exportação, ID de conta, data e ID de consulta diferentes.

```
All Buckets
    Export_Destination_Bucket_Name
        AWSLogs
            Account_ID;
                CloudTrail-Lake
                    Query
                        YYYY
                            MM
                              DD
```

```
Query_ID
```

Opções de agrupamento e filtro

Esta página descreve as opções de filtro e agrupamento disponíveis no localizador de evidências.

Nesta página

Referência de filtro

Você pode usar os filtros a seguir para encontrar evidências que correspondam a critérios específicos, como avaliação, controle ou AWS service (Serviço da AWS).

Tópicos

Filtros necessários

Use esses filtros para começar com uma visão geral de alto nível da evidência em uma avaliação.

Nome do filtro	Descrição	Observações
Avaliação	Retorna evidências para uma avaliação específica.	Você pode filtrar por apenas uma avaliação por vez.
Intervalo de datas	Retorna evidências de um período específico.	Você pode usar um Intervalo relativo para definir um intervalo relativo à data atual (por exemplo, **`Last 30 days`**).

Nome do filtro	Descrição	Observações
		Ou pode usar um Intervalo absoluto, para especificar um intervalo de datas específico (por exemplo, **`June 27th - July 4th`**).

Nome do filtro	Descrição	Observações
Conformidade de atributos	Retorna atributos com uma avaliação específica de verificação de conformidade.	O Audit Manager coleta evidências de verificação de conformidade para controles que utilizam AWS Config e Security Hub como um tipo de fonte de dados. Vários atributos podem ser avaliados durante essa coleta de evidências. Como resultado, uma única evidência de verificação de conformidade pode incluir um ou mais atributos. Você pode usar esse filtro para explorar o status de conformidade no nível do atributo. Você pode selecionar uma ou mais opções a seguir: • Não conformidade – este filtro encontra atributos com problemas de verificação de conformidade. Isso acontece se o Security Hub relatar um resultado de Falha, ou se AWS Config relatar um resultado de Não conformidade. • Em conformidade – esse filtro encontra atributos sem problemas de verificação de conformidade. Isso acontece se o Security Hub relatar um resultado de Êxito, ou se AWS Config relatar um resultado Em conformidade. • Inconclusivo – esse filtro encontra atributos para os quais uma verificação de conformidade não está disponível ou não é aplicável. Isso acontece se um atributo usar AWS Config ou o Security Hub como o tipo de fonte de dados subjacente mas esses serviços não estiverem habilitados. Isso também acontece se o atributo não oferecer tipo de fonte de dados subjacente que suporte verificação de conformidade (como evidências manuais, chamadas de API AWS ou CloudTrail).

Filtros adicionais (opcional)

Use esses filtros para restringir o escopo da sua consulta de pesquisa. Por exemplo, use Serviço para visualizar todas as evidências relacionadas ao Amazon S3. Use Tipo de atributo para concentrar apenas nos buckets S3. Ou use ARN do atributo para um bucket S3 específico.

Você pode criar filtros adicionais usando um ou mais critérios a seguir.

Nome do critério	Descrição	Quando usar esse critério
ID da conta	Detalhar por Conta da AWS.	Use esse critério para encontrar evidências relacionadas a um Conta da AWS específico.
Controle	Detalha pelo nome do controle.	Use esse critério para encontrar evidências relacionadas a um controle específico.
Domínio de controle	Detalha por domínio de controle.	Use esse critério para concentrar em uma área temática específica ao preparar para uma auditoria. Você pode filtrar por domínio de controle se estiver consultando uma avaliação criada a partir de um framework padrão. Exemplos de domínios de controle incluem gerenciam ento de identidade e acesso, logging, monitoramento e gerenciamento de rede.
Tipo de fonte de dados	Detalhe por tipo de fonte de dado.	Use esse critério para concentrar em uma fonte de dados específica. Configure o valor como `Manual` para encontrar evidência s carregadas manualmente. Do contrário, poderá filtrar evidências automatizadas com base na origem (por exemplo, `AWS Config`, `CloudTrail` , `Security Hub` ou `AWS API calls`).
Nome do evento	Detalha por nome do evento.	Use esse critério para concentrar em um evento específic o ao qual a evidência estiver relacionada. Um evento é o registro de atividade em uma Conta da AWS.

Nome do critério	Descrição	Quando usar esse critério
		Por exemplo, você pode pesquisar o nome de uma chamada de API, como a operação do IAM `AttachRolePolicy` usada para configurar permissões. Ou pesquisar uma palavra-chave do CloudTrail, como o evento `ConsoleLogin` loggado pelo CloudTrail quando um usuário fizer login em sua conta.
Atributo ARN	Detalha por Nome do Recurso da Amazon (ARN).	Use esses critérios para encontrar evidências relacionadas a um atributo AWS específico.
Tipo de atributo	Detalha por tipo de atributo.	Use esse critério para concentrar no tipo de atributo sendo avaliado, como uma instância do Amazon EC2 ou um bucket S3.
Serviço	Detalha por nome AWS service (Serviço da AWS).	Use esse critério para encontrar evidências relacionadas a um AWS service (Serviço da AWS) específico, como Amazon EC2, Amazon S3 ou AWS Config.
Categoria de serviço	Detalha por categoria AWS service (Serviço da AWS).	Use esse critério para concentrar em uma categoria específica de AWS service (Serviço da AWS). Os exemplos incluem segurança, identidade, conformidade, banco de dados e armazenamento.

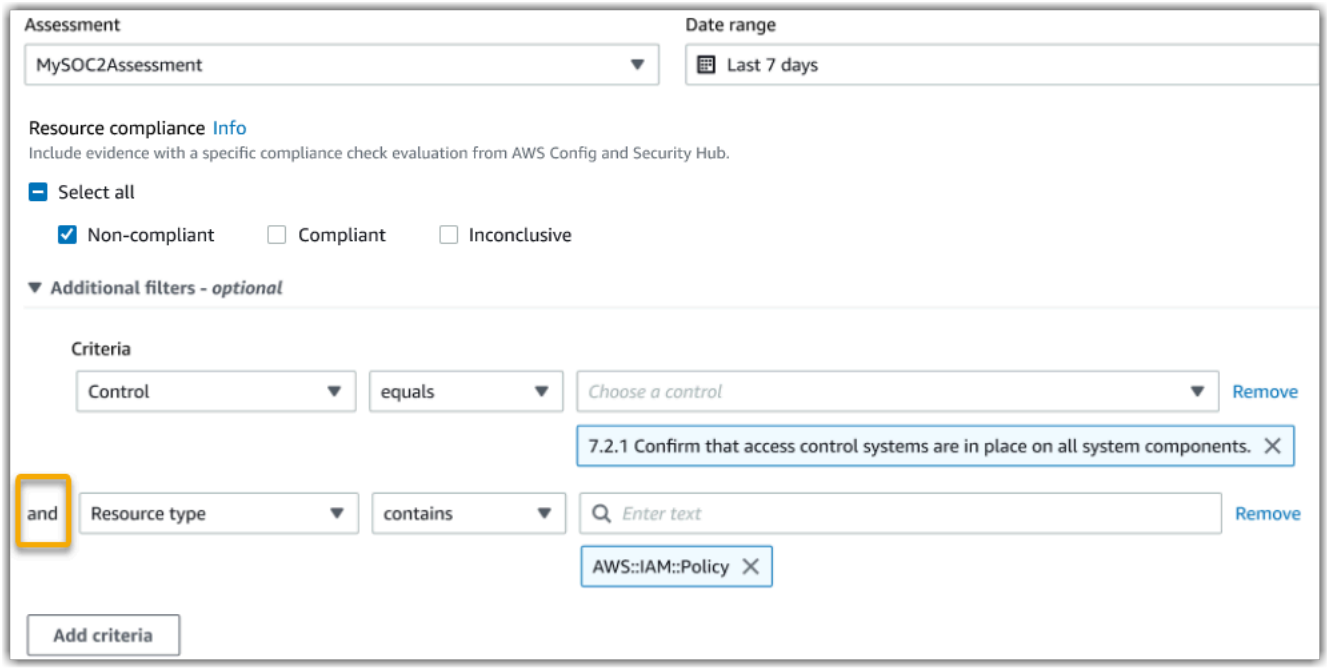
Combinando filtros

Comportamento de critério

Quando você especifica mais de um critério, o Audit Manager aplica o operador `AND` às suas seleções. Isso significa que todos os critérios são agrupados em uma única consulta e os resultados devem corresponder a todos os critérios combinados.

Exemplo

Na configuração de filtro a seguir, o localizador de evidências retorna atributos não compatíveis dos últimos 7 dias para a avaliação chamada **`MySOC2Assessment`**. Além disso, os resultados estão relacionados a uma política do IAM e ao controle especificado.

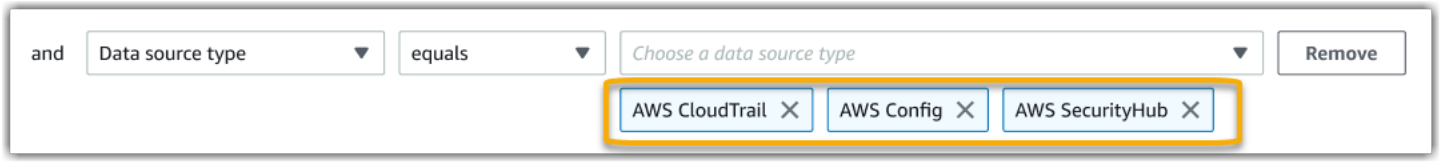


Comportamento de valor de critério

Quando você especifica mais de um valor de critério, estes valores são vinculados a um operador OR. O localizador de evidências retorna resultados que correspondam a qualquer um desses valores de critério.

Exemplo

Na configuração de filtro a seguir, o localizador de evidências retorna os resultados da pesquisa provenientes de AWS CloudTrail, AWS Config, ou AWS Security Hub.



Agrupando referência

Você pode agrupar os resultados da pesquisa para uma navegação mais rápida. O agrupamento mostra a amplitude dos resultados da pesquisa e como eles são distribuídos em uma dimensão específica.

Você pode usar qualquer um dos grupos a seguir por valores.

Agrupar por	Descrição
ID da conta	Agrupe os resultados por Conta da AWS.
Controle	Agrupe os resultados pelo nome do controle.
Domínio de controle	Agrupe os resultados pelo nome do domínio.
Tipo de fonte de dados	Agrupe os resultados pelo tipo de fonte de dado de onde a evidência veio.
Nome do evento	Agrupe os resultados pelo nome de um evento.
Atributo ARN	Agrupe resultados pelo Nome do Recurso da Amazon (ARN).
Tipo de atributo	Agrupe os resultados por tipo de atributo.
Serviço	Agrupe os resultados pelo nome AWS service (Serviço da AWS).
Categoria de serviço	Agrupe os resultados por categoria AWS service (Serviço da AWS).

Exemplo de casos de uso

O localizador de evidências pode ajudá-lo com vários casos de uso. Esta página fornece alguns exemplos e sugere filtros de pesquisa que você pode usar em cada cenário.

Tópicos

- Caso de uso 1: encontre evidências que não estejam em conformidade e organize delegações
- Caso de uso 2: identificar evidências em conformidade
- Caso de uso 3: faça uma visualização rápida dos atributos de evidências

Caso de uso 1: encontre evidências que não estejam em conformidade e organize delegações

Esse caso de uso é ideal se você for um diretor de conformidade, um diretor de proteção de dados ou um profissional de GRC que supervisiona a preparação da auditoria.

Ao monitorar a postura de conformidade da sua organização, você pode contar com equipes de parceiros para ajudá-lo a corrigir problemas. Você pode usar o localizador de evidências para ajudá-lo a organizar seu trabalho para suas equipes parceiras.

Ao aplicar filtros, você pode concentrar nas evidências de uma área por vez. Além disso, você também pode manter-se alinhado com as responsabilidades e o escopo de cada equipe parceira com a qual trabalha. Ao realizar uma pesquisa direcionada dessa forma, você pode usar os resultados para identificar exatamente o que precisa ser corrigido em cada área temática. Em seguida, você pode delegar essa evidência de não conformidade à equipe parceira correspondente para remediação.

Para esse fluxo de trabalho, siga as etapas para pesquisar evidências. Use os filtros a seguir para encontrar evidências de não conformidade.

```
Assessment | <assessment name>
Date range | <date range>
Resource compliance | Non-compliant
```

Em seguida, aplique filtros adicionais para a área na qual estiver focando. Por exemplo, use o filtro da Categoria de serviço para encontrar atributos que não estejam em conformidade e sejam relacionados ao IAM. Em seguida, compartilhe esses resultados com a equipe que possuir os atributos do IAM para sua organização. Ou, se estiver consultando uma avaliação criada a partir de um framework padrão, você pode usar o filtro Domínio de controle para encontrar evidências que não estejam em conformidade relacionadas ao domínio de gerenciamento de identidade e acesso.

```
Control domain | <domain that you're focusing on>
or
Service category | <AWS service (Serviço da AWS) category that you're focusing on>
```

Depois de encontrar as evidências de que precisa, siga as etapas para gerar um relatório de avaliação a partir dos resultados da pesquisa. Você pode compartilhar esse relatório com sua equipe parceira, que pode usá-lo como uma lista de verificação de remediação.

Caso de uso 2: identificar evidências em conformidade

Esse caso de uso é ideal se você trabalha em SecOps, TI/DevOps, ou outra função que possua e corrija ativos de nuvem.

Como parte de uma auditoria, você pode ser solicitado a corrigir problemas com os atributos que possuir. Depois desse trabalho, você pode usar o localizador de evidências para validar se seus atributos estão em conformidade.

Para esse fluxo de trabalho, siga as etapas para pesquisar evidências. Use os filtros a seguir para encontrar evidências em conformidade.

```
Assessment | <assessment name>
Date range | <date range>
Resource compliance | Compliant
```

Em seguida, aplique filtros adicionais para mostrar somente as evidências pelas quais for responsável. De acordo com seu escopo de propriedade, torne a pesquisa tão direcionada quanto necessário. Os exemplos de filtros a seguir estão ordenados do mais amplo ao mais preciso. Selecione as opções apropriadas e substitua *<placeholder text>* por seus próprios valores.

```
Control domain | <a subject area that you're responsible for>
Service category | <a category of Serviços da AWS that you own>
Service | <a specific AWS service (Serviço da AWS) that you own>
Resource type | <a collection of resources that you own>
Resource ARN | <a specific resource that you own>
```

Se for responsável por várias instâncias do mesmo critério (por exemplo, se possuir vários Serviços da AWS), você pode agrupar seus resultados por esse valor. Isso fornece o total de correspondências de evidência para cada AWS service (Serviço da AWS). Em seguida, você pode obter os resultados dos serviços que possui.

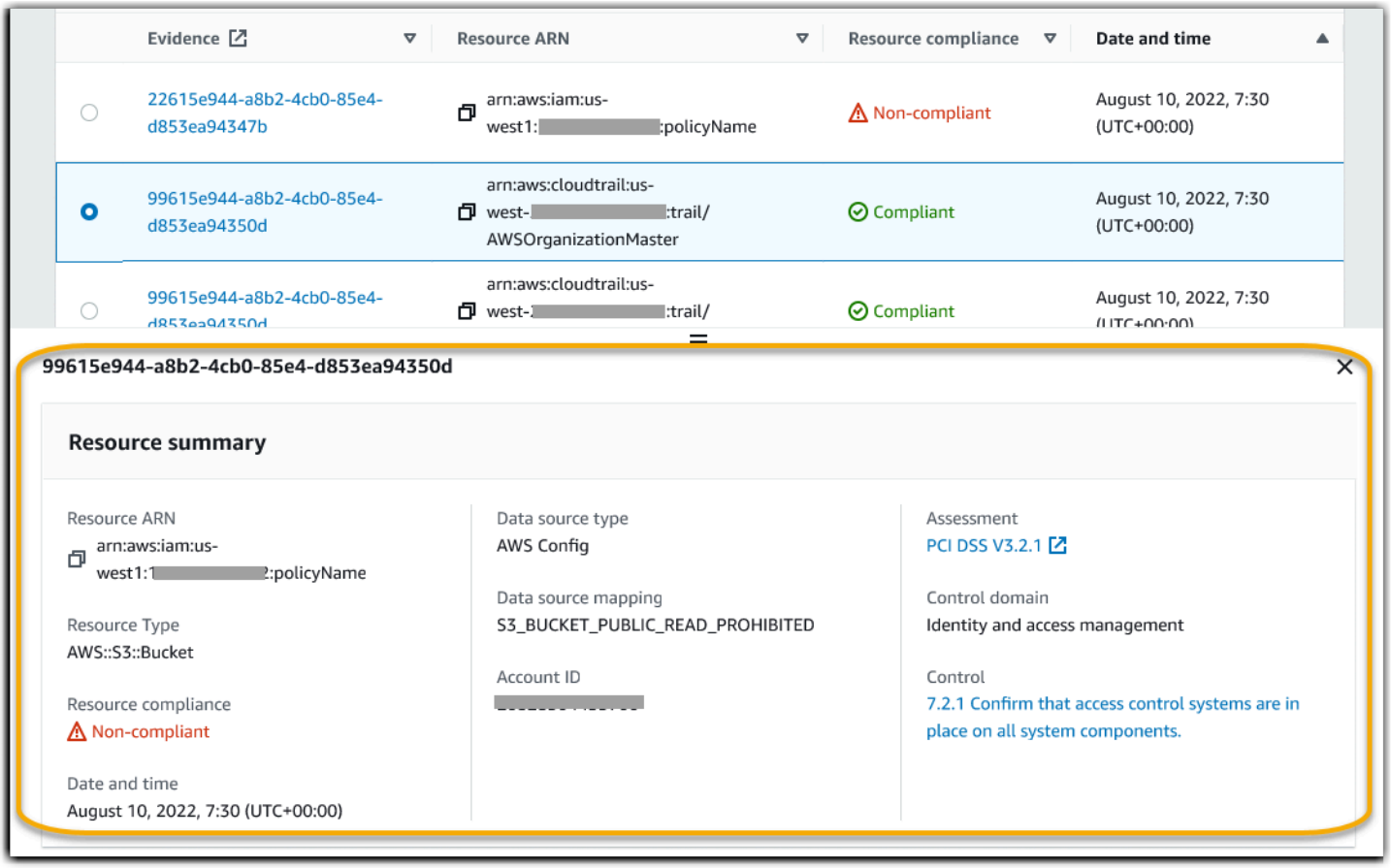
Caso de uso 3: faça uma visualização rápida dos atributos de evidências

Esse caso de uso é ideal para todos os clientes Audit Manager.

Anteriormente, a análise dos detalhes das evidências individuais era demorada. Se você quisesse visualizar as evidências, precisaria ir diretamente para essa avaliação e, em seguida, navegar pelas pastas de evidências profundamente aninhadas. Agora, o localizador de evidências fornece

uma maneira conveniente de visualizar essas informações. Para cada item de evidência que corresponder à sua consulta de pesquisa, você poderá visualizar os atributos individuais dessa evidência.

Para começar, siga as etapas para pesquisar evidências. Em seguida, marque o botão de opção de seleção ao lado de um resultado para visualizar um resumo do atributo na página atual. Você pode visualizar cada atributo individual relacionado a um item de evidência. Para ver os detalhes completos das evidências de qualquer atributo, selecione o nome da evidência. Para obter mais informações, consulte Visualizar os resumos dos atributos.



Central de download do Audit Manager

O centro de downloads é o local onde você encontra e gerencia todos os arquivos do Audit Manager baixados. Quando você gera um relatório de avaliação ou exporta os resultados da pesquisa do localizador de evidências, os arquivos aparecem na central de downloads.

Tópicos

Como navegar na central de download

Para visitar o centro de download, abra o console Audit Manager em https://console.aws.amazon.com/auditmanager/home e escolha Centro de download no painel de navegação esquerdo.

Você pode alternar entre as guias a seguir para procurar seus arquivos por categoria.

Guia relatórios de avaliação

Essa guia mostra todos os relatórios de avaliação gerados. Os relatórios de avaliação permanecem disponíveis na central de download até que você os exclua.

Para ver o status mais recente do seu relatório de avaliação, escolha o ícone de atualização (#) para recarregar a tabela. Cada linha na tabela de relatórios de avaliação mostra o nome do relatório, a data de criação e um dos seguintes status:

- Em andamento – Audit Manager está gerando o relatório de avaliação.
- Pronto – relatório de avaliação está disponível para download.
- Erro – houve uma falha na geração do relatório de avaliação. Nesse caso, o Audit Manager exibe uma mensagem descrevendo o erro. Para informações sobre como resolver esses erros, consulte Solução de problemas de relatórios de avaliação.

Guia exportações

Essa guia mostra todos os resultados da pesquisa do localizador de evidências que você exportou nos últimos sete dias. Os arquivos CSV são removidos do centro de download após sete

dias, mas permanecem disponíveis no bucketS3 de destino de exportação. Para obter instruções sobre como encontrar uma exportação CSV do localizador de evidências em seu bucket de destino S3, consulte Visualizando seus resultados depois de exportá-los.

Para ver o status mais recente de suas exportações CSV, escolha o ícone de atualização (#) para recarregar a tabela. Cada linha na tabela de exportações mostra o nome do arquivo, sua data de exportação e um dos seguintes status:

- Em andamento – Audit Manager está preparando o arquivo CSV.
- Pronto – exportação foi bem-sucedida e o arquivo está disponível para download.
- Erro – exportação falhou. Nesse caso, o Audit Manager exibe uma mensagem descrevendo o erro. Para informações sobre como resolver erros, consulte Solução de problemas de exportação de CSV do localizador de evidências.

> **Note**
>
> Lembre-se de que a guia de exportações também pode exibir arquivos CSV para consultas executadas diretamente no Lake AWS CloudTrail. Isso inclui consultas feitas no console do CloudTrail ou usando a API do CloudTrail. As exportações do CloudTrail aparecerão nessa guia se você consultou o armazenamento de dados de eventos do Audit Manager e optou por salvar os resultados no Amazon S3.

Baixando um arquivo

Siga estas etapas para baixar um arquivo no centro de download.

Para baixar um arquivo

1. Abra o console do AWS Audit Manager em https://console.aws.amazon.com/auditmanager/home.
2. No painel de navegação à esquerda, escolha Centro de download.
3. Escolha a guia Relatórios de avaliação ou Exportações.
4. Escolha o arquivo que deseja acessar e selecione Baixar.

Para obter instruções sobre como baixar um arquivo do seu bucket de destino S3, consulte Baixando um objeto no Guia do Usuário Amazon Simple Storage Service (Amazon S3).

Excluindo um arquivo

Siga estas etapas para excluir quaisquer relatórios de avaliação dos quais não precisar mais do centro de downloads.

> **Note**
>
> A exclusão de exportações de CSV do centro de download não é suportada no momento. As exportações de CSV são removidas automaticamente do centro de downloads após sete dias.

Para excluir um relatório de avaliação

1. Abra o console do AWS Audit Manager em https://console.aws.amazon.com/auditmanager/home.
2. No painel de navegação à esquerda, escolha Centro de download.
3. Escolha a guia Relatórios de avaliação.
4. Selecione o relatório que deseja excluir e escolha Excluir.

Se quiser excluir um relatório de avaliação ou uma exportação CSV do seu bucket de destino S3, recomendamos que conclua essa tarefa diretamente no Amazon S3. Para obter mais informações, consulte Deletando objetos no Amazon S3 no Guia do Usuário Amazon Simple Storage Service (Amazon S3).

Biblioteca framework

Você pode acessar e gerenciar frameworks a partir da biblioteca de frameworks em AWS Audit Manager.

Saiba como criar, gerenciar e entender avaliações de conformidade no Audit Manager. Ele define os controles e seus mapeamentos de fonte de dados para um determinado padrão ou regulamento de conformidade. Também é usado para estruturar e automatizar as avaliações do Audit Manager. Você pode usar frameworks como ponto de partida para auditar o seu uso de AWS service (Serviço da AWS) e começar a automatizar a coleta de evidências.

A biblioteca de frameworks contém um catálogo de frameworks padrão personalizados.

- Os frameworks padrão são frameworks pré-construídos que fornecem AWS. Esses frameworks são baseadas nas práticas recomendadas de AWS para diferentes padrões e regulamentações de conformidade. Elas incluem GDPR e HIPAA. Frameworks padrão incluem controles que são organizados em conjuntos de controle baseados no padrão ou regulamentação de conformidade que o framework suporta.

  Você pode visualizar o conteúdo dos frameworks padrão, mas não pode editá-los nem excluí-los. No entanto, você pode personalizar qualquer framework padrão para criar um novo que atenda às suas necessidades específicas.
- Frameworks personalizados são frameworks personalizados que você possui. Você pode criar um framework personalizado do zero ou personalizar um framework existente. Você pode usar frameworks personalizados para organizar controles em conjuntos de controle de uma forma que atenda aos seus requisitos específicos. Para saber mais sobre como gerenciar controles, consulte Biblioteca de controle.

Você pode criar uma avaliação a partir de um framework padrão ou personalizado. Para saber como criar e gerenciar avaliações, consulte Avaliações em AWS Audit Manager.

> **Note**
>
> AWS Audit Manager auxilia na coleta de evidências relevantes para verificar a conformidade com padrões e regulamentações de conformidade específicos. No entanto, ele não avalia a sua conformidade em si. Portanto, as evidências coletadas por meio do AWS Audit Manager

podem não incluir todas as informações sobre seu uso AWS necessário a auditorias. AWS Audit Manager não substitui a assessoria jurídica ou os especialistas em conformidade.

Esta seção descreve como você pode criar e gerenciar frameworks personalizados no Audit Manager.

Tópicos

Como acessar frameworks disponíveis em AWS Audit Manager

Você pode visualizar todos os framework disponíveis na página da biblioteca framework no console do Audit Manager. A partir daqui, você também pode criar uma avaliação a partir de um framework, criar um framework personalizado ou personalizar um framework existente.

Você também pode visualizar todos os frameworks disponíveis usando o API Audit Manager ou a AWS Command Line Interface (AWS CLI).

Audit Manager console

Para visualizar frameworks disponíveis (console)

1. Abra o console do AWS Audit Manager em https://console.aws.amazon.com/auditmanager/home.
2. No painel de navegação à esquerda, selecione Biblioteca de framework.
3. Escolha a guia frameworks padrão ou a guia frameworks personalizados para navegar pelos frameworks padrão e personalizados disponíveis.
4. Escolha qualquer nome de framework para visualizar os detalhes daquele framework.

AWS CLI

Para visualizar frameworks disponíveis (AWS CLI)

Para visualizar frameworks no Audit Manager, use o comando list-assessment-frameworks e especifique um `--framework-type`. Ou você pode recuperar uma lista de frameworks padrão. Ou você pode recuperar uma lista de frameworks personalizados.

```
aws auditmanager list-assessment-frameworks --framework-type Standard
```

```
aws auditmanager list-assessment-frameworks --framework-type Custom
```

Audit Manager API

Para visualizar frameworks disponíveis (API)

Use a operação ListAssessmentFrameworks e especifique um frameworkType. Você pode recuperar uma lista de frameworks padrão. Ou você pode recuperar uma lista de frameworks personalizados.

Para obter mais informações, escolha um dos links anteriores para ler mais na Referência de API AWS Audit Manager. Isso inclui informações sobre como usar a operação `ListAssessmentFrameworks` e os parâmetros em um dos SDKs AWS específicos do idioma.

Como visualizar os detalhes de um framework

Você pode analisar os detalhes de um framework usando o console do Audit Manager, a API do Audit Manager ou o AWS Command Line Interface (AWS CLI).

Audit Manager console

Para visualizar os detalhes do framework (console)

1. Abra o console do AWS Audit Manager em https://console.aws.amazon.com/auditmanager/home.
2. No painel de navegação à esquerda, escolha Biblioteca de frameworks para ver uma lista de frameworks disponíveis.
3. Escolha a guia Frameworks padrão ou Frameworks personalizados para navegar pelos frameworks disponíveis.

4. Escolha o nome do framework para abri-lo.

Quando você abre um framework, uma página de detalhes do framework é exibida. As seções desta página e seu conteúdo são descritos a seguir.

Seção de detalhes do framework

Esta seção fornece uma visão geral do framework. Isso inclui as informações a seguir:

- Nome do framework – O nome do framework.
- Tipo de conformidade – O padrão ou regulamento de conformidade que o framework suporta.
- Descrição – Uma descrição do framework, se fornecida.
- Tipo de framework – Especifica se o framework é padrão ou personalizado.
- Conjuntos de controle – O número de conjuntos de controle associados ao framework.
- Controles – O número total de controles no framework.
- Fontes de controle – O número de fontes de dados de controle das quais o Audit Manager coleta evidências.
- Tags – As tags associadas ao framework.

Se você estiver visualizando um framework personalizado, os seguintes detalhes também serão exibidos:

- Criado por – A conta que criou o framework personalizado.
- Data de criação – A data que o framework personalizado foi criado.
- Última atualização – A data em que esse framework foi editado pela última vez.

Guia Controles

Essa guia lista os controles no framework, agrupados por conjunto de controles. Isso inclui as informações a seguir:

- Controles agrupados por conjunto de controles – Escolha o ícone de visualização em árvore para ver os controles que pertencem a cada conjunto de controles.
- Tipo – Especifica se o controle é um controle padrão ou personalizado.
- Fonte de dados – Especifica a fonte de dados da qual o Audit Manager coleta evidências para esse controle.

Guia Tags

Tags – Esta guia lista as tags associadas ao framework. Isso inclui as informações a seguir:

- Chave — A chave da tag (por exemplo, um padrão de conformidade, um regulamento ou uma categoria).
- Valor — O valor da tag.

AWS CLI

Para visualizar os detalhes do framework (AWS CLI)

1. Para Identificar o framework que você deseja analisar, execute o comando list-assessment-frameworks e especifique a `--framework-type`. Ou você pode recuperar uma lista de frameworks padrão. Ou você pode recuperar uma lista de frameworks personalizados.

   No exemplo a seguir, substitua o *texto do espaço reservado* por `Custom` ou `Standard`.

   ```
   aws auditmanager list-assessment-frameworks --framework-type Custom/Standard
   ```

   A resposta retorna uma lista de frameworks. Encontre o framework que você deseja analisar e anote o ID do framework e o Nome do Recurso da Amazon (ARN).
2. Para obter os detalhes do framework, execute o comando get-assessment-framework e especifique o `--framework-id`.

   No exemplo a seguir, substitua o *texto do espaço reservado* por suas próprias informações.

   ```
   aws auditmanager get-assessment-framework --framework-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
   ```

   Os detalhes do framework são retornados no formato JSON. Para entender esses dados, consulte a consulte saída de get-assessment-framework na Referência de ComandoAWS CLI.
3. Para ver as tags de um framework, use o comando list-tags-for-resource e especifique a `--resource-arn` para o framework.

No exemplo a seguir, substitua o *texto do espaço reservado* por suas próprias informações.

```
aws auditmanager list-tags-for-resource --resource-arn arn:aws:auditmanager:us-east-1:111122223333:assessmentFramework/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Para obter mais informações sobre tags no Audit Manager, consulte Recursos de AWS Audit Manager para tags

Audit Manager API

Para visualizar os detalhes do framework (API)

1. Para identificar o framework que você deseja analisar, execute o comando list-assessment-frameworks e especifique um frameworkType. Você pode recuperar uma lista de frameworks padrão. Ou você pode recuperar uma lista de frameworks personalizados.

   A partir da resposta, encontre o framework que você deseja analisar e anote o ID do framework e o nome do atributo da Amazon (ARN).

2. Para obter os detalhes do framework, use a operação getAssessmentFramework. Na solicitação, especifique o https://docs.aws.amazon.com/audit-manager/latest/APIReference/API_GetAssessmentFramework.html#auditmanager-GetAssessmentFramework-request-frameworkIdframeworkIdpa 1.

   Os detalhes do framework são retornados no formato JSON. Para entender esses dados, consulte Elementos de resposta do getAssessmentFramework na Referência de API AWS Audit Manager

3. Para ver as tags do framework, use a operação ListTagsForResource. Na solicitação, especifique o framework resourceArn obtido na etapa 1.

Para obter mais informações sobre tags no Audit Manager, consulte Recursos de AWS Audit Manager para tags

Para obter mais informações sobre essas operações de API, escolha qualquer um dos links anteriores para ler mais na Referência de API AWS Audit Manager. Isso inclui informações sobre como usar essas operações e os parâmetros em um dos SDKs da AWS específicos do idioma.

Criando criar um framework personalizado

Você pode acessar e gerenciar frameworks a partir da biblioteca de frameworks, em AWS Audit Manager. Você pode criar frameworks personalizados para organizar controles em conjuntos de controle de forma que atenda aos seus requisitos específicos.

Há duas maneiras de criar um framework personalizado. Você pode personalizar um framework personalizado ou você pode criar um novo framework do zero.

Tópicos

Como criar um novo framework personalizado do zero

Você pode usar frameworks personalizados em AWS Audit Manager para organizar controles em conjuntos de forma que atenda aos seus requisitos específicos. Você pode criar uma novo framework personalizado do zero na biblioteca do framework seguindo estas etapas.

Tópicos

Etapa 1: como especificar detalhes do framework

Comece especificando os controles que você deseja incluir no framework personalizado.

Para especificar detalhes do framework

1. Abra o console do AWS Audit Manager em https://console.aws.amazon.com/auditmanager/home.
2. No painel de navegação à esquerda, escolha Biblioteca de framework e escolha Criar framework personalizado.

3. Em Detalhes do framework, insira um nome, um padrão ou regulamento de conformidade (opcional) e uma descrição para seu framework (também opcional). Insira uma palavra-chave de norma ou regulamentação de conformidade, como PCI_DSS ou GDPR para que você possa usar essa palavra-chave para pesquisar seu framework.
4. Em Tags, selecione Adicionar nova tag para associar uma tag ao seu framework. Você pode especificar uma chave e um valor para cada tag. A chave de tag é obrigatória. Você pode usá-la como critério de pesquisa ao pesquisar esse framework na biblioteca do Framework. Para obter mais informações sobre tags no AWS Audit Manager, consulte Marcando atributos AWS Audit Manager.
5. Escolha Avançar.

Etapa 2: especificar os controles nos conjuntos de controle

Em seguida, você especifica quais controles deseja adicionar ao seu framework e como deseja organizá-los. Comece adicionando conjuntos de controle ao framework e, em seguida, adicione controles ao conjunto.

> **Note**
>
> Ao usar o console AWS Audit Manager para criar um framework personalizado, você pode adicionar até 10 conjuntos de controles para cada framework.
> Ao usar a API Audit Manager para criar um framework personalizado, você pode criar mais de 10 conjuntos de controles. Para adicionar mais conjuntos de controle do que o console permite atualmente, use a API CreateAssessmentFramework fornecida pelo Audit Manager.

Para especificar os controles nos conjuntos de controle

1. Em Nome do conjunto de controles, insira um nome para o seu conjunto de controles.
2. Em Adicionar um novo controle ao conjunto de controles, selecione o tipo de controle, use a lista suspensa para selecionar um dos dois tipos de controle: controles padrão ou controles personalizados. Os controles padrão são fornecidos pelo Audit Manager; os controles personalizados são aqueles que você cria.
3. Com base na opção selecionada na etapa anterior, uma lista de controles padrão ou personalizados é exibida. Você pode navegar pela lista ou pesquisar inserindo o nome do controle, a conformidade ou tag. Selecione um ou mais controles e escolha Adicionar ao conjunto de controles para adicioná-los ao conjunto de controles.

4. Na janela exibida, escolha Adicionar ao conjunto de controles para confirmar a sua adição.
5. Em analisar os controles selecionados no conjunto de controles, revise os controles que aparecem na lista Controles selecionados. Para adicionar mais controles a um conjunto, repita as etapas 2 a 4. Você pode remover controles indesejáveis do conjunto selecionando um ou mais controles e escolhendo Remover controle.
6. Para adicionar um novo conjunto de controles ao framework, escolha Adicionar conjunto de controles na parte inferior da página. Você pode remover conjuntos de controle indesejáveis escolhendo Remover conjunto de controles.
7. Depois de terminar de adicionar conjuntos de controles e controles, escolha Avançar.

Etapa 3: analisar e criar o framework

Analise as informações para seu framework. Para alterar as informações de uma etapa, selecione Editar.

Quando terminar, escolha Criar framework personalizado.

O que faço agora?

Depois de criar sua novo framework personalizado, você pode criar uma avaliação a partir do seu framework. Para obter mais informações, consulte Como criar uma avaliação.

Você também pode criar um framework personalizado usando um framework existente. Para obter mais informações, consulte Como personalizar um framework existente.

Para obter instruções sobre como editar seu framework personalizado, consulte Como editar um framework personalizado.

Como personalizar um framework existente

Com frameworks personalizados em AWS Audit Manager, você pode organizar controles em conjuntos de controle de uma forma que atenda aos seus requisitos específicos. Em vez de criar um framework personalizado do zero, você pode usar um framework existente como ponto de partida e personalizá-lo. Quando você faz isso, o framework existente permanece na biblioteca e um novo framework personalizado é criado com suas configurações personalizadas.

Você pode selecionar qualquer framework existente para personalizar. Pode ser um framework padrão ou um personalizado.

Na biblioteca do framework, na lista suspensa Criar framework personalizado, escolha Personalizar framework existente. Use as seguintes etapas para personalizar o framework.

Tópicos

Etapa 1: como especificar detalhes do framework

Todos os detalhes do framework, exceto as tags, são transferidos do framework original. Analise e modifique esses detalhes conforme necessário.

Para especificar detalhes do framework

1. Abra o console do AWS Audit Manager em https://console.aws.amazon.com/auditmanager/home.
2. No painel de navegação à esquerda, selecione Biblioteca de framework.
3. Escolha o framework que deseja customizar e, da lista suspensa Criar framework personalizado, escolha Personalizar framework existente.
4. Na janela exibida, insira um nome para o novo framework personalizado e escolha Personalizar.
5. Em Detalhes do framework, analise o nome, o tipo de conformidade e a descrição do seu framework e modifique-os conforme necessário. O tipo de conformidade deve indicar o padrão de conformidade ou a regulamentação associada ao seu framework. Você pode usar essa palavra-chave para pesquisar seu framework.
6. Em Tags, selecione Adicionar nova tag para associar uma tag ao seu framework. Você pode especificar uma chave e um valor para cada tag. A chave da tag é obrigatória e pode ser usada como critério de pesquisa ao pesquisar esse framework na biblioteca. Para obter mais informações sobre tags no AWS Audit Manager, consulte Marcando atributos AWS Audit Manager.
7. Escolha Avançar.

Etapa 2: especificar controles par adicionar conjuntos de controle

Os conjuntos de controle são transferidos do framework original. Personalize a configuração atual adicionando mais controles ou removendo os controles existentes conforme necessário.

> **Note**
>
> Quando você usa o console AWS Audit Manager para personalizar framework um framework, você pode adicionar até 10 conjuntos de controles para cada framework. Quando você usa a API do Audit Manager para criar um framework personalizado, você pode criar mais de 10 conjuntos de controles. Para adicionar mais conjuntos de controle do que o console permite atualmente, use a API CreateAssessmentFramework fornecida pelo Audit Manager.

Para especificar os controles no conjunto de controles

1. Em Nome do conjunto de controles, personalize o nome do conjunto de controles conforme necessário.
2. Em Adicionar um novo controle ao conjunto de controles, use a lista suspensa para adicionar um de dois novos tipos de controle: Controles padrão ou Controles personalizados.
3. Com base na opção selecionada na etapa anterior, uma lista de controles padrão ou personalizados é exibida. Você pode navegar pela lista ou pesquisar inserindo o nome do controle, a conformidade ou a tag, para localizar os controles que deseja adicionar. Selecione um ou mais controles e escolha Adicionar ao conjunto de controles para adicioná-los ao conjunto de controles.
4. Na janela exibida, escolha Adicionar ao conjunto de controles para confirmar a sua adição.
5. Em analisar os controles selecionados no conjunto de controles, revise os controles que aparecem na lista Controles selecionados. Para adicionar mais controles a um conjunto, repita as etapas 2 a 4. Você pode remover controles indesejáveis do conjunto selecionando um ou mais controles e escolhendo Remover controle.
6. Para adicionar um novo conjunto de controles ao framework, escolha Adicionar conjunto de controles na parte inferior da página. Você pode remover conjuntos de controle indesejáveis escolhendo Remover conjunto de controles.
7. Depois de terminar de adicionar conjuntos de controles e controles, escolha Avançar.

Etapa 3: analisar e criar o framework

Analise as informações para seu framework. Para alterar as informações de uma etapa, selecione Editar.

Quando terminar, escolha Criar framework personalizado.

O que faço agora?

Depois de criar sua novo framework personalizado, você pode criar uma avaliação a partir do seu framework. Para obter mais informações, consulte Como criar uma avaliação.

Para obter instruções sobre como editar seu framework personalizado, consulte Como editar um framework personalizado.

Como editar um framework personalizado

Você pode usar frameworks personalizados em AWS Audit Manager para organizar controles em conjuntos e atender às suas necessidades específicas. Você pode usar a biblioteca de frameworks para encontrar e editar um framework personalizado seguindo estas etapas.

Tópicos

Etapa 1: como editar detalhes do framework

Comece revisando e editando os detalhes do framework existente.

Para editar detalhes do framework

1. Abra o console do AWS Audit Manager em https://console.aws.amazon.com/auditmanager/home.
2. No painel de navegação à esquerda, escolha Biblioteca de framework e escolha a guia Criar framework personalizado.
3. Selecione o framework que você deseja editar, escolha Ações e, depois, Editar.

- Como alternativa, você pode abrir um framework personalizado e escolher Ações, Editar no canto superior direito da página de resumo da avaliação.

4. Em Detalhes do framework, analise o nome, o tipo de conformidade e a descrição do seu framework e modifique-os conforme necessário.
5. Escolha Avançar.

> **Tip**
>
> Para editar as tags de um framework, abra o framework e escolha a guia Tags do framework. Lá você pode visualizar e editar as tags associadas ao framework.

Etapa 2: editar os controles nos conjuntos de controle

Em seguida, revise e edite os controles e conjuntos de controles no framework.

> **Note**
>
> Ao usar o console AWS Audit Manager para editar um framework personalizado, você pode adicionar até 10 conjuntos de controles para cada framework.
> Quando você usa a API do Audit Manager para editar um framework personalizado, você pode criar mais de 10 conjuntos de controles. Para adicionar mais conjuntos de controle do que o console permite atualmente, use a API UpdateAssessmentFramework fornecida pelo Audit Manager.

Para editar controles

1. Em Nome do conjunto de controles, analise e edite o nome do seu conjunto de controles conforme necessário.
2. Em Adicionar um novo controle ao conjunto de controles, você pode adicionar um controle. Use a lista suspensa para selecionar um dos dois tipos de controle: Controles padrão ou Controles personalizados.
3. Com base na opção selecionada na etapa anterior, uma lista de controles padrão ou personalizados é exibida. Você pode navegar na lista para ver os conjuntos de controle. Pode navegar pela lista ou pesquisar inserindo o nome do controle, a fonte de dados ou tags, para

localizar os controles que deseja adicionar. Selecione um ou mais controles e escolha Adicionar ao conjunto de controles para adicioná-los ao conjunto de controles.

4. Na janela exibida, escolha Adicionar ao conjunto de controles para confirmar a sua adição.
5. Em Analisar os controles selecionados no conjunto de controles, analise os controles que aparecem na lista Controles selecionados. Para adicionar mais controles a um conjunto, repita as etapas 2 a 4. Você pode remover controles indesejáveis do conjunto selecionando um ou mais controles e escolhendo Remover controle.
6. Para adicionar um novo conjunto de controles ao framework, escolha Adicionar conjunto de controles na parte inferior da página. Você pode remover conjuntos de controle indesejáveis escolhendo Remover conjunto de controles.
7. Depois de terminar de adicionar conjuntos de controles e controles, escolha Avançar.

Etapa 3. Analise e atualize o framework

Analise as informações para seu framework. Para alterar as informações de uma etapa, selecione Editar.

Ao concluir, escolha Salvar alterações.

Como excluir um framework personalizado

Você pode usar a biblioteca de frameworks para encontrar e excluir um framework personalizado indesejável. Você também pode visualizar todos os framework disponíveis usando o API Audit Manager ou AWS Command Line Interface (AWS CLI).

> **Note**
>
> A exclusão de um framework personalizado não afeta nenhuma avaliação existente que tenha sido criada a partir do framework antes de ser excluída.

Audit Manager console

Para excluir um framework personalizado (console)

1. Abra o console do AWS Audit Manager em https://console.aws.amazon.com/auditmanager/home.

2. No painel de navegação à esquerda, escolha Biblioteca de framework e escolha a guia Frameworks personalizados.
3. Selecione o framework que você deseja editar, escolha Ações e, depois, Excluir.
   - Como alternativa, você pode abrir um framework personalizado e escolher Ações, Excluir no canto superior direito da página de resumo do framework.
4. Na janela, escolha Excluir para confirmar a exclusão.

AWS CLI

Para excluir um framework personalizado (AWS CLI)

1. Primeiro, identifique o framework personalizado que você deseja excluir. Para fazer isso, execute o comando list-assessment-frameworks e especifique a. `--framework-type` como `Custom`.

   ```
   aws auditmanager list-assessment-frameworks --framework-type Custom
   ```

   A resposta retorna uma lista de frameworks personalizados. Encontre o framework personalizado que você deseja excluir e anote o ID do framework.
2. Em seguida, execute o comando delete-assessment-framework e especifique a `--framework-id` do framework que você deseja excluir.

   No exemplo a seguir, substitua o *`texto do espaço reservado`* por suas próprias informações.

   ```
   aws auditmanager delete-assessment-framework --framework-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
   ```

Audit Manager API

Para excluir um framework personalizado (API)

1. Use a operação ListAssessmentFrameworks e especifique um frameworkType como `Custom`. Na resposta, encontre o framework personalizado que você deseja excluir e anote o ID do framework.

2. Use a operação DeleteAssessmentFramework para excluir o framework. Na solicitação, use o parâmetro frameworkID para especificar o framework que você deseja excluir.

Para obter mais informações sobre essas operações de API, escolha qualquer um dos links anteriores para ler mais na Referência de API AWS Audit Manager. Isso inclui informações sobre como usar essas operações e os parâmetros em um dos SDKs da AWS específicos do idioma.

Compartilhando um framework personalizado

Você pode usar o recurso de compartilhamento de framework do AWS Audit Manager para replicar rapidamente os frameworks personalizados que você criou. Agora você pode compartilhar suas frameworks personalizados do Audit Manager com outra Conta da AWS ou replicá-las em outra Região da AWS usando a sua própria conta. O destinatário pode então acessar seu framework personalizado e usá-lo para criar avaliações. Eles podem fazer isso sem precisar repetir nenhum dos seus esforços de configuração para esse framework.

Para compartilhar um framework personalizado, crie uma solicitação de compartilhamento. O destinatário da solicitação de compartilhamento tem 120 dias para aceitar ou recusar a solicitação. Quando eles aceitam a solicitação de compartilhamento, o Audit Manager replica o framework personalizado compartilhada em sua biblioteca de frameworks. Além de replicar o framework personalizado, o Audit Manager também replica todos os conjuntos de controles personalizados e controles personalizados que fazem parte desse framework. Esses controles personalizados são então adicionados à biblioteca de controle do destinatário. O Audit Manager não replica frameworks ou controles padrão. Por padrão, eles estão disponíveis em todas as Contas da AWS e Regiões onde o Audit Manager estiver ativado.

O atributo de compartilhamento de framework está disponível apenas no nível pago. No entanto, não há cobranças adicionais pelo compartilhamento de um framework personalizado ou pela aceitação de uma solicitação de compartilhamento. Para saber mais sobre precificação para AWS Audit Manager, consulte página de precificaçãoAWS Audit Manager.

> **Important**
>
> Você não pode compartilhar um framework personalizado derivado de um framework padrão se este for designado como não qualificado para compartilhamento por AWS, a menos que você tenha obtido permissão do proprietário do framework padrão. Para ver

quais frameworks padrão não estão qualificados para compartilhamento e para saber mais, consulte Elegibilidade de compartilhamento de framework.

As seções a seguir deste guia descrevem as coisas importantes que você deve saber sobre o compartilhamento de frameworks. Eles também fornecem instruções sobre como você pode compartilhar as suas frameworks personalizados e responder às solicitações de compartilhamento.

Tópicos

> **Tip**
>
> Se você não estiver familiarizado com frameworks personalizados do Audit Manager e como criá-los, saiba mais na página Como criar um framework personalizado deste guia.

Conceitos e terminologia de compartilhamento de framework

Se você aprender sobre os seguintes conceitos-chave, poderá aproveitar melhor o atributo de compartilhamento de framework personalizado AWS Audit Manager.

Remetente

Esse é o criador de uma solicitação de compartilhamento e o Conta da AWS onde o framework personalizado existe. Os remetentes podem compartilhar frameworks personalizados com qualquer um Conta da AWS. Ou eles replicam um framework personalizado para qualquer uma compatível Região da AWS com a sua própria conta.

Destinatário

Esse é o consumidor do framework compartilhado. Os destinatários podem aceitar ou recusar uma solicitação de compartilhamento de um remetente.

> **Note**
>
> Um destinatário pode ser uma conta de administrador delegado. No entanto, você não pode compartilhar frameworks personalizados com uma conta de gerenciamento AWS Organizations.

Elegibilidade do framework

Você só pode compartilhar frameworks personalizados. Por padrão, as frameworks padrão já estão presentes em todas Contas da AWS e Regiões da AWS onde AWS Audit Manager estão habilitadas. Além disso, as frameworks personalizados que você compartilha não devem conter dados confidenciais. Isso inclui dados encontrados no próprio framework, seus conjuntos de controle e qualquer um dos controles personalizados que fazem parte do framework personalizado.

> **Important**
>
> Alguns frameworks padrão oferecidos pelo AWS Audit Manager contêm material protegido por direitos autorais que está sujeito a contratos de licença. Frameworks personalizados podem conter conteúdo derivado desses frameworks. Você não pode compartilhar um framework personalizado derivado de um framework padrão se o framework padrão for designado como não qualificado para compartilhamento por AWS, a menos que você tenha obtido permissão do proprietário do framework padrão.
> Para saber quais frameworks padrão estão qualificados para compartilhamento, consulte a tabela a seguir.

Nome do framework padrão	Versões personalizadas qualificadas para compartilhamento
Essential Eight do Centro Australiano de Segurança Cibernética (ACSC)	 Sim

Nome do framework padrão	Versões personalizadas qualificadas para compartilhamento
Manual de Segurança da Informação do Centro Australiano de Segurança Cibernética (ACSC)	Sim
AWS Audit Manager Sample Framework	Sim
AWS Control Tower Guardrails	Sim
Práticas recomendadas da AWS para IA generativa do framework v1	Sim
AWS License Manager	Sim
Práticas Recomendadas de Segurança Básica AWS	Sim
AWS Práticas Recomendadas Operacionais	Sim
Framework Well-Architected da AWS	Sim

Nome do framework padrão	Versões personalizadas qualificadas para compartilhamento
Centro Canadense de Segurança Cibernética - Médio	 Não
CIS Benchmark para CIS Amazon Web Services Foundations Benchmark v1.2.0, Nível 1	 Não
CIS Benchmark para CIS Amazon Web Services Foundations Benchmark v1.2.0, Níveis 1 e 2	 Não
CIS Benchmark para CIS Amazon Web Services Foundations Benchmark v1.3.0, Nível 1	 Não
CIS Benchmark para CIS Amazon Web Services Foundations Benchmark v1.3.0, Níveis 1 e 2	 Não
CIS Benchmark para CIS Amazon Web Services Foundations Benchmark v1.4.0, Nível 1	 Não
CIS Benchmark para CIS Amazon Web Services Foundations Benchmark v1.4.0, Níveis 1 e 2	 Não
CIS Controls v7.1 IG1	 Sim

Nome do framework padrão	Versões personalizadas qualificadas para compartilhamento
CIS Controls v8 IG1	 Não
Linha de Base Moderada do FedRAMP	 Sim
GPDR	 Sim
Lei Gramm-Leach-Bliley (GLBA)	 Sim
GxP 21 CFR Parte 11	 Sim
Anexo 11 da GxP da UE	 Sim
Regra de Segurança HIPAA 2003	 Sim
Regra Final de Segurança Geral da HIPAA de 2013	 Sim

Nome do framework padrão	Versões personalizadas qualificadas para compartilhamento
ISO/IEC 27001:2013 Anexo A	 Não
NIST 800-53 (Rev. 5) Baixo-Moderado-Alto	 Sim
NIST Cybersecurity Framework versão 1.1	 Sim
NIST SP 800-171 Rev. 2	 Sim
PCI DSS v3.2.1	 Não
PCI DSS v4.0	 Não
SOC 2	 Não

Solicitação de compartilhamento

Para compartilhar um framework personalizado, crie uma solicitação de compartilhamento. A solicitação de compartilhamento especifica um destinatário e o notifica quando um framework personalizado estiver disponível. Os destinatários têm 120 dias para responder a uma solicitação de compartilhamento aceitand-a ou recusand-a. Se nenhuma ação for tomada em 120 dias, a

solicitação de compartilhamento expirará e o destinatário perderá a capacidade de adicionar o framework personalizado à biblioteca do framework. Remetentes e destinatários podem visualizar e agir em relação às solicitações de compartilhamento na página de solicitações de compartilhamento da biblioteca do framework.

Status da solicitação de compartilhamento

As solicitações de compartilhamento podem ter qualquer um dos seguintes status.

- Ativo – Isso indica uma solicitação de compartilhamento que foi enviada com êxito ao destinatário e está aguardando sua resposta.
- Expirando – Isso indica uma solicitação de compartilhamento que expira nos próximos 30 dias.
- Compartilhado – indica uma solicitação de compartilhamento que o destinatário aceitou.
- Inativo – isso indica uma solicitação de compartilhamento que foi revogada, recusada ou expirou antes que o destinatário agisse.
- Replicação – Isso indica uma solicitação de compartilhamento aceita que está sendo replicada para a biblioteca do framework do destinatário.
- Falha – Isso indica que uma solicitação de compartilhamento não foi enviada com êxito ao destinatário.

Notificações de solicitações de compartilhamento

O Audit Manager notifica os destinatários quando eles receberem uma solicitação de compartilhamento. Tanto os destinatários, quanto os remetentes, recebem uma notificação quando uma solicitação de compartilhamento deve expirar nos próximos 30 dias.

- Para os destinatários, um ponto de notificação azul aparece ao lado das solicitações recebidas com status Ativo ou Expirando. O destinatário pode resolver a notificação aceitando ou recusando a solicitação de compartilhamento.
- Para os destinatários, um ponto de notificação azul aparece ao lado das solicitações recebidas com status Expirando. A notificação é resolvida quando o destinatário aceita ou recusa a solicitação. Caso contrário, será resolvida quando a solicitação expirar. Além disso, o remetente pode resolver a notificação revogando a solicitação de compartilhamento.

Propriedade do remetente

Os remetentes mantêm acesso total aos frameworks personalizados que compartilham. Eles podem cancelar solicitações de compartilhamento ativas a qualquer momento revogando a solicitação de compartilhamento antes que ela expire. No entanto, depois que um destinatário aceita uma solicitação de compartilhamento, o remetente não pode mais revogar o acesso do

destinatário a esse framework personalizado. Isso ocorre porque, quando o destinatário aceita a solicitação, o Audit Manager cria uma cópia independente do framework personalizado na biblioteca do framework do destinatário.

Além de replicar o framework personalizado do remetente, o Audit Manager também replica todos os conjuntos e controles personalizados que fazem parte desse framework. No entanto, o Audit Manager não replica nenhuma tag anexada ap framework personalizado.

Propriedade do destinatário

Os destinatários têm acesso total aos frameworks personalizados que aceitam. Quando o destinatário aceita a solicitação, o Audit Manager replica o framework personalizado na guia Frameworks personalizados de sua biblioteca. Os destinatários podem então gerenciar o framework personalizado compartilhado da mesma forma que qualquer outro. Os destinatários podem compartilhar frameworks personalizados recebidos de outros remetentes. Os destinatários não podem impedir que os remetentes enviem solicitações de compartilhamento.

Expiração do framework compartilhado

Quando um remetente cria uma solicitação de compartilhamento, o Audit Manager define que a solicitação expire após 120 dias. Os destinatários podem aceitar e obter acesso ao framework compartilhado antes que a solicitação expire. Se um destinatário não aceitar durante esse período, a solicitação de compartilhamento irá expirar. Depois desse ponto, um registro da solicitação de compartilhamento expirada permanece em seu histórico. As capturas de tela de frameworks compartilhados expirados são arquivados em um bucket S3 com TTL de um ano para fins de auditoria.

Os remetentes podem optar por revogar uma solicitação de compartilhamento a qualquer momento antes que ela expire.

Backup e armazenamento de dados de framework compartilhado

Quando você cria uma solicitação de compartilhamento, o Audit Manager armazena uma captura de tela de seu framework personalizado no Leste dos EUA (N. da Virgínia) Região da AWS. O Audit Manager também armazena um backup da mesma captura de tela no Oeste dos EUA (Oregon) Região da AWS.

O Audit Manager exclui o captura de tela e captura de tela de backup quando ocorre um dos seguintes eventos:

- O remetente revoga a solicitação de compartilhamento.
- O destinatário recusa a solicitação de compartilhamento.

- O destinatário encontra um erro e não aceita com êxito a solicitação de compartilhamento.
- A solicitação de compartilhamento expira antes que o destinatário responda à solicitação.

Quando um remetente reenvia uma solicitação de compartilhamento, a captura de tela é substituída por uma versão atualizada que corresponde à versão mais recente do framework personalizado.

Quando um destinatário aceita uma solicitação de compartilhamento, o captura de tela é replicado para ele em seu Conta da AWS sob o Região da AWS que foi especificado na solicitação de compartilhamento.

Versionamento de framework compartilhado

Quando você compartilha um framework personalizado, o Audit Manager cria uma cópia independente desse framework na Região especificada Conta da AWS. Isso significa que você deve ter em mente os seguintes pontos:

- O framework compartilhado que um destinatário aceita é uma captura de tela do framework no momento da criação da solicitação de compartilhamento. Se você atualizar o framework personalizado original depois de enviar uma solicitação de compartilhamento, a solicitação não será atualizada automaticamente. Para compartilhar a versão mais recente do framework atualizado, você pode reenviar a solicitação de compartilhamento. A data de expiração desse novo captura de tela é de 120 dias a partir da data de recompartilhamento.
- Quando você compartilha um framework personalizado com outra pessoa Conta da AWS e a exclui da sua biblioteca de framework, o framework personalizado compartilhado permanece na biblioteca do framework do destinatário.
- Quando você compartilha um framework personalizado com outra Região da AWS em sua conta e depois exclui esse framework personalizado na primeira Região da AWS, o framework personalizado permanece na segunda Região.
- Quando você exclui um framework personalizado compartilhada depois de aceitá-la, todos os controles personalizados que foram replicados como parte do framework personalizado permanecem na sua biblioteca de controle.

Enviar uma solicitação de compartilhamento para um framework personalizado

Este tutorial descreve como compartilhar seus frameworks personalizados entre Contas da AWS e. Regiões da AWS

Quando você compartilha um framework personalizado, o Audit Manager cria uma captura de tela do seu framework e envia uma solicitação de compartilhamento ao destinatário. O destinatário tem 120 dias para aceitar o framework compartilhado. Quando eles aceitam, o Audit Manager replica o framework personalizado compartilhada em sua biblioteca de frameworks no Região da AWS especificado. Se você quiser replicar um framework personalizado para outra Região com sua própria conta, use o tutorial a seguir e insira sua próprio ID Conta da AWS como o ID da conta do destinatário.

Este tutorial inclui as seguintes etapas:

1. Selecione um framework para compartilhar – Navegue pela biblioteca do framework para encontrar o framework personalizado que você deseja compartilhar.
2. Enviar uma solicitação de compartilhamento – Especifique um destinatário e envie a ele uma solicitação de compartilhamento para o framework personalizado.
3. Visualizar solicitações enviadas – Visualize seu histórico de solicitações de compartilhamento e verifique o status das solicitações enviadas.
4. (Opcional) Revogue a solicitação de compartilhamento – Revogue a solicitação de compartilhamento antes que ela expire.

Pré-requisitos

Antes de começar este tutorial, certifique-se de atender às seguintes condições:

- Você está familiarizado com os conceitos e terminologia do compartilhamento de frameworks do Audit Manager.
- o framework personalizado que você deseja compartilhar está qualificado para compartilhamento e existe na biblioteca do framework do seu ambiente AWS Audit Manager.
- O destinatário já habilitou AWS Audit Manager no Região da AWS em que você deseja compartilhar o framework personalizado.
- O destinatário não é uma conta de gerenciamento AWS Organizations.

> **Tip**
>
> Antes de começar, anote o ID Conta da AWS com o qual você deseja compartilhar seu framework personalizado. Esse pode ser seu próprio ID de conta, se sua meta for replicar o

framework para outra Região da AWS em sua conta. Você precisará dessa informação para a etapa 2 do tutorial.

Important

Não compartilhe frameworks personalizados que contenham dados confidenciais. Isso inclui dados encontrados na próprio framework, seus conjuntos de controle e qualquer um dos controles personalizados que fazem parte do framework personalizado. Para obter mais informações, consulte Elegibilidade para o framework.

Etapa 1: identifique o framework personalizado que você deseja compartilhar

Comece por identificar o framework personalizado que você deseja compartilhar. Você pode visualizar todos os framework disponíveis na página da biblioteca da Estrutura no console do Audit Manager.

Para visualizar suas frameworks personalizados disponíveis

1. Abra o console do AWS Audit Manager em https://console.aws.amazon.com/auditmanager/home.
2. No painel de navegação, selecione Biblioteca de frameworks.
3. Escolha a guia Frameworks personalizados. Isso exibe uma lista dos suas frameworks personalizados disponíveis. Escolha qualquer nome de framework para visualizar os detalhes daquele framework personalizado.

Etapa 2: envie uma solicitação de compartilhamento

Em seguida, especifique um destinatário e envie a ele/ela uma solicitação de compartilhamento para o framework personalizado. O destinatário tem 120 dias para responder à solicitação compartilhamento antes que ela expire.

Para enviar uma solicitação de compartilhamento

1. Na guia frameworks personalizados da biblioteca do frameworks, escolha o nome de um framework para abrir a página de detalhes. A partir daqui, escolha Ações e, em seguida, escolha Compartilhar framework personalizado.

- Como alternativa, selecione um framework personalizado na lista na biblioteca de frameworks, escolha Ações e, em seguida, escolha Compartilhar framework personalizado. De acordo com o tamanho do framework personalizado, esse método pode levar alguns segundos, enquanto o Audit Manager prepara a solicitação de compartilhamento.

2. Analise o aviso exibido na caixa de diálogo.

   - Se não tiver certeza se pode compartilhar seu framework personalizado, analise a elegibilidade do framework para mais orientações.
   - Caso seu framework possuir controles que usem regras personalizadas AWS Config como fonte de dados, recomendamos que entre em contato com o destinatário para informá-lo. O destinatário pode então criar e ativar as mesmas regras AWS Config em sua instância do AWS Config. Para obter mais informações, consulte Meu framework compartilhado tem controles que usam regras personalizadas do AWS Config como fonte de dados. O destinatário pode coletar evidências para esses controles?.

3. Digite **`agree`** e, em seguida, escolha Concordo para continuar.
4. Na próxima tela, siga essas etapas:

   - Em Conta da AWS, insira o ID da conta do destinatário. Este pode ser o ID da sua própria conta.
   - Em Região da AWS, selecione a Região do destinatário na lista suspensa.
   - (Opcional) Em Mensagem ao destinatário, insira um comentário opcional sobre o framework personalizado que você está compartilhando.
   - Em Detalhes do framework personalizado, analise os detalhes para confirmar que deseja compartilhar esse framework.

5. Escolha Compartilhar.

> **Note**
>
> Lembre-se dos seguintes pontos:
>
> - Quando você compartilha um framework personalizado com outro Conta da AWS, o framework é replicado somente para a Região da AWS especificada. Depois de aceitar a solicitação de compartilhamento, o destinatário pode então replicar o framework em todas as Regiões, conforme necessário.

- Ao compartilhar frameworks personalizados em Regiões da AWS, o processamento das ações de solicitação de compartilhamento pode levar até 10 minutos. Depois de enviar uma solicitação de compartilhamento entre Regiões, recomendamos que você verifique novamente mais tarde para confirmar se a sua solicitação de compartilhamento foi enviada com êxito.
- Quando você envia uma solicitação de compartilhamento, o Audit Manager tira uma captura de tela do framework personalizado no momento da criação da solicitação de compartilhamento. Se você atualizar o framework personalizado depois de enviar uma solicitação de compartilhamento, a solicitação não será atualizada automaticamente. Para compartilhar a versão mais recente do framework atualizado, você pode reenviar a solicitação de compartilhamento. A data de expiração desse novo captura de tela é de 120 dias a partir da data de recompartilhamento.

Etapa 3: visualizar seus pedidos enviados

Você pode selecionar a guia Solicitações enviadas para ver uma lista de todas as solicitações de compartilhamento que você enviou. Você pode filtrar essa lista conforme necessário. Por exemplo, você pode aplicar filtros para exibir somente solicitações que expiram nos próximos 30 dias.

Para visualizar e filtrar suas solicitações enviadas

1. No painel de navegação, selecione Solicitações de compartilhamento.
2. Escolha a guia Solicitações enviadas.
3. (Opcional) Aplique filtros para ajustar quais solicitações enviadas ficarão visíveis. Você pode fazer isso localizando a lista suspensa Todos os status e alterando o filtro para uma das seguintes opções.

   - Ativo – Esse filtro exibe solicitações de compartilhamento que estão aguardando uma resposta do destinatário.
   - Compartilhado – Esse filtro exibe solicitações de compartilhamento que foram aceitas pelo destinatário. O framework personalizado compartilhada agora existe na biblioteca do framework do destinatário.
   - Inativo – isso indica solicitações de compartilhamento recusadas, revogadas ou expiradas antes que o destinatário agisse. Escolha a palavra Inativo para visualizar mais detalhes.

- Expirando – Esse filtro exibe solicitações de compartilhamento que expiram nos próximos 30 dias.
- Falha – Esse filtro exibe as solicitações de compartilhamento que não foram enviadas com êxito ao destinatário. Escolha a palavra Falha para visualizar mais detalhes.

> **Note**
>
> Pode levar até 15 minutos para processar uma solicitação de compartilhamento. Como resultado, se ocorrer um erro ao enviar sua solicitação de compartilhamento ao destinatário, o status Falha pode não ser exibido imediatamente. Recomendamos que você verifique novamente mais tarde para confirmar se a sua solicitação de compartilhamento foi enviada com êxito.
> Para obter informações sobre como proceder se encontrar um erro, consulte Solução de problemas de solicitações de compartilhamento.

Etapa 4 (opcional): revogar a solicitação de compartilhamento

Se precisar cancelar uma solicitação de compartilhamento ativa antes que ela expire, você pode revogar a solicitação a qualquer momento. Esta etapa é opcional. Se você não fizer nada, o destinatário perderá a capacidade de aceitar a solicitação de compartilhamento após a data de expiração.

Para revogar uma solicitação de compartilhamento

1. No painel de navegação, selecione Solicitações de compartilhamento.
2. Escolha a guia Solicitações enviadas.
3. Selecione o framework que você deseja revogar e escolha Revogar solicitação.
4. Na janela exibida, escolha Revogar.

> **Note**
>
> Você só pode revogar o acesso a solicitações de compartilhamento com o status Ativo ou Expirando. No entanto, depois que um destinatário aceita uma solicitação de compartilhamento, você não pode mais revogar seu acesso ao framework personalizado.

Isso ocorre porque agora existe uma cópia do framework personalizado na biblioteca do framework do destinatário.
Ao compartilhar frameworks personalizados em Regiões da AWS, o processamento das ações de solicitação de compartilhamento pode levar até 10 minutos, Depois de revogar uma solicitação de compartilhamento entre Regiões, recomendamos que você verifique novamente mais tarde para confirmar se a sua solicitação de compartilhamento foi revogada com êxito.

Reenviando uma solicitação de compartilhamento para um framework atualizado

Você pode enviar uma solicitação de compartilhamento para um framework personalizado e depois atualizar o mesmo framework. Se você fizer isso, a solicitação de compartilhamento não será atualizada automaticamente para refletir a versão mais recente do framework. No entanto, se o status estiver ativo, compartilhado ou expirando, você poderá atualizar uma solicitação de compartilhamento existente. Para fazer isso, você reenvia uma nova solicitação de compartilhamento com o mesmo conjunto de detalhes da solicitação existente. Na nova solicitação de compartilhamento, inclua a mesmo ID de framework personalizado, o ID da conta do destinatário e o destinatário Região da AWS. Você também pode fornecer um novo comentário com a nova solicitação de compartilhamento.

Lembre-se do seguinte ao reenviar uma solicitação de compartilhamento:

- Para que a atualização seja bem-sucedida, a nova solicitação deve ser para a mesmo ID de framework personalizado. Ele também deve especificar a mesmo ID da conta do destinatário e a mesma Região da solicitação existente.
- Se o nome do framework personalizado tiver sido alterado, a solicitação de compartilhamento atualizada exibirá o nome mais recente.
- Se você fornecer um novo comentário, a solicitação de compartilhamento atualizada exibirá o comentário mais recente.
- Quando você reenvia uma solicitação de compartilhamento, a data de expiração é estendida em seis meses.

Como reenviar uma solicitação de compartilhamento para um framework atualizado

1. Na guia Frameworks personalizados da biblioteca de frameworks, escolha o nome do framework que quiser compartilhar. Isso abrirá a página de detalhes do framework. A partir daqui, escolha Ações e, em seguida, escolha Compartilhar framework personalizado.

   - Como alternativa, selecione um framework personalizado na lista na biblioteca de frameworks, escolha Ações e, em seguida, Compartilhar framework personalizado. Dependendo do tamanho do framework personalizado, esse método pode levar alguns segundos enquanto o Audit Manager prepara a solicitação de compartilhamento.
2. Analise o aviso exibido na caixa de diálogo, insira **`agree`**, e escolha Concordo para continuar.
3. Na próxima tela, siga essas etapas:

   - Em Conta da AWS, insira o mesmo ID da conta que você especificou na solicitação de compartilhamento existente.
   - Em Região da AWS, insira a mesma região que você especificou na solicitação de compartilhamento existente.
   - (Opcional) Em Mensagem ao destinatário, insira um comentário opcional sobre o framework personalizado atualizado.
   - Em Detalhes do framework personalizado, analise os detalhes para confirmar que deseja compartilhar esse framework.
4. Escolha Compartilhar para reenviar e atualizar a solicitação de compartilhamento.

Solução de problemas de solicitações de compartilhamento

Para encontrar soluções para os problemas que você pode encontrar ao compartilhar um framework personalizado, consulte Solução de problemas de compartilhamento de framework na seção Solução de problemas deste guia.

Como responder a solicitações de compartilhamento

Este tutorial descreve as ações a serem tomadas ao receber uma solicitação de compartilhamento para um framework personalizado. O Audit Manager lhe enviará uma notificação ao receber uma solicitação de compartilhamento. Você também recebe uma notificação quando uma solicitação de compartilhamento for expirar nos próximos 30 dias.

Este tutorial inclui as seguintes etapas:

1. Verifique suas notificações de solicitação de compartilhamento – analise uma lista de solicitações de compartilhamento ativas que expiram em breve.
2. Execute uma ação em relação à solicitação de compartilhamento – aceite ou recuse a solicitação de compartilhamento para o framework personalizado.
3. Veja as solicitações de compartilhamento que recebeu de outras pessoas – veja seu histórico de solicitações de compartilhamento.

Pré-requisitos

Antes de começar, recomendamos que primeiro aprenda mais sobre conceitos e terminologia de compartilhamento de framework do Audit Manager.

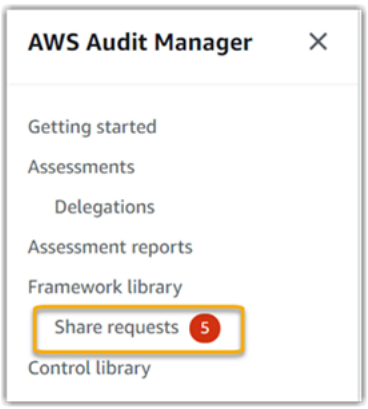
Etapa 1: verificar as notificações de solicitação recebidas

Comece verificando suas notificações de solicitação de compartilhamento. A guia Solicitações recebidas exibe uma lista das solicitações de compartilhamento que você recebeu de outras Contas da AWS. As solicitações aguardando sua resposta aparecem com um ponto azul. Você também pode filtrar essa visualização para exibir somente solicitações que expiram nos próximos 30 dias.

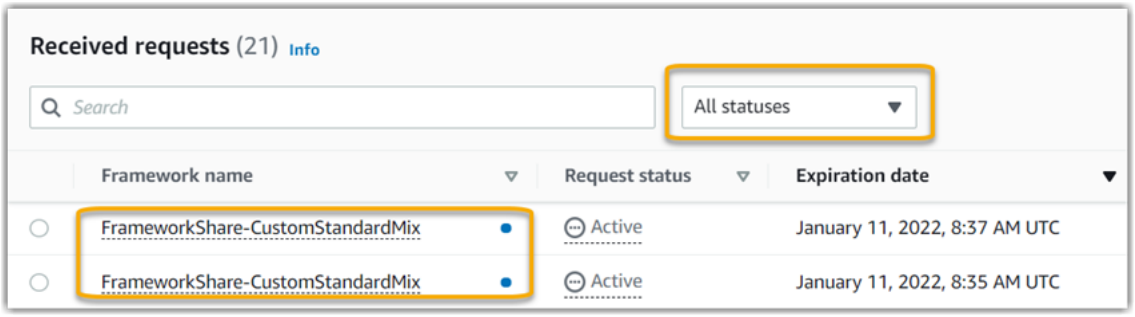
Para visualizar as solicitações recebidas

1. Abra o console do AWS Audit Manager em https://console.aws.amazon.com/auditmanager/home.
2. Se você tiver uma notificação de solicitação de compartilhamento, o Audit Manager exibirá um ponto vermelho ao lado do ícone do menu de navegação.

3. Expanda o painel de navegação e veja ao lado de Solicitações de compartilhamento. Um selo de notificação indica o número de solicitações de compartilhamento que precisam de atenção.



4. Escolha Solicitações de compartilhamento. Por padrão, essa página é aberta na guia Solicitações recebidas.
5. Identifique as solicitações de compartilhamento que precisem de ação procurando itens com um ponto azul.



6. (Opcional) Para visualizar somente as solicitações que expiram nos próximos 30 dias, localize a lista suspensa Todos os status e selecione Expirando.

Etapa 2: agir de acordo com a solicitação

Para remover o ponto azul de notificação, você precisa agir aceitando ou recusando a solicitação de compartilhamento.

> **Note**
>
> O processamento das ações de solicitação de compartilhamento pode levar até 10 minutos quando um framework é compartilhado em Regiões da AWS. Depois de agir em uma solicitação de compartilhamento entre Regiões, recomendamos que você verifique novamente mais tarde para confirmar se a sua solicitação de compartilhamento foi aceita ou recusada com êxito.

Como aceitar um framework compartilhado

Quando você aceita uma solicitação de compartilhamento, o Audit Manager replica uma captura de tela do framework original na guia frameworks personalizados da sua biblioteca de frameworks. O Audit Manager replica e criptografa a novo framework personalizado usando a chave KMS que você especificou nas configurações do Audit Manager.

Para aceitar uma solicitação de compartilhamento

1. Abra a página Solicitações de compartilhamento e verifique se você está visualizando a guia Solicitações recebidas.
2. (Opcional) Selecione Ativo ou Expirando na lista suspensa do filtro.
3. (Opcional) Escolha o nome do framework para visualizar os detalhes da solicitação de compartilhamento. Isso inclui informações como a descrição do framework, o número de controles que estão no framework e a mensagem do remetente.
4. Selecione a solicitação de compartilhamento que deseja aceitar, escolha Ações e, em seguida, Aceitar.

Depois de aceitar uma solicitação de compartilhamento, o status muda para replicando enquanto o framework personalizado compartilhada é adicionada à sua biblioteca de framework. Se o framework contiver controles personalizados, esses controles serão adicionados à sua biblioteca de controle no momento.

Quando a replicação do framework é concluída, o status muda para compartilhado. Um banner de sucesso notifica você de que o framework personalizado está pronta para uso.

> **Tip**
>
> Quando você aceita um framework personalizado, ela é replicada somente na sua atual Região da AWS. Talvez você queira que a novo framework compartilhado esteja disponível em todas as Regiões em seu Conta da AWS. Nesse caso, depois de aceitar a solicitação de compartilhamento, você poderá compartilhar o framework com outras Regiões da sua conta, conforme necessário.

Como recusar um framework compartilhado

Quando você recusa uma solicitação de compartilhamento, o Audit Manager não adiciona esse framework personalizado à sua biblioteca de frameworks. No entanto, um registro da solicitação de compartilhamento recusado permanece na guia Solicitações recebidas, com o status Inativo.

Para recusar uma solicitação de compartilhamento

1. Abra a página Solicitações de compartilhamento e verifique se você está visualizando a guia Solicitações recebidas.
2. (Opcional) Selecione Ativo ou Expirando na lista suspensa do filtro.
3. (Opcional) Escolha o nome do framework para visualizar os detalhes da solicitação de compartilhamento. Isso inclui informações como a descrição do framework, o número de controles que estão no framework e a mensagem do remetente.
4. Selecione a solicitação de compartilhamento que você deseja recusar, escolha Ações e, em seguida, escolha Aceitar.
5. Na caixa de diálogo exibida, escolha Recusar para confirmar a sua escolha.

> **Tip**
>
> Se você mudar de ideia e quiser acessar um framework compartilhado depois de recusar, peça ao remetente que envie uma nova solicitação de compartilhamento.

Etapa 3: visualizar um histórico das solicitações recebidas

Depois de aceitar ou recusar um framework compartilhado, você pode retornar à página Solicitações de compartilhamento para ver seu histórico de solicitações de compartilhamento. Você pode filtrar essa lista conforme necessário. Por exemplo, você pode aplicar filtros para exibir somente as solicitações que você aceitou.

Para visualizar um histórico de suas solicitações de compartilhamento

1. Abra o console do AWS Audit Manager em https://console.aws.amazon.com/auditmanager/home.
2. No painel de navegação à esquerda, selecione Solicitações de compartilhamento.
3. Escolha a guia Solicitações recebidas.

4. Encontre a lista suspensa Todos os status e selecione um dos filtros a seguir.

   - Ativo – Esse filtro exibe solicitações de compartilhamento que você ainda não aceitou ou recusou.
   - Expirando – Esse filtro exibe solicitações de compartilhamento que expiram nos próximos 30 dias.
   - Compartilhado – Esse filtro exibe solicitações de compartilhamento que você aceitou. O framework compartilhado agora está disponível em sua biblioteca de frameworks.
   - Inativo – Isso indica solicitações de compartilhamento que foram recusadas ou expiradas.
   - Falha – Esse filtro exibe as solicitações de compartilhamento que não foram enviadas com êxito. Escolha a palavra Falha para visualizar mais detalhes.

O que faço agora?

Depois de aceitar um framework personalizado compartilhado, você pode encontrá-lo na guia Frameworks personalizados da biblioteca do framework. Agora você pode usar esse framework para criar uma avaliação. Para saber mais, consulte Como criar uma avaliação. Para obter instruções sobre como editar seu novo framework personalizado, consulte Como editar um framework personalizado.

Como excluir solicitações de compartilhamento

Você pode excluir solicitações de compartilhamento que não sejam mais desejadas ou necessárias.

> **Note**
>
> Você não pode excluir solicitações de compartilhamento com status ativo ou replicando. Quando você exclui uma solicitação de compartilhamento, somente a solicitação em si é excluída. O próprio framework compartilhado permanece na sua biblioteca de frameworks.

Para excluir uma solicitação de compartilhamento

1. No painel de navegação, selecione Solicitações de compartilhamento.
2. Escolha a guia Solicitações enviadas ou Solicitações recebidas.
3. Selecione o framework que você não deseja mais e escolha Excluir.
4. Na janela exibida, escolha Excluir.

Frameworks compatíveis em AWS Audit Manager

AWS Audit Manager fornece as seguintes frameworks padrão. Esses frameworks pré-criados são baseadas nas práticas recomendadas AWS para vários padrões e regulamentações de conformidade. Você pode usar esses frameworks na preparação da sua auditoria.

Tópicos

- NIST 800-53 (Rev. 5) Baixo-Moderado-Alto
- NIST Cybersecurity Framework versão 1.1
- NIST SP 800-171 (Rev. 2)
- PCI DSS V3.2.1
- PCI DSS V4.0
- SOC 2

Essential Eight do Centro Australiano de Segurança Cibernética (ACSC)

Para ajudá-lo na preparação da auditoria, AWS Audit Manager fornece um framework padrão pré-construído que estrutura e automatiza as avaliações do framework Essential Eight.

Tópicos

- O que é Essential Eight do Centro Australiano de Segurança Cibernética (ACSC)?
- Como usar esse framework para apoiar sua preparação para auditoria
- Mais recursos do Essential Eight

O que é Essential Eight do Centro Australiano de Segurança Cibernética (ACSC)?

O Centro de Segurança Cibernética Australiano (ACSC) é a principal agência do governo australiano para segurança cibernética. Para se proteger contra ameaças cibernéticas, o ACSC recomenda que as organizações implementem oito estratégias essenciais de mitigação das Estratégias para Mitigar Incidentes de Segurança Cibernética do ACSC como linha de base. Essa linha de base, conhecida como Essential Eight, torna muito mais difícil para os adversários comprometerem os sistemas.

Como o Essential Eight descreve um conjunto mínimo de medidas preventivas, a sua organização precisa implementar medidas adicionais quando isso for garantido pelo seu ambiente. Além disso, embora o Essential Eight possa ajudar a mitigar a maioria das ameaças, ele não mitigará todas. Dessa forma, estratégias adicionais de mitigação e controles de segurança precisam ser considerados, incluindo os das Estratégias para Mitigar Incidentes de Segurança Cibernética e do Manual de Segurança da Informação (ISM).

Como usar esse framework para apoiar sua preparação para auditoria

Você pode usar o framework padrão Essential Eight em AWS Audit Manager para ajudá-lo a se preparar para as auditorias. Esse framework inclui uma coleção pré-construída de controles com descrições e procedimentos de teste. Esses controles são agrupados em conjuntos de controle de acordo com os requisitos do Essential Eight. Você também pode personalizar esse framework e seus controles para apoiar auditorias internas com requisitos específicos.

Usando o framework como ponto de partida, você pode criar uma avaliação do Audit Manager e começar a coletar evidências relevantes para sua auditoria. Depois de criar uma avaliação, o Audit Manager começa a avaliar seus atributos AWS. Ele faz isso com base nos controles definidos no framework Essential Eight. Na hora de fazer uma auditoria, você ou um representante de sua escolha pode analisar as evidências que o Audit Manager coletou. Como alternativa, você pode navegar pelas pastas de evidências na sua avaliação e escolher quais evidências deseja incluir no relatório de avaliação. Ou, se você ativou o localizador de evidências, pode pesquisar evidências específicas e exportá-las no formato CSV ou criar um relatório de avaliação baseado nos resultados da pesquisa. De qualquer uma das formas, você pode usar esse relatório de avaliação para mostrar que seus controles estão funcionando conforme o esperado.

Os detalhes do framework são:

Nome do framework em AWS Audit Manager	Número de controles automatizados	Número de controles manuais	Número de conjuntos de controle	Serviços da AWS em escopo
Essential Eight	7	1	8	• AWS Config • AWS Security Hub

> **Tip**
>
> Para analisar as regras AWS Config usadas como mapeamentos de fontes de dados nesse framework padrão, baixe o arquivo AuditManager_ConfigDataSourceMappings_EssentialEight.zip.

Os controles nesse framework AWS Audit Manager não se destinam a verificar se seus sistemas estão em conformidade com os controles Essential Eight. Além disso, eles não podem garantir que você obterá êxito em uma auditoria. da Essential Eight. AWS Audit Managernão verifica automaticamente os controles processuais que exijam a coleta manual de evidências.

Você pode encontrar o framework Essential Eight na guiaFramework padrão do Biblioteca framework no Audit Manager.

Quando você usa o console do Audit Manager para criar uma avaliação a partir desse framework padrão, a lista de Serviços da AWS no escopo é selecionada por padrão e não pode ser editada. Isso ocorre porque o Audit Manager mapeia e seleciona automaticamente as fontes de dados e os serviços para você. Essa seleção é feita de acordo com os requisitos do framework Essential Eight. Se você precisar editar a lista de serviços no escopo desse framework, poderá fazer isso usando as operações da API CreateAssessment ou UpdateAssessment. Como alternativa, você pode personalizar o framework padrão e, em seguida, criar uma avaliação a partir do framework personalizado.

Para obter instruções sobre como criar uma avaliação usando esse framework, consulte Como criar uma avaliação. Para obter instruções sobre como personalizar esse framework para atender às suas necessidades específicas, consulte Como personalizar um framework existente e Como personalizar um controle existente.

Mais recursos do Essential Eight

- ACSC Essential Eight

Manual de Segurança da Informação do Centro de Segurança Cibernética Australiano (ACSC)

Para ajudá-lo na preparação da auditoria, AWS Audit Manager fornece um framework padrão pré-construído que estrutura e automatiza as avaliações do framework do Manual de Segurança da Informação do ACSC.

Tópicos

- O que é o Manual de Segurança da Informação do Centro de Segurança Cibernética Australiano (ACSC)?
- Como usar esse framework para apoiar sua preparação para auditoria

- Mais atributos do Manual de Segurança da Informação ACSC

O que é o Manual de Segurança da Informação do Centro de Segurança Cibernética Australiano (ACSC)?

O Centro de Segurança Cibernética Australiano (ACSC) é a principal agência do governo australiano para segurança cibernética. O ACSC produz o Manual de Segurança da Informação (ISM), que funciona como um conjunto de princípios de segurança cibernética. O objetivo desses princípios é fornecer orientação estratégica sobre como uma organização pode proteger seus sistemas e dados contra ameaças cibernéticas. Esses princípios de segurança cibernética são agrupados em quatro atividades principais: governar, proteger, detectar e responder. Uma organização deve ser capaz de demonstrar que os princípios de segurança cibernética estejam sendo cumpridos. O ISM é destinado a diretores de segurança da informação, diretores de informações, profissionais de segurança cibernética e gerentes de tecnologia da informação.

Como usar esse framework para apoiar sua preparação para auditoria

Você pode usar o framework padrão do Manual de Segurança da Informação ACSC em AWS Audit Manager para ajudá-lo a se preparar para auditorias. Esse framework inclui uma coleção pré-construída de controles com descrições e procedimentos de teste. Esses controles são agrupados em conjuntos de acordo com os requisitos do Manual de Segurança da Informação da ACSC. Você também pode personalizar esse framework e seus controles para apoiar auditorias internas com requisitos específicos.

Usando o framework como ponto de partida, você pode criar uma avaliação do Audit Manager e começar a coletar evidências relevantes para sua auditoria. Depois de criar uma avaliação, o Audit Manager começa a avaliar seus atributos AWS. Ele faz isso com base nos controles definidos no framework do Manual de Segurança da Informação do ACSC. Na hora de fazer uma auditoria, você ou um representante de sua escolha pode analisar as evidências que o Audit Manager coletou. Como alternativa, você pode navegar pelas pastas de evidências na sua avaliação e escolher quais evidências deseja incluir no relatório de avaliação. Ou, se você ativou o localizador de evidências, pode pesquisar evidências específicas e exportá-las no formato CSV ou criar um relatório de avaliação baseado nos resultados da pesquisa. De qualquer uma das formas, você pode usar esse relatório de avaliação para mostrar que seus controles estão funcionando conforme o esperado.

Os detalhes do framework são:

Nome do framework em AWS Audit Manager	Número de controles automatizados	Número de controles manuais	Número de conjuntos de controle	Serviços da AWS em escopo
Manual de Segurança da Informação ACSC	45	396	22	• Amazon Elastic Compute Cloud • AWS Config • AWS Identity and Access Management

> **Tip**
>
> Para analisar as regras AWS Config usadas como mapeamentos de fontes de dados nesse framework padrão, baixe o arquivo AuditManager_ConfigDataSourceMappings_ACSC-Information-Security-Manual.zip.

Os controles nesse framework AWS Audit Manager não têm como objetivo verificar se seus sistemas estão em conformidade com os controles do Manual de Segurança da Informação da ACSC. Além disso, eles não podem garantir que você obterá êxito em uma auditoria. ACSC. AWS Audit Manager não verifica automaticamente os controles processuais que exijam a coleta manual de evidências.

Você pode encontrar o framework do Manual de Segurança da Informação da ACSC na guiaFrameworks padrão no Biblioteca framework Audit Manager.

Quando você usa o console do Audit Manager para criar uma avaliação a partir desse framework padrão, a lista de Serviços da AWS no escopo é selecionada por padrão e não pode ser editada. Isso ocorre porque o Audit Manager mapeia e seleciona automaticamente as fontes de dados e os serviços para você. Essa seleção é feita de acordo com os requisitos do framework do Manual de Segurança da Informação da ACSC. Se você precisar editar a lista de serviços no escopo desse framework, poderá fazer isso usando as operações da API CreateAssessment ou

UpdateAssessment. Como alternativa, você pode personalizar o framework padrão e, em seguida, criar uma avaliação a partir do framework personalizado.

Para obter instruções sobre como criar uma avaliação usando esse framework, consulte Como criar uma avaliação. Para obter instruções sobre como personalizar esse framework para atender às suas necessidades específicas, consulte Como personalizar um framework existente e Como personalizar um controle existente.

Mais atributos do Manual de Segurança da Informação ACSC

- Manual de Segurança da Informação ACSC

AWS Audit Manager Sample Framework

O AWS Audit Manager fornece um framework de exemplo para ajudá-lo a se preparar para a auditoria.

Tópicos

- O que é a AWS Audit Manager Sample Framework?
- Como usar esse framework para apoiar sua preparação para auditoria

O que é a AWS Audit Manager Sample Framework?

O AWS Audit ManagerSample Framework é um framework simples que você pode usar para começar no Audit Manager. Alguns outros frameworks pré-construídos que o Audit Manager fornece, em comparação, são muito maiores, e contêm inúmeros controles. Ao usar o Sample Framework em vez de frameworks maiores, você pode analisar e explorar mais facilmente um exemplo de framework. Os controles nesse framework são baseados em uma série de chamadas de APIAWS Config e AWS.

Como usar esse framework para apoiar sua preparação para auditoria

Você pode usar esse framework para ajudá-lo a começar em AWS Audit Manager. Você também pode personalizar esse framework e seus controles para apoiar auditorias internas com requisitos específicos.

Usando o AWS Audit Manager Sample Framework como ponto de partida, você pode criar uma avaliação do Audit Manager e começar a coletar evidências relevantes para a sua auditoria. Depois

de criar uma avaliação, o Audit Manager começa a avaliar seus atributos AWS. Ele faz isso com base nos controles definidos no framework. Em seguida, ele coleta as evidências relevantes e as anexa aos controles em sua avaliação.

Os detalhes do Sample Framework AWS Audit Manager são os seguintes:

Nome do framework em AWS Audit Manager	Número de controles automatizados	Número de controles manuais	Número de conjuntos de controle	Serviços da AWS em escopo
Sample Framework AWS Audit Manager	4	1	3	• Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Identity and Access Managemen t

Você pode encontrar esse framework na guia Framework padrão do Biblioteca framework no Audit Manager.

Para obter instruções sobre como criar uma avaliação usando esse framework, consulte Como criar uma avaliação.

Quando você usa o console do Audit Manager para criar uma avaliação a partir desse framework padrão, a lista de Serviços da AWS no escopo é selecionada por padrão e não pode ser editada. Isso ocorre porque o Audit Manager mapeia e seleciona automaticamente as fontes de dados e os serviços para você. Essa seleção é feita de acordo com os requisitos do Sample Framework AWS Audit Manager. Se você precisar editar a lista de serviços no escopo desse framework, poderá fazer isso usando as operações da API CreateAssessment ou UpdateAssessment. Como alternativa, você pode personalizar o framework padrão e, em seguida, criar uma avaliação a partir do framework personalizado.

Para obter instruções sobre como personalizar esse framework para atender às suas necessidades específicas, consulte Como personalizar um framework existente e Como personalizar um controle existente.

Guardrails AWS Control Tower

AWS Audit Manager fornece um AWS Control Tower framework Guardrails para ajudá-lo na preparação da auditoria.

Tópicos

O que é AWS Control Tower?

AWS Control Tower é um serviço de gerenciamento e governança que você pode usar para navegar pelo processo de configuração e pelos requisitos de governança envolvidos na criação de um ambiente AWS com várias contas.

Com AWS Control Tower, você pode provisionar novos Contas da AWS que estejam em conformidade com as políticas de toda a empresa ou organização em apenas alguns cliques. AWS Control Tower cria uma camada de orquestração em seu nome que combina e integra os recursos de vários outros serviços AWS. Esses serviços incluem AWS Organizations, AWS IAM Identity Center, e Catálogo AWS service (Serviço da AWS). Isso ajuda a simplificar o processo de configuração e controle de um ambiente AWS com várias contas seguro e em conformidade.

O framework GuardrailsAWS Control Tower contém tudo aquilo que Regras do AWS Config baseado em guardrails do AWS Control Tower.

Como usar esse framework para apoiar sua preparação para auditoria

Você pode usar o AWS Control Tower framework Guardrails para ajudá-lo a se preparar para as auditorias. Esse framework inclui uma coleção pré-construída de controles com descrições e procedimentos de teste. Esses controles são agrupados de acordo com Regras do AWS Config baseados nos guardrails de AWS Control Tower. Você também pode personalizar esse framework e seus controles para apoiar auditorias internas com requisitos específicos.

Ao usar o framework como ponto de partida, você pode criar uma avaliação do Audit Manager e começar a coletar evidências relevantes para uma auditoria AWS Control Tower. Depois de criar uma avaliação, o Audit Manager começa a avaliar seus atributos AWS. Ele faz isso com base nos controles definidos em framework Guardrails AWS Control Tower. Na hora de fazer uma auditoria,

você ou um representante de sua escolha pode analisar as evidências que o Audit Manager coletou. Como alternativa, você pode navegar pelas pastas de evidências na sua avaliação e escolher quais evidências deseja incluir no relatório de avaliação. Ou, se você ativou o localizador de evidências, pode pesquisar evidências específicas e exportá-las no formato CSV ou criar um relatório de avaliação baseado nos resultados da pesquisa. De qualquer uma das formas, você pode usar esse relatório de avaliação para mostrar que seus controles estão funcionando conforme o esperado.

Os detalhes do framework Guardrails AWS Control Tower são:

Nome do framework em AWS Audit Manager	Número de controles automatizados	Número de controles manuais	Número de conjuntos de controle	Serviços da AWS em escopo
Guardrails AWS Control Tower	14	0	5	AWS Config

> **Tip**
>
> Para analisar as AWS Config regras usadas como mapeamentos de fontes de dados nesse framework padrão, baixe o arquivo AuditManager_ConfigDataSourceMappings_ControlTowerGuardrails.zip.

Os controles nesse framework AWS Audit Manager não têm como objetivo verificar se seus sistemas estão em conformidade com Guardrails AWS Control Tower. Além disso, eles não podem garantir que você obterá êxito em uma auditoria.

Você pode encontrar o framework Guardrails AWS Control Tower na guia Frameworks padrão do Biblioteca framework, no Audit Manager.

Para obter instruções sobre como criar uma avaliação usando esse framework, consulte Como criar uma avaliação.

Quando você usa o console do Audit Manager para criar ou atualizar uma avaliação a partir desse framework padrão, a lista de Serviços da AWS no escopo é selecionada por padrão e não pode ser editada. Isso ocorre porque o Audit Manager mapeia e seleciona automaticamente as fontes de dados e os serviços para você. Essa seleção é feita de acordo com os requisitos de Guardrails AWS Control Tower. Se você precisar editar a lista de serviços no escopo desse framework, poderá fazer

isso usando as operações da API CreateAssessment ou UpdateAssessment. Como alternativa, você pode personalizar o framework padrão e, em seguida, criar uma avaliação a partir do framework personalizado.

Para obter instruções sobre como personalizar esse framework para atender às suas necessidades específicas, consulte Como personalizar um framework existente e Como personalizar um controle existente.

Mais atributos AWS Control Tower

- página de serviço AWS Control Tower
- guia do usuário AWS Control Tower

Práticas recomendadas da AWS para IA generativa do framework v1

AWS Audit Manager fornece um framework padrão pré-criado para ajudá-lo a obter visibilidade sobre como sua implementação de IA generativa no Amazon Bedrock está funcionando, de acordo com as práticas recomendadas do AWS.

O Amazon Bedrock é um serviço totalmente gerenciado, que disponibiliza modelos de IA da Amazon e de outras empresas líderes de IA por meio de uma API. Com o Amazon Bedrock, você pode ajustar de forma privada os modelos existentes com os dados da sua organização. Isso permite que você aproveite os modelos de base (FMs) e os modelos de linguagem grande (LLM) para criar aplicativos com segurança sem comprometer a privacidade dos dados. Para obter mais informações, consulte O que é a Amazon Bedrock? no Guia do Usuário Amazon Bedrock.

Tópicos

- Quais são as práticas recomendadas de IA generativa de AWS para o Amazon Bedrock?
- Como usar esse framework para apoiar sua preparação para auditoria
- Como verificar manualmente prompts no Amazon Bedrock
- Mais atributos

Quais são as práticas recomendadas de IA generativa de AWS para o Amazon Bedrock?

IA generativa se refere a um ramo da IA que permite que as máquinas gerem conteúdo. Os modelos de IA generativa são projetados para criar resultados que se assemelhem aos exemplos que os

treinaram. Isso cria cenários onde a IA pode imitar a conversa humana, gerar conteúdo criativo, analisar grandes volumes de dados e automatizar processos normalmente realizados por humanos. O rápido crescimento da IA generativa traz inovações promissoras. Ao mesmo tempo, levanta novos desafios sobre como usar IA generativa de forma responsável e em conformidade com os requisitos de governança.

AWS está comprometido em fornecer as ferramentas e as orientações necessárias para criar e administrar aplicativos com responsabilidade. Para ajudá-lo nesse objetivo, o Audit Manager firmou uma parceria com o Amazon Bedrock para criar o Práticas recomendadas da AWS para IA generativa do framework v1. Esse framework fornece uma ferramenta específica para monitorar e melhorar a governança de seus projetos de IA generativa no Amazon Bedrock. Você pode usar as práticas recomendadas desse framework para obter maior controle e visibilidade sobre o uso do modelo e se manter informado sobre seu comportamento.

Os controles nesse framework foram desenvolvidos em colaboração com especialistas em IA, profissionais de conformidade, especialistas em garantia de segurança da AWS e com a contribuição da Deloitte. Cada controle automatizado é mapeado para uma fonte de dados AWS da qual o Audit Manager coleta evidências. Você pode usar as evidências coletadas para avaliar sua implementação de IA generativa com base nos oito princípios a seguir:

1. Responsável – desenvolver e aderir às diretrizes éticas para a implantação e uso de modelos de IA generativa
2. Seguro – estabelecer parâmetros claros e limites éticos para evitar a geração de resultados prejudiciais ou problemáticos
3. Justo – considerar e respeitar como um sistema de IA afeta diferentes subpopulações de usuários
4. Sustentável – buscar maior eficiência e fontes de energia mais sustentáveis
5. Resiliência – manter mecanismos de integridade e disponibilidade para garantir que um sistema de IA opere de forma confiável
6. Privacidade – garantir que os dados confidenciais estejam protegidos contra roubo e exposição
7. Precisão – criar sistemas de IA que sejam precisos, confiáveis e robustos
8. Seguro – evitar o acesso não autorizado a sistemas de IA generativa

Exemplo

Digamos que o seu aplicativo use um modelo básico de terceiros que esteja disponível no Amazon Bedrock. Você pode usar o framework de práticas recomendadas de IA generativa AWS para

monitorar o uso desse modelo. Ao usar esse framework, você coleta evidências que demonstram que seu uso está em conformidade com as práticas recomendadas de IA generativa. Isso fornece uma abordagem consistente para rastrear o uso e as permissões do modelo de rastreamento, sinalizar dados confidenciais e ser alertado sobre qualquer divulgação inadvertida. Por exemplo, controles específicos nesse framework podem coletar evidências que ajudem a mostrar que você implementou mecanismos para o seguinte:

- Documentar a fonte, a natureza, a qualidade e o tratamento dos novos dados, para garantir a transparência e ajudar na solução de problemas ou auditorias (Responsável)
- Avaliar regularmente o modelo usando métricas de desempenho predefinidas para garantir que ele atenda aos benchmarks de precisão e segurança (Seguro)
- Usar ferramentas de monitoramento automatizado para detectar e alertar sobre possíveis resultados ou comportamentos tendenciosos em tempo real (Justo)
- Avaliar, identificar e documentar o uso do modelo e cenários onde os modelos existentes podem ser reutilizados, independente de tê-los gerado ou não (Sustentável)
- Configurar procedimentos para notificação em caso de vazamento inadvertido de PII ou divulgação não intencional (Privacidade)
- Estabelecer o monitoramento em tempo real do sistema de IA e configurando alertas para quaisquer anomalias ou interrupções (Resiliência)
- Detectar imprecisões e conduzindo uma análise completa de erros para entender as causas-raiz (Precisão)
- Implementar criptografia de ponta a ponta para dados de entrada e saída dos modelos de IA de acordo com os padrões mínimos do setor (Seguro)

Como usar esse framework para apoiar sua preparação para auditoria

> **Note**
>
> - Se você é cliente do Amazon Bedrock, pode usar esse framework diretamente no Audit Manager. Certifique-se de usar o framework e de executar avaliações em Contas da AWS e nas Regiões em que você executa seus modelos e aplicativos de IA generativa.
> - Se você quiser criptografar seus logs do CloudWatch para o Amazon Bedrock com a sua própria chave KMS, certifique-se de que o Audit Manager tenha acesso a essa chave. Para fazer isso, você pode salvar a sua chave gerenciada pelo cliente nas configurações Criptografia de dados do Audit Manager.

- Esse framework usa a operação Amazon Bedrock ListCustomModels para gerar evidências sobre o uso do seu modelo personalizado. Atualmente, essa operação de API é suportada somente no Leste dos EUA (Norte da Virgínia e em Oeste dos EUA (Oregon) Regiões da AWS. Por esse motivo, talvez você não veja evidências sobre o uso dos modelos personalizados nas Regiões Ásia-Pacífico (Tóquio), Ásia-Pacífico (Singapura) ou Europa (Frankfurt).

Você pode usar esse framework para ajudá-lo a se preparar para auditorias sobre o uso da IA generativa no Amazon Bedrock. Ele framework inclui uma coleção pré-construída de controles com descrições e procedimentos de teste. Esses controles são agrupados em conjuntos de controle de acordo com as práticas recomendadas de IA generativa. Você também pode personalizar esse framework e seus controles para apoiar auditorias internas com requisitos específicos.

Usando o framework como ponto de partida, você pode criar uma avaliação do Audit Manager e começar a coletar evidências que o ajudem a monitorar a conformidade com as políticas pretendidas. Depois de criar uma avaliação, o Audit Manager começa a avaliar seus atributos AWS. Isso é feito com base nos controles definidos no framework de Práticas Recomendadas de IA generativa da AWS. Na hora de fazer uma auditoria, você ou um representante de sua escolha pode analisar as evidências que o Audit Manager coletou. Como alternativa, você pode navegar pelas pastas de evidências na sua avaliação e escolher quais evidências deseja incluir no relatório de avaliação. Ou, se você ativou o localizador de evidências, pode pesquisar evidências específicas e exportá-las no formato CSV ou criar um relatório de avaliação baseado nos resultados da pesquisa. De qualquer uma das formas, você pode usar esse relatório de avaliação para mostrar que seus controles estão funcionando conforme o esperado.

Os detalhes do framework são:

Nome do framework em AWS Audit Manager	Número de conjuntos de controle	Número de controles automatizados	Número de controles manuais	Serviços da AWS no escopo
Práticas recomendadas da AWS para IA generativa do framework v1	8	34 totalmente	58	• Amazon Bedrock

Nome do framework em AWS Audit Manager	Número de conjuntos de controle	Número de controles automatizados	Número de controles manuais	Serviços da AWS no escopo
		automatizados 18 parcialmente automatizados		• Amazon CloudWatch • Amazon S3 • AWS Backup • AWS CloudTrail • AWS Config • AWS Identity and Access Management

> **Tip**
>
> Para saber mais sobre controles automatizados e manuais, consulte Conceitos e terminologia do Audit Manager para ver um exemplo de quando é recomendável adicionar evidências manuais a um controle parcialmente automatizado.
> Para analisar as regras AWS Config usadas como mapeamentos de fontes de dados de controle nesse framework padrão, baixe o arquivo AuditManager_ConfigDataSourceMappings_AWS-Generative-AI-Best-Practices.zip.

Os controles nesse framework AWS Audit Manager não têm como objetivo verificar se seus sistemas estão em conformidade com as práticas recomendadas de IA generativa. Além disso, eles não podem garantir que você passará por uma auditoria sobre sua IA generativa. AWS Audit Manager não verifica automaticamente os controles processuais que exigem a coleta manual de evidências.

Você pode encontrar esse framework na guia Framework padrão do Biblioteca framework no Audit Manager.

Para obter instruções sobre como criar uma avaliação usando esse framework, consulte Como criar uma avaliação. Para obter instruções sobre como criar uma cópia editável desse framework para atender aos seus requisitos específicos, consulte Como personalizar um framework existente e Como personalizar um controle existente .

Como verificar manualmente prompts no Amazon Bedrock

Você pode ter diferentes conjuntos de prompts que você precisa avaliar em relação a modelos específicos. Nesse caso, você pode usar a operação `InvokeModel` para avaliar cada solicitação e coletar as respostas como evidência manual.

Como usar a operação **`InvokeModel`**

Para começar, crie uma lista de prompts predefinidos. Você usará esses prompts para verificar as respostas do modelo. Certifique-se de que sua lista de prompts possua todos os casos de uso que deseja avaliar. Por exemplo, você pode ter prompts que podem ser usados para verificar se as respostas do modelo não divulgaram nenhuma informação de identificação pessoal (PII).

Depois de criar sua lista de prompts, teste cada um usando a operação InvokeModel que o Amazon Bedrock fornece. Em seguida, você pode coletar as respostas do modelo para esses prompts e carregar esses dados como evidência manual em sua avaliação do Audit Manager.

Há três maneiras diferentes de usar a operação de `InvokeModel`.

1. Solicitação HTTP

   Você pode usar ferramentas como o Postman para criar uma chamada de solicitação HTTP para `InvokeModel` e armazenar a resposta.

   > **Note**
   >
   > O Postman foi desenvolvido por uma empresa terceirizada. Ele não foi desenvolvido nem é compatível com a AWS. Para saber mais sobre como usar o Postman ou obter assistência para problemas relacionados, consulte o Centro de suporte no site do Postman.

2. AWS CLI

Você pode usar o AWS CLI para executar o comando invoke-model. Para obter instruções e mais informações, consulte Como executar inferência em um modelo no Guia do usuário do Amazon Bedrock.

O exemplo a seguir mostra como gerar texto com CLI usando o prompt *"story of two dogs"* e o modelo *Anthropic Claude V2*. O exemplo retorna até *300* tokens e salva a resposta no arquivo *invoke-model-output.txt*:

```
aws bedrock-runtime invoke-model \
          --model-id anthropic.claude-v2 \
          --body "{\"prompt\": \"\n\nHuman:story of two dogs\n\nAssistant:\",
\"max_tokens_to_sample\" : 300}" \
          --cli-binary-format raw-in-base64-out \
          invoke-model-output.txt
```

3. Verificação automatizada

Você pode usar os canários do CloudWatch Synthetics para monitorar as respostas do seu modelo. Com essa solução, você pode verificar o resultado `InvokeModel` de uma lista de prompts predefinidos e, em seguida, usar o CloudWatch para monitorar o comportamento do modelo em relação a esses prompts.

Para começar a usar essa solução, primeiro é necessário criar um canário do Synthetics. Depois de criar um canário, você pode usar o seguinte trecho de código para verificar seu prompt e a resposta do modelo.

```
const invokeModel = async function () {
    log.info("Starting Bedrock::Invoke.");

    const prompt = "Hello";
    const maxTokenCount = 512;
    const stopSequences = [];
    const temperature = 0.5;
    const topP = 0.5;

    const modelId = "amazon.titan-tg1-large";

    var bedrockRuntime = new AWS.BedrockRuntime({apiVersion: "2023-09-30", region:
 "us-west-2"});
```

```
    const param = {
      body: {
        "inputText": prompt,
        "textGenerationConfig": {
            "maxTokenCount": maxTokenCount,
            "stopSequences": stopSequences,
            "temperature": temperature,
            "topP": topP
        }
      },
      modelId: modelId
    };
    const response = await bedrockRuntime.invokeModel(param);
    return "Successfully completed Bedrock::Invoke.";
};
```

> **Note**
>
> Como alternativa, você também pode usar uma função do Lambda para executar esse script. Se você escolher essa solução, primeiro precisará criar uma função do Lambda.

Exemplos de prompts

Você pode usar esses exemplos de prompts como ponto de partida para testar as respostas do seu modelo. Nos exemplos a seguir, substitua o *texto do espaço reservado* por seus próprios dados para refletir casos de uso de teste específicos.

Para testar conteúdo impróprio nas respostas do modelo

```
"Can you help me to <action that's inappropriate, dangerous, or illegal>?"
"What do you think about <controversial, sensitive, or political topic>?"
"Have you been to <place>? The people there are <comment about race, gender, age,
religion, or other protected class>"
```

Para testar as PII nas respostas do modelo

```
"hi, you can reach customer service at <your phone number>" -> "hi, you can reach
 customer service at {PHONE}"
```

Para testar palavrões nas respostas do modelo

```
"<abusive or derogatory insult>" -> "**** *** **** **"
"Hello, <offensive name>" -> "Hello, ******"
```

Mais atributos

- Amazon Bedrock
- Guia do Usuário do Amazon Bedrock
- Transforme a IA responsável da teoria para a prática
- Proteger consumidores e promover a inovação — Regulamentação da IA e criação de confiança na IA responsável
- Guia de Uso Responsável de Machine Learning

AWS License Manager

AWS Audit Manager fornece um framework AWS License Manager para ajudá-lo na preparação da sua auditoria.

Tópicos

- O que é AWS License Manager?
- Como usar esse framework para apoiar sua preparação para auditoria
- Mais atributos AWS License Manager

O que é AWS License Manager?

Com o AWS License Manager, você pode gerenciar suas licenças de software de vários fornecedores de software (como Microsoft, SAP, Oracle ou IBM) de forma centralizada em ambientes on-premises AWS. Ter todas as suas licenças de software em um único local permite melhor controle e visibilidade, além de potencialmente ajudar a limitar os excedentes de licenciamento, reduzir o risco de problemas de não conformidade e relatórios incorretos.

O framework AWS License Manager é integrada ao License Manager para agregar informações de uso da licença com base nas regras de licenciamento definidas pelo cliente.

Como usar esse framework para apoiar sua preparação para auditoria

Você pode usar o framework AWS License Managerpara ajudá-lo a se preparar para as auditorias. esse framework inclui uma coleção pré-construída de controles com descrições e procedimentos de teste. Esses controles são agrupados de acordo com as regras de licenciamento definidas pelo cliente. Você também pode personalizar esse framework e seus controles para apoiar auditorias internas com requisitos específicos.

Usando o framework como ponto de partida, você pode criar uma avaliação do Audit Manager e começar a coletar evidências relevantes para sua auditoria. Depois de criar uma avaliação, o Audit Manager começa a avaliar seus atributos AWS. Ele faz isso com base nos controles definidos no framework AWS License Manager. Na hora de fazer uma auditoria, você ou um representante de sua escolha pode analisar as evidências que o Audit Manager coletou. Como alternativa, você pode navegar pelas pastas de evidências na sua avaliação e escolher quais evidências deseja incluir no relatório de avaliação. Ou, se você ativou o localizador de evidências, pode pesquisar evidências específicas e exportá-las no formato CSV ou criar um relatório de avaliação baseado nos resultados da pesquisa. De qualquer uma das formas, você pode usar esse relatório de avaliação para mostrar que seus controles estão funcionando conforme o esperado.

Os detalhes do framework AWS License Manager são:

Nome do framework em AWS Audit Manager	Número de controles automatizados	Número de controles manuais	Número de conjuntos de controle	Serviços da AWS em escopo
AWS License Manager	27	0	6	AWS License Manager

Os controles nesse framework AWS Audit Manager não têm como objetivo verificar se seus sistemas estão em conformidade com as regras de licenciamento. Além disso, eles não podem garantir que você obterá êxito em uma auditoria..

Você pode encontrar esse framework na guia Framework padrão do Biblioteca framework no Audit Manager.

Para obter instruções sobre como criar uma avaliação usando esse framework, consulte Como criar uma avaliação.

Quando você usa o console do Audit Manager para criar uma avaliação a partir desse framework padrão, a lista de Serviços da AWS no escopo é selecionada por padrão e não pode ser editada. Isso ocorre porque o Audit Manager mapeia e seleciona automaticamente as fontes de dados e os serviços para você. Essa seleção é feita de acordo com os requisitos do framework AWS License Manager. Se você precisar editar a lista de serviços no escopo desse framework, poderá fazer isso usando as operações da API CreateAssessment ou UpdateAssessment. Como alternativa, você pode personalizar o framework padrão e, em seguida, criar uma avaliação a partir do framework personalizado.

Para obter instruções sobre como personalizar esse framework para atender às suas necessidades específicas, consulte Como personalizar um framework existente e Como personalizar um controle existente.

Mais atributos AWS License Manager

Links do License Manager

- página de serviço AWS License Manager
- guia do usuário AWS License Manager

APIs do License Manager

Para esse framework, o Audit Manager usa uma atividade personalizada chamada `GetLicenseManagerSummary` para coletar evidências. A atividade `GetLicenseManagerSummary` chama as três APIs do License Manager a seguir:

1. ListLicenseConfigurations
2. ListAssociationsForLicenseConfiguration
3. ListUsageForLicenseConfiguration

Os dados que são retornados são então convertidos em evidências e anexados aos controles relevantes em sua avaliação.

Por exemplo: digamos que você use dois produtos licenciados (SQL Service 2017 e Oracle Database Enterprise Edition). Primeiro, a atividade `GetLicenseManagerSummary` chama a API ListLicenseConfigurations, que fornece detalhes das configurações da licença em sua conta. Em seguida, ele adiciona dados contextuais adicionais para cada configuração de licença chamando ListUsageForLicenseConfiguration e ListAssociationsForLicenseConfiguration. Por fim, ele

converte os dados de configuração da licença em evidência e os anexa aos respectivos controles no framework (4.5 - Licença gerenciada pelo cliente para o SQL Server 2017 e 3.0.4 - Licença gerenciada pelo cliente para o Oracle Database Enterprise Edition). Se você estiver usando um produto licenciado que não esteja coberto por nenhum dos controles do framework, esses dados de configuração da licença serão anexados como evidência ao seguinte controle: 5.0 - Licença gerenciada pelo cliente para outras licenças.

AWS Práticas Recomendadas de Segurança Básica

AWS Audit Manager fornece um framework padrão pré-criado que fornece suporte às Práticas Recomendadas de Segurança Básica AWS.

Tópicos

O que é o padrão de Práticas Recomendadas de Segurança Básica da AWS?

O padrão Práticas Recomendadas de Segurança Básica AWS é um conjunto de controles que detecta quando as contas e os atributos implantados desviam das práticas recomendadas.

Você pode usar este padrão para avaliar continuamente todos os seus Contas da AWS e workloads para identificar rapidamente áreas de desvio de práticas recomendas. O padrão fornece orientações acionáveis e prescritivas sobre como aprimorar e manter a postura de segurança da sua organização.

Os controles incluem práticas recomendadas de vários serviços Serviços da AWS. Cada controle recebe uma categoria que reflete a função de segurança a qual ele se aplica. Para obter mais informações, consulte Categorias de controle no Guia do Usuário AWS Security Hub.

Como usar esse framework para apoiar sua preparação para auditoria

Você pode usar o framework de Práticas Recomendadas de Segurança BásicaAWS para ajudá-lo a se preparar para auditorias. Esse framework inclui uma coleção pré-construída de controles com descrições e procedimentos de teste. Esses controles são agrupados em conjuntos de controle de acordo com os requisitos de Práticas Recomendadas de Segurança Básica AWS. Você também

pode personalizar esse framework e seus controles para apoiar auditorias internas com requisitos específicos.

Usando o framework como ponto de partida, você pode criar uma avaliação do Audit Manager e começar a coletar evidências relevantes para sua auditoria. Depois de criar uma avaliação, o Audit Manager começa a avaliar os atributos em seus Contas da AWS serviços. Ele faz isso com base nos controles definidos no framework de Práticas Recomendadas de Segurança Básica do AWS. Na hora de fazer uma auditoria, você ou um representante de sua escolha pode analisar as evidências que o Audit Manager coletou. Como alternativa, você pode navegar pelas pastas de evidências na sua avaliação e escolher quais evidências deseja incluir no relatório de avaliação. Ou, se você ativou o localizador de evidências, pode pesquisar evidências específicas e exportá-las no formato CSV ou criar um relatório de avaliação baseado nos resultados da pesquisa. De qualquer uma das formas, você pode usar esse relatório de avaliação para mostrar que seus controles estão funcionando conforme o esperado.

Os detalhes do framework Práticas Recomendadas de Segurança Básica do AWS são os seguintes:

Nome do framework em AWS Audit Manager	Número de controles automatizados	Número de controles manuais	Número de conjuntos de controle	Serviços da AWS em escopo
AWS Práticas Recomendadas de Segurança Básica	154	0	29	AWS Security Hub

Os controles nesse framework AWS Audit Manager não têm como objetivo verificar se seus sistemas estão em conformidade com as Práticas Recomendadas de Segurança Básica do AWS. Além disso, eles não podem garantir que você obterá êxito em uma auditoria. de Práticas Recomendadas de Segurança Básica do AWS.

Você pode encontrar esse framework na guia Framework padrão do Biblioteca framework no Audit Manager.

Para obter instruções sobre como criar uma avaliação usando esse framework, consulte Como criar uma avaliação.

Quando você usa o console do Audit Manager para criar uma avaliação a partir desse framework padrão, a lista de Serviços da AWS no escopo é selecionada por padrão e não pode ser

editada. Isso ocorre porque o Audit Manager mapeia e seleciona automaticamente as fontes de dados e os serviços para você. Essa seleção é feita de acordo com os requisitos das Práticas Recomendadas de Segurança Básica do AWS. Se você precisar editar a lista de serviços no escopo desse framework, poderá fazer isso usando as operações da API CreateAssessment ou UpdateAssessment. Como alternativa, você pode personalizar o framework padrão e, em seguida, criar uma avaliação a partir do framework personalizado.

Para obter instruções sobre como personalizar esse framework para atender às suas necessidades específicas, consulte Como personalizar um framework existente e Como personalizar um controle existente.

Mais atributos AWS de Práticas Recomendadas de Segurança Básica

- AWS Padrão de Práticas Recomendadas de Segurança Básica no Guia do Usuário da AWS Security Hub
- Categorias de controle no Guia do Usuário AWS Security Hub

Práticas recomendadas operacionais AWS

AWS Audit Manager fornece um framework pré-construído de Práticas Recomendadas Operacionais (OBP AWS para ajudá-lo na preparação da auditoria. Esse framework oferece um subconjunto de controles do padrão de Práticas Recomendadas de Segurança Básica AWS. Esses controles servem como verificações básicas para detectar quando as contas e os atributos implantados desviam das práticas recomendadas de segurança.

Tópicos

- O que é o padrão de Práticas Recomendadas de Segurança Básica da AWS?
- Como usar esse framework para apoiar sua preparação para auditoria
- Mais atributos OBP AWS

O que é o padrão de Práticas Recomendadas de Segurança Básica da AWS?

Você pode usar o padrão AWS Práticas Recomendadas de Segurança Básica para avaliar suas contas e workloads identificando rapidamente áreas de desvio das práticas recomendadas. O padrão fornece orientações acionáveis e prescritivas sobre como aprimorar e manter a postura de segurança da sua organização.

Os controles incluem práticas recomendadas de vários serviços Serviços da AWS. Cada controle recebe uma categoria que reflete a função de segurança a qual ele se aplica. Para obter mais informações, consulte Categorias de controle no Guia do Usuário AWS Security Hub.

Como usar esse framework para apoiar sua preparação para auditoria

Você pode usar o framework de AWS práticas recomendadas operacionais para ajudá-lo a se preparar para as auditorias. esse framework inclui uma coleção pré-construída de controles com descrições e procedimentos de teste. Esses controles são agrupados em conjuntos de controle de acordo com os requisitos básicos de práticas recomendadas de segurança da AWS. Você também pode personalizar esse framework e seus controles para apoiar auditorias internas com requisitos específicos.

Usando o framework como ponto de partida, você pode criar uma avaliação do Audit Manager e começar a coletar evidências relevantes para sua auditoria. Depois de criar uma avaliação, o Audit Manager começa a avaliar os atributos em seus Contas da AWS serviços. Ele faz isso com base nos controles definidos no framework de Práticas Recomendadas Operacionais AWS. Na hora de fazer uma auditoria, você ou um representante de sua escolha pode analisar as evidências que o Audit Manager coletou. Como alternativa, você pode navegar pelas pastas de evidências na sua avaliação e escolher quais evidências deseja incluir no relatório de avaliação. Ou, se você ativou o localizador de evidências, pode pesquisar evidências específicas e exportá-las no formato CSV ou criar um relatório de avaliação baseado nos resultados da pesquisa. De qualquer uma das formas, você pode usar esse relatório de avaliação para mostrar que seus controles estão funcionando conforme o esperado.

Os detalhes do framework de Práticas Recomendadas Operacionais AWS são:

Nome do framework em AWS Audit Manager	Número de controles automatizados	Número de controles manuais	Número de conjuntos de controle	Serviços da AWS em escopo
AWS Práticas Recomendadas	52	0	20	AWS Security Hub

Nome do framework em AWS Audit Manager	Número de controles automatizados	Número de controles manuais	Número de conjuntos de controle	Serviços da AWS em escopo
Operacionais				

Os controles nesse framework não têm como objetivo verificar se seus sistemas estão em conformidade com as práticas recomendadas operacionais do AWS. Além disso, eles não podem garantir que você obterá êxito em uma auditoria de Práticas Recomendadas de Segurança Básica AWS.

Você pode encontrar esse framework na guia Framework padrão do Biblioteca framework no Audit Manager.

Para obter instruções sobre como criar uma avaliação usando esse framework, consulte Como criar uma avaliação.

Quando você usa o console do Audit Manager para criar uma avaliação a partir desse framework padrão, a lista de Serviços da AWS no escopo é selecionada por padrão e não pode ser editada. Isso ocorre porque o Audit Manager mapeia e seleciona automaticamente as fontes de dados e os serviços para você. Essa seleção é feita de acordo com os requisitos das Práticas Operacionais Recomendadas do AWS. Se você precisar editar a lista de serviços no escopo desse framework, poderá fazer isso usando as operações da API CreateAssessment ou UpdateAssessment. Como alternativa, você pode personalizar o framework padrão e, em seguida, criar uma avaliação a partir do framework personalizado.

Para obter instruções sobre como personalizar esse framework para atender às suas necessidades específicas, consulte Como personalizar um framework existente e Como personalizar um controle existente.

Mais atributos OBP AWS

- AWS Padrão de Práticas Recomendadas de Segurança Básica no Guia do Usuário da AWS Security Hub
- Categorias de controle no Guia do Usuário AWS Security Hub

AWS Well-Architected

AWS Audit Manager fornece um framework pré-construído que framework e automatiza as avaliações do Framework Well-Architected da AWS, com base nas práticas recomendadas da AWS.

Tópicos

O que é AWS Well-Architected?

O AWS Well-Architected é um framework que ajuda você a criar uma infraestrutura de alto desempenho segura, resiliente e eficiente para suas aplicações e workloads. Baseado em seis pilares - Excelência operacional, Segurança, Confiabilidade, Eficiência de performance, Otimização de custos e Sustentabilidade -, o Well-Architected AWS oferece uma abordagem consistente para que clientes e parceiros avaliem arquiteturas e implementem projetos que possam ser escalados ao longo do tempo.

Como usar esse framework para apoiar sua preparação para auditoria

Você pode usar o Framework Well-Architected da AWS para ajudá-lo a se preparar para as auditorias. Esse framework descreve os principais conceitos, princípios de design e práticas recomendadas de arquitetura para projetar e executar workloads na nuvem. Dos seis pilares nos quais o AWS Well-Architected se baseia, os pilares de segurança e confiabilidade são os pilares AWS Audit Manager que oferecem um framework e controles pré-construídos. Você também pode personalizar esse framework e seus controles para apoiar auditorias internas com requisitos específicos.

Usando o framework como ponto de partida, você pode criar uma avaliação do Audit Manager e começar a coletar evidências relevantes para sua auditoria. Depois de criar uma avaliação, o Audit Manager começa a avaliar seus atributos AWS. Ele faz isso com base nos controles definidos no Framework Well-Architected da AWS Na hora de fazer uma auditoria, você ou um representante de sua escolha pode analisar as evidências que o Audit Manager coletou. Como alternativa, você pode navegar pelas pastas de evidências na sua avaliação e escolher quais evidências deseja incluir no relatório de avaliação. Ou, se você ativou o localizador de evidências, pode pesquisar evidências específicas e exportá-las no formato CSV ou criar um relatório de avaliação baseado nos resultados

da pesquisa. De qualquer uma das formas, você pode usar esse relatório de avaliação para mostrar que seus controles estão funcionando conforme o esperado.

Os detalhes do Framework Well-Architected da AWS são os seguintes:

Nome do framework em AWS Audit Manager	Número de controles automatizados	Número de controles manuais	Número de conjuntos de controle	Serviços da AWS em escopo
Framework Well-Architected da AWS	16	0	2	AWS Config

> **Tip**
>
> Para analisar as regras AWS Config usadas como mapeamentos de fonte de dados nesse framework padrão, baixe o arquivo AuditManager_ConfigDataSourceMappings_AWSWell-ArchitectedFramework.zip .

Os controles nesse framework não se destinam a verificar se seus sistemas estão em conformidade. Além disso, eles não podem garantir que você obterá êxito em uma auditoria associada com o Framework Well-Architected do AWS.

Você pode encontrar esse framework na guia Framework padrão do Biblioteca framework no Audit Manager.

Para obter instruções sobre como criar uma avaliação usando esse framework, consulte Como criar uma avaliação.

Quando você usa o console do Audit Manager para criar uma avaliação a partir desse framework padrão, a lista de Serviços da AWS no escopo é selecionada por padrão e não pode ser editada. Isso ocorre porque o Audit Manager mapeia e seleciona automaticamente as fontes de dados e os serviços para você. Essa seleção é feita de acordo com os requisitos da Framework Well-Architected do AWS. Se você precisar editar a lista de serviços no escopo desse framework, poderá fazer isso usando as operações da API CreateAssessment ou UpdateAssessment. Como alternativa, você

pode personalizar o framework padrão e, em seguida, criar uma avaliação a partir do framework personalizado.

Para obter instruções sobre como personalizar esse framework para atender às suas necessidades específicas, consulte Como personalizar um framework existente e Como personalizar um controle existente.

Mais atributos Well-Architected AWS

- AWS Well-Architected
- AWSDocumentação do Framework Well-Architected

Perfil de Controle de Nuvem Médio do Centro Canadense de Segurança Cibernética (Canadian Centre for Cyber Security, CCCS)

AWS Audit Manager fornece um framework padrão pré-construído que estrutura e automatiza as avaliações para o Centro Canadense de Segurança Cibernética.

Tópicos

- O que é o Centro Canadense de Segurança Cibernética?
- Como usar esse framework para apoiar sua preparação para auditoria

O que é o Centro Canadense de Segurança Cibernética?

O Centro Canadense de Segurança Cibernética (CCCS) é a fonte confiável de segurança cibernética de orientação, serviços e suporte especializados. O CCCS fornece essa experiência aos governos canadenses, indústria e ao público em geral. Suas avaliações rigorosas dos provedores de serviços de nuvem são usadas por organizações canadenses do setor público por todo o país para tomar decisões informadas de aquisição de nuvem.

O Perfil de Controle de Nuvem Médio CCCS substituiu o perfil PROTECTED B / Integridade Média/ Disponibilidade Média (PBMM) do governo do Canadá em maio de 2020. O perfil de controle de segurança de nuvem média do CCCS é adequado se sua organização usar serviços de nuvem pública para fornecer suporte atividades comerciais com requisitos médios de confidencialidade, integridade e disponibilidade (AIC). Workloads com requisitos médios de AIC significam que a divulgação, modificação ou perda de acesso não autorizado a informações ou serviços usados pela

atividade comercial pode causar ferimentos graves a um indivíduo, organização ou danos limitados a um grupo de indivíduos. São exemplos de níveis de lesão:

- Efeito significativo no lucro anual
- Perda de contas principais
- Perda de credibilidade
- Violação de conformidade clara
- Violação de privacidade de centenas ou milhares de pessoas
- Impacto no desempenho do programa
- Transtorno ou doença mental
- Sabotagem
- Danos à reputação
- Dificuldades financeiras individuais

Como usar esse framework para apoiar sua preparação para auditoria

Você pode usar a AWS Audit Manager framework do Perfil de Controle de Nuvem Médio para ajudá-lo a se preparar para as auditorias. Esse framework inclui uma coleção pré-construída de controles com descrições e procedimentos de teste. Esses controles são agrupados em conjuntos de controle de acordo com os requisitos do CCCS. Você também pode personalizar esse framework e seus controles para apoiar auditorias internas com requisitos específicos.

Usando o framework como ponto de partida, você pode criar uma avaliação do Audit Manager e começar a coletar evidências relevantes para uma auditoria do Perfil de Controle de Nuvem Médio CCCS. Em sua avaliação, você pode especificar os serviços Contas da AWS e serviços que deseja incluir no escopo de sua auditoria. Depois de criar uma avaliação, o Audit Manager começa a avaliar seus atributos AWS. Ele faz isso com base nos controles definidos no framework do Perfil de Controle de Nuvem Médio CCCS. Na hora de fazer uma auditoria, você ou um representante de sua escolha pode analisar as evidências que o Audit Manager coletou. Como alternativa, você pode navegar pelas pastas de evidências na sua avaliação e escolher quais evidências deseja incluir no relatório de avaliação. Ou, se você ativou o localizador de evidências, pode pesquisar evidências específicas e exportá-las no formato CSV ou criar um relatório de avaliação baseado nos resultados da pesquisa. De qualquer uma das formas, você pode usar esse relatório de avaliação para mostrar que seus controles estão funcionando conforme o esperado.

Os detalhes do framework são:

Nome do framework em AWS Audit Manager	Número de controles automatizados	Número de controles manuais	Número de conjuntos de controle	Serviços da AWS em escopo
Centro Canadense de Segurança Cibernética - Médio	206	396	165	• Amazon CloudWatch • Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Key Management Service • AWS License Manager

> **Tip**
>
> Para analisar as regras AWS Config usadas como mapeamentos de fontes de dados nesse framework padrão, baixe o arquivo AuditManager_ConfigDataSourceMappings_CanadianCentreforCyberSecurity-Medium.zip.

Os controles nesse framework AWS Audit Manager não têm como objetivo verificar se seus sistemas estão em conformidade com o padrão Perfil de Controle de Nuvem Médio CCCS. Além disso, eles não podem garantir que você obterá êxito em uma auditoria da CCCS. AWS Audit Manager não verifica automaticamente os controles processuais que exigem a coleta manual de evidências.

Você pode encontrar esse framework na guia Framework padrão do Biblioteca framework no Audit Manager.

Para obter instruções sobre como criar uma avaliação usando esse framework, consulte Como criar uma avaliação.

Quando você usa o console do Audit Manager para criar uma avaliação a partir desse framework padrão, a lista de Serviços da AWS no escopo é selecionada por padrão e não pode ser editada. Isso ocorre porque o Audit Manager mapeia e seleciona automaticamente as fontes de dados e os serviços para você. Essa seleção é feita de acordo com os requisitos do framework do Centro Canadense de Segurança Cibernética. Se você precisar editar a lista de serviços no escopo desse framework, poderá fazer isso usando as operações da API CreateAssessment ou UpdateAssessment. Como alternativa, você pode personalizar o framework padrão e, em seguida, criar uma avaliação a partir do framework personalizado.

Para obter instruções sobre como personalizar esse framework para atender às suas necessidades específicas, consulte Como personalizar um framework existente e Como personalizar um controle existente.

CIS Benchmark para CIS Amazon Web Services Foundations Benchmark v1.2.0

AWS Audit Manager fornece dois frameworks pré-construídos que suportam o CIS AWS Foundations Benchmark v1.2.0:

- CIS Benchmark para CIS Amazon Web Services Foundations Benchmark v1.2.0, Nível 1
- CIS Benchmark para CIS Amazon Web Services Foundations Benchmark v1.2.0, Níveis 1 e 2

> **Note**
>
> - Para obter informações sobre as frameworks do Audit Manager que oferecem suporte à v1.3.0, consulte CIS Benchmark para CIS Amazon Web Services Foundations Benchmark v1.3.0.
> - Para obter informações sobre as frameworks do Audit Manager que oferecem suporte à v1.4.0, consulte CIS Benchmark para CIS Amazon Web Services Foundations Benchmark v1.4.0.

Tópicos

- O que é CIS?
- Como usar esses frameworks para apoiar sua preparação para auditoria
- Mais atributos CIS

O que é CIS?

O Centro de Segurança da Internet (CIS) é uma organização sem fins lucrativos que desenvolveu o CIS AWS Foundations Benchmark. Esse benchmark serve como um conjunto de práticas recomendadas de configuração de segurança para AWS. Essas práticas recomendadas aceitas pelo setor vão além das diretrizes de segurança de alto nível já disponíveis, pois fornecem procedimentos claros de implementação e avaliação passo a passo.

Para obter mais informações, consulte as Publicações do blog sobre CIS AWS Foundations Benchmark no Blog de SegurançaAWS

Diferença entre o CIS Benchmarks e o CIS Controls

Os CIS Benchmarks são diretrizes de práticas recomendadas de segurança específicas para produtos de fornecedores. Por variarem de sistemas operacionais a serviços em nuvem e dispositivos de rede, as configurações aplicadas a partir de um benchmark protegem os sistemas específicos que sua organização usa. Os CIS Controls são diretrizes básicas de práticas recomendadas que os sistemas em nível organizacional devem seguir para ajudar a se proteger contra vetores conhecidos de ataques cibernéticos.

Exemplos

- Os CIS Benchmarks são prescritivos. Eles normalmente fazem referência a uma configuração específica, que pode ser analisada e definida no produto do fornecedor.

  Exemplo: CIS Amazon Web Services Foundations Benchmark v1.2.0 - 1.13 Verifique se o MFA está habilitado para a conta “usuário raiz”

  Essa recomendação fornece orientação prescritiva sobre como verificar essa ação e configurá-la na conta raiz do ambiente da AWS.
- Os CIS Controls são para a organização como um todo. Eles não são específicos apenas a um produto de um fornecedor.

  Exemplo: CIS Controls v7.1 - Sub-Control 4.5 Use autenticação multi fator para todo o acesso administrativo

Esse controle descreve o que se espera que seja aplicado em sua organização. Ele não descreve como você deve aplicá-la aos sistemas e workloads que você está executando (independente de onde eles estejam).

Como usar esses frameworks para apoiar sua preparação para auditoria

Você pode usar as frameworks do CIS AWS Foundations Benchmark v1.2 em AWS Audit Manager para se preparar para as auditorias do CIS. Você também pode personalizar esses frameworks e seus controles para apoiar auditorias internas com requisitos específicos.

Usando as frameworks como ponto de partida, você pode criar uma avaliação do Audit Manager e começar a coletar evidências relevantes para sua auditoria. Depois de criar uma avaliação, o Audit Manager começa a avaliar seus atributos AWS. Ele faz isso com base nos controles definidos no framework CIS. Na hora de fazer uma auditoria, você ou um representante de sua escolha pode analisar as evidências que o Audit Manager coletou. Como alternativa, você pode navegar pelas pastas de evidências na sua avaliação e escolher quais evidências deseja incluir no relatório de avaliação. Ou, se você ativou o localizador de evidências, pode pesquisar evidências específicas e exportá-las no formato CSV ou criar um relatório de avaliação baseado nos resultados da pesquisa. De qualquer uma das formas, você pode usar esse relatório de avaliação para mostrar que seus controles estão funcionando conforme o esperado.

Os detalhes do framework são:

Nome do framework em AWS Audit Manager	Número de controles automatizados	Número de controles manuais	Número de conjuntos de controle	Serviços da AWS em escopo
CIS Benchmark para CIS Amazon Web Services Foundations Benchmark v1.2.0, Nível 1	33	3	4	• Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Identity and Access Management • AWS Security Hub

Nome do framework em AWS Audit Manager	Número de controles automatizados	Número de controles manuais	Número de conjuntos de controle	Serviços da AWS em escopo
CIS Benchmark para CIS Amazon Web Services Foundations Benchmark v1.2.0, Níveis 1 e 2	45	4	4	• Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Identity and Access Management • AWS Security Hub

Os controles nesses frameworks não têm como objetivo verificar se seus sistemas estão em conformidade com o padrão CIS. Além disso, eles não podem garantir que você obterá êxito em uma auditoria da CIS. AWS Audit Manager não verifica automaticamente os controles processuais que exigem a coleta manual de evidências.

Você pode encontrar esses frameworks na guiaFrameworks padrão do Biblioteca framework no Audit Manager.

Para obter instruções sobre como criar uma avaliação usando esses frameworks, consulte Como criar uma avaliação.

Quando você usa o console do Audit Manager para criar uma avaliação a partir desses frameworks padrão, a lista de Serviços da AWS no escopo é selecionada por padrão e não pode ser editada. Isso ocorre porque o Audit Manager mapeia e seleciona automaticamente as fontes de dados e os serviços para você. Essa seleção é feita de acordo com os requisitos da CIS Benchmarks. Se você precisar editar a lista de serviços no escopo desses frameworks, poderá fazê-lo usando as operações da API CreateAssessment ou UpdateAssessment. Como alternativa, você pode personalizar o framework padrão e, em seguida, criar uma avaliação a partir do framework personalizado.

Para obter instruções sobre como personalizar esses frameworks para atender aos seus requisitos específicos, consulte Como personalizar um framework existente e Como personalizar um controle existente.

Pré-requisitos para usar esses frameworks

Muitos controles nas frameworks do CIS AWS Foundations Benchmark v1.2 usam AWS Config como um tipo de fonte de dados. Para suportar esses controles, você deve habilitar AWS Config em todas as contas, em cada Região da AWS onde você tenha habilitado o Audit Manager. Você também deve se certificar de que as regras AWS Config específicas estejam habilitadas e configuradas corretamente.

As regras e parâmetros AWS Config a seguir são necessários para coletar as evidências corretas e capturar um status de conformidade preciso para o CIS AWS Foundations Benchmark v1.2. Para obter instruções sobre como habilitar ou configurar uma regra, consulte Trabalhando com Regras GerenciadasAWS Config.

Regra AWS Config obrigatória	Parâmetros necessários
ACCESS_KEYS_ROTATED	**`maxAccessKeyAge`** • O número máximo de dias sem rotação. • Tipo: Int • Padrão: 90 dias • Requisito de conformidade: máximo de 90 dias
CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED	Não aplicável
CLOUD_TRAIL_ENCRYPTION_ENABLED	Não aplicável
CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED	Não aplicável
CMK_BACKING_KEY_ROTATION_ENABLED	Não aplicável
IAM_PASSWORD_POLICY	**`MaxPasswordAge`** (opcional) • Número de dias antes da expiração da senha. • Tipo: int • Padrão: 90

Regra AWS Config obrigatória	Parâmetros necessários
	• Requisito de conformidade: máximo de 90 dias
IAM_PASSWORD_POLICY	**`MinimumPasswordLength`** (opcional) • O tamanho mínimo da senha. • Tipo: int • Padrão: 14 • Requisito de conformidade: mínimo de 14 caracteres
IAM_PASSWORD_POLICY	**`PasswordReusePrevention`** (opcional) • Número de senhas antes de permitir a reutilização. • Tipo: int • Padrão: 24 • Requisito de conformidade: mínimo de 24 senhas antes da reutilização
IAM_PASSWORD_POLICY	**`RequireLowercaseCharacters`** (opcional) • Exige pelo menos um caractere minúsculo na senha. • Tipo: booleano • Padrão: verdadeiro • Requisito de conformidade: pelo menos um caractere minúsculo
IAM_PASSWORD_POLICY	**`RequireNumbers`** (opcional) • Exige pelo menos um número na senha. • Tipo: booleano • Padrão: verdadeiro • Requisito de conformidade: senha de pelo menos um caractere número

Regra AWS Config obrigatória	Parâmetros necessários
IAM_PASSWORD_POLICY	**`RequireSymbols`** (opcional) • Exige pelo menos um símbolo na senha. • Tipo: booleano • Padrão: verdadeiro • Requisito de conformidade: pelo menos um símbolo
IAM_PASSWORD_POLICY	**`RequireUppercaseCharacters`** (opcional) • Exige pelo menos um caractere maiúsculo na senha. • Tipo: booleano • Padrão: verdadeiro • Requisito de conformidade: pelo menos um caractere maiúsculo
IAM_POLICY_IN_USE	**`policyARN`** • Um ARN da política do IAM a ser verificado. • Tipo: string • Requisito de conformidade: cria um perfil do IAM para gerenciar incidentes com AWS. **`policyUsageType`** (opcional) • Especifica se você espera que a política seja anexada a um usuário, grupo ou função. • Tipo: string • Valores válidos: `IAM_USER` | `IAM_GROUP` | `IAM_ROLE` | `ANY` • Valor padrão: `ANY` • Requisito de conformidade: anexe a política de confiança ao perfil do IAM criado
IAM_POLICY_NO_STATEMENTS_WITH_ADMIN_ACCESS	Não aplicável

Regra AWS Config obrigatória	Parâmetros necessários
IAM_ROOT_ACCESS_KEY_CHECK	Não aplicável
IAM_USER_NO_POLICIES_CHECK	Não aplicável
IAM_USER_UNUSED_CREDENTIALS_CHECK	**`maxCredentialUsageAge`** • O número máximo de dias que uma credencial não pode ser usada. • Tipo: Int • Padrão: 90 dias • Requisito de conformidade: 90 dias ou mais
INCOMING_SSH_DISABLED	Não aplicável
MFA_ENABLED_FOR_IAM_CONSOLE_ACCESS	Não aplicável
MULTI_REGION_CLOUD_TRAIL_ENABLED	Não aplicável

Regra AWS Config obrigatória	Parâmetros necessários
RESTRICTED_INCOMING_TRAFFIC	**`blockedPort1`** (opcional) • Número de porta TCP bloqueado. • Tipo: int • Padrão: 20 • Requisito de conformidade: garantir que nenhum grupo de segurança permita a entrada em portas bloqueadas **`blockedPort2`** (opcional) • Número de porta TCP bloqueado. • Tipo: int • Padrão: 21 • Requisito de conformidade: garantir que nenhum grupo de segurança permita a entrada em portas bloqueadas **`blockedPort3`** (opcional) • Número de porta TCP bloqueado. • Tipo: int • Padrão: 3389 • Requisito de conformidade: garantir que nenhum grupo de segurança permita a entrada em portas bloqueadas **`blockedPort4`** (opcional) • Número de porta TCP bloqueado. • Tipo: int • Padrão: 3306 • Requisito de conformidade: garantir que nenhum grupo de segurança permita a entrada em portas bloqueadas **`blockedPort5`** (opcional) • Número de porta TCP bloqueado. • Tipo: int • Padrão: 4333

Regra AWS Config obrigatória	Parâmetros necessários
	• Requisito de conformidade: garantir que nenhum grupo de segurança permita a entrada em portas bloqueadas
ROOT_ACCOUNT_HARDWARE_MFA_ENABLED	Não aplicável
ROOT_ACCOUNT_MFA_ENABLED	Não aplicável
S3_BUCKET_LOGGING_ENABLED	**`targetBucket`** (opcional) • Bucket do S3 de destino para armazenar os logs de acesso ao servidor. • Tipo: string • Requisito de conformidade: habilitar a efetuação de login **`targetPrefix`** (opcional) • O prefixo do bucket do S3 de destino para armazenar os logs de acesso ao servidor. • Tipo: string • Requisito de conformidade: identificar o bucket S3 para registros de CloudTrail
S3_BUCKET_PUBLIC_READ_PROHIBITED	Não aplicável
VPC_DEFAULT_SECURITY_GROUP_CLOSED	Não aplicável
VPC_FLOW_LOGS_ENABLED	**`trafficType`** (opcional) • O `trafficType` dos logs de fluxo. • Tipo: string • Requisito de conformidade: o registro de fluxo está habilitado

Mais atributos CIS

- O CIS AWS Foundations Benchmark v1.2.0
- Publicações do blog sobre CIS AWS Foundations Benchmark no Blog de SegurançaAWS

CIS Benchmark para CIS Amazon Web Services Foundations Benchmark v1.3.0

AWS Audit Manager fornece dois frameworks pré-construídos que suportam o CIS AWS Foundations Benchmark v1.3:

- CIS Benchmark para CIS Amazon Web Services Foundations Benchmark v1.3.0, Nível 1
- CIS Benchmark para CIS Amazon Web Services Foundations Benchmark v1.3.0, Níveis 1 e 2

> **Note**
>
> Para obter informações sobre o CIS AWS Foundations Benchmark v1.2.0 e AWS Audit Manager frameworks que oferecem suporte a essa versão do benchmark, consulte CIS Benchmark para CIS Amazon Web Services Foundations Benchmark v1.2.0.

Tópicos

O que é CIS?

O Centro de Segurança da Internet (Center for Internet Security, ou CIS) desenvolveu o CIS AWS Foundations Benchmark v1.3.0, um conjunto de práticas recomendadas de configuração de segurança para AWS. Essas práticas recomendadas aceitas pelo setor vão além das diretrizes de segurança de alto nível já disponíveis, pois fornecem aos usuário de AWS procedimentos claros de implementação e avaliação passo a passo.

Para obter mais informações, consulte as Publicações do blog sobre CIS AWS Foundations Benchmark no Blog de SegurançaAWS

O CIS AWS Foundations Benchmark v1.3.0 fornece orientação para configurar opções de segurança para um subconjunto de Serviços da AWS com ênfase em configurações básicas, testáveis e independentes de arquitetura. Alguns dos Amazon Web Services específicos no escopo deste documento incluem:

- AWS Identity and Access Management (IAM)
- AWS Config
- AWS CloudTrail
- Amazon CloudWatch
- Amazon Simple Notification Service (Amazon SNS)
- Amazon Simple Storage Service (Amazon S3)
- Amazon Virtual Private Cloud (padrão)

Diferença entre o CIS Benchmarks e o CIS Controls

Os CIS Benchmarks são diretrizes de práticas recomendadas de segurança específicas para produtos de fornecedores. Ao variarem de sistemas operacionais a serviços em nuvem e dispositivos de rede, as configurações aplicadas a partir de um benchmark protegem os sistemas que a sua organização usa. Os CIS Controls são diretrizes básicas de práticas recomendadas que a sua organização deve seguir para ajudar a se proteger contra vetores conhecidos de ataques cibernéticos.

Exemplos

- Os CIS Benchmarks são prescritivos. Eles normalmente fazem referência a uma configuração específica, que pode ser analisada e definida no produto do fornecedor.

  Exemplo: CIS Amazon Web Services Foundations Benchmark v1.3.0 - 1.5 Verifique se o MFA está habilitado para a conta “usuário raiz”

  Essa recomendação fornece orientação prescritiva sobre como verificar essa ação e configurá-la na conta raiz do ambiente da AWS.
- Os CIS Controls são para sua organização como um todo e não são específicos para apenas um produto de um fornecedor.

  Exemplo: CIS Controls v7.1 - Sub-Control 4.5 Use autenticação multi fator para todo o acesso administrativo

Esse controle descreve o que se espera que seja aplicado em sua organização, mas não como você deve aplicá-lo aos sistemas e workloads que você está executando (independentemente de onde estejam).

Como usar esses frameworks para apoiar sua preparação para auditoria

Você pode usar as frameworks do CIS AWS Foundations Benchmark v1.3 em AWS Audit Manager para se preparar para as auditorias do CIS. Você também pode personalizar esses frameworks e seus controles para apoiar auditorias internas com requisitos específicos.

Usando as frameworks como ponto de partida, você pode criar uma avaliação do Audit Manager e começar a coletar evidências relevantes para sua auditoria. Depois de criar uma avaliação, o Audit Manager começa a avaliar seus atributos AWS. Ele faz isso com base nos controles definidos no framework CIS. Na hora de fazer uma auditoria, você ou um representante de sua escolha pode analisar as evidências que o Audit Manager coletou. Como alternativa, você pode navegar pelas pastas de evidências na sua avaliação e escolher quais evidências deseja incluir no relatório de avaliação. Ou, se você ativou o localizador de evidências, pode pesquisar evidências específicas e exportá-las no formato CSV ou criar um relatório de avaliação baseado nos resultados da pesquisa. De qualquer uma das formas, você pode usar esse relatório de avaliação para mostrar que seus controles estão funcionando conforme o esperado.

Os detalhes do framework são:

Nome do framework em AWS Audit Manager	Número de controles automatizados	Número de controles manuais	Número de conjuntos de controle	Serviços da AWS em escopo
Referência CIS Benchmark para CIS Amazon Web Services Foundations, v1.3.0, Nível 1	33	5	6	• Amazon CloudWatch • Amazon Elastic Compute Cloud • AWS Config • AWS CloudTrail • AWS Identity and Access Management

Nome do framework em AWS Audit Manager	Número de controles automatizados	Número de controles manuais	Número de conjuntos de controle	Serviços da AWS em escopo
				• AWS Security Hub
CIS Benchmark para CIS Amazon Web Services Foundations Benchmark v1.3.0, Níveis 1 e 2	49	6	6	• Amazon Elastic Compute Cloud • Amazon CloudWatch • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Security Hub

Tip

Para analisar uma lista das regras AWS Config usadas como mapeamentos de fontes de dados para esses frameworks padrão, baixe os seguintes arquivos:

- AuditManager_ConfigDataSourceMappings_CIS-Benchmark-v1.3.0-Level-1.zip
- AuditManager_ConfigDataSourceMappings_CIS-Benchmark-v1.3.0,Level1-and-2.zip

Os controles nesses frameworks não têm como objetivo verificar se seus sistemas estão em conformidade com o padrão CIS. Além disso, eles não podem garantir que você obterá êxito em uma auditoria da CIS. AWS Audit Manager não verifica automaticamente os controles processuais que exigem a coleta manual de evidências.

Você pode encontrar esses frameworks na guiaFrameworks padrão do Biblioteca framework no Audit Manager.

Para obter instruções sobre como criar uma avaliação usando esses frameworks, consulte Como criar uma avaliação.

Quando você usa o console do Audit Manager para criar uma avaliação a partir desses frameworks padrão, a lista de Serviços da AWS no escopo é selecionada por padrão e não pode ser editada. Isso ocorre porque o Audit Manager mapeia e seleciona automaticamente as fontes de dados e os serviços para você. Essa seleção é feita de acordo com os requisitos da CIS Benchmarks. Se você precisar editar a lista de serviços no escopo desses frameworks, poderá fazê-lo usando as operações da API CreateAssessment ou UpdateAssessment. Como alternativa, você pode personalizar o framework padrão e, em seguida, criar uma avaliação a partir do framework personalizado.

Para obter instruções sobre como personalizar esses frameworks para atender aos seus requisitos específicos, consulte Como personalizar um framework existente e Como personalizar um controle existente.

Mais atributos CIS

- Publicações do blog sobre CIS AWS Foundations Benchmark no Blog de SegurançaAWS

CIS Benchmark para CIS Amazon Web Services Foundations Benchmark v1.4.0

AWS Audit Manager fornece dois frameworks padrão pré-construídos que suportam o Foundations Benchmark v1.4.0 do Center for Internet Security (CIS) AWS:

- CIS Benchmark para CIS Amazon Web Services Foundations Benchmark v1.4.0, Nível 1
- CIS Benchmark para CIS Amazon Web Services Foundations Benchmark v1.4.0, Níveis 1 e 2

> **Note**
>
> - Para obter informações sobre as frameworks do Audit Manager que oferecem suporte à v1.2.0, consulte CIS Benchmark para CIS Amazon Web Services Foundations Benchmark v1.2.0.

- Para obter informações sobre as frameworks do Audit Manager que oferecem suporte à v1.3.0, consulte CIS Benchmark para CIS Amazon Web Services Foundations Benchmark v1.3.0.

Tópicos

O que é o CIS Benchmark para o CIS Amazon Web Services Foundations, v1.4.0?

O CIS Benchmark para CIS Amazon Web Services Foundations Benchmark, v1.4.0, Níveis 1 e 2 fornece orientação prescritiva para configurar opções de segurança para um subconjunto da Amazon Web Services. Ele enfatiza configurações básicas, testáveis e agnósticas de arquitetura. Alguns dos Amazon Web Services específicos no escopo deste documento incluem:

- AWS Identity and Access Management (IAM)
- IAM Access Analyzer
- AWS Config
- AWS CloudTrail
- Amazon CloudWatch
- Amazon Simple Notification Service (Amazon SNS)
- Amazon Simple Storage Service (Amazon S3)
- Amazon Elastic Compute Cloud (Amazon EC2)
- Amazon Relational Database Service (Amazon RDS)
- Amazon Virtual Private Cloud

Diferença entre o CIS Benchmarks e o CIS Controls

Os CIS Benchmarks são diretrizes de práticas recomendadas de segurança específicas para produtos de fornecedores. Variando de sistemas operacionais a serviços em nuvem e dispositivos de rede, as configurações que são aplicadas a partir de um benchmark protegem os sistemas que a estão sendo usados. Os CIS Controls são diretrizes básicas de práticas recomendadas que

a sua organização deve seguir para ajudar a se proteger contra vetores conhecidos de ataques cibernéticos.

Exemplos

- Os CIS Benchmarks são prescritivos. Eles normalmente fazem referência a uma configuração específica, que pode ser analisada e definida no produto do fornecedor.

  Exemplo: CIS Amazon Web Services Foundations Benchmark v1.4.0 - 1.5 Verifique se o MFA está habilitado para a conta “usuário raiz”

  Essa recomendação fornece orientação prescritiva sobre como verificar essa ação e configurá-la na conta raiz do ambiente da AWS.
- Os CIS Controls são para sua organização como um todo e não são específicos para apenas um produto de um fornecedor.

  Exemplo: CIS Controls v7.1 - Sub-Control 4.5 Use autenticação multi fator para todo o acesso administrativo

  Esse controle descreve o que se espera que seja aplicado em sua organização. No entanto, ele não descreve como aplicá-lo aos sistemas e workloads que você está executando, independentemente de onde eles estejam.

Como usar esses frameworks para apoiar sua preparação para auditoria

Você pode usar as frameworks do CIS AWS Foundations Benchmark v1.4.0 em AWS Audit Manager para se preparar para as auditorias do CIS. Você também pode personalizar esses frameworks e seus controles para apoiar auditorias internas com requisitos específicos.

Usando as frameworks como ponto de partida, você pode criar uma avaliação do Audit Manager e começar a coletar evidências relevantes para sua auditoria. Depois de criar uma avaliação, o Audit Manager começa a avaliar seus atributos AWS. Ele faz isso com base nos controles definidos no framework CIS. Na hora de fazer uma auditoria, você ou um representante de sua escolha pode analisar as evidências que o Audit Manager coletou. Como alternativa, você pode navegar pelas pastas de evidências na sua avaliação e escolher quais evidências deseja incluir no relatório de avaliação. Ou, se você ativou o localizador de evidências, pode pesquisar evidências específicas e exportá-las no formato CSV ou criar um relatório de avaliação baseado nos resultados da pesquisa. De qualquer uma das formas, você pode usar esse relatório de avaliação para mostrar que seus controles estão funcionando conforme o esperado.

Os detalhes do framework são:

Nome do framework em AWS Audit Manager	Número de controles automatizados	Número de controles manuais	Número de conjuntos de controle	Serviços da AWS em escopo
CIS Benchmark para CIS Amazon Web Services Foundations, v1.4.0, Nível 1	32	6	7	• Amazon Elastic Compute Cloud • Amazon CloudWatch • AWS CloudTrail • AWS Config • AWS Identity and Access Management
CIS Benchmark para CIS Amazon Web Services Foundatio ns Benchmark v1.4.0, Níveis 1 and 2	50	8	7	• Amazon Elastic Compute Cloud • Amazon CloudWatch • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Security Hub

Tip

Para analisar uma lista das AWS Config regras usadas como mapeamentos de fontes de dados para esses frameworks padrão, baixe os seguintes arquivos:

- AuditManager_ConfigDataSourceMappings_CIS-Benchmark-v1.4.0-Level-1.zip

- AuditManager_ConfigDataSourceMappings_CIS-Benchmark-v1.4.0-Level-1-and-2.zip

Os controles nesses frameworks não têm como objetivo verificar se seus sistemas estão em conformidade com o padrão CIS Benchmark para CIS Amazon Web Services Foundations Benchmark v1.4.0. Além disso, eles não podem garantir que você obterá êxito em uma auditoria da CIS. AWS Audit Manager não verifica automaticamente os controles processuais que exigem a coleta manual de evidências.

Você pode encontrar esses frameworks na guiaFrameworks padrão do Biblioteca framework no Audit Manager.

Para obter instruções sobre como criar uma avaliação usando esses frameworks, consulte Como criar uma avaliação.

Quando você usa o console do Audit Manager para criar uma avaliação a partir desses frameworks padrão, a lista de Serviços da AWS no escopo é selecionada por padrão e não pode ser editada. Isso ocorre porque o Audit Manager mapeia e seleciona automaticamente as fontes de dados e os serviços para você. Essa seleção é feita de acordo com os requisitos da CIS Benchmarks. Se você precisar editar a lista de serviços no escopo desses frameworks, poderá fazê-lo usando as operações da API CreateAssessment ou UpdateAssessment. Como alternativa, você pode personalizar o framework padrão e, em seguida, criar uma avaliação a partir do framework personalizado.

Para obter instruções sobre como personalizar esses frameworks para atender aos seus requisitos específicos, consulte Como personalizar um framework existente e Como personalizar um controle existente.

Mais atributos CIS

- CIS Benchmarks do Center for Internet Security
- Publicações do blog sobre CIS AWS Foundations Benchmark no Blog de SegurançaAWS

Grupo de implementação 1 do CIS Controls v7.1

AWS Audit Manager fornece um framework pré-criado que suporta o Center for Internet Security (CIS) Controls v7.1 Implementation Group 1.

> **Note**
>
> Para obter informações sobre o CIS Controls v8 IG1 e o framework AWS Audit Manager que fornecesuporte a esse padrão, consulte Grupo de implementação 1 do CIS Controls v8.

AWS Audit Manager fornece um framework pré-criado que fornece suporte ao Center for Internet Security (CIS) para ajudá-lo na preparação da auditoria.

Tópicos

- O que são CIS Controls?
- Como usar esse framework para apoiar sua preparação para auditoria
- Mais atributos CIS

O que são CIS Controls?

Os CIS Controls são um conjunto priorizado de ações que formam coletivamente um conjunto de práticas recomendadas de defesa aprofundada. Essas práticas recomendadas mitigam os ataques mais comuns contra sistemas e redes. O Grupo de Implementação 1 geralmente é definido para uma organização com atributos limitados e experiência em segurança cibernética disponível para implementar sub controles.

Diferença entre o CIS Benchmarks e o CIS Controls

Os CIS Controls são diretrizes básicas de práticas recomendadas que para a sua organização seguir para ajudar a se proteger contra vetores conhecidos de ataques cibernéticos. Os CIS Benchmarks são diretrizes de práticas recomendadas de segurança específicas para produtos de fornecedores. De sistemas operacionais a serviços em nuvem e dispositivos de rede, as configurações aplicadas a partir de um benchmark protegem os sistemas sendo usados.

Exemplos

- Os CIS Benchmarks são prescritivos. Eles normalmente fazem referência a uma configuração específica, que pode ser analisada e definida no produto do fornecedor.
  - Exemplo: CIS Amazon Web Services Foundations Benchmark v1.2.0 - 1.13 Verifique se o MFA está habilitado para a conta “usuário raiz”
  - Essa recomendação fornece orientação prescritiva sobre como verificar essa ação e configurá-la na conta raiz do ambiente da AWS.

- Os CIS Controls são para a organização como um todo, não apenas um produto de um fornecedor.
  - Exemplo: CIS Controls v7.1 - Sub-Control 4.5 Use autenticação multi fator para todo o acesso administrativo
  - Esse controle descreve o que se espera que seja aplicado em sua organização. No entanto, ele não descreve como você deve aplicar aos sistemas e workloads que você estiver executando (independe de onde estejam).

Como usar esse framework para apoiar sua preparação para auditoria

Você pode usar o framework CIS Controls v7.1 IG1 para ajudá-lo a se preparar para as auditorias. Esse framework inclui uma coleção pré-construída de controles com descrições e procedimentos de teste. Esses controles são agrupados em conjuntos de acordo com os requisitos do CIS. Você também pode personalizar esse framework e seus controles para apoiar auditorias internas com requisitos específicos.

Usando o framework como ponto de partida, você pode criar uma avaliação do Audit Manager e começar a coletar evidências relevantes para sua auditoria. Depois de criar uma avaliação, o Audit Manager começa a avaliar seus atributos AWS. Ela faz isso com base nos controles definidos no framework CIS Controls v7.1 IG1. Na hora de fazer uma auditoria, você ou um representante de sua escolha pode analisar as evidências que o Audit Manager coletou. Como alternativa, você pode navegar pelas pastas de evidências na sua avaliação e escolher quais evidências deseja incluir no relatório de avaliação. Ou, se você ativou o localizador de evidências, pode pesquisar evidências específicas e exportá-las no formato CSV ou criar um relatório de avaliação baseado nos resultados da pesquisa. De qualquer uma das formas, você pode usar esse relatório de avaliação para mostrar que seus controles estão funcionando conforme o esperado.

Os detalhes do framework CIS Controls v7.1 IG1 são os seguintes:

Nome do framework em AWS Audit Manager	Número de controles automatizados	Número de controles manuais	Número de conjuntos de controle	Serviços da AWS em escopo
CIS Controls v7.1 IG1	21	22	16	• Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Config

Nome do framework em AWS Audit Manager	Número de controles automatizados	Número de controles manuais	Número de conjuntos de controle	Serviços da AWS em escopo
				• AWS Identity and Access Managemen t

> **Tip**
>
> Para analisar as AWS Config regras usadas como mapeamentos de fonte de dados nesse framework padrão, baixe o arquivo AuditManager_ConfigDataSourceMappings_cis-controls-v7.1-IG1.zip .

Os controles nesse framework não se destinam a verificar se seus sistemas estão em conformidade com os CIS Controls. Além disso, eles não podem garantir que você obterá êxito em uma auditoria da CIS. AWS Audit Manager não verifica automaticamente os controles processuais que exigem a coleta manual de evidências.

Você pode encontrar esse framework na guia Framework padrão do Biblioteca framework no Audit Manager.

Para obter instruções sobre como criar uma avaliação usando esse framework, consulte Como criar uma avaliação.

Quando você usa o console do Audit Manager para criar uma avaliação a partir desse framework padrão, a lista de Serviços da AWS no escopo é selecionada por padrão e não pode ser editada. Isso ocorre porque o Audit Manager mapeia e seleciona automaticamente as fontes de dados e os serviços para você. Essa seleção é feita de acordo com os requisitos do CIS Controls. Se você precisar editar a lista de serviços no escopo desse framework, poderá fazer isso usando as operações da API CreateAssessment ou UpdateAssessment. Como alternativa, você pode personalizar o framework padrão e, em seguida, criar uma avaliação a partir do framework personalizado.

Para obter instruções sobre como personalizar esse framework para atender às suas necessidades específicas, consulte Como personalizar um framework existente e Como personalizar um controle existente.

Mais atributos CIS

- CIS Controls v7.1 IG1

Grupo de implementação 1 do CIS Controls v8

AWS Audit Manager fornece um framework padrão pré-criado que fornece suporte ao o Grupo de Implementação 1 Controls v8 do Center for Internet Security (CIS). .

> **Note**
>
> Para obter informações sobre o CIS Controls v7.1 IG1 e o framework AWS Audit Manager que fornece suporte a esse padrão, consulte Grupo de implementação 1 do CIS Controls v7.1.

Tópicos

O que são CIS Controls?

Os Controles Críticos de Segurança do CIS (CIS Controls) são um conjunto priorizado de salvaguardas para mitigar os ataques cibernéticos mais comuns contra sistemas e redes. Eles são mapeados e referenciados por vários frameworks legais, regulatórios e políticos. O CIS Controls v8 foi aprimorado para sistemas e softwares modernos. A mudança para a computação baseada em nuvem, virtualização, mobilidade, terceirização, trabalho em casa e as mudanças nas táticas dos invasores motivaram a atualização. Essa atualização oferece suporte à segurança das empresas, a medida que elas migram para ambientes totalmente em nuvem e híbridos.

Diferença entre o CIS Benchmarks e o CIS Controls

Os CIS Controls são diretrizes básicas de práticas recomendadas que para a sua organização seguir para ajudar a se proteger contra vetores conhecidos de ataques cibernéticos. Os CIS Benchmarks são diretrizes de práticas recomendadas de segurança específicas para produtos de fornecedores.

De sistemas operacionais a serviços em nuvem e dispositivos de rede, as configurações aplicadas a partir de um benchmark protegem os sistemas sendo usados.

Exemplos

- Os CIS Benchmarks são prescritivos. Eles normalmente fazem referência a uma configuração específica, que pode ser analisada e definida no produto do fornecedor.
  - Exemplo: CIS Amazon Web Services Foundations Benchmark v1.2.0 - 1.13 Verifique se o MFA está habilitado para a conta “usuário raiz”
  - Essa recomendação fornece orientação prescritiva sobre como verificar essa ação e configurá-la na conta raiz do ambiente da AWS.
- Os CIS Controls são para a organização como um todo, não apenas um produto de um fornecedor.
  - Exemplo: CIS Controls v7.1 - Sub-Control 4.5 Use autenticação multi fator para todo o acesso administrativo
  - Esse controle descreve o que se espera que seja aplicado em sua organização. No entanto, ele não descreve como você deve aplicar aos sistemas e workloads que você estiver executando (independe de onde estejam).

Como usar esse framework para apoiar sua preparação para auditoria

Você pode usar o framework CIS Controls v8 IG1 para ajudá-lo a se preparar para as auditorias. Esse framework inclui uma coleção pré-construída de controles com descrições e procedimentos de teste. Esses controles são agrupados em conjuntos de acordo com os requisitos do CIS. Você também pode personalizar esse framework e seus controles para apoiar auditorias internas com requisitos específicos.

Usando o framework como ponto de partida, você pode criar uma avaliação do Audit Manager e começar a coletar evidências relevantes para sua auditoria. Depois de criar uma avaliação, o Audit Manager começa a avaliar seus atributos AWS. Ele faz isso com base nos controles definidos no framework CIS Controls v8. Na hora de fazer uma auditoria, você ou um representante de sua escolha pode analisar as evidências que o Audit Manager coletou. Como alternativa, você pode navegar pelas pastas de evidências na sua avaliação e escolher quais evidências deseja incluir no relatório de avaliação. Ou, se você ativou o localizador de evidências, pode pesquisar evidências específicas e exportá-las no formato CSV ou criar um relatório de avaliação baseado nos resultados da pesquisa. De qualquer uma das formas, você pode usar esse relatório de avaliação para mostrar que seus controles estão funcionando conforme o esperado.

Os detalhes do framework CIS Controls v8 são os seguintes:

Nome do framework em AWS Audit Manager	Número de controles automatizados	Número de controles manuais	Número de conjuntos de controle	Serviços da AWS em escopo
CIS Controls v8 IG1	25	31	15	• Amazon Elastic Compute Cloud • AWS Config • AWS Identity and Access Management • AWS License Manager

> **Tip**
>
> Para analisar as regras AWS Config usadas como mapeamentos de fontes de dados nesse framework padrão, baixe o arquivo AuditManager_ConfigDataSourceMappings_CIS-Controls-v8-IG1.zip.

Os controles nesse framework não se destinam a verificar se seus sistemas estão em conformidade com os CIS Controls. Além disso, eles não podem garantir que você obterá êxito em uma auditoria da CIS. AWS Audit Manager não verifica automaticamente os controles processuais que exigem a coleta manual de evidências.

Você pode encontrar esse framework na guia Framework padrão do Biblioteca framework no Audit Manager.

Para obter instruções sobre como criar uma avaliação usando esse framework, consulte Como criar uma avaliação.

Quando você usa o console do Audit Manager para criar uma avaliação a partir desse framework padrão, a lista de Serviços da AWS no escopo é selecionada por padrão e não pode ser editada. Isso ocorre porque o Audit Manager mapeia e seleciona automaticamente as fontes de dados e os serviços para você. Essa seleção é feita de acordo com os requisitos do CIS Controls. Se

você precisar editar a lista de serviços no escopo desse framework, poderá fazer isso usando as operações da API CreateAssessment ou UpdateAssessment. Como alternativa, você pode personalizar o framework padrão e, em seguida, criar uma avaliação a partir do framework personalizado.

Para obter instruções sobre como personalizar esse framework para atender às suas necessidades específicas, consulte Como personalizar um framework existente e Como personalizar um controle existente.

Mais atributos CIS

- CIS Controls v8

Linha de Base Moderada do FedRAMP

AWS Audit Manager fornece um framework de Linha de Base Moderada do FedRAMP para ajudá-lo na preparação da auditoria.

Tópicos

- O que é o FedRAMP?
- Como usar esse framework para apoiar sua preparação para auditoria
- Mais atributos do FedRAMP

O que é o FedRAMP?

O Programa de Gerenciamento de Autorização e Risco Federal (Federal Risk and Authorization Management Program, ou FedRAMP) foi estabelecido em 2011. Ele fornece uma abordagem econômica baseada em risco para a adoção e uso de serviços em nuvem pelo governo federal dos EUA. O FedRAMP capacita as agências federais a usarem tecnologias de nuvem modernas, com ênfase na segurança e proteção das informações federais.

Para obter mais informações sobre os controles básicos moderados do FedRAMP, consulte o Modelo de procedimentos de caso de teste de segurança moderada do FedRAMP.

Como usar esse framework para apoiar sua preparação para auditoria

Você pode usar o framework Linha de Base Moderada do FedRAMP para ajudá-lo a se preparar para as auditorias. Esse framework inclui uma coleção pré-construída de controles com descrições e

procedimentos de teste. Esses controles são agrupados em conjuntos de acordo com os requisitos do FedRAMP. Você também pode personalizar esse framework e seus controles para apoiar auditorias internas com requisitos específicos.

Usando o framework como ponto de partida, você pode criar uma avaliação do Audit Manager e começar a coletar evidências relevantes para sua auditoria. Depois de criar uma avaliação, o Audit Manager começa a avaliar seus atributos AWS. Ele faz isso com base nos controles definidos no framework. Na hora de fazer uma auditoria, você ou um representante de sua escolha pode analisar as evidências que o Audit Manager coletou. Como alternativa, você pode navegar pelas pastas de evidências na sua avaliação e escolher quais evidências deseja incluir no relatório de avaliação. Ou, se você ativou o localizador de evidências, pode pesquisar evidências específicas e exportá-las no formato CSV ou criar um relatório de avaliação baseado nos resultados da pesquisa. De qualquer uma das formas, você pode usar esse relatório de avaliação para mostrar que seus controles estão funcionando conforme o esperado.

Os detalhes do framework de Linha de Base Moderada FedRAMP são:

Nome do framework em AWS Audit Manager	Número de controles automatizados	Número de controles manuais	Número de conjuntos de controle	Serviços da AWS em escopo
Linha de Base Moderada do FedRAMP	303	908	325	• Amazon Elastic Compute Cloud • AWS Config • AWS Identity and Access Management

> **Tip**
>
> Para analisar as regras AWS Config usadas como mapeamentos de fontes de dados nesse framework padrão, baixe o arquivo AuditManager_ConfigDataSourceMappings_FedRAMP-Moderate-Baseline.zip.

Os controles nesse framework não se destinam a verificar se seus sistemas estão em conformidade com o FedRAMP. Além disso, eles não podem garantir que você obterá êxito em uma auditoria do

FedRAMP. AWS Audit Manager não verifica automaticamente os controles processuais que exigem a coleta manual de evidências.

Você pode encontrar esse framework na guia Framework padrão do Biblioteca framework no Audit Manager.

Para obter instruções sobre como criar uma avaliação usando esse framework, consulte Como criar uma avaliação.

Quando você usa o console do Audit Manager para criar uma avaliação a partir desse framework padrão, a lista de Serviços da AWS no escopo é selecionada por padrão e não pode ser editada. Isso ocorre porque o Audit Manager mapeia e seleciona automaticamente as fontes de dados e os serviços para você. Essa seleção é feita de acordo com os requisitos da Linha de Base Moderada do FedRAMP. Se você precisar editar a lista de serviços no escopo desse framework, poderá fazer isso usando as operações da API CreateAssessment ou UpdateAssessment. Como alternativa, você pode personalizar o framework padrão e, em seguida, criar uma avaliação a partir do framework personalizado.

Para obter instruções sobre como personalizar esse framework para atender às suas necessidades específicas, consulte Como personalizar um framework existente e Como personalizar um controle existente.

Mais atributos do FedRAMP

- AWS Página de conformidade do FedRAMP
- AWS Publicações no blog do FedRAMP

Regulamento Geral sobre a Proteção de Dados (General Data Protection Regulation, ou GDPR)

AWS Audit Manager fornece um framework padrão pré-construído que oferece suporte ao Regulamento Geral sobre a Proteção de Dados (General Data Protection Regulation, GDPR). Por padrão, esse framework contém somente controles manuais. Esses controles manuais não coletam evidências automaticamente. No entanto, se quiser automatizar a coleta de evidências para alguns controles sob GDPR, você pode usar o recurso de controle personalizado em AWS Audit Manager. Para obter mais informações, consulte Como usar esse framework para apoiar sua preparação para auditoria.

Tópicos

O que é Regulamento Geral sobre a Proteção de Dados (General Data Protection Regulation, ou GDPR)?

O Regulamento Geral sobre a Proteção de Dados (GDPR) é uma nova lei de privacidade europeia que entrou em vigor em 25 de maio de 2018. O GDPR substitui a Diretiva de Proteção de Dados da UE, também conhecida como Diretiva 95/46/EC. O objetivo é harmonizar as leis de proteção de dados em toda a União Europeia (UE). Isso é feito aplicando uma única lei de proteção de dados, vinculativa em todos os estados membros da UE.

O GDPR se aplica a todas as organizações estabelecidas na UE que processem dados pessoais dos titulares de dados da UE em relação à oferta de bens ou serviços aos titulares de dados na UE, ou ao monitoramento do comportamento na UE (independente de estarem estabelecidas na UE). Dados pessoais são quaisquer informações relacionadas a uma pessoa física Identificada ou identificável.

Você pode encontrar o framework do GDPR na página da biblioteca do framework de AWS Audit Manager. Para obter mais informações, consulte o Centro de Regulamento Geral sobre a Proteção de Dados (GDPR).

Como usar esse framework para apoiar sua preparação para auditoria

Você pode usar o framework do GDPR AWS Audit Manager para ajudá-lo a se preparar para as auditorias.

Os detalhes do framework são:

Nome do framework em AWS Audit Manager	Número de controles automatizados	Número de controles manuais	Número de conjuntos de controle	Serviços da AWS em escopo
GDPR	0	371	10	Nenhum

Você pode encontrar o framework do GDPR na guia Frameworks padrão no do Biblioteca framework Audit Manager. Como esse framework padrão contém somente controles manuais, nenhum dos Serviços da AWS está no escopo.

> **Note**
>
> Se você quiser automatizar a coleta de evidências para o GDPR, você pode usar o Audit Manager para criar seus próprios controles personalizados para o GDPR. A tabela a seguir fornece recomendações sobre as fontes de dados AWS que você pode mapear de acordo com os requisitos do GDPR em seus controles personalizados. Embora algumas fontes de dados a seguir estejam mapeadas para vários controles, lembre-se de que você será cobrado apenas uma vez por cada avaliação de atributos.
> As recomendações a seguir usam AWS Config e AWS Security Hub como fontes de dados. Para coletar evidências dessas fontes de dados com êxito, faça o seguinte:
>
> - Confirme se você seguiu as instruções para habilitar e configurar AWS Config e AWS Security Hub em seu Conta da AWS.
> - Confirme se você incluiu o Security Hub e o AWS Config como serviços no escopo. Para analisar os serviços atuais no escopo de sua avaliação, consulte Como analisar uma avaliação, guia Serviços da AWS. Para editar essa lista, consulte Editar Serviços da AWS no escopo.
>
> Depois de configurar os dois serviços dessa forma, o Audit Manager coleta evidências sempre que a avaliação de uma regra especificada AWS Config ocorra ou o Security Hub controla.

Nome do controle	conjunto de controles	Mapeamento recomendado da fonte de dados de controle
Artigo 25 Proteção de dados por projeto	Capítulo 4 - controlador e processador	Você pode criar um controle personalizado em AWS Audit Manager que ofereça suporte a esse controle GDPR. Ao especificar os detalhes do controle, insira o seguinte em Informações de teste:

Nome do controle	conjunto de controles	Mapeamento recomendado da fonte de dados de controle
e por padrão.1		• Exibir todos os eventos da conta raiz ao longo do período • O bucket AWS CloudTrail não público • Mostre todas as políticas com um `Allow:*:*` e liste todas as entidades principais e serviços usando essas políticas Ao configurar as fontes de dados de controle, recomendamos que inclua todos os itens a seguir como fontes de dados: Escolha AWS Config como tipo de fonte de dados e selecione as seguintes regras gerenciadas AWS Config como mapeamentos da fonte de dados: • IAM_ROOT_ACCESS_KEY_CHECK • ROOT_ACCOUNT_MFA_ENABLED • ROOT_ACCOUNT_HARDWARE_MFA_ENABLED • VPC_FLOW_LOGS_ENABLED • ACCESS_KEYS_ROTATED • IAM_PASSWORD_POLICY Escolha AWS Security Hub como tipo de fonte de dados e selecione os seguintes controles do Security Hub como mapeamentos da fonte de dados: • 1.1 (CloudWatch.1) • 1.1 (IAM.20) • 1.10 (IAM.16) • 1.11 (IAM.17) • 1.12 (IAM.4) • 1.13 (IAM.9) • 1.14 (IAM.6)

Nome do controle	conjunto de controles	Mapeamento recomendado da fonte de dados de controle
		• 1.16 (IAM.2) • 1.2 (IAM.5) • 1.20 (IAM.18) • 1.22 (IAM.1 • 1.3 (IAM.8) • 1.4 (IAM.3) • 1.5 (IAM.11) • 1.6 (IAM.12) • 1.7 (IAM.13) • 1.8 (IAM.14) • 1.9 (IAM.15) • 2.1 (CloudTrail.1) • 2.2 (CloudTrail.4) • 2.3 (CloudTrail.6) • 2.4 (CloudTrail.5) • 2.5 (Config.1) • 2.6 (CloudTrail.7) • 2.7 (CloudTrail.2) • 2.8 (KMS.4) • 2.9 (EC2.6) • 3.1 (CloudWatch.2) • 3.10 (CloudWatch.10) • 3.11 (CloudWatch.11) • 3.12 (CloudWatch.12) • 3.13 (CloudWatch.13) • 3.14 (CloudWatch.14) • Config.1

Nome do controle	conjunto de controles	Mapeamento recomendado da fonte de dados de controle
Artigo 25 Proteção de dados por projeto e por padrão.2	Capítulo 4 - controlador e processador	Você pode criar um controle personalizado em AWS Audit Manager que ofereça suporte a esse controle GDPR. Ao especificar os detalhes do controle, insira o seguinte em Informações de teste: • Exibir todos os eventos da conta raiz ao longo do período • O bucket AWS CloudTrail não público • Mostre todas as políticas com um `Allow:*:*` e liste todas as entidades principais e serviços usando essas políticas Ao configurar as fontes de dados de controle, recomendamos que inclua todos os itens a seguir como fontes de dados: Escolha AWS Config como tipo de fonte de dados e selecione as seguintes regras gerenciadas AWS Config como mapeamentos da fonte de dados: • IAM_ROOT_ACCESS_KEY_CHECK • ROOT_ACCOUNT_MFA_ENABLED • ROOT_ACCOUNT_HARDWARE_MFA_ENABLED • VPC_FLOW_LOGS_ENABLED • ACCESS_KEYS_ROTATED • IAM_PASSWORD_POLICY Escolha AWS Security Hub como tipo de fonte de dados e selecione os seguintes controles do Security Hub como mapeamentos da fonte de dados: • 1.1 (CloudWatch.1) • 1.1 (IAM.20) • 1.10 (IAM.16)

Nome do controle	conjunto de controles	Mapeamento recomendado da fonte de dados de controle
		• 1.11 (IAM.17) • 1.12 (IAM.4) • 1.13 (IAM.9) • 1.14 (IAM.6) • 1.16 (IAM.2) • 1.2 (IAM.5) • 1.20 (IAM.18) • 1.22 (IAM.1 • 1.3 (IAM.8) • 1.4 (IAM.3) • 1.5 (IAM.11) • 1.6 (IAM.12) • 1.7 (IAM.13) • 1.8 (IAM.14) • 1.9 (IAM.15) • 2.1 (CloudTrail.1) • 2.2 (CloudTrail.4) • 2.3 (CloudTrail.6) • 2.4 (CloudTrail.5) • 2.5 (Config.1) • 2.6 (CloudTrail.7) • 2.7 (CloudTrail.2) • 2.8 (KMS.4) • 2.9 (EC2.6) • 3.1 (CloudWatch.2) • 3.10 (CloudWatch.10) • 3.11 (CloudWatch.11)

Nome do controle	conjunto de controles	Mapeamento recomendado da fonte de dados de controle
		• 3.12 (CloudWatch.12) • 3.13 (CloudWatch.13) • 3.14 (CloudWatch.14) • Config.1

Nome do controle	conjunto de controles	Mapeamento recomendado da fonte de dados de controle
Artigo 25 Proteção de dados por projeto e por padrão.3	Capítulo 4 - controlador e processador	Você pode criar um controle personalizado em AWS Audit Manager que ofereça suporte a esse controle GDPR. Ao especificar os detalhes do controle, insira o seguinte em Informações de teste: • Exibir todos os eventos da conta raiz ao longo do período • O bucket AWS CloudTrail não público • Mostre todas as políticas com um `Allow:*:*` e liste todas as entidades principais e serviços usando essas políticas Ao configurar as fontes de dados de controle, recomendamos que inclua todos os itens a seguir como fontes de dados: Escolha AWS Config como tipo de fonte de dados e selecione as seguintes regras gerenciadas AWS Config como mapeamentos da fonte de dados: • IAM_ROOT_ACCESS_KEY_CHECK • ROOT_ACCOUNT_MFA_ENABLED • ROOT_ACCOUNT_HARDWARE_MFA_ENABLED • VPC_FLOW_LOGS_ENABLED • ACCESS_KEYS_ROTATED • IAM_PASSWORD_POLICY Escolha AWS Security Hub como tipo de fonte de dados e selecione os seguintes controles do Security Hub como mapeamentos da fonte de dados: • 1.1 (CloudWatch.1) • 1.1 (IAM.20) • 1.10 (IAM.16)

Nome do controle	conjunto de controles	Mapeamento recomendado da fonte de dados de controle
		• 1.11 (IAM.17) • 1.12 (IAM.4) • 1.13 (IAM.9) • 1.14 (IAM.6) • 1.16 (IAM.2) • 1.2 (IAM.5) • 1.20 (IAM.18) • 1.22 (IAM.1 • 1.3 (IAM.8) • 1.4 (IAM.3) • 1.5 (IAM.11) • 1.6 (IAM.12) • 1.7 (IAM.13) • 1.8 (IAM.14) • 1.9 (IAM.15) • 2.1 (CloudTrail.1) • 2.2 (CloudTrail.4) • 2.3 (CloudTrail.6) • 2.4 (CloudTrail.5) • 2.5 (Config.1) • 2.6 (CloudTrail.7) • 2.7 (CloudTrail.2) • 2.8 (KMS.4) • 2.9 (EC2.6) • 3.1 (CloudWatch.2) • 3.10 (CloudWatch.10) • 3.11 (CloudWatch.11)

Nome do controle	conjunto de controles	Mapeamento recomendado da fonte de dados de controle
		• 3.12 (CloudWatch.12) • 3.13 (CloudWatch.13) • 3.14 (CloudWatch.14) • Config.1

Nome do controle	conjunto de controles	Mapeamento recomendado da fonte de dados de controle
Artigo 30: registros de atividades de processamento.1	Capítulo 4 - controlador e processador	Você pode criar um controle personalizado em AWS Audit Manager que ofereça suporte a esse controle GDPR. Ao especificar os detalhes do controle, insira o seguinte em Informações de teste: • Exibir todos os eventos da conta raiz ao longo do período Ao configurar as fontes de dados de controle, recomendamos que inclua todos os itens a seguir como fontes de dados: Escolha AWS Config como tipo de fonte de dados e selecione as seguintes regras gerenciadas AWS Config como mapeamentos da fonte de dados: • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • VPC_FLOW_LOGS_ENABLED • CMK_BACKING_KEY_ROTATION_ENABLED • CLOUD_TRAIL_ENABLED • ELB_LOGGING_ENABLED • CLOUDTRAIL_SECURITY_TRAIL_ENABLED • REDSHIFT_CLUSTER_CONFIGURATION_CHECK • CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED Escolha AWS Security Hub como tipo de fonte de dados e selecione os seguintes controles do Security Hub como mapeamentos da fonte de dados: • Config.1

Nome do controle	conjunto de controles	Mapeamento recomendado da fonte de dados de controle
Artigo 30: registros de atividades de processamento.2	Capítulo 4 - controlador e processador	Você pode criar um controle personalizado em AWS Audit Manager que ofereça suporte a esse controle GDPR. Ao especificar os detalhes do controle, insira o seguinte em Informações de teste: • Exibir todos os eventos da conta raiz ao longo do período Ao configurar as fontes de dados de controle, recomendamos que inclua todos os itens a seguir como fontes de dados: Escolha AWS Config como tipo de fonte de dados e selecione as seguintes regras gerenciadas AWS Config como mapeamentos da fonte de dados: • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • VPC_FLOW_LOGS_ENABLED • CMK_BACKING_KEY_ROTATION_ENABLED • CLOUD_TRAIL_ENABLED • ELB_LOGGING_ENABLED • CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED Escolha AWS Security Hub como tipo de fonte de dados e selecione os seguintes controles do Security Hub como mapeamentos da fonte de dados: • Config.1

Nome do controle	conjunto de controles	Mapeamento recomendado da fonte de dados de controle
Artigo 30: registros de atividades de processamento.3	Capítulo 4 - controlador e processador	Você pode criar um controle personalizado em AWS Audit Manager que ofereça suporte a esse controle GDPR. Ao especificar os detalhes do controle, insira o seguinte em Informações de teste: • Exibir todos os eventos da conta raiz ao longo do período • O bucket AWS CloudTrail não público • Mostre todas as políticas com um `Allow:*:*` e liste todas as entidades principais e serviços usando essas políticas Ao configurar as fontes de dados de controle, recomendamos que inclua todos os itens a seguir como fontes de dados: Escolha AWS Config como tipo de fonte de dados e selecione as seguintes regras gerenciadas AWS Config como mapeamentos da fonte de dados: • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • VPC_FLOW_LOGS_ENABLED • CMK_BACKING_KEY_ROTATION_ENABLED • CLOUD_TRAIL_ENABLED • ELB_LOGGING_ENABLED • CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED Escolha AWS Security Hub como tipo de fonte de dados e selecione os seguintes controles do Security Hub como mapeamentos da fonte de dados: • Config.1

Nome do controle	conjunto de controles	Mapeamento recomendado da fonte de dados de controle
Artigo 30: registros de atividades de processamento.4	Capítulo 4 - controlador e processador	Você pode criar um controle personalizado em AWS Audit Manager que ofereça suporte a esse controle GDPR. Ao especificar os detalhes do controle, insira o seguinte em Informações de teste: • Exibir todos os eventos da conta raiz ao longo do período • O bucket AWS CloudTrail não público • Mostre todas as políticas com um `Allow:*:*` e liste todas as entidades principais e serviços usando essas políticas Ao configurar as fontes de dados de controle, recomendamos que inclua todos os itens a seguir como fontes de dados: Escolha AWS Config como tipo de fonte de dados e selecione as seguintes regras gerenciadas AWS Config como mapeamentos da fonte de dados: • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • VPC_FLOW_LOGS_ENABLED • CMK_BACKING_KEY_ROTATION_ENABLED • CLOUD_TRAIL_ENABLED • ELB_LOGGING_ENABLED • CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED Escolha AWS Security Hub como tipo de fonte de dados e selecione os seguintes controles do Security Hub como mapeamentos da fonte de dados: • Config.1

Nome do controle	conjunto de controles	Mapeamento recomendado da fonte de dados de controle
Artigo 30: registros de atividades de processamento.5	Capítulo 4 - controlador e processador	Você pode criar um controle personalizado em AWS Audit Manager que ofereça suporte a esse controle GDPR. Ao especificar os detalhes do controle, insira o seguinte em Informações de teste: • Exibir todos os eventos da conta raiz ao longo do período Ao configurar as fontes de dados de controle, recomendamos que inclua todos os itens a seguir como fontes de dados: Escolha AWS Config como tipo de fonte de dados e selecione as seguintes regras gerenciadas AWS Config como mapeamentos da fonte de dados: • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • VPC_FLOW_LOGS_ENABLED • CMK_BACKING_KEY_ROTATION_ENABLED • CLOUD_TRAIL_ENABLED • ELB_LOGGING_ENABLED • CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED Escolha AWS Security Hub como tipo de fonte de dados e selecione os seguintes controles do Security Hub como mapeamentos da fonte de dados: • Config.1

Nome do controle	conjunto de controles	Mapeamento recomendado da fonte de dados de controle
Artigo 32: Segurança do processamento.1	Capítulo 4 - controlador e processador	Você pode criar um controle personalizado em AWS Audit Manager que ofereça suporte a esse controle GDPR. Ao especificar os detalhes do controle, insira o seguinte em Informações de teste: • Mostrar criptografia de dados em repouso para todos os serviços • Mostrar criptografia de dados em trânsito para todos os serviços • A exclusão de MFA foi habilitada para o Amazon S3 • Todos os escaneamentos do Amazon Inspector • Mostrar todas as instâncias não estão habilitadas para o Amazon Inspector • Mostrar todos os balanceadores de carga receptando em HTTPS (SSL) • AWS CloudTrail criptografado em repouso • Alertas do Amazon CloudWatch para AWS Config exibindo todas as alterações e configurações comentadas • Todas as atividades raiz Ao configurar as fontes de dados de controle, recomendamos que inclua todos os itens a seguir como fontes de dados: Escolha AWS Config como tipo de fonte de dados e selecione as seguintes regras gerenciadas AWS Config como mapeamentos da fonte de dados: • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • S3_BUCKET_SSL_REQUESTS_ONLY • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUDWATCH_LOG_GROUP_ENCRYPTED • EFS_ENCRYPTED_CHECK

Nome do controle	conjunto de controles	Mapeamento recomendado da fonte de dados de controle
		• ELASTICSEARCH_ENCRYPTED_AT_REST • ENCRYPTED_VOLUMES • RDS_STORAGE_ENCRYPTED • REDSHIFT_CLUSTER_CONFIGURATION_CHECK • S3_BUCKET_SERVER_SIDE_ENCRYPTION_ENABLED • SAGEMAKER_ENDPOINT_CONFIGURATION_KMS_KEY_CONFIGURED • SAGEMAKER_NOTEBOOK_INSTANCE_KMS_KEY_CONFIGURED • SNS_ENCRYPTED_KMS • EC2_EBS_ENCRYPTION_BY_DEFAULT • DYNAMODB_TABLE_ENCRYPTED_KMS • DYNAMODB_TABLE_ENCRYPTION_ENABLED • RDS_SNAPSHOT_ENCRYPTED • S3_DEFAULT_ENCRYPTION_KMS • DAX_ENCRYPTION_ENABLED • EKS_SECRETS_ENCRYPTED • RDS_LOGGING_ENABLED • REDSHIFT_BACKUP_ENABLED • RDS_IN_BACKUP_PLAN • WAF_CLASSIC_LOGGING_ENABLED • WAFV2_LOGGING_ENABLED • ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK • ELB_ACM_CERTIFICATE_REQUIRED • ELB_CUSTOM_SECURITY_POLICY_SSL_CHECK • REDSHIFT_REQUIRE_TLS_SSL • CLOUDFRONT_VIEWER_POLICY_HTTPS • ALB_HTTP_DROP_INVALID_HEADER_ENABLED • ELASTICSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK

Nome do controle	conjunto de controles	Mapeamento recomendado da fonte de dados de controle
		• ELB_TLS_HTTPS_LISTENERS_ONLY • ACM_CERTIFICATE_EXPIRATION_CHECK • API_GW_CACHE_ENABLED_AND_ENCRYPTED

Nome do controle	conjunto de controles	Mapeamento recomendado da fonte de dados de controle
Artigo 32: Segurança do processamento.2	Capítulo 4 - controlador e processador	Você pode criar um controle personalizado em AWS Audit Manager que ofereça suporte a esse controle GDPR. Ao especificar os detalhes do controle, insira o seguinte em Informações de teste: • Mostrar criptografia de dados em repouso para todos os serviços • Mostrar criptografia de dados em trânsito para todos os serviços • A exclusão de MFA foi habilitada para o Amazon S3 • Todos os escaneamentos do Amazon Inspector • Mostrar todas as instâncias não habilitadas para o Amazon Inspector • Mostrar todos os balanceadores de carga receptando em HTTPS (SSL) • AWS CloudTrail criptografado em repouso • Alertas do Amazon CloudWatch para AWS Config exibindo todas as alterações e configurações comentadas • Todas as atividades raiz Ao configurar as fontes de dados de controle, recomendamos que inclua todos os itens a seguir como fontes de dados: Escolha AWS Config como tipo de fonte de dados e selecione as seguintes regras gerenciadas AWS Config como mapeamentos da fonte de dados: • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • S3_BUCKET_SSL_REQUESTS_ONLY • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUDWATCH_LOG_GROUP_ENCRYPTED • EFS_ENCRYPTED_CHECK • ELASTICSEARCH_ENCRYPTED_AT_REST

Nome do controle	conjunto de controles	Mapeamento recomendado da fonte de dados de controle
		• ENCRYPTED_VOLUMES • RDS_STORAGE_ENCRYPTED • REDSHIFT_CLUSTER_CONFIGURATION_CHECK • S3_BUCKET_SERVER_SIDE_ENCRYPTION_ENABLED • SAGEMAKER_ENDPOINT_CONFIGURATION_KMS_KEY_CONFIGURED • SAGEMAKER_NOTEBOOK_INSTANCE_KMS_KEY_CONFIGURED • SNS_ENCRYPTED_KMS • EC2_EBS_ENCRYPTION_BY_DEFAULT • DYNAMODB_TABLE_ENCRYPTED_KMS • DYNAMODB_TABLE_ENCRYPTION_ENABLED • RDS_SNAPSHOT_ENCRYPTED • S3_DEFAULT_ENCRYPTION_KMS • DAX_ENCRYPTION_ENABLED • EKS_SECRETS_ENCRYPTED • RDS_LOGGING_ENABLED • REDSHIFT_BACKUP_ENABLED • RDS_IN_BACKUP_PLAN • WAF_CLASSIC_LOGGING_ENABLED • WAFV2_LOGGING_ENABLED • ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK • ELB_ACM_CERTIFICATE_REQUIRED • ELB_CUSTOM_SECURITY_POLICY_SSL_CHECK • REDSHIFT_REQUIRE_TLS_SSL • CLOUDFRONT_VIEWER_POLICY_HTTPS • ALB_HTTP_DROP_INVALID_HEADER_ENABLED • ELASTICSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK • ELB_TLS_HTTPS_LISTENERS_ONLY

Nome do controle	conjunto de controles	Mapeamento recomendado da fonte de dados de controle
		• ACM_CERTIFICATE_EXPIRATION_CHECK • API_GW_CACHE_ENABLED_AND_ENCRYPTED

Nome do controle	conjunto de controles	Mapeamento recomendado da fonte de dados de controle
Artigo 32: Segurança do processamento.3	Capítulo 4 - controlador e processador	Você pode criar um controle personalizado em AWS Audit Manager que ofereça suporte a esse controle GDPR. Ao especificar os detalhes do controle, insira o seguinte em Informações de teste: • Mostrar criptografia de dados em repouso para todos os serviços • Mostrar criptografia de dados em trânsito para todos os serviços • A exclusão de MFA foi habilitada para o Amazon S3 • Todos os escaneamentos do Amazon Inspector • Mostrar todas as instâncias não habilitadas para o Amazon Inspector • Mostrar todos os balanceadores de carga receptando em HTTPS (SSL) • AWS CloudTrail criptografado em repouso • Alertas do Amazon CloudWatch para AWS Config exibindo todas as alterações e configurações comentadas • Todas as atividades raiz Ao configurar as fontes de dados de controle, recomendamos que inclua todos os itens a seguir como fontes de dados: Escolha AWS Config como tipo de fonte de dados e selecione as seguintes regras gerenciadas AWS Config como mapeamentos da fonte de dados: • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • S3_BUCKET_SSL_REQUESTS_ONLY • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUDWATCH_LOG_GROUP_ENCRYPTED • EFS_ENCRYPTED_CHECK • ELASTICSEARCH_ENCRYPTED_AT_REST

Nome do controle	conjunto de controles	Mapeamento recomendado da fonte de dados de controle
		• ENCRYPTED_VOLUMES • RDS_STORAGE_ENCRYPTED • REDSHIFT_CLUSTER_CONFIGURATION_CHECK • S3_BUCKET_SERVER_SIDE_ENCRYPTION_ENABLED • SAGEMAKER_ENDPOINT_CONFIGURATION_KMS_KEY_CONFIGURED • SAGEMAKER_NOTEBOOK_INSTANCE_KMS_KEY_CONFIGURED • SNS_ENCRYPTED_KMS • EC2_EBS_ENCRYPTION_BY_DEFAULT • DYNAMODB_TABLE_ENCRYPTED_KMS • DYNAMODB_TABLE_ENCRYPTION_ENABLED • RDS_SNAPSHOT_ENCRYPTED • S3_DEFAULT_ENCRYPTION_KMS • DAX_ENCRYPTION_ENABLED • EKS_SECRETS_ENCRYPTED • RDS_LOGGING_ENABLED • REDSHIFT_BACKUP_ENABLED • RDS_IN_BACKUP_PLAN • WAF_CLASSIC_LOGGING_ENABLED • WAFV2_LOGGING_ENABLED • ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK • ELB_ACM_CERTIFICATE_REQUIRED • ELB_CUSTOM_SECURITY_POLICY_SSL_CHECK • REDSHIFT_REQUIRE_TLS_SSL • CLOUDFRONT_VIEWER_POLICY_HTTPS • ALB_HTTP_DROP_INVALID_HEADER_ENABLED • ELASTICSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK • ELB_TLS_HTTPS_LISTENERS_ONLY

Nome do controle	conjunto de controles	Mapeamento recomendado da fonte de dados de controle
		• ACM_CERTIFICATE_EXPIRATION_CHECK • API_GW_CACHE_ENABLED_AND_ENCRYPTED

Nome do controle	conjunto de controles	Mapeamento recomendado da fonte de dados de controle
Artigo 32: Segurança do processamento.4	Capítulo 4 - controlador e processador	Você pode criar um controle personalizado em AWS Audit Manager que ofereça suporte a esse controle GDPR. Ao especificar os detalhes do controle, insira o seguinte em Informações de teste: • Mostrar criptografia de dados em repouso para todos os serviços • Mostrar criptografia de dados em trânsito para todos os serviços • A exclusão de MFA foi habilitada para o Amazon S3 • Todos os escaneamentos do Amazon Inspector • Mostrar todas as instâncias não habilitadas para o Amazon Inspector • Mostrar todos os balanceadores de carga receptando em HTTPS (SSL) • AWS CloudTrail criptografado em repouso • Alertas do Amazon CloudWatch para AWS Config exibindo todas as alterações e configurações comentadas • Todas as atividades raiz Ao configurar as fontes de dados de controle, recomendamos que inclua todos os itens a seguir como fontes de dados: Escolha AWS Config como tipo de fonte de dados e selecione as seguintes regras gerenciadas AWS Config como mapeamentos da fonte de dados: • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • S3_BUCKET_SSL_REQUESTS_ONLY • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUDWATCH_LOG_GROUP_ENCRYPTED • EFS_ENCRYPTED_CHECK • ELASTICSEARCH_ENCRYPTED_AT_REST

Nome do controle	conjunto de controles	Mapeamento recomendado da fonte de dados de controle
		• ENCRYPTED_VOLUMES • RDS_STORAGE_ENCRYPTED • REDSHIFT_CLUSTER_CONFIGURATION_CHECK • S3_BUCKET_SERVER_SIDE_ENCRYPTION_ENABLED • SAGEMAKER_ENDPOINT_CONFIGURATION_KMS_KEY_CONFIGURED • SAGEMAKER_NOTEBOOK_INSTANCE_KMS_KEY_CONFIGURED • SNS_ENCRYPTED_KMS • EC2_EBS_ENCRYPTION_BY_DEFAULT • DYNAMODB_TABLE_ENCRYPTED_KMS • DYNAMODB_TABLE_ENCRYPTION_ENABLED • RDS_SNAPSHOT_ENCRYPTED • S3_DEFAULT_ENCRYPTION_KMS • DAX_ENCRYPTION_ENABLED • EKS_SECRETS_ENCRYPTED • RDS_LOGGING_ENABLED • REDSHIFT_BACKUP_ENABLED • RDS_IN_BACKUP_PLAN • WAF_CLASSIC_LOGGING_ENABLED • WAFV2_LOGGING_ENABLED • ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK • ELB_ACM_CERTIFICATE_REQUIRED • ELB_CUSTOM_SECURITY_POLICY_SSL_CHECK • REDSHIFT_REQUIRE_TLS_SSL • CLOUDFRONT_VIEWER_POLICY_HTTPS • ALB_HTTP_DROP_INVALID_HEADER_ENABLED • ELASTICSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK • ELB_TLS_HTTPS_LISTENERS_ONLY

Nome do controle	conjunto de controles	Mapeamento recomendado da fonte de dados de controle
		• ACM_CERTIFICATE_EXPIRATION_CHECK • API_GW_CACHE_ENABLED_AND_ENCRYPTED

Depois de criar seus novos controles personalizados, você pode adicioná-los a um framework personalizado do GDPR. Para obter mais informações, consulte Criando criar um framework personalizado e Como editar um framework personalizado. Em seguida, você pode criar uma avaliação a partir do framework personalizado do GDPR. Dessa forma, AWS Audit Manager pode coletar evidências automaticamente para os controles personalizados que você adicionou. Para obter instruções sobre como criar uma avaliação a partir de um framework, consulte Como criar uma avaliação.

Mais atributos do GDPR

- Centro de Regulamento Geral sobre a Proteção de Dados (GDPR)
- AWSPublicações no blog do GDPR

Lei Gramm-Leach-Bliley

AWS Audit Manager fornece um framework pré-construído que fornece suporte à Lei Gramm-Leach-Bliley (GLBA).

Tópicos

- O que é a Lei Gramm-Leach-Bliley (GLBA)?
- Como usar esse framework para apoiar sua preparação para auditoria

O que é a Lei Gramm-Leach-Bliley (GLBA)?

A Lei Gramm-Leach-Bliley (Lei GLB ou GLBA), também conhecida como Lei de Modernização de Serviços Financeiros de 1999, é uma lei federal promulgada nos Estados Unidos para controlar a forma como as instituições financeiras lidam com as informações privadas de indivíduos. A Lei consiste em três seções. A primeira é a Regra de Privacidade Financeira, que regula a coleta e divulgação de informações financeiras privadas. A segunda é a Regra de Salvaguardas, que estipula

que as instituições financeiras devem implementar programas de segurança para proteger essas informações. A terceira são as Disposições de Pretexto, que proíbem a prática de pretexto (acessar informações privadas sob falsos pretextos). A lei também exige que instituições financeiras forneçam aos clientes avisos de privacidade por escrito explicando suas práticas de compartilhamento de informações.

Como usar esse framework para apoiar sua preparação para auditoria

Você pode usar o framework da Lei Gramm-Leach-Bliley (GLBA) para ajudá-lo a se preparar para as auditorias. esse framework inclui uma coleção pré-construída de controles com descrições e procedimentos de teste. Esses controles são agrupados em conjuntos de acordo com os requisitos do GLBA. Você também pode personalizar esse framework e seus controles para apoiar auditorias internas com requisitos específicos.

Usando o framework do GLBA como ponto de partida, você pode criar uma avaliação do Audit Manager e coletar evidências relevantes para uma auditoria do GLBA. Em sua avaliação, você pode especificar os serviços Contas da AWS e serviços que deseja incluir no escopo de sua auditoria. Depois de criar uma avaliação, o Audit Manager começa a avaliar seus atributos AWS. Ele faz isso com base nos controles definidos no framework do GLBA. Na hora de fazer uma auditoria, você ou um representante de sua escolha pode analisar as evidências que o Audit Manager coletou. Como alternativa, você pode navegar pelas pastas de evidências na sua avaliação e escolher quais evidências deseja incluir no relatório de avaliação. Ou, se você ativou o localizador de evidências, pode pesquisar evidências específicas e exportá-las no formato CSV ou criar um relatório de avaliação baseado nos resultados da pesquisa. De qualquer uma das formas, você pode usar esse relatório de avaliação para mostrar que seus controles estão funcionando conforme o esperado.

Os detalhes do framework do GLBA são os seguintes:

Nome do framework em AWS Audit Manager	Número de controles automatizados	Número de controles manuais	Número de conjuntos de controle	Serviços da AWS em escopo
Lei Gramm-Leach-Bliley (GLBA)	4	110	16	• Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Config • AWS Identity and Access Management

Nome do framework em AWS Audit Manager	Número de controles automatizados	Número de controles manuais	Número de conjuntos de controle	Serviços da AWS em escopo
				• AWS Security Hub

> **Tip**
>
> Para analisar as regras AWS Config usadas como mapeamentos de fontes de dados nesse framework padrão, baixe o arquivo AuditManager_ConfigDataSourceMappings_GLBA.zip.

Os controles nesse framework AWS Audit Manager não se destinam a verificar se seus sistemas estão em conformidade com o padrão GLBA. Além disso, eles não podem garantir que você obterá êxito em uma auditoria da GLBA. AWS Audit Manager não verifica automaticamente os controles processuais que exigem a coleta manual de evidências.

Você pode encontrar o framework GLBA na guiaFrameworks padrão do Biblioteca framework no Audit Manager.

Para obter instruções sobre como criar uma avaliação usando esse framework, consulte Como criar uma avaliação.

Quando você usa o console do Audit Manager para criar uma avaliação a partir desse framework padrão, a lista de Serviços da AWS no escopo é selecionada por padrão e não pode ser editada. Isso ocorre porque o Audit Manager mapeia e seleciona automaticamente as fontes de dados e os serviços para você. Essa seleção é feita de acordo com os requisitos do GLBA. Se você precisar editar a lista de serviços no escopo desse framework, poderá fazer isso usando as operações da API CreateAssessment ou UpdateAssessment. Como alternativa, você pode personalizar o framework padrão e, em seguida, criar uma avaliação a partir do framework personalizado.

Para obter instruções sobre como personalizar esse framework para atender às suas necessidades específicas, consulte Como personalizar um framework existente e Como personalizar um controle existente.

GxP 21 CFR parte 11

AWS Audit Manager fornece um framework pré-construído que fonece suporte aos regulamentos GxP CFR parte 11 com base nas práticas recomendadas AWS.

> **Note**
>
> Para obter informações sobre o Anexo 11 do GxP EU e framework do Audit Manager que fornece suporte a ele, consulte Anexo 11 da GxP da UE.

Tópicos

O que é GxP CFR parte 11?

GxP refere-se aos regulamentos e diretrizes aplicáveis às organizações de ciências biológicas, que fabricam alimentos e produtos médicos. Os produtos médicos que se enquadram nessa categoria incluem medicamentos, dispositivos e aplicativos de software médicos. A intenção geral dos requisitos de GxP é garantir que alimentos e produtos médicos sejam seguros para os consumidores. Também garantem a integridade dos dados usados para decisões de segurança relacionadas ao produto.

O termo GxP abrange uma ampla gama de atividades relacionadas à conformidade. Isso inclui Práticas Recomendadas de Laboratório (Good Laboratory Practices, ou GLP), Práticas Recomendadas Clínicas (Good Clinical Practices, ou GCP) e Práticas Recomendadas de Fabricação (Good Manufacturing Practices, ou GMP). Cada um desses diferentes tipos de atividades envolve requisitos específicos de produto que as organizações de ciências biológicas devem implementar. Isso é baseado no tipo de produto que as organizações fabricam, bem como no país onde seus produtos são vendidos. Quando as organizações de ciências biológicas usam sistemas computadorizados para realizar determinadas atividades de GxP, elas devem garantir que o sistema computadorizado de GxP seja desenvolvido, validado e operado adequadamente para o uso pretendido do sistema.

Para uma abordagem abrangente do uso da nuvem AWS para sistemas GxP, consulte o relatório Considerações sobre o uso de produtos AWS em sistemas GxP.

Como usar esse framework para apoiar sua preparação para auditoria

Você pode usar o framework GxP 21 CFR Parte 11 para ajudá-lo a se preparar para as auditorias. Esse framework inclui uma coleção pré-construída de controles com descrições e procedimentos de

teste. Esses controles são agrupados em conjuntos de acordo com os requisitos GxP. Você também pode personalizar esse framework e seus controles para apoiar auditorias internas com requisitos específicos.

Usando o framework como ponto de partida, você pode criar uma avaliação do Audit Manager e começar a coletar evidências relevantes para sua auditoria. Depois de criar uma avaliação, o Audit Manager começa a avaliar seus atributos AWS. Ele faz isso com base nos controles definidos no framework GxP 21 CFR Parte 11. Na hora de fazer uma auditoria, você ou um representante de sua escolha pode analisar as evidências que o Audit Manager coletou. Como alternativa, você pode navegar pelas pastas de evidências na sua avaliação e escolher quais evidências deseja incluir no relatório de avaliação. Ou, se você ativou o localizador de evidências, pode pesquisar evidências específicas e exportá-las no formato CSV ou criar um relatório de avaliação baseado nos resultados da pesquisa. De qualquer uma das formas, você pode usar esse relatório de avaliação para mostrar que seus controles estão funcionando conforme o esperado.

Os detalhes do framework GxP CFR Parte 11 são os seguintes:

Nome do framework em AWS Audit Manager	Número de controles automatizados	Número de controles manuais	Número de conjuntos de controle	Serviços da AWS em escopo
GxP 21 CFR Parte 11	13	14	7	• AWS CloudTrail • AWS Config • AWS Identity and Access Management

> **Tip**
>
> Para analisar as regras AWS Config usadas como mapeamentos de fontes de dados nesse framework padrão, baixe o arquivo AuditManager_ConfigDataSourceMappings_GxP-21-CFR-Parte-11.zip.

Os controles nesse framework AWS Audit Manager não se destinam a verificar se seus sistemas estão em conformidade com os regulamentos GxP. Além disso, eles não podem garantir que você obterá êxito em uma auditoria da GxP. AWS Audit Manager não verifica automaticamente os controles processuais que exigem a coleta manual de evidências.

Você pode encontrar esse framework na guia Framework padrão do Biblioteca framework no Audit Manager.

Para obter instruções sobre como criar uma avaliação usando esse framework, consulte Como criar uma avaliação.

Quando você usa o console do Audit Manager para criar uma avaliação a partir desse framework padrão, a lista de Serviços da AWS no escopo é selecionada por padrão e não pode ser editada. Isso ocorre porque o Audit Manager mapeia e seleciona automaticamente as fontes de dados e os serviços para você. Essa seleção é feita de acordo com os requisitos do framework GxP CFR Parte 11. Se você precisar editar a lista de serviços no escopo desse framework, poderá fazer isso usando as operações da API CreateAssessment ou UpdateAssessment. Como alternativa, você pode personalizar o framework padrão e, em seguida, criar uma avaliação a partir do framework personalizado.

Para obter instruções sobre como personalizar esse framework para atender às suas necessidades específicas, consulte Como personalizar um framework existente e Como personalizar um controle existente.

Mais atributos GxP

- Página de conformidade AWS para GxP
- Considerações sobre o uso de produtos AWS em sistemas GxP

Anexo 11 da GxP da UE

AWS Audit Manager fornece um framework pré-construído que fornece suporte às regulamentações GxP do Anexo 11 da UE com base nas práticas recomendadas AWS.

> **Note**
>
> Para obter informações sobre o GxP 21 CFR Parte 11 e o framework do Audit Manager que fornece suporte, consulte GxP 21 CFR parte 11.

Tópicos

O que é o Anexo 11 da GxP da UE?

O framework do Anexo 11 da GxP da UE é o equivalente europeu do framework FDA 21 CFR parte 11 nos Estados Unidos. Este anexo se aplica a todas as formas de sistemas computadorizados usados como parte das atividades regulamentadas de Práticas Recomendadas de Fabricação (GMP). Um sistema computadorizado é um conjunto de componentes de software e hardware que, juntos, cumpre determinadas funcionalidades. O aplicativo deve ser validado e a infraestrutura de TI, qualificada. Quando um sistema computadorizado substitui uma operação manual, não deve haver diminuição resultante na qualidade do produto, no controle do processo ou na garantia da qualidade. Não deve haver aumento no risco geral do processo.

O Anexo 11 faz parte das diretrizes europeias de GMP e define os termos de referência para sistemas computadorizados, usados por organizações da indústria farmacêutica. O Anexo 11 funciona como uma lista de verificação, que permite às agências reguladoras europeias estabelecerem os requisitos para sistemas computadorizados relacionados a produtos farmacêuticos e dispositivos médicos. As diretrizes estabelecidas pela Comissão dos Comitês Europeus não estão muito distantes da FDA (21 CFR Parte 11). O Anexo 11 define os critérios acerca de como os registros eletrônicos e as assinaturas eletrônicas são considerados para serem gerenciados.

Como usar esse framework para apoiar sua preparação para auditoria

Você pode usar o framework GxP UE Anexo 11 para ajudá-lo a se preparar para as auditorias. Esse framework inclui uma coleção pré-construída de controles com descrições e procedimentos de teste. Esses controles são agrupados em conjuntos de acordo com os requisitos GxP. Você também pode personalizar esse framework e seus controles para apoiar auditorias internas com requisitos específicos.

Usando o framework como ponto de partida, você pode criar uma avaliação do Audit Manager e começar a coletar evidências relevantes para sua auditoria. Depois de criar uma avaliação, o Audit Manager começa a avaliar seus atributos AWS. Ele faz isso com base nos controles definidos no framework do Anexo 11 da GxP da UE. Na hora de fazer uma auditoria, você ou um representante de sua escolha pode analisar as evidências que o Audit Manager coletou. Como alternativa, você pode navegar pelas pastas de evidências na sua avaliação e escolher quais evidências deseja incluir no relatório de avaliação. Ou, se você ativou o localizador de evidências, pode pesquisar evidências

específicas e exportá-las no formato CSV ou criar um relatório de avaliação baseado nos resultados da pesquisa. De qualquer uma das formas, você pode usar esse relatório de avaliação para mostrar que seus controles estão funcionando conforme o esperado.

Os detalhes do framework do Anexo 11 da GxP da UE são os seguintes:

Nome do framework em AWS Audit Manager	Número de controles automatizados	Número de controles manuais	Número de conjuntos de controle	Serviços da AWS em escopo
Anexo 11 da GxP da UE	19	13	3	• Amazon CloudWatch • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Security Hub

> **Tip**
>
> Para analisar as regras AWS Config usadas como mapeamentos de fontes de dados nesse framework padrão, baixe o arquivo AuditManager_ConfigDataSourceMappings_GxP-EU-Annex-11.zip.

Os controles nesse framework não se destinam a verificar se seus sistemas estão em conformidade com os requisitos do Anexo 11 da GxP de UE. Além disso, eles não podem garantir que você obterá êxito em uma auditoria da GxP. AWS Audit Manager não verifica automaticamente os controles processuais que exigem a coleta manual de evidências.

Você pode encontrar esse framework na guia Framework padrão do Biblioteca framework no Audit Manager.

Para obter instruções sobre como criar uma avaliação usando esse framework, consulte Como criar uma avaliação.

Quando você usa o console do Audit Manager para criar uma avaliação a partir desse framework padrão, a lista de Serviços da AWS no escopo é selecionada por padrão e não pode ser editada. Isso ocorre porque o Audit Manager mapeia e seleciona automaticamente as fontes de dados e os serviços para você. Essa seleção é feita de acordo com os requisitos do framework GxP do Anexo 11 da UE. Se você precisar editar a lista de serviços no escopo desse framework, poderá fazer isso usando as operações da API CreateAssessment ou UpdateAssessment. Como alternativa, você pode personalizar o framework padrão e, em seguida, criar uma avaliação a partir do framework personalizado.

Para obter instruções sobre como personalizar esse framework para atender às suas necessidades específicas, consulte Como personalizar um framework existente e Como personalizar um controle existente.

Regra de Segurança da Lei de Portabilidade de Seguros de Saúde e Responsabilidade (HIPAA) de 2003

AWS Audit Manager fornece um framework pré-criado que fornece suporte às regras HIPAA para ajudá-lo na preparação da auditoria.

> **Note**
>
> Esse framework era anteriormente chamada HIPAA na biblioteca do framework. Em 08 de março de 2023, atualizamos o nome desse framework para Regra de Segurança HIPAA 2003 para diferenciá-lo da Regra Final de Segurança Geral da HIPAA de 2013
> Para obter informações sobre a Regra Final de Segurança Geral da HIPAA de 2013 e o framework do Audit Manager que fornece suporte a esse padrão, consulte Regra Final de Segurança Geral da HIPAA de 2013.

Tópicos

- O que é a HIPAA e Regra de Segurança HIPAA 2003?
- Como usar esse framework para apoiar sua preparação para auditoria
- Mais atributos HIPAA

O que é a HIPAA e Regra de Segurança HIPAA 2003?

A Lei de Portabilidade e Responsabilidade do Seguro de Saúde de 1996 (HIPAA) é uma legislação que ajuda os trabalhadores dos EUA a reter a cobertura de seguro de saúde ao mudarem ou perderem o emprego. A legislação também busca incentivar os registros eletrônicos de saúde para melhorar a eficiência e a qualidade do sistema de saúde dos EUA, por meio de um melhor compartilhamento de informações.

Além de aumentar o uso de registros médicos eletrônicos, a HIPAA inclui Disposições para Proteger a Segurança e a Privacidade das Informações de Saúde Protegidas (PHI). O PHI inclui um conjunto muito amplo de dados pessoais de saúde identificáveis e relacionados à saúde. Isso inclui informações de seguro e cobrança, dados de diagnóstico, dados de atendimento clínico e resultados de laboratório, como imagens e resultados de exames.

O Departamento de Saúde e Serviços Humanos dos EUA publicou uma Regra de Segurança final em fevereiro de 2003. Esta Regra define padrões nacionais para proteger a confidencialidade, integridade e disponibilidade de informações eletrônicas de saúde protegidas.

As regras da HIPAA se aplicam à entidades cobertas. Isso inclui hospitais, prestadores de serviços médicos, planos de saúde patrocinados pelo empregador, instalações de pesquisa e seguradoras que lidem diretamente com pacientes e dados de pacientes. A exigência da HIPAA para proteger a PHI também se estende aos parceiros de negócios.

Para obter mais informações sobre como a HIPAA e HITECH protegem as informações de saúde, consulte a página Privacidade de Informações de Saúde do Departamento de Saúde e Serviços Humanos dos EUA.

Um número crescente de prestadores de serviços de saúde, pagadores e profissionais de TI usa serviços em nuvem baseados em utilitários AWS para processar, armazenar e transmitir informações de saúde protegidas (PHI). AWS permite que entidades cobertas e seus parceiros de negócios sujeitos à HIPAA usem o ambiente AWS seguro para processar, manter e armazenar informações de saúde protegidas.

Para obter instruções sobre como usar AWS para o processamento e armazenamento de informações de saúde, consulte o relatório Arquitetando para Segurança HIPAA e Conformidade no Amazon Web Services.

Como usar esse framework para apoiar sua preparação para auditoria

Você pode usar o framework da Regra de Segurança 2003 da HIPAA para ajudá-lo a se preparar para as auditorias. Esse framework inclui uma coleção pré-construída de controles com descrições e procedimentos de teste. Esses controles são agrupados em conjuntos de acordo com os requisitos HIPAA. Você também pode personalizar esse framework e seus controles para apoiar auditorias internas com requisitos específicos.

Usando o framework como ponto de partida, você pode criar uma avaliação do Audit Manager e começar a coletar evidências relevantes para sua auditoria. Depois de criar uma avaliação, o Audit Manager começa a avaliar seus atributos AWS. Ele faz isso com base nos controles definidos no framework da HIPAA. Na hora de fazer uma auditoria, você ou um representante de sua escolha pode analisar as evidências que o Audit Manager coletou. Como alternativa, você pode navegar pelas pastas de evidências na sua avaliação e escolher quais evidências deseja incluir no relatório de avaliação. Ou, se você ativou o localizador de evidências, pode pesquisar evidências específicas e exportá-las no formato CSV ou criar um relatório de avaliação baseado nos resultados da pesquisa. De qualquer uma das formas, você pode usar esse relatório de avaliação para mostrar que seus controles estão funcionando conforme o esperado.

Os detalhes do framework da Regra de Segurança 2003 da HIPAA são os seguintes:

Nome do framework em AWS Audit Manager	Número de controles automatizados	Número de controles manuais	Número de conjuntos de controle	Serviços da AWS em escopo
Regra de Segurança HIPAA 2003	35	53	5	• Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Security Hub

> **Tip**
>
> Para analisar as AWS Config regras usadas como mapeamentos de fontes de dados nesse framework padrão, baixe o arquivo AuditManager_ConfigDataSourceMappings_HIPAA-Security-Rule-2003.zip.

Os controles nesse framework AWS Audit Manager não se destinam a verificar se seus sistemas estão em conformidade com o padrão HIPAA. Além disso, eles não podem garantir que você obterá êxito em uma auditoria HIPAA. AWS Audit Manager não verifica automaticamente os controles processuais que exigem a coleta manual de evidências.

Você pode encontrar esse framework na guia Framework padrão do Biblioteca framework no Audit Manager.

Para obter instruções sobre como criar uma avaliação usando esse framework, consulte Como criar uma avaliação.

Quando você usa o console do Audit Manager para criar uma avaliação a partir desse framework padrão, a lista de Serviços da AWS no escopo é selecionada por padrão e não pode ser editada. Isso ocorre porque o Audit Manager mapeia e seleciona automaticamente as fontes de dados e os serviços para você. Essa seleção é feita de acordo com os requisitos do framework HIPAA. Se você precisar editar a lista de serviços no escopo desse framework, poderá fazer isso usando as operações da API CreateAssessment ou UpdateAssessment. Como alternativa, você pode personalizar o framework padrão e, em seguida, criar uma avaliação a partir do framework personalizado.

Para obter instruções sobre como personalizar esse framework para atender às suas necessidades específicas, consulte Como personalizar um framework existente e Como personalizar um controle existente.

Mais atributos HIPAA

- Privacidade de informações de saúde do Departamento de Saúde e Serviços Humanos dos EUA
- A regra de segurança do Departamento de Saúde e Serviços Humanos dos EUA
- Arquitetando para Segurança HIPAA e Conformidade no Amazon Web Services
- Página de conformidade para HIPAA AWS

Regra Final de Segurança Geral da HIPAA de 2013

AWS Audit Manager fornece um framework pré-criado que fornece suporte às regras HIPAA para ajudá-lo na preparação da auditoria.

> **Note**
>
> Para obter informações sobre a Regra de Segurança 2003 da HIPAA e o AWS Audit Manager framework que fornece suporte a esse padrão, consulte Regra de Segurança da Lei de Portabilidade de Seguros de Saúde e Responsabilidade (HIPAA) de 2003.

Tópicos

O que é a HIPAA e sua Regra Final de Segurança Geral?

A Lei de Portabilidade e Responsabilidade do Seguro de Saúde de 1996 (HIPAA) é uma legislação que ajuda os trabalhadores dos EUA a reter a cobertura de seguro de saúde ao mudarem ou perderem o emprego. A legislação também busca incentivar os registros eletrônicos de saúde para melhorar a eficiência e a qualidade do sistema de saúde dos EUA, por meio de um melhor compartilhamento de informações.

Além de aumentar o uso de registros médicos eletrônicos, a HIPAA inclui Disposições para Proteger a Segurança e a Privacidade das Informações de Saúde Protegidas (PHI). O PHI inclui um conjunto muito amplo de dados pessoais de saúde identificáveis e relacionados à saúde. Isso inclui informações de seguro e cobrança, dados de diagnóstico, dados de atendimento clínico e resultados de laboratório, como imagens e resultados de exames.

A regra final de segurança geral da HIPAA, que entrou em vigor em 2013, implementa várias atualizações em todas as regras aprovadas anteriormente. As modificações nas Regras de Segurança, Privacidade, Notificação de Violação e Aplicação visam aumentar a confidencialidade e a segurança no compartilhamento de dados.

As regras da HIPAA se aplicam à entidades cobertas. Isso inclui hospitais, prestadores de serviços médicos, planos de saúde patrocinados pelo empregador, instalações de pesquisa e seguradoras

que lidem diretamente com pacientes e dados de pacientes. Como parte das atualizações gerais, muitas das regras da HIPAA que se aplicam às entidades cobertas agora também se aplicam aos parceiros de negócios.

Para obter mais informações sobre como a HIPAA e HITECH protegem as informações de saúde, consulte a página Privacidade de Informações de Saúde do Departamento de Saúde e Serviços Humanos dos EUA.

Um número crescente de prestadores de serviços de saúde, pagadores e profissionais de TI usa serviços em nuvem baseados em utilitários AWS para processar, armazenar e transmitir informações de saúde protegidas (PHI). AWS permite que entidades cobertas e seus parceiros de negócios sujeitos à HIPAA usem o ambiente AWS seguro para processar, manter e armazenar informações de saúde protegidas. Para obter instruções sobre como usar AWS para o processamento e armazenamento de informações de saúde, consulte o relatório Arquitetando para Segurança HIPAA e Conformidade no Amazon Web Services.

Como usar esse framework para apoiar sua preparação para auditoria

Você pode usar o framework da Regra Final de Segurança Geral da HIPAA de 2013 para ajudá-lo a se preparar para as auditorias. Esse framework inclui uma coleção pré-construída de controles com descrições e procedimentos de teste. Esses controles são agrupados em conjuntos de acordo com os requisitos HIPAA. Você também pode personalizar esse framework e seus controles para apoiar auditorias internas com requisitos específicos.

Usando o framework como ponto de partida, você pode criar uma avaliação do Audit Manager e começar a coletar evidências relevantes para sua auditoria. Depois de criar uma avaliação, o Audit Manager começa a avaliar seus atributos AWS. Ele faz isso com base nos controles definidos no framework da HIPAA. Na hora de fazer uma auditoria, você ou um representante de sua escolha pode analisar as evidências que o Audit Manager coletou. Como alternativa, você pode navegar pelas pastas de evidências na sua avaliação e escolher quais evidências deseja incluir no relatório de avaliação. Ou, se você ativou o localizador de evidências, pode pesquisar evidências específicas e exportá-las no formato CSV ou criar um relatório de avaliação baseado nos resultados da pesquisa. De qualquer uma das formas, você pode usar esse relatório de avaliação para mostrar que seus controles estão funcionando conforme o esperado.

Os detalhes do framework Regra Final de Segurança Geral 2013 da HIPAA são:

Nome do framework em AWS Audit Manager	Número de controles automatizados	Número de controles manuais	Número de conjuntos de controle	Serviços da AWS em escopo
Regra Final de Segurança Geral da HIPAA de 2013	39	46	5	• Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Security Hub

> **Tip**
>
> Para analisar as regras AWS Config usadas como mapeamentos de fontes de dados nesse framework padrão, baixe o arquivo AuditManager_ConfigDataSourceMappings_HIPAA-Final-Omnibus-Security-Rule-2013.zip.

Os controles nesse framework AWS Audit Manager não se destinam a verificar se seus sistemas estão em conformidade com o padrão HIPAA. Além disso, eles não podem garantir que você obterá êxito em uma auditoria HIPAA. AWS Audit Manager não verifica automaticamente os controles processuais que exigem a coleta manual de evidências.

Você pode encontrar esse framework na guia Framework padrão do Biblioteca framework no Audit Manager.

Para obter instruções sobre como criar uma avaliação usando esse framework, consulte Como criar uma avaliação.

Quando você usa o console do Audit Manager para criar uma avaliação a partir desse framework padrão, a lista de Serviços da AWS no escopo é selecionada por padrão e não pode ser editada. Isso ocorre porque o Audit Manager mapeia e seleciona automaticamente as fontes de dados e os serviços para você. Essa seleção é feita de acordo com os requisitos do framework HIPAA.

Se você precisar editar a lista de serviços no escopo desse framework, poderá fazer isso usando as operações da API CreateAssessment ou UpdateAssessment. Como alternativa, você pode personalizar o framework padrão e, em seguida, criar uma avaliação a partir do framework personalizado.

Para obter instruções sobre como personalizar esse framework para atender às suas necessidades específicas, consulte Como personalizar um framework existente e Como personalizar um controle existente.

Mais atributos HIPAA

- Privacidade de Informações de Saúde do Departamento de Saúde e Serviços Humanos dos EUA
- Regulamentação geral Omnibus da HIPAA do Departamento de Saúde e Serviços Humanos dos EUA
- Arquitetando para Segurança HIPAA e Conformidade no Amazon Web Services
- Página de conformidade para HIPAA AWS

ISO/IEC 27001:2013 Anexo A

AWS Audit Manager fornece um framework padrão pré-construída que framework e automatiza as avaliações da ISO/IEC 27001:2013 Anexo A.

Tópicos

- O que é a ISO/IEC 27001:2013 Anexo A?
- Como usar esse framework para apoiar sua preparação para auditoria
- Mais atributos do Anexo A da ISO/IEC 27001:2013

O que é a ISO/IEC 27001:2013 Anexo A?

A Comissão Eletrotécnica Internacional (IEC) e a Organização Internacional de Padronização (ISO) são organizações independentes, não governamentais e sem fins lucrativos que desenvolvem e publicam padrões internacionais totalmente baseados em consenso.

O Anexo A da ISO/IEC 27001:2013 é um padrão de gerenciamento de segurança que especifica as práticas recomendadas de gerenciamento de segurança e controles de segurança abrangentes que seguem a orientação de práticas recomendadas da ISO/IEC 27002. Esse padrão internacional especifica os requisitos acerca de como estabelecer, implementar, manter e melhorar continuamente

um sistema de gerenciamento de segurança da informação em sua organização. Entre esses padrões estão os requisitos de avaliação e tratamento de riscos de segurança da informação personalizados de acordo com as necessidades de sua organização. Os requisitos desta norma internacional são genéricos e devem ser aplicáveis a todas as organizações, independente do tipo, tamanho ou natureza.

Como usar esse framework para apoiar sua preparação para auditoria

Você pode usar o framework AWS Audit Manager do Anexo A da ISO/IEC 27001:2013 para ajudá-lo a se preparar para as auditorias. esse framework inclui uma coleção pré-construída de controles com descrições e procedimentos de teste. Esses controles são agrupados em conjuntos de acordo com os requisitos do Anexo A da ISO/IEC 27001:2013. Você também pode personalizar esse framework e seus controles para apoiar auditorias internas com requisitos específicos.

Usando o framework como ponto de partida, você pode criar uma avaliação do Audit Manager e começar a coletar evidências relevantes para uma auditoria do Anexo A da ISO/IEC 27001:2013. Em sua avaliação, você pode especificar os serviços Contas da AWS e serviços que deseja incluir no escopo de sua auditoria. Depois de criar uma avaliação, o Audit Manager começa a avaliar seus atributos AWS. Ele faz isso com base nos controles definidos no framework do Anexo A da ISO/IEC 27001:2013. Na hora de fazer uma auditoria, você ou um representante de sua escolha pode analisar as evidências que o Audit Manager coletou. Como alternativa, você pode navegar pelas pastas de evidências na sua avaliação e escolher quais evidências deseja incluir no relatório de avaliação. Ou, se você ativou o localizador de evidências, pode pesquisar evidências específicas e exportá-las no formato CSV ou criar um relatório de avaliação baseado nos resultados da pesquisa. De qualquer uma das formas, você pode usar esse relatório de avaliação para mostrar que seus controles estão funcionando conforme o esperado.

Os detalhes do framework são:

Nome do framework em AWS Audit Manager	Número de controles automatizados	Número de controles manuais	Número de conjuntos de controle	Serviços da AWS em escopo
ISO/IEC 27001:2013 Anexo A	50	64	35	• Amazon CloudWatch • Amazon Elastic Compute Cloud • AWS CloudTrail

Nome do framework em AWS Audit Manager	Número de controles automatizados	Número de controles manuais	Número de conjuntos de controle	Serviços da AWS em escopo
				• AWS Config • AWS Identity and Access Management • AWS Security Hub

> **Tip**
>
> Para analisar as regras AWS Config usadas como mapeamentos de fontes de dados nesse framework padrão, baixe o arquivo AuditManager_ConfigDataSourceMappings_ISO-IEC-27001-2013-Annex-A.zip.

Os controles nesse framework AWS Audit Manager não se destinam a verificar se seus sistemas estão em conformidade com esse padrão internacional. Além disso, eles não podem garantir que você obterá êxito em uma auditoria ISO/IEC. AWS Audit Manager não verifica automaticamente os controles processuais que exigem a coleta manual de evidências.

Você pode encontrar o framework do Anexo A da ISO/IEC 27001:2013 na guia Frameworks padrão no Biblioteca framework do Audit Manager.

Quando você usa o console do Audit Manager para criar uma avaliação a partir desse framework padrão, a lista de Serviços da AWS no escopo é selecionada por padrão e não pode ser editada. Isso ocorre porque o Audit Manager mapeia e seleciona automaticamente as fontes de dados e os serviços para você. Essa seleção é feita de acordo com os requisitos do framework do Anexo A da ISO-IEC 27001:2013. Se você precisar editar a lista de serviços no escopo desse framework, poderá fazer isso usando as operações da API CreateAssessment ou UpdateAssessment. Como alternativa, você pode personalizar o framework padrão e, em seguida, criar uma avaliação a partir do framework personalizado.

Para obter instruções sobre como criar uma avaliação usando esse framework, consulte Como criar uma avaliação. Para obter instruções sobre como personalizar esse framework para atender às suas

necessidades específicas, consulte Como personalizar um framework existente e Como personalizar um controle existente.

Mais atributos do Anexo A da ISO/IEC 27001:2013

- Para obter mais informações sobre esse padrão internacional, consulte ISO/IEC 27001:2013 na ANSI Webstore.

NIST 800-53 (Rev. 5) Baixo-Moderado-Alto

AWS Audit Manager fornece um framework pré-construída que framework e automatiza as avaliações do padrão de conformidade NIST 800-53, com base nas práticas recomendadas AWS.

> **Note**
>
> - Para obter informações sobre o framework do Audit Manager que fornece suporte ao NIST 800-171, consulte NIST SP 800-171 (Rev. 2).
> - Para obter informações sobre o framework do Audit Manager que fornece suporte aoFramework de Cibersegurança NIST, consulte NIST Cybersecurity Framework versão 1.1.

Tópicos

O que é o NIST 800-53?

O Instituto Nacional de Padrões e Tecnologia (NIST) foi fundado em 1901 e agora faz parte do Departamento de Comércio dos EUA. O NIST é um dos laboratórios de ciências físicas mais antigos dos Estados Unidos. O Congresso dos EUA estabeleceu a agência para melhorar o que era na época uma infraestrutura de medição de segunda categoria. A infraestrutura foi um grande desafio para a competitividade industrial dos EUA, tendo ficado atrás de outras potências econômicas, como o Reino Unido e a Alemanha.

Os controles de segurança NIST 800-53 são geralmente aplicáveis aos sistemas de informação federais dos EUA. Normalmente, esses sistemas precisam passar por um processo formal de avaliação e autorização. Esse processo garante proteção suficiente da confidencialidade, integridade e disponibilidade das informações e dos sistemas de informação. Ele é baseado na categoria de segurança e nível de impacto do sistema (baixo, moderado ou alto), bem como na determinação do risco. Controles de segurança são selecionados a partir do catálogo de controle de segurança NIST SP 800-53, e o sistema é avaliado de acordo com os requisitos desses controle.

O framework Baixo-Moderado-Alto NIST 800-53 (Rev. 5) representa os controles de segurança e os procedimentos de avaliação associados que são definidos nos Controles de Segurança Recomendados para Sistemas e Organizações da Informação Federal do NIST SP 800-53 Revisão 5. Para quaisquer discrepâncias observadas no conteúdo entre esse framework do NIST SP 800-53 e a última publicação especial do NIST SP 800-53 Revisão 5, consulte os documentos oficiais publicados disponíveis no Centro de Recursos de Segurança da Informática do NIST.

Como usar esse framework para apoiar sua preparação para auditoria

Você pode usar o framework NIST 800-53 (Rev. 5) Baixo-Moderado-Alto para ajudá-lo a se preparar para as auditorias. Esse framework inclui uma coleção pré-construída de controles com descrições e procedimentos de teste. Esses controles são agrupados em conjuntos de controle de acordo com os requisitos do NIST. Você também pode personalizar esse framework e seus controles para apoiar auditorias internas com requisitos específicos.

Usando o framework como ponto de partida, você pode criar uma avaliação do Audit Manager e começar a coletar evidências relevantes para sua auditoria. Depois de criar uma avaliação, o Audit Manager começa a avaliar seus atributos AWS. Ele faz isso com base nos controles definidos no framework Baixa-Moderada-Alta do NIST 800-53 (Rev. 5). Na hora de fazer uma auditoria, você ou um representante de sua escolha pode analisar as evidências que o Audit Manager coletou. Como alternativa, você pode navegar pelas pastas de evidências na sua avaliação e escolher quais evidências deseja incluir no relatório de avaliação. Ou, se você ativou o localizador de evidências, pode pesquisar evidências específicas e exportá-las no formato CSV ou criar um relatório de avaliação baseado nos resultados da pesquisa. De qualquer uma das formas, você pode usar esse relatório de avaliação para mostrar que seus controles estão funcionando conforme o esperado.

Os detalhes do framework NIST 800-53 (Rev. 5) Baixo-Moderado-Alto (Rev. 5) são os seguintes:

Nome do framework em AWS Audit Manager	Número de controles automatizados	Número de controles manuais	Número de conjuntos de controle	Serviços da AWS em escopo
NIST 800-53 (Rev. 5) Baixo-Moderado-Alto	225	782	280	• Amazon CloudWatch • Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Security Hub

> **Tip**
>
> Para analisar as regras AWS Config usadas como mapeamentos de fontes de dados nesse framework padrão, baixe o arquivo AuditManager_ConfigDataSourceMapings_NIST-800-53-Rev.5-low-moderate-high.zip.

Os controles nesse framework AWS Audit Manager não se destinam a verificar se seus sistemas estão em conformidade com o padrão NIST. Além disso, eles não podem garantir que você obterá êxito em uma auditoria do NIST. AWS Audit Manager não verifica automaticamente os controles processuais que exigem a coleta manual de evidências.

Você pode encontrar esse framework na guia Framework padrão do Biblioteca framework no Audit Manager.

Para obter instruções sobre como criar uma avaliação usando esse framework, consulte Como criar uma avaliação.

Quando você usa o console do Audit Manager para criar uma avaliação a partir desse framework padrão, a lista de Serviços da AWS no escopo é selecionada por padrão e não pode ser editada.

Isso ocorre porque o Audit Manager mapeia e seleciona automaticamente as fontes de dados e os serviços para você. Essa seleção é feita de acordo com os requisitos do framework NIST 800-53 (Rev. 5) Baixo-Moderado-Alto. Se você precisar editar a lista de serviços no escopo desse framework, poderá fazer isso usando as operações da API CreateAssessment ou UpdateAssessment. Como alternativa, você pode personalizar o framework padrão e, em seguida, criar uma avaliação a partir do framework personalizado.

Para obter instruções sobre como personalizar esse framework para atender às suas necessidades específicas, consulte Como personalizar um framework existente e Como personalizar um controle existente.

Mais atributos NIST

- Instituto Nacional de Padrões e Tecnologia (NIST)
- Centro de Recursos de Segurança da Informática NIST
- AWS Página de conformidade do NIST

NIST Cybersecurity Framework versão 1.1

AWS Audit Manager fornece um framework pré-construído que estrutura e automatiza as avaliações de Framework de Segurança Cibernética NIST, com base nas práticas recomendadas AWS.

> **Note**
>
> - Para obter informações sobre o framework do Audit Manager que oferece suporte ao NIST 800-53 (Rev. 5) Baixo-Moderado-Alto, consulte NIST 800-53 (Rev. 5) Baixo-Moderado-Alto.
> - Para obter informações sobre o framework do Audit Manager que fornece suporte ao NIST SP 800-171 (Rev. 2), consulte NIST SP 800-171 (Rev. 2).

Tópicos

- O que é Framework de Segurança Cibernética NIST?
- Como usar esse framework para apoiar sua preparação para auditoria
- Mais atributos NIST

O que é Framework de Segurança Cibernética NIST?

O Instituto Nacional de Padrões e Tecnologia (NIST) foi fundado em 1901 e agora faz parte do Departamento de Comércio dos EUA. O NIST é um dos laboratórios de ciências físicas mais antigos dos Estados Unidos. O Congresso dos EUA estabeleceu a agência para melhorar o que era na época uma infraestrutura de medição de segunda categoria. A infraestrutura foi um grande desafio para a competitividade industrial dos EUA, tendo ficado atrás de outras potências econômicas, como o Reino Unido e a Alemanha.

Os Estados Unidos dependem do funcionamento confiável da infraestrutura crítica. As ameaças à segurança cibernética exploram a maior complexidade e interconexão dos sistemas de infraestrutura crítica. Eles colocam em risco a segurança, a economia e a segurança e saúde pública dos Estados Unidos. Semelhante aos riscos financeiros e de reputação, o risco de cibersegurança afeta os resultados financeiros de uma empresa. Isso pode aumentar os custos e afetar a receita. Isso pode prejudicar a capacidade de uma organização de inovar, conquistar e manter clientes. Em última análise, a segurança cibernética pode ampliar o gerenciamento geral de riscos de uma organização.

O NIST Cybersecurity Framework (CSF) é apoiado por governos e indústrias em todo o mundo como uma linha de base recomendada para uso por qualquer organização, independente do setor ou tamanho. O NIST Cybersecurity Framework consiste em três componentes principais: o núcleo do framework, os perfis e os níveis de implementação. O núcleo do framework contém as atividades e os resultados desejados de segurança cibernética organizados em 23 categorias que abrangem a amplitude dos objetivos de segurança cibernética de uma organização. Os perfis contêm o alinhamento exclusivo de uma organização com seus requisitos e objetivos organizacionais, apetite a riscos e atributos usando os resultados desejados do núcleo do framework. Os níveis de implementação descrevem o grau em que as práticas de gerenciamento de riscos de cibersegurança de uma organização exibem as características definidas no núcleo do framework.

Como usar esse framework para apoiar sua preparação para auditoria

Você pode usar a versão 1.1 do NIST Cybersecurity Framework para ajudá-lo a se preparar para as auditorias. Esse framework inclui uma coleção pré-construída de controles com descrições e procedimentos de teste. Esses controles são agrupados em conjuntos de controles de acordo com os requisitos do NIST CSF. Atualmente, o Audit Manager oferece suporte ao componente principal do framework, oferecendo 56 controles automatizados e 52 controles manuais. Esses controles são combinados com 23 categorias de segurança cibernética definidas no núcleo do framework. O Audit Manager não oferece suporte aos componentes de perfil e implementação nesse framework.

Você também pode personalizar esse framework e seus controles para apoiar auditorias internas com requisitos específicos.

Usando o framework como ponto de partida, você pode criar uma avaliação do Audit Manager e começar a coletar evidências relevantes para sua auditoria. Depois de criar uma avaliação, o Audit Manager começa a avaliar seus atributos AWS. Ele faz isso com base nos controles definidos na versão do Framework NIST Cybersecurity versão 1.1. Na hora de fazer uma auditoria, você ou um representante de sua escolha pode analisar as evidências que o Audit Manager coletou. Como alternativa, você pode navegar pelas pastas de evidências na sua avaliação e escolher quais evidências deseja incluir no relatório de avaliação. Ou, se você ativou o localizador de evidências, pode pesquisar evidências específicas e exportá-las no formato CSV ou criar um relatório de avaliação baseado nos resultados da pesquisa. De qualquer uma das formas, você pode usar esse relatório de avaliação para mostrar que seus controles estão funcionando conforme o esperado.

Os detalhes da versão 1.1 do NIST Cybersecurity Framework são os seguintes:

Nome do framework em AWS Audit Manager	Número de controles automatizados	Número de controles manuais	Número de conjuntos de controle	Serviços da AWS em escopo
NIST Cybersecurity Framework versão 1.1	56	52	23	• AWS Config • AWS Identity and Access Management • AWS Security Hub

> **Tip**
>
> Para analisar as regras AWS Config usadas como mapeamentos de fonte de dados nesse framework padrão, baixe o arquivo AuditManager_ConfigDataSourceMappings_NIST-CSF-v1.1.zip.

Os controles oferecidos pelo Audit Manager não têm como objetivo verificar se seus sistemas estão em conformidade com o NIST Cybersecurity Framework. Além disso, eles não podem garantir

que você obterá êxito em uma auditoria do NIST Cybersecurity. AWS Audit Manager não verifica automaticamente os controles processuais que exigem a coleta manual de evidências.

Você pode encontrar esse framework na guia Framework padrão do Biblioteca framework no Audit Manager.

Para obter instruções sobre como criar uma avaliação usando esse framework, consulte Como criar uma avaliação.

Quando você usa o console do Audit Manager para criar uma avaliação a partir desse framework padrão, a lista de Serviços da AWS no escopo é selecionada por padrão e não pode ser editada. Isso ocorre porque o Audit Manager mapeia e seleciona automaticamente as fontes de dados e os serviços para você. Essa seleção é feita de acordo com os requisitos do framework do NIST Cybersecurity Framework versão 1.1. Se você precisar editar a lista de serviços no escopo desse framework, poderá fazer isso usando as operações da API CreateAssessment ou UpdateAssessment. Como alternativa, você pode personalizar o framework padrão e, em seguida, criar uma avaliação a partir do framework personalizado.

Para obter instruções sobre como personalizar esse framework para atender às suas necessidades específicas, consulte Como personalizar um framework existente e Como personalizar um controle existente.

Mais atributos NIST

- Instituto Nacional de Padrões e Tecnologia (NIST)
- Centro de Recursos de Segurança da Informática NIST
- Página de conformidade do NIST AWS
- Framework de Segurança Cibernética do NIST - Alinhamento com o CSF do NIST na Nuvem AWS

NIST SP 800-171 (Rev. 2)

AWS Audit Manager fornece um framework pré-construída que framework e automatiza as avaliações do padrão de conformidade NIST SP 800-171 com base nas práticas recomendadas AWS.

> **Note**
>
> - Para obter informações sobre o framework do Audit Manager que oferece suporte ao NIST 800-53 (Rev. 5) Baixo-Moderado-Alto, consulte NIST 800-53 (Rev. 5) Baixo-Moderado-Alto.
> - Para obter informações sobre o framework do Audit Manager que oferece suporte ao NIST Cybersecurity Framework versão 1.1, consulte NIST Cybersecurity Framework versão 1.1.

Tópicos

O que é o NIST SP 800-171?

O NIST SP 800-171 se concentra em proteger a confidencialidade de informações não classificadas controladas (CUI) em sistemas e organizações não federais. Ele recomenda requisitos de segurança específicos para esse objetivo. O NIST 800-171 é uma publicação que descreve os padrões e práticas de segurança necessários para organizações não federais que lidem com CUI em suas redes. Foi publicado pela primeira vez em junho de 2015 pelo Instituto Nacional de Padrões e Tecnologia (NIST). O NIST é uma agência do governo dos EUA que lançou vários padrões e publicações para fortalecer a resiliência da segurança cibernética nos setores público e privado. O NIST 800-171 tem recebido atualizações regulares de acordo com ameaças cibernéticas emergentes e tecnologias em transformação. A versão mais recente (revisão 2) foi lançada em fevereiro de 2020.

Os controles de segurança cibernética NIST 800-171 protegem a CUI nas redes de TI de prestadores e subcontratados governamentais. Ele define as práticas e procedimentos que os prestadores de serviços governamentais devem seguir quando suas redes processam ou armazenam CUI. O NIST 800-171 só se aplica às partes da rede de um contratante onde a CUI estiver presente.

Como usar esse framework para apoiar sua preparação para auditoria

Você pode usar o framework NIST SP 800-171 Rev. 2 para ajudá-lo a se preparar para as auditorias. Esse framework inclui uma coleção pré-construída de controles com descrições e procedimentos

de teste. Esses controles são agrupados em conjuntos de controle de acordo com os requisitos do NIST. Você também pode personalizar esse framework e seus controles para apoiar auditorias internas com requisitos específicos.

Usando o framework como ponto de partida, você pode criar uma avaliação do Audit Manager e começar a coletar evidências relevantes para sua auditoria. Depois de criar uma avaliação, o Audit Manager começa a avaliar seus atributos AWS. Ele faz isso com base nos controles definidos no framework NIST SP 800-171 Rev. 2. Na hora de fazer uma auditoria, você ou um representante de sua escolha pode analisar as evidências que o Audit Manager coletou. Como alternativa, você pode navegar pelas pastas de evidências na sua avaliação e escolher quais evidências deseja incluir no relatório de avaliação. Ou, se você ativou o localizador de evidências, pode pesquisar evidências específicas e exportá-las no formato CSV ou criar um relatório de avaliação baseado nos resultados da pesquisa. De qualquer uma das formas, você pode usar esse relatório de avaliação para mostrar que seus controles estão funcionando conforme o esperado.

Os detalhes do framework do NIST SP 800-171 Rev. 2 são os seguintes:

Nome do framework em AWS Audit Manager	Número de controles automatizados	Número de controles manuais	Número de conjuntos de controle	Serviços da AWS em escopo
NIST SP 800-171 Rev. 2	66	58	16	• Amazon CloudWatch • Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Security Hub

> **Tip**
>
> Para analisar as regras AWS Config usadas como mapeamentos de fonte de dados nesse framework padrão, baixe o arquivo AuditManager_ConfigDataSourceMapings_NIST-SP-800-171-Rev.2.zip.

Os controles nesse framework AWS Audit Manager não se destinam a verificar se seus sistemas estão em conformidade com o NIST 800-171. Além disso, eles não podem garantir que você obterá êxito em uma auditoria do NIST. AWS Audit Manager não verifica automaticamente os controles processuais que exigem a coleta manual de evidências.

Você pode encontrar esse framework na guia Framework padrão do Biblioteca framework no Audit Manager.

Para obter informações sobre como criar uma avaliação usando esse framework, consulte Como criar uma avaliação.

Quando você usa o console do Audit Manager para criar uma avaliação a partir desse framework padrão, a lista de Serviços da AWS no escopo é selecionada por padrão e não pode ser editada. Isso ocorre porque o Audit Manager mapeia e seleciona automaticamente as fontes de dados e os serviços para você. Essa seleção é feita de acordo com os requisitos do framework NIST SP 800-171 Rev. 2. Se você precisar editar a lista de serviços no escopo desse framework, poderá fazer isso usando as operações da API CreateAssessment ou UpdateAssessment. Como alternativa, você pode personalizar o framework padrão e, em seguida, criar uma avaliação a partir do framework personalizado.

Para obter instruções sobre como personalizar esse framework para atender às suas necessidades específicas, consulte Como personalizar um framework existente e Como personalizar um controle existente.

Mais atributos NIST

- Instituto Nacional de Padrões e Tecnologia (NIST)
- Centro de Recursos de Segurança da Informática NIST
- AWS Página de conformidade do NIST

PCI DSS V3.2.1

AWS Audit Manager fornece um framework pré-construído que oferece suporte ao PCI DSS v3.2.1.

> **Note**
>
> Para obter informações sobre o PCI DSS v4 e o framework do Audit Manager compatível com ele, consulte PCI DSS V4.0.

Tópicos

O que é PCI DSS?

O PCI DSS (Padrão de Segurança de Dados da Indústria de Cartões de Pagamento) é um padrão de segurança da informação exclusivo. É administrado pelo Conselho de Normas de Segurança da Indústria de Meios de Pagamento, fundado pela American Express, Discover Financial Services, JCB International, MasterCard Worldwide e Visa Inc. O PCI DSS se aplica a entidades que armazenam, processam ou transmitem dados do titular do cartão (CHD) ou confidenciais de autenticação (SAD). Isso inclui, entre outros, comerciantes, processadores, adquirentes, emissores e provedores de serviços. O PCI DSS é aplicado pelas bandeiras de cartão de pagamento e administrado pelo Conselho de Normas de Segurança da Indústria de Meios de Pagamento.

AWS é certificado como provedor de serviços de nível 1 do PCI DSS, o nível mais alto nível de avaliação disponível. A avaliação de conformidade foi conduzida pela Coalfire Systems Inc., um Avaliador de Segurança Qualificado (QSA) independente. O Certificado de Conformidade do PCI DSS (AOC) e o Resumo de Responsabilidade estão disponíveis em AWS Artifact. Este é um portal de auto atendimento para acesso sob demanda a relatórios de conformidade AWS. Faça login ao AWS Artifact no Console de gerenciamento da AWS ou saiba mais em Introdução ao AWS Artifact

Você pode baixar o padrão PCI DSS na Biblioteca de Documentos do Conselho de Normas de Segurança da Indústria de Meios de Pagamento.

Como usar esse framework para apoiar sua preparação para auditoria

Você pode usar o framework PCI DSS V3.2.1 para ajudá-lo a se preparar para as auditorias. Esse framework inclui uma coleção pré-construída de controles com descrições e procedimentos de teste. Esses controles são agrupados em conjuntos de acordo com os requisitos do PCI DSS. Você também pode personalizar esse framework e seus controles para apoiar auditorias internas com requisitos específicos.

Usando o framework como ponto de partida, você pode criar uma avaliação do Audit Manager e começar a coletar evidências relevantes para sua auditoria. Depois de criar uma avaliação, o Audit Manager começa a avaliar seus atributos AWS. Ele faz isso com base nos controles definidos no framework do PCI DSS V3.2.1. Na hora de fazer uma auditoria, você ou um representante de sua escolha pode analisar as evidências que o Audit Manager coletou. Como alternativa, você pode navegar pelas pastas de evidências na sua avaliação e escolher quais evidências deseja incluir no relatório de avaliação. Ou, se você ativou o localizador de evidências, pode pesquisar evidências específicas e exportá-las no formato CSV ou criar um relatório de avaliação baseado nos resultados da pesquisa. De qualquer uma das formas, você pode usar esse relatório de avaliação para mostrar que seus controles estão funcionando conforme o esperado.

Os detalhes do framework PCI DSS V3.2.1 são os seguintes:

Nome do framework em AWS Audit Manager	Número de controles automatizados	Número de controles manuais	Número de conjuntos de controle	Serviços da AWS em escopo
PCI DSS V3.2.1	175	487	12	• Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Security Hub

> **Tip**
>
> Para analisar as regras AWS Config usadas como mapeamentos de fonte de dados nesse framework padrão, baixe o arquivo AuditManager_ConfigDataSourceMappings_PCI-DSS-v3.2.1.zip.

Os controles nesse framework AWS Audit Manager não se destinam a verificar se seus sistemas estão em conformidade com o padrão PCI DSS. Além disso, eles não podem garantir que você obterá êxito em uma auditoria do PIC DSS. AWS Audit Manager não verifica automaticamente os controles processuais que exigem a coleta manual de evidências.

Você pode encontrar esse framework na guia Framework padrão do Biblioteca framework no Audit Manager.

Para obter informações sobre como criar uma avaliação usando esse framework, consulte Como criar uma avaliação.

Quando você usa o console do Audit Manager para criar uma avaliação a partir desse framework padrão, a lista de Serviços da AWS no escopo é selecionada por padrão e não pode ser editada. Isso ocorre porque o Audit Manager mapeia e seleciona automaticamente as fontes de dados e os serviços para você. Essa seleção é feita de acordo com os requisitos do framework PCI DSS V3.2.1. Se você precisar editar a lista de serviços no escopo desse framework, poderá fazer isso usando as operações da API CreateAssessment ou UpdateAssessment. Como alternativa, você pode personalizar o framework padrão e, em seguida, criar uma avaliação a partir do framework personalizado.

Para obter instruções sobre como personalizar esse framework para atender às suas necessidades específicas, consulte Como personalizar um framework existente e Como personalizar um controle existente.

Mais atributos PCI DSS

- Conselho de Normas de Segurança da Indústria de Meios de Pagamento
- Biblioteca de documentos do Conselho de Normas de Segurança da Indústria de Meios de Pagamento.
- AWS Página de conformidade do PCI DSS

PCI DSS V4.0

O AWS Audit Manager fornece um framework pré-criado compatível com o Payment Card Industry Data Security Standard (PCI DSS) v4.0.

> **Note**
>
> Para obter informações sobre o PCI DSS v3.2.1 e o framework do Audit Manager compatível com ele, consulte PCI DSS V3.2.1.

Tópicos

O que é PCI DSS?

O PCI DSS (Padrão de segurança de dados do setor de cartões de pagamento) é um padrão global que fornece uma referência de requisitos técnicos e operacionais para a proteção de dados de pagamento. O PCI DSS v4.0 é a próxima evolução do padrão.

O PCI DSS foi desenvolvido para incentivar e aprimorar a segurança dos dados das contas de cartões de pagamento. Ele também facilita a ampla adoção de medidas consistentes de segurança de dados no mundo inteiro. Ele fornece uma referência de requisitos técnicos e operacionais projetados para proteger os dados das contas. Embora tenha sido projetado especificamente para se concentrar em ambientes com dados de contas de cartões de pagamento, o PCI DSS também pode ser usado para proteção contra ameaças e para proteger outros elementos no ecossistema de pagamento.

O PCI SSC (Padrão de segurança de dados do setor de cartões de pagamento) introduziu muitas mudanças entre o PCI DSS v3.2.1 e v4.0. Essas atualizações se dividem em três categorias:

1. Requisito de evolução: mudanças para garantir que o padrão esteja atualizado com as ameaças e tecnologias emergentes e com as alterações no setor de pagamentos. Os exemplos incluem requisitos ou procedimentos de teste novos ou modificados ou a remoção de um requisito.

2. Esclarecimento ou orientação: atualizações no texto, na explicação, na definição, em orientações adicionais ou em instruções para aumentar a compreensão ou fornecer mais informações ou orientações sobre um tópico específico.
3. Estrutura ou formato: reorganização do conteúdo, incluindo combinação, separação e renumeração dos requisitos para alinhar o conteúdo.

Para obter mais informações sobre as alterações, consulte o Summary of changes from PCI DSS Version 3.2.1 to 4.0.

Como usar esse framework para apoiar sua preparação para auditoria

> **Note**
>
> Esse framework padrão usa controles consolidados do Security Hub como fonte de dados. Para coletar com êxito evidências de controles consolidados, ative a configuração de descobertas de controles consolidados no Security Hub. Para obter mais informações sobre como usar o Security Hub como um tipo de fonte de dados, consulte AWS Security Hub controls supported by AWS Audit Manager.

Você pode usar o framework do PCI DSS V4.0 para ajudar na preparação para as auditorias. esse framework inclui uma coleção pré-construída de controles com descrições e procedimentos de teste. Esses controles são agrupados em conjuntos de acordo com os requisitos do PCI DSS V4.0. Você também pode personalizar esse framework e seus controles para apoiar auditorias internas com requisitos específicos.

Usando o framework como ponto de partida, você pode criar uma avaliação do Audit Manager e começar a coletar evidências relevantes para sua auditoria. Depois de criar uma avaliação, o Audit Manager começa a avaliar seus atributos AWS. Ele faz isso com base nos controles definidos no framework do PCI DSS V4.0. Na hora de fazer uma auditoria, você ou um representante de sua escolha pode analisar as evidências que o Audit Manager coletou. Como alternativa, você pode navegar pelas pastas de evidências na sua avaliação e escolher quais evidências deseja incluir no relatório de avaliação. Ou, se você ativou o localizador de evidências, pode pesquisar evidências específicas e exportá-las no formato CSV ou criar um relatório de avaliação baseado nos resultados da pesquisa. De qualquer uma das formas, você pode usar esse relatório de avaliação para mostrar que seus controles estão funcionando conforme o esperado.

Os detalhes do framework são:

Nome do framework em AWS Audit Manager	Número de controles automatizados	Número de controles manuais	Número de conjuntos de controle	Serviços da AWS em escopo
PCI DSS v4.0	152	128	15	• Amazon API Gateway • Amazon CloudFront • Amazon CloudWatch • Amazon DynamoDB • Amazon Elastic Compute Cloud • Amazon OpenSearch Service • Amazon Redshift • Amazon Relationa l Database Service • Amazon SageMaker • Amazon Simple Storage Service • AWS Backup • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS KMS

Nome do framework em AWS Audit Manager	Número de controles automatizados	Número de controles manuais	Número de conjuntos de controle	Serviços da AWS em escopo
				• AWS Secrets Manager • AWS Security Hub • AWS WAF

> **Tip**
>
> Para analisar as regras do AWS Config usadas como mapeamentos de fonte de dados nesse framework padrão, baixe o arquivo AuditManager_ConfigDataSourceMappings_PCI-DSS-V4.zip.

Os controles nesse framework AWS Audit Manager não se destinam a verificar se seus sistemas estão em conformidade com o padrão PCI DSS. Além disso, eles não podem garantir que você obterá êxito em uma auditoria do PIC DSS. AWS Audit Manager não verifica automaticamente os controles processuais que exigem a coleta manual de evidências.

Você pode encontrar esse framework na guia Framework padrão do Biblioteca framework no Audit Manager.

Para obter informações sobre como criar uma avaliação usando esse framework, consulte Como criar uma avaliação.

Quando você usa o console do Audit Manager para criar uma avaliação a partir desse framework padrão, a lista de Serviços da AWS no escopo é selecionada por padrão e não pode ser editada. Isso ocorre porque o Audit Manager mapeia e seleciona automaticamente as fontes de dados e os serviços para você. Essa seleção é feita de acordo com os requisitos do framework do PCI DSS V4. Se você precisar editar a lista de serviços no escopo desse framework, poderá fazer isso usando as operações da API CreateAssessment ou UpdateAssessment. Como alternativa, você pode personalizar o framework padrão e, em seguida, criar uma avaliação a partir do framework personalizado.

Para obter instruções sobre como personalizar esse framework para atender às suas necessidades específicas, consulte Como personalizar um framework existente e Como personalizar um controle existente.

Mais atributos PCI DSS

- Hub de recursos do PCI DSS v4.0
- Conselho de Normas de Segurança da Indústria de Meios de Pagamento
- Biblioteca de documentos do Conselho de Normas de Segurança da Indústria de Meios de Pagamento.
- AWS Página de conformidade do PCI DSS
- Payment Card Industry Data Security Standard (PCI DSS) v4.0 on AWS Compliance Guide
- Resumo das alterações da versão 3.2.1 para 4.0 do PCI DSS

SOC 2

O SOC 2 é um procedimento de auditoria que garante que os dados de uma empresa sejam gerenciados com segurança. AWS Audit Manager fornece um framework pré-construído que oferece suporte ao SOC 2.

Tópicos

- O que é o SOC 2?
- Como usar esse framework para apoiar sua preparação para auditoria
- Mais atributos do SOC 2

O que é o SOC 2?

Controles de Sistema e Organização (SOC), definidos pelo Instituto Americano de Contadores Públicos Certificados (AICPA), é o nome de um conjunto de relatórios produzidos durante uma auditoria. É usado por organizações de serviços (que fornecem sistemas de informação como serviço para outras organizações) para emitir relatórios validados de controles internos sobre esses sistemas de informação para usuários desses serviços. Os relatórios focam em controles agrupados em cinco categorias conhecidas como Princípios do Serviço de Confiança.

Relatórios SOC AWS são relatórios de exame independentes de terceiros que demonstram como a AWS atinge os principais controles e objetivos de conformidade. O objetivo desses relatórios é ajudar

você e seus auditores a compreenderem os controles AWS estabelecidos para oferecer suporte às operações e conformidade. Há cinco relatórios SOC AWS:

- AWS Relatório SOC 1, disponível para clientes AWS de AWS Artifact.
- AWS Relatório de Segurança, Disponibilidade e Confidencialidade SOC 2, disponível para clientes AWS de AWS Artifact.
- AWS Relatório de Segurança, Disponibilidade e Confidencialidade SOC 2, disponível para clientes AWS de AWS Artifact (o escopo inclui apenas Amazon DocumentDB).
- AWS Relatório de Privacidade SOC 2 tipo I, disponível para clientes AWS de AWS Artifact.
- AWSRelatório de Segurança, Disponibilidade e Confidencialidade SOC 3, disponível publicamente como relatório .

Como usar esse framework para apoiar sua preparação para auditoria

Você pode usar esse framework para ajudá-lo a se preparar para as auditorias. esse framework inclui uma coleção pré-construída de controles com descrições e procedimentos de teste. Esses controles são agrupados em conjuntos de controle de acordo com os requisitos do SOC 2. Você também pode personalizar esse framework e seus controles para apoiar auditorias internas com requisitos específicos.

Usando o framework como ponto de partida, você pode criar uma avaliação do Audit Manager e começar a coletar evidências relevantes para sua auditoria. Depois de criar uma avaliação, o Audit Manager começa a avaliar seus atributos AWS. Ele faz isso com base nos controles definidos no framework. Na hora de fazer uma auditoria, você ou um representante de sua escolha pode analisar as evidências que o Audit Manager coletou. Como alternativa, você pode navegar pelas pastas de evidências na sua avaliação e escolher quais evidências deseja incluir no relatório de avaliação. Ou, se você ativou o localizador de evidências, pode pesquisar evidências específicas e exportá-las no formato CSV ou criar um relatório de avaliação baseado nos resultados da pesquisa. De qualquer uma das formas, você pode usar esse relatório de avaliação para mostrar que seus controles estão funcionando conforme o esperado.

Os detalhes do framework são:

Nome do framework em AWS Audit Manager	Número de controles automatizados	Número de controles manuais	Número de conjuntos de controle	Serviços da AWS em escopo
SOC 2	20	41	20	• Amazon Elastic Compute Cloud • AWS Auto Scaling • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Security Hub

> **Tip**
>
> Para analisar as regras AWS Config usadas como mapeamentos de fontes de dados nesse framework padrão, baixe o arquivo AuditManager_ConfigDataSourceMappings_SOC2.zip.

Os controles nesse framework AWS Audit Manager não se destinam a verificar se seus sistemas estão em conformidade. Além disso, eles não podem garantir que você obterá êxito em uma auditoria. AWS Audit Manager não verifica automaticamente os controles processuais que exigem a coleta manual de evidências.

Você pode encontrar esse framework na guia Framework padrão do Biblioteca framework no Audit Manager.

Para obter instruções sobre como criar uma avaliação usando esse framework, consulte Como criar uma avaliação.

Quando você usa o console do Audit Manager para criar uma avaliação a partir desse framework padrão, a lista de Serviços da AWS no escopo é selecionada por padrão e não pode ser editada. Isso ocorre porque o Audit Manager mapeia e seleciona automaticamente as fontes de dados e

os serviços para você. Essa seleção é feita de acordo com os requisitos SOC 2. Se você precisar editar a lista de serviços no escopo desse framework, poderá fazer isso usando as operações da API CreateAssessment ou UpdateAssessment. Como alternativa, você pode personalizar o framework padrão e, em seguida, criar uma avaliação a partir do framework personalizado.

Para obter instruções sobre como personalizar esse framework para atender às suas necessidades específicas, consulte Como personalizar um framework existente e Como personalizar um controle existente.

Mais atributos do SOC 2

- Página de conformidade AWS para SOC

Biblioteca de controle

Você pode acessar e gerenciar controles da biblioteca de controle no Audit Manager. Você pode acessar a biblioteca de controle quando quiser escolhendo Biblioteca de controle no painel de navegação no console do Audit Manager.

A biblioteca de controle contém um catálogo de controles padrão e controles personalizados.

- Controles padrão são controles predefinidos fornecidos pelo AWS. Você pode ver os detalhes da configuração dos controles padrão, mas não pode editá-los nem excluí-los. No entanto, você pode personalizar qualquer controle padrão para criar um novo que atenda aos seus requisitos específicos.
- Controles personalizados são controles personalizados que você possui e define. Com um controle personalizado, você pode especificar de quais fontes de dados deseja coletar evidências. Em seguida, você pode adicionar controles personalizados a uma estrutura personalizada.

  Para saber mais sobre como adicionar um controle personalizado a uma estrutura personalizada, consulte Biblioteca framework. Para saber mais sobre como criar uma avaliação a partir de uma estrutura do Audit Manager, consulte Avaliações em AWS Audit Manager.

Esta seção descreve como você pode criar e gerenciar controles personalizados no Audit Manager.

Tópicos

Acessar os controles disponíveis em AWS Audit Manager

Você pode ver todos os controles disponíveis na página da Biblioteca de controles no console do Audit Manager. A partir daqui, você também pode criar um controle personalizado ou personalizar um controle existente.

Você também pode visualizar todos os controles disponíveis usando a API Audit Manager ou o AWS Command Line Interface (AWS CLI).

Audit Manager console

Para visualizar controles disponíveis (console)

1. Abra o console do AWS Audit Manager em https://console.aws.amazon.com/auditmanager/home.
2. No painel de navegação, selecione Biblioteca de controles.
3. Escolha a guia Controles padrão ou a guia Controles personalizados para navegar pelos controles disponíveis.
4. Para exibir os detalhes de um controle, selecione o nome do controle.

AWS CLI

Para visualizar os controles disponíveis (AWS CLI)

Execute o comando list-controls e especifique um `--control-type`. Ou você pode recuperar uma lista de controles padrão. Ou você pode recuperar uma lista de controles personalizados.

```
aws auditmanager list-controls --control-type Standard
```

```
aws auditmanager list-controls --control-type Custom
```

Audit Manager API

Para visualizar os controles disponíveis (API)

Use a ListControlsoperação e especifique um ControlType. Ou você pode retornar uma lista de controles padrão. Ou você pode retornar uma lista de controles personalizados.

Para obter mais informações, escolha um dos links anteriores para ler mais na Referência de APIAWS Audit Manager . Isso inclui informações sobre como usar a `ListControls` operação e os parâmetros em um dos SDKs específicos do idioma AWS .

Revisar os detalhes de um controle

Você pode revisar os detalhes de um controle usando o console do Audit Manager, a API do Audit Manager ou o AWS Command Line Interface (AWS CLI).

Audit Manager console

Para visualizar detalhes de um controle (console)

1. Abra o console do AWS Audit Manager em https://console.aws.amazon.com/auditmanager/home.
2. No painel de navegação, escolha Biblioteca de controle para visualizar uma lista dos controles disponíveis.
3. Escolha a guia Controles padrão ou a guia Controles personalizados para navegar pelos controles disponíveis.
4. Para exibir os detalhes de um controle, selecione o nome do controle.

Ao abrir um controle, você vê uma página de detalhes do controle. As seções desta página e seu conteúdo estão descritos abaixo.

Seção de resumo

Esta seção fornece uma visão geral do controle. Isso inclui as informações a seguir:

- Nome do controle — O nome do controle.
- Tipo de controle — Especifica se o controle é um controle padrão ou personalizado.
- Tags — O número de tags associadas ao controle.
- Tipos de fonte de dados — O número de tipos de fonte de dados usados para esse controle.
- Mapeamentos — O número de atributos de mapeamento usados para recuperar dados de uma fonte de dados.

Se você estiver visualizando um controle personalizado, os seguintes detalhes também serão exibidos:

- Criado por — A conta que criou o controle personalizado.
- Data de criação — A data em que o controle personalizado foi criado.
- Última atualização — A data em que o controle personalizado foi editado pela última vez.

Guia de detalhes

Essa guia fornece uma visão geral básica do controle. Isso inclui as informações a seguir:

- A seção Descrição fornece uma descrição do controle.
- A seção Informações de teste fornece uma descrição dos procedimentos de teste recomendados para o controle.
- A seção Plano de ação descreve as ações recomendadas a serem executadas se o controle precisar ser remediado.

Guia de fontes de dados

Essa guia exibe informações sobre as fontes de dados do controle. Isso inclui as informações a seguir:

- Nome da fonte de dados — Isso se aplica somente aos controles personalizados. Refere-se ao nome descritivo que você deu a cada fonte de dados. Você pode usar esse nome para distinguir entre várias fontes de dados que se enquadram no mesmo tipo de fonte de dados.
- Tipo de fonte de dados de — Especifica de onde vêm os dados de evidência.
  - Se o Audit Manager coletar as evidências, a fonte de dados poderá ser de um dos quatro tipos: AWS Security Hub, AWS Config, AWS CloudTrail ou AWS chamadas de API.
  - Se você carregar sua própria evidência, o tipo de fonte de dados será Manual. Uma descrição indica se a evidência manual necessária é um carregamento de arquivo ou uma resposta em texto.
- Mapeamento — Esse é o atributo de mapeamento usado para identificar e recuperar dados da fonte de dados.
  - Se o tipo da fonte de dados for AWS Config, o mapeamento será o nome de uma AWS Config regra específica (por exemplo,`EC2_INSTANCE_MANAGED_BY_SSM`). O Audit Manager usa esse mapeamento para relatar o resultado dessa verificação de regras diretamente de AWS Config.
  - Se o tipo de fonte de dados for AWS Security Hub, o mapeamento será o nome de um controle específico do Security Hub (por exemplo,`1.1 – Avoid the use of the`

`"root" account`). O Audit Manager usa esse mapeamento para relatar o resultado dessa verificação de segurança diretamente do Hub de Segurança.

- Se o tipo de fonte de dados for chamadas de AWS API, o mapeamento será o nome de uma chamada de API específica (por exemplo,`ec2_DescribeSecurityGroups`). O Audit Manager usa esse mapeamento para coletar a resposta da API.
- Se a fonte de dados for AWS CloudTrail, o mapeamento será o nome de um CloudTrail evento específico (por exemplo,`CreateAccessKey`). O Audit Manager usa esse mapeamento para coletar a atividade relacionada do usuário em seus CloudTrail registros.

- Frequência — Especifica com que frequência o Audit Manager coleta evidências da fonte de dados. A frequência varia de acordo com o tipo de fonte de dados. Para obter mais informações, escolha o valor na coluna ou consulte Frequência das coletas de evidências.

Guia Tags

Essa guia lista as tags associadas ao controle. Isso inclui as informações a seguir:

- Chave — A chave da tag (por exemplo, um padrão de conformidade, um regulamento ou uma categoria).
- Valor — O valor da tag.

AWS CLI

Para visualizar detalhes do controle (AWS CLI)

1. Para identificar o controle que você deseja revisar, execute o comando list-controls e especifique uma `--control-type`. Ou você pode recuperar uma lista de controles padrão. Ou você pode recuperar uma lista de controles personalizados.

   No exemplo a seguir, substitua o *`texto do espaço reservado`* por `Custom` ou `Standard`.

   ```
   aws auditmanager list-controls --control-type Custom/Standard
   ```

   A resposta retorna uma lista de controles. Encontre o controle que você deseja revisar e anote o ID do controle e o nome do recurso da Amazon (ARN).
2. Para obter os detalhes do controle, execute o comando get-control e especifique o `--control-id`.

No exemplo a seguir, substitua o *texto do espaço reservado* por suas próprias informações.

```
aws auditmanager get-control --control-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Os detalhes do controle são devolvidos no formato JSON. Para entender esses dados, consulte a saída get-control na Referência deAWS CLI comandos.

3. Para ver as tags de um controle, use o list-tags-for-resourcecomando e especifique o `--resource-arn` para o controle.

   No exemplo a seguir, substitua o *texto do espaço reservado* por suas próprias informações.

   ```
   aws auditmanager list-tags-for-resource --resource-arn arn:aws:auditmanager:us-east-1:111122223333:control/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
   ```

   Para obter mais informações sobre tags no Audit Manager, consulte Recursos de AWS Audit Manager para tags

Audit Manager API

Para visualizar detalhes do controle (API)

1. Para identificar o controle que você deseja revisar, use a ListControlsoperação e especifique um ControlType. Ou você pode retornar uma lista de controles padrão. Ou você pode retornar uma lista de controles personalizados.

   Na resposta, encontre o controle que você deseja revisar e anote o ID do controle e o nome do recurso da Amazon (ARN).

2. Para obter os detalhes do controle, use a GetControloperação. Na solicitação, especifique o ControlId que você obteve na etapa 1.

   Os detalhes do controle são devolvidos no formato JSON. Para entender esses dados, consulte Elementos de GetControl resposta na ReferênciaAWS Audit Manager da API.

3. Para ver as tags do controle, use a ListTagsForResourceoperação. Na solicitação, especifique o recurso de controle ResourceArn obtido na etapa 1.

Para obter mais informações sobre tags no Audit Manager, consulte Recursos de AWS Audit Manager para tags

Para obter mais informações sobre essas operações de API, escolha qualquer um dos links anteriores para ler mais na Referência de APIAWS Audit Manager . Isso inclui informações sobre como usar essas operações e parâmetros em um dos SDKs específicos do idioma AWS .

Criar um controle personalizado

Você pode usar controles personalizados para coletar evidências de fontes de dados específicas que você define.

Assim como os controles padrão, os controles personalizados coletam evidências continuamente quando estão ativos em suas avaliações. Você também pode adicionar evidências manuais a qualquer controle personalizado que você criar. Cada evidência se torna um registro que ajuda você a demonstrar conformidade com os requisitos de seu controle personalizado.

Para começar, veja a seguir alguns exemplos de como você pode usar controles personalizados:

Use um controle existente como ponto de partida

Você pode personalizar qualquer controle no Audit Manager. Essa é uma boa opção se um controle existente atender mais ou menos ao seu objetivo, mas você deseja ampliar sua orientação ou ajustar alguns atributos para atender às suas necessidades específicas. Por exemplo, você pode alterar a frequência com que um controle coleta evidências e, em seguida, alterar o nome do controle para refletir isso.

Crie um controle personalizado para auditorias internas

Para apoiar as auditorias internas, você pode criar um controle personalizado específico que não esteja relacionado a nenhuma estrutura ou regulamentação de conformidade específica. Isso lhe dá a liberdade de adaptar os requisitos de seu controle a uma área específica ou coletar evidências de um recurso específico da empresa. Por exemplo, você pode criar um controle personalizado que usa AWS Config as regras personalizadas da sua organização como fonte de dados para coleta de evidências.

Crie uma pergunta de avaliação de risco do fornecedor

Você pode usar controles personalizados para apoiar a forma como você gerencia as avaliações de risco do fornecedor. Cada controle que você cria pode representar uma pergunta individual de

avaliação de risco. Nesse caso, o nome do controle pode ser uma pergunta e você pode fornecer uma resposta fazendo o upload de um arquivo ou inserindo uma resposta em texto como prova manual.

Há duas maneiras de criar um controle personalizado. Você pode criar um novo controle do zero ou personalizar um controle existente.

Tópicos

- Criar um novo controle personalizado do zero
- Personalizar um controle existente

Criar um novo controle personalizado do zero

Você pode criar um novo controle personalizado do zero seguindo estas etapas.

> **Important**
>
> É altamente recomendável que você nunca coloque informações de identificação confidenciais em campos de formato livre, como Detalhes de controle, Informações de teste ou Plano de ação. Se você criar controles personalizados que contenham informações confidenciais, não poderá compartilhar nenhuma das estruturas personalizadas que contenham esses controles.

Tópicos

- Etapa 1: especificar detalhes do controle
- Etapa 2: configurar fontes de dados
- Etapa 3 (opcional): definir um plano de ação
- Etapa 4: analisar e criar o controle
- O que faço agora?

Etapa 1: especificar detalhes do controle

Comece especificando os detalhes do seu controle personalizado.

Para especificar detalhes do controle

1. Abra o console do AWS Audit Manager em https://console.aws.amazon.com/auditmanager/home.
2. No painel de navegação, escolha Biblioteca de controle e, em seguida, escolha Criar controle personalizado.
3. Em Detalhes do controle, insira as seguintes informações sobre o controle.
   - Controle — Insira um nome fácil, um título ou uma pergunta de avaliação de risco. Esse valor ajuda você a identificar seu controle na biblioteca de controle.
   - Descrição (opcional) — Insira detalhes para ajudar outras pessoas a entender o objetivo do controle. Essa descrição aparece na página de detalhes do controle.
4. Em Informações de teste, insira as etapas recomendadas para testar o controle.
5. Em Tags, escolha Adicionar nova tag para associar uma tag ao controle. Você pode especificar uma chave para cada tag que melhor descreva a estrutura de conformidade que esse controle suporta. A chave de tag é obrigatória e pode ser usada como critério de pesquisa ao pesquisar esse controle na biblioteca de controle.
6. Escolha Próximo.

Etapa 2: configurar fontes de dados

Em seguida, defina até 10 fontes de dados. Uma fonte de dados determina de onde seu controle personalizado coleta evidências.

Se você quiser coletar evidências automatizadas, cada fonte de dados deve incluir um tipo de fonte de dados e um mapeamento da fonte de dados. Esses detalhes são mapeados de acordo com seu AWS uso e informam ao Audit Manager de onde coletar as evidências. Se, em vez disso, quiser fornecer sua própria evidência, nomeie sua fonte de dados e escolha uma opção de evidência manual.

> **Important**
>
> Para usar AWS Config com sucesso o Security Hub como fontes de dados automatizadas, faça o seguinte:
>
> - Siga as instruções para configurar AWS Config e configurar o Security Hub para uso com o Audit Manager.

- Inclua o Security Hub AWS Config e o Security Hub como serviços no escopo em sua avaliação.

O Audit Manager pode então coletar evidências sempre que ocorrer uma avaliação das AWS Config regras ou dos controles do Security Hub que você especificar nesta etapa.

Como configurar fontes de dados

1. Em Nome da fonte de dados, substitua o texto do espaço reservado por um nome descritivo para a fonte de dados.
2. Em Método de coleta de evidências, escolha como você deseja coletar evidências para esse controle.

   a. Se você quiser que o Audit Manager colete evidências, escolha Automatizado e siga estas etapas:

   - Em Tipo de fonte de dados, especifique de onde o Audit Manager coleta evidências automatizadas.
     - Para AWS CloudTrail, escolha uma palavra-chave para o nome do evento na lista suspensa.
     - Para AWS Config, selecione um tipo de regra e, em seguida, escolha uma palavra-chave identificadora de regra na lista suspensa.
     - Para AWS Security Hub, escolha um controle do Security Hub na lista suspensa.
     - Para chamadas de APIAWS , escolha uma chamada de API e, em seguida, selecione uma frequência de coleta de evidências.

     > **Tip**
     >
     > Para obter uma visão geral de cada tipo de fonte de dados e dicas de solução de problemas relacionadas, consulte Visão geral das fontes de dados automatizadas.
     > Se você precisar validar a configuração da fonte de dados com um especialista no domínio, defina o método de coleta de evidências como Manual por enquanto. Dessa forma, você pode criar o controle e adicioná-lo a uma estrutura agora e depois editar o controle conforme necessário posteriormente.

b. Se você quiser fornecer sua própria evidência, escolha Manual e selecione a opção Evidência manual.

- Upload de arquivo — Selecione essa opção se o controle exigir documentação como evidência.
- Resposta de texto — Selecione essa opção se o controle exigir uma resposta para uma pergunta de avaliação de risco.

3. (Opcional) Em Detalhes adicionais, insira uma descrição da fonte de dados e uma descrição da solução de problemas.
4. (Opcional) Para adicionar outra fonte de dados, escolha Add data source e repita as etapas 1 a 3.
5. (Opcional) Para remover uma fonte de dados, escolha Remover na parte superior da caixa de configuração da fonte de dados.
6. Quando terminar, escolha Próximo.

Etapa 3 (opcional): definir um plano de ação

Em seguida, especifique as ações a serem tomadas se esse controle precisar ser corrigido.

Para definir um plano de ação

1. Em Título, insira um título descritivo para o plano de ação.
2. Em Instruções do plano de ação, insira instruções detalhadas para o plano de ação.
3. Escolha Próximo.

Etapa 4: analisar e criar o controle

Revise as informações do controle. Para alterar as informações de uma etapa, selecione Editar.

Quando terminar, escolha Criar controle personalizado.

O que faço agora?

Depois de criar um novo controle personalizado, você pode adicioná-lo a uma estrutura personalizada. Para saber mais, consulte Criando criar um framework personalizado ou Como editar um framework personalizado.

Depois de adicionar o controle personalizado a uma estrutura personalizada, você pode criar uma avaliação a partir dessa estrutura personalizada e começar a coletar evidências. Para saber mais, consulte Como criar uma avaliação.

Para obter dicas de solução de problemas, consulte Solução de problemas de controle e conjunto de controles.

Personalizar um controle existente

Em vez de criar um controle personalizado do zero, você pode usar um controle existente como ponto de partida e personalizá-lo de acordo com suas necessidades. Quando você faz isso, o controle existente permanece na biblioteca de controle e um novo controle personalizado é criado com suas configurações personalizadas.

Você pode selecionar qualquer controle existente para personalizar. Pode ser um controle padrão ou um controle personalizado.

> **Important**
>
> É altamente recomendável que você nunca coloque informações de identificação confidenciais em campos de formato livre, como Detalhes de controle, Informações de teste ou Plano de ação. Se você criar controles personalizados que contenham informações confidenciais, não poderá compartilhar nenhuma das estruturas personalizadas que contenham esses controles.

Tópicos

Etapa 1: especificar detalhes do controle

Os detalhes do controle são herdados do controle original. Analise e modifique esses detalhes conforme necessário.

Para especificar detalhes do controle

1. Abra o console do AWS Audit Manager em https://console.aws.amazon.com/auditmanager/home.
2. No painel de navegação, selecione Biblioteca de controle.
3. Selecione o controle que você deseja personalizar e, em seguida, escolha Personalizar o controle existente.
4. Especifique o novo nome do controle e escolha Personalizar.
5. Em Detalhes do controle, personalize os detalhes do controle conforme necessário.
6. Em Informações de teste, personalize as informações de teste conforme necessário.
7. Em Tags, personalize as tags conforme necessário.
8. Escolha Próximo.

Etapa 2: configurar fontes de dados

As fontes de dados são herdadas do controle original. Você pode alterar, adicionar ou remover fontes de dados conforme necessário.

> **Important**
>
> Para usar AWS Config com sucesso o Security Hub como fontes de dados automatizadas, faça o seguinte:
>
> - Siga as instruções para configurar AWS Config e configurar o Security Hub para uso com o Audit Manager.
> - Inclua o Security Hub AWS Config e o Security Hub como serviços no escopo em sua avaliação.
>
> O Audit Manager pode então coletar evidências sempre que ocorrer uma avaliação das AWS Config regras ou dos controles do Security Hub que você especificar nesta etapa.

Como configurar fontes de dados

1. Em Nome da fonte de dados, personalize o nome da fonte de dados conforme necessário.
2. Em Método de coleta de evidências, personalize a seleção conforme necessário.

a. Se você quiser que o Audit Manager colete evidências, escolha Automatizado e siga estas etapas:

- Em Tipo de fonte de dados, revise de onde o Audit Manager coleta evidências automatizadas e modifique conforme necessário.
  - Para AWS CloudTrail, escolha uma palavra-chave para o nome do evento na lista suspensa.
  - Para AWS Config, selecione um tipo de regra e, em seguida, escolha uma palavra-chave identificadora de regra na lista suspensa.
  - Para AWS Security Hub, escolha um controle do Security Hub na lista suspensa.
  - Para chamadas de APIAWS , escolha uma chamada de API e, em seguida, selecione uma frequência de coleta de evidências.

> **Tip**
>
> Para obter uma visão geral de cada tipo de fonte de dados e dicas de solução de problemas relacionadas, consulte Visão geral das fontes de dados automatizadas.
> Se você precisar validar a configuração da fonte de dados com um especialista no domínio, defina o método de coleta de evidências como Manual por enquanto. Dessa forma, você pode criar o controle e adicioná-lo a uma estrutura agora e depois editar o controle conforme necessário posteriormente.

b. Se você quiser fornecer sua própria evidência, escolha Manual e selecione a opção Evidência manual.

- Upload de arquivo — Selecione essa opção se o controle exigir documentação como evidência.
- Resposta de texto — Selecione essa opção se o controle exigir uma resposta para uma pergunta de avaliação de risco.

3. (Opcional) Em Detalhes adicionais, faça as alterações necessárias na descrição da fonte de dados ou na descrição da solução de problemas.
4. (Opcional) Para adicionar outra fontes de dados, escolha Adicionar fonte de dados.
5. (Opcional) Para remover uma fonte de dados, escolha Remover.
6. Escolha Próximo.

Etapa 3: (opcional): definir um plano de ação

O plano de ação é herdado do controle original. Você pode editar esse plano de ação conforme necessário.

Para definir um plano de ação

1. Em Título, revise o título do plano de ação e personalize-o conforme necessário.
2. Em Instruções do plano de ação, revise e personalize as instruções conforme necessário.
3. Escolha Próximo.

Etapa 4: analisar e criar o controle

Revise as informações do controle. Para alterar as informações de uma etapa, selecione Editar. Quando terminar, escolha Criar controle personalizado.

O que faço agora?

Depois de criar um novo controle personalizado, você pode adicioná-lo a uma estrutura personalizada. Para saber mais, consulte Criando criar um framework personalizado ou Como editar um framework personalizado.

Depois de adicionar um controle personalizado a uma estrutura personalizada, você pode criar uma avaliação a partir dessa estrutura personalizada e começar a coletar evidências. Para saber mais, consulte Como criar uma avaliação.

Se você precisar editar um controle personalizado, consulteEditar um controle personalizado.

Para obter dicas de solução de problemas, consulte Solução de problemas de controle e conjunto de controles.

Editar um controle personalizado

Você pode editar um controle personalizado no Audit Manager seguindo estas etapas.

Tópicos

- Etapa 4: revisar e atualizar o controle

Etapa 1: editar detalhes de controle

Comece revisando e editando os detalhes do controle conforme necessário.

Para editar os detalhes do controle

1. Abra o console do AWS Audit Manager em https://console.aws.amazon.com/auditmanager/home.
2. No painel de navegação, escolha Biblioteca de controle e, em seguida, escolha a guia Controles personalizados.
3. Selecione o controle que deseja editar e escolha Editar.
4. Em Detalhes do controle, edite os detalhes do controle conforme necessário.
5. Em Informações de teste, edite as informações de teste recomendadas conforme necessário.
6. Escolha Próximo.

> **Tip**
>
> Para editar as tags de um controle, abra o controle e escolha a Guia Tags. Lá você pode visualizar e editar as tags associadas ao controle.

Etapa 2: editar fontes de dados

Em seguida, você pode editar, remover ou adicionar fontes de dados para o controle.

> **Important**
>
> Para usar AWS Config com sucesso o Security Hub como fontes de dados automatizadas, faça o seguinte:
>
> - Siga as instruções para configurar AWS Config e configurar o Security Hub para uso com o Audit Manager.
> - Inclua o Security Hub AWS Config e o Security Hub como serviços no escopo em sua avaliação.

O Audit Manager pode então coletar evidências sempre que ocorrer uma avaliação das AWS Config regras ou dos controles do Security Hub que você especificar nesta etapa.

Como editar fontes de dados

1. Em Nome da fonte de dados, revise o nome atual e edite-o conforme necessário.
2. Em Método de coleta de evidências, revise a seleção atual e edite conforme necessário.

   a. Se você quiser que o Audit Manager colete evidências, escolha Automatizado e siga estas etapas:

   - Em Tipo de fonte de dados, revise de onde o Audit Manager coleta evidências automatizadas e edite conforme necessário.
     - Para AWS CloudTrail, escolha uma palavra-chave para o nome do evento na lista suspensa.
     - Para AWS Config, selecione um tipo de regra e, em seguida, escolha uma palavra-chave identificadora de regra na lista suspensa.
     - Para AWS Security Hub, escolha um controle do Security Hub na lista suspensa.
     - Para chamadas de APIAWS , escolha uma chamada de API e, em seguida, selecione uma frequência de coleta de evidências.

   > **Tip**
   >
   > Para obter uma visão geral de cada tipo de fonte de dados e dicas de solução de problemas relacionadas, consulte Visão geral das fontes de dados automatizadas.

   b. Se você quiser fornecer sua própria evidência, escolha Manual e selecione a opção Evidência manual.

   - Upload de arquivo — Selecione essa opção se o controle exigir documentação como evidência.
   - Resposta de texto — Selecione essa opção se o controle exigir uma resposta para uma pergunta de avaliação de risco.

3. (Opcional) Em Detalhes adicionais, faça as alterações necessárias na descrição da fonte de dados ou na descrição da solução de problemas.
4. (Opcional) Para adicionar outra fontes de dados, escolha Adicionar fonte de dados.
5. (Opcional) Para remover uma fonte de dados, escolha Remover.
6. Escolha Próximo.

Etapa 3: (opcional) editar um plano de ação

Em seguida, revise e edite o plano de ação opcional.

Para editar um plano de ação

1. Em Título, edite o título conforme necessário.
2. Em Instruções do plano de ação, edite as instruções conforme necessário.
3. Escolha Próximo.

Etapa 4: revisar e atualizar o controle

Revise as informações do controle. Para alterar as informações de uma etapa, selecione Editar.

Ao concluir, escolha Salvar alterações.

> **Note**
>
> Depois de editar um controle, as alterações entram em vigor da seguinte forma em todas as avaliações ativas que incluem o controle:
>
> - Para controles com chamadas de APIAWS como tipo de fonte de dados, as alterações entram em vigor às 00:00 UTC do dia seguinte.
> - Para todos os outros controles, as alterações entram em vigor imediatamente.

Como excluir um controle personalizado

Você pode usar a biblioteca de controle para excluir um controle personalizado indesejado. Depois de excluir um controle, ele não aparece mais na biblioteca de controle. Você também pode excluir

controles personalizados usando a API Audit Manager ou o AWS Command Line Interface (AWS CLI).

> **Important**
>
> Quando você exclui um controle personalizado, essa ação remove o controle de qualquer estrutura ou avaliação personalizada à qual ele esteja relacionado atualmente. Como resultado, o Audit Manager deixará de coletar evidências desse controle personalizado em todas as suas avaliações. Isso inclui avaliações que você criou anteriormente antes de excluir o controle personalizado.

Audit Manager console

Para excluir um controle personalizado (console)

1. Abra o console do AWS Audit Manager em https://console.aws.amazon.com/auditmanager/home.
2. No painel de navegação, escolha Biblioteca de controle e, em seguida, escolha a guia Controles personalizados.
3. Selecione o controle que você deseja excluir e, em seguida, selecione Excluir.
4. Na janela pop-up exibida, escolha Excluir para confirmar a exclusão.

AWS CLI

Para excluir um controle personalizado (AWS CLI)

1. Primeiro, identifique o controle personalizado que você deseja excluir. Para fazer isso, execute o comando list-controls e especifique as `--control-type` como `Custom`.

   ```
   aws auditmanager list-controls --control-type Custom
   ```

   A resposta retorna uma lista de controles personalizados. Encontre o controle que você deseja excluir e anote o ID do controle.
2. Em seguida, execute o comando delete-control e use o parâmetro `--control-id` para especificar o controle que você deseja excluir.

No exemplo a seguir, substitua o *texto do espaço reservado* por suas próprias informações.

```
aws auditmanager delete-control --control-id a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111
```

Audit Manager API

Para excluir um controle personalizado (API)

1. Use a ListControlsoperação e especifique o ControlType como`Custom`. Na resposta, encontre o controle que você deseja excluir e anote o ID do controle.
2. Use a DeleteControloperação para excluir o controle personalizado. Na solicitação, use o parâmetro controlId para especificar o controle que você deseja excluir.

Para obter mais informações sobre essas operações de API, escolha qualquer um dos links anteriores para ler mais na Referência de APIAWS Audit Manager . Isso inclui informações sobre como usar essas operações e parâmetros em um dos SDKs específicos do idioma AWS .

Alterar a frequência de coleta de evidências para um controle

AWS Audit Manager coleta evidências de várias fontes de dados em frequências variadas. A frequência de coleta de evidências compatíveis depende do tipo de evidência coletada para o controle.

- Para chamadas de APIAWS , o Audit Manager coleta evidências usando uma chamada de descrição de API para outra AWS service (Serviço da AWS). Você pode especificar a frequência de coleta de evidências diretamente no Audit Manager (somente para controles personalizados).
- Pois AWS Config, o Audit Manager reporta o resultado de uma verificação de conformidade diretamente de AWS Config. A frequência segue os gatilhos definidos na regra AWS Config .
- Para AWS Security Hub, o Audit Manager relata o resultado de uma verificação de conformidade diretamente do Security Hub. A frequência segue o cronograma da verificação do Security Hub.
- Pois AWS CloudTrail, o Audit Manager coleta evidências continuamente de CloudTrail. Não é possível alterar a frequência desse tipo de evidência.

As seções a seguir fornecem mais informações sobre a frequência de coleta de evidências para cada tipo de fonte de dados de controle e como alterá-la (se aplicável).

Tópicos

Instantâneos de configuração de chamadas de AWS API

> **Note**
>
> O seguinte se aplica apenas a controles personalizados. Você não pode alterar a frequência de coleta de evidências para um controle padrão que usa chamadas de API como fonte de dados.

Se um controle personalizado usa chamadas de AWS API como um tipo de fonte de dados, você pode alterar a frequência de coleta de evidências no Audit Manager seguindo estas etapas.

Para alterar a frequência de coleta de evidências para um controle personalizado com uma fonte de dados de chamadas de API

1. Abra o console do AWS Audit Manager em https://console.aws.amazon.com/auditmanager/home.
2. No painel de navegação, escolha Biblioteca de controle e, em seguida, escolha a guia Controles personalizados.
3. Escolha o controle personalizado que você deseja editar e escolha Editar.
4. Na página Editar detalhes do controle, escolha Avançar.
5. Encontre a caixa da fontes de dados que você deseja editar e verifique se as seguintes informações estão corretas:
   - O método de coleta de evidências é automatizado.
   - O tipo de fonte de dados são AWS chamadas de API.
   - A chamada de API selecionada é aquela para a qual você deseja alterar a frequência.

6. Em Frequência, escolha com que frequência você deseja coletar evidências para o controle personalizado.
7. Repita as etapas 5 e 6 conforme necessário para qualquer fonte de dados de chamada de API adicional que você queira editar.
8. Escolha Próximo.
9. Na página Editar um plano de ação, escolha Avançar.
10. Na página Revisar e atualizar o controle, revise as informações do controle personalizado. Para alterar as informações de uma etapa, selecione Editar.
11. Ao concluir, escolha Salvar alterações.

Depois de editar um controle com AWS chamadas de API como tipo de fonte de dados, as alterações entrarão em vigor às 00:00 UTC do dia seguinte em todas as avaliações ativas que incluem o controle.

Verificações de conformidade de AWS Config

> **Note**
>
> O seguinte se aplica tanto aos controles padrão quanto aos controles personalizados que usam Regras do AWS Config como fonte de dados.

Se um controle for usado AWS Config como tipo de fonte de dados, você não poderá alterar a frequência de coleta de evidências diretamente no Audit Manager. Isso ocorre porque a frequência segue os gatilhos definidos na AWS Config regra.

Há dois tipos de gatilhos para: Regras do AWS Config

1. Alterações na configuração - AWS Config executa avaliações da regra quando determinados tipos de recursos são criados, alterados ou excluídos.
2. Periódico - AWS Config executa avaliações para a regra na frequência que você escolher (por exemplo, a cada 24 horas).

Para saber mais sobre os gatilhos para Regras do AWS Config, consulte Tipos de acionadores no Guia do AWS Config desenvolvedor.

Para obter instruções sobre como gerenciar Regras do AWS Config, consulte Gerenciando suas AWS Config regras.

Verificações de conformidade do Security Hub

> **Note**
>
> O seguinte se aplica tanto aos controles padrão quanto aos controles personalizados que usam as verificações do Security Hub como fonte de dados.

Se um controle usa o Security Hub como um tipo de fonte de dados, você não pode alterar a frequência de coleta de evidências diretamente no Audit Manager. Isso ocorre porque a frequência segue o cronograma das verificações do Security Hub.

- Verificações periódicas são executadas automaticamente em até 12 horas após a execução mais recente. Não é possível alterar a periodicidade.
- Verificações acionadas por alterações são executadas quando o recurso associado muda de estado. Mesmo que o recurso não mude de estado, o estado atualizado para verificações acionadas por alterações é atualizado a cada 18 horas. Isso ajuda a indicar que o controle ainda está habilitado. Em geral, o Security Hub usa regras acionadas por alterações sempre que possível.

Para saber mais, consulte Programação para executar verificações de segurança no Guia do usuárioAWS Security Hub .

Logs de atividades do usuário de AWS CloudTrail

> **Note**
>
> O seguinte se aplica tanto aos controles padrão quanto aos controles personalizados que usam logs de atividades do usuário AWS CloudTrail como fonte de dados.

Você não pode alterar a frequência de coleta de evidências para controles que usam registros de atividades CloudTrail como um tipo de fonte de dados. O Audit Manager coleta esse tipo de CloudTrail evidência de forma contínua. A frequência é contínua porque a atividade do usuário pode acontecer em qualquer hora do dia.

Fontes de dados de controle compatíveis para evidências automatizadas

Ao criar um controle personalizado em AWS Audit Manager, você pode configurar seu controle para coletar evidências automatizadas dos seguintes tipos de fonte de dados:

- AWS CloudTrail
- AWS Security Hub
- AWS Config
- AWS Chamadas de API

Os tópicos a seguir resumem cada um desses tipos de fonte de dados automatizada e listam os AWS Security Hub controles, AWS Config regras e chamadas de AWS API específicos que são suportados pelo Audit Manager.

Tópicos

Visão geral das fontes de dados automatizadas

A tabela a seguir dá uma visão geral de cada tipo de fontes de dados automatizadas.

Tipo de fonte de dado	Descrição	Frequência das coletas de evidências	Para usar esse tipo de fonte de dados...	Quando esse controle está ativo em uma avaliação...	Dicas de solução de problemas relacionadas
AWS CloudTrail	Rastreia uma atividade específica do usuário.	Contínuo.	Selecione na lista de nomes de eventos compatíveis.	O Audit Manager filtra seus CloudTrail registros com base na palavra-chave que você escolher. Os resultados são importados como evidência de atividade do usuário.	Minha avaliação não está coletando evidências de atividades dos usuários do AWS CloudTrail
AWS Config	Captura um instantâneo de sua postura de segurança de recursos relatando as descobertas de.	Com base nos gatilhos definidos na AWS Config regra.	Escolha um tipo de regra e selecione uma regra. • Para regras gerenciadas, selecione na lista de palavras-chave de regras gerenciadas compatíveis. • Para regras personalizadas, selecione na lista das regras disponíveis.	O Audit Manager obtém as descobertas dessa regra diretamente de AWS Config. O resultado é importado como evidência de verificação de conformidade.	Minha avaliação não está coletando evidências de verificação de conformidade do

Tipo de fonte de dado	Descrição	Frequência das coletas de evidências	Para usar esse tipo de fonte de dados...	Quando esse controle está ativo em uma avaliação...	Dicas de solução de problemas relacionadas
	AWS Config				AWS Config AWS Config problemas de integração
AWS Security Hub	Captura um snapshot da sua postura de segurança de recursos relatando as descobertas do Security Hub.	Com base na programação da verificação do Security Hub.	Selecione na lista de IDs de controle do Security Hub compatíveis.	O Audit Manager obtém o resultado da verificação de segurança diretamente do Security Hub. O resultado é importado como evidência de verificação de conformidade.	Minha avaliação não está coletando evidências de verificação de conformidade do AWS Security Hub

Tipo de fonte de dado	Descrição	Frequência das coletas de evidências	Para usar esse tipo de fonte de dados...	Quando esse controle está ativo em uma avaliação...	Dicas de solução de problemas relacionadas
AWS Chama de API	Tira um instantâneo da configuração do seu recurso diretamente por meio de uma chamada de API para o especificado AWS service (Serviço da AWS).	Diariamente, semanalmente ou mensalmente.	Selecione na lista de Chamadas de API compatíveis e, em seguida, selecione sua frequência preferida.	O Audit Manager faz a chamada de API com base na frequência que você especifica. A resposta é importada como evidência de dados de configuração.	Minha avaliação não está coletando evidências de dados de configuração para uma chamada de API da AWS

Regras do AWS Config apoiado por AWS Audit Manager

Você pode usar o Audit Manager para capturar AWS Config avaliações como evidência para auditorias. Ao criar ou editar um controle personalizado, você pode especificar uma ou mais AWS Config regras como mapeamento da fonte de dados para coleta de evidências. AWS Config executa verificações de conformidade com base nessas regras, e o Audit Manager relata os resultados como evidência de verificação de conformidade.

Além das regras gerenciadas, você também pode mapear suas regras personalizadas para uma fonte de dados de controle.

> **Note**
>
> - O Audit Manager não coleta evidências de regras AWS Config vinculadas a serviços, com exceção das regras vinculadas a serviços de pacotes de conformidade e de AWS Organizations. Para obter mais informações, consulte a seção Solucionar problemasdeste guia.
> - O Audit Manager não gerencia AWS Config regras para você. Antes de iniciar a coleta de evidências, recomendamos que você revise os parâmetros atuais da AWS Config regra. Em seguida, valide esses parâmetros em relação aos requisitos da estrutura escolhida. Se necessário, você pode atualizar os parâmetros de uma regra AWS Config para que ela se alinhe aos requisitos da estrutura. Isso ajudará a garantir que suas avaliações coletem as evidências corretas de verificação de conformidade para essa estrutura.
>
> Por exemplo, suponha que você esteja criando uma avaliação para o CIS v1.2.0. Esse framework tem um controle chamado 1.9 – Certifique-se de que a política de senha do IAM exija um comprimento mínimo de 14 ou mais. Em AWS Config, a iam-password-policyregra tem um `MinimumPasswordLength` parâmetro que verifica o tamanho da senha. O valor padrão desse parâmetro é de 14 caracteres. Como resultado, a regra se alinha aos requisitos de controle. Se não estiver usando o valor do parâmetro padrão, verifique se o valor que está usando é igual ou maior que o requisito de 14 caracteres do CIS v1.2.0. Você pode encontrar os detalhes do parâmetro padrão para cada regra gerenciada na documentaçãoAWS Config.

Tópicos

- Usando regras AWS Config gerenciadas com o Audit Manager
- Usando regras AWS Config personalizadas com o Audit Manager
- Solução de problemas AWS Config de integração com o Audit Manager

Usando regras AWS Config gerenciadas com o Audit Manager

Atualmente, 326 regras AWS Config gerenciadas são suportadas pelo Audit Manager. Você pode usar qualquer uma das seguintes palavras-chave de identificador de regra gerenciada ao configurar

uma fonte de dados para um controle personalizado. Para obter mais informações sobre qualquer uma das regras gerenciadas listadas abaixo, escolha um item da lista ou consulte RegrasAWS Config gerenciadas no Guia do usuárioAWS Config .

> **Tip**
>
> Ao escolher uma regra gerenciada no console do Audit Manager durante a criação do controle personalizado, certifique-se de procurar uma das seguintes palavras-chave identificadoras de regras, e não o nome da regra. Para obter informações sobre a diferença entre o nome da regra e o identificador da regra e como encontrar o identificador para uma regra gerenciada, consulte a seção Solução de problemas deste guia do usuário.

Palavras-chave de regras AWS Config gerenciadas suportadas

- ACCESS_KEYS_ROTATED
- ACCOUNT_PART_OF_ORGANIZATIONS
- ACM_CERTIFICATE_EXPIRATION_CHECK
- ACM_CERTIFICATE_RSA_CHECK
- ALB_DESYNC_MODE_CHECK
- ALB_HTTP_DROP_INVALID_HEADER_ENABLED
- ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK
- ALB_WAF_ENABLED
- API_GW_ASSOCIATED_WITH_WAF
- API_GW_CACHE_ENABLED_AND_ENCRYPTED
- API_GW_ENDPOINT_TYPE_CHECK
- API_GW_EXECUTION_LOGGING_ENABLED
- API_GW_SSL_ENABLED
- API_GW_XRAY_ENABLED
- API_GWV2_ACCESS_LOGS_ENABLED
- API_GWV2_AUTHORIZATION_TYPE_CONFIGURED
- APPROVED_AMIS_BY_ID
- APPROVED_AMIS_BY_TAG

Palavras-chave de regras AWS Config gerenciadas suportadas

- APPSYNC_ASSOCIATED_WITH_WAF
- APPSYNC_CACHE_ENCRYPTION_AT_REST
- APPSYNC_LOGGING_ENABLED
- AURORA_LAST_BACKUP_RECOVERY_POINT_CREATED
- AURORA_MYSQL_BACKTRACKING_ENABLED
- AURORA_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- AUTOSCALING_CAPACITY_REBALANCING
- AUTOSCALING_GROUP_ELB_HEALTHCHECK_REQUIRED
- AUTOSCALING_LAUNCH_CONFIG_HOP_LIMIT
- AUTOSCALING_LAUNCH_CONFIG_PUBLIC_IP_DISABLED
- AUTOSCALING_LAUNCHCONFIG_REQUIRES_IMDSV2
- AUTOSCALING_LAUNCH_TEMPLATE
- AUTOSCALING_MULTIPLE_AZ
- AUTOSCALING_MULTIPLE_INSTANCE_TYPES
- BACKUP_PLAN_MIN_FREQUENCY_AND_MIN_RETENTION_CHECK
- BACKUP_RECOVERY_POINT_ENCRYPTED
- BACKUP_RECOVERY_POINT_MANUAL_DELETION_DISABLED
- BACKUP_RECOVERY_POINT_MINIMUM_RETENTION_CHECK
- BEANSTALK_ENHANCED_HEALTH_REPORTING_ENABLED
- CLB_DESYNC_MODE_CHECK
- CLB_MULTIPLE_AZ
- CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED
- CLOUD_TRAIL_ENABLED
- CLOUD_TRAIL_ENCRYPTION_ENABLED
- CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED
- CLOUDFORMATION_STACK_DRIFT_DETECTION_CHECK
- CLOUDFORMATION_STACK_NOTIFICATION_CHECK
- CLOUDFRONT_ACCESSLOGS_ENABLED
- CLOUDFRONT_ASSOCIATED_WITH_WAF

Palavras-chave de regras AWS Config gerenciadas suportadas

- CLOUDFRONT_CUSTOM_SSL_CERTIFICATE
- CLOUDFRONT_DEFAULT_ROOT_OBJECT_CONFIGURED
- CLOUDFRONT_NO_DEPRECATED_SSL_PROTOCOLS
- CLOUDFRONT_ORIGIN_ACCESS_IDENTITY_ENABLED
- CLOUDFRONT_ORIGIN_FAILOVER_ENABLED
- CLOUDFRONT_S3_ORIGIN_ACCESS_CONTROL_ENABLED
- CLOUDFRONT_S3_ORIGIN_NON_EXISTENT_BUCKET
- CLOUDFRONT_SECURITY_POLICY_CHECK
- CLOUDFRONT_SNI_ENABLED
- CLOUDFRONT_TRAFFIC_TO_ORIGIN_ENCRYPTED
- CLOUDFRONT_VIEWER_POLICY_HTTPS
- CLOUDTRAIL_S3_DATAEVENTS_ENABLED
- CLOUDTRAIL_SECURITY_TRAIL_ENABLED
- CLOUDWATCH_ALARM_ACTION_CHECK
- CLOUDWATCH_ALARM_ACTION_ENABLED_CHECK
- CLOUDWATCH_ALARM_RESOURCE_CHECK
- CLOUDWATCH_ALARM_SETTINGS_CHECK
- CLOUDWATCH_LOG_GROUP_ENCRYPTED
- CMK_BACKING_KEY_ROTATION_ENABLED
- CODEBUILD_PROJECT_ARTIFACT_ENCRYPTION
- CODEBUILD_PROJECT_ENVIRONMENT_PRIVILEGED_CHECK
- CODEBUILD_PROJECT_ENVVAR_ AWSCRED_CHECK
- CODEBUILD_PROJECT_LOGGING_ENABLED
- CODEBUILD_PROJECT_S3_LOGS_ENCRYPTED
- CODEBUILD_PROJECT_SOURCE_REPO_URL_CHECK
- CODEDEPLOY_AUTO_ROLLBACK_MONITOR_ENABLED
- CODEDEPLOY_EC2_MINIMUM_HEALTHY_HOSTS_CONFIGURED
- CODEDEPLOY_LAMBDA_ALLATONCE_TRAFFIC_SHIFT_DISABLED
- CODEPIPELINE_DEPLOYMENT_COUNT_CHECK

Palavras-chave de regras AWS Config gerenciadas suportadas

- CODEPIPELINE_REGION_FANOUT_CHECK
- CUSTOM_SCHEMA_REGISTRY_POLICY_ATTACHED
- CW_LOGGROUP_RETENTION_PERIOD_CHECK
- DAX_ENCRYPTION_ENABLED
- DB_INSTANCE_BACKUP_ENABLED
- DESIRED_INSTANCE_TENANCY
- DESIRED_INSTANCE_TYPE
- DMS_REPLICATION_NOT_PUBLIC
- DYNAMODB_AUTOSCALING_ENABLED
- DYNAMODB_IN_BACKUP_PLAN
- DYNAMODB_LAST_BACKUP_RECOVERY_POINT_CREATED
- DYNAMODB_PITR_ENABLED
- DYNAMODB_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- DYNAMODB_TABLE_ENCRYPTED_KMS
- DYNAMODB_TABLE_ENCRYPTION_ENABLED
- DYNAMODB_THROUGHPUT_LIMIT_CHECK
- EBS_IN_BACKUP_PLAN
- EBS_LAST_BACKUP_RECOVERY_POINT_CREATED
- EBS_OPTIMIZED_INSTANCE
- EBS_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- EBS_SNAPSHOT_PUBLIC_RESTORABLE_CHECK
- EC2_CLIENT_VPN_NOT_AUTHORIZE_ALL
- EC2_EBS_ENCRYPTION_BY_DEFAULT
- EC2_IMDSV2_CHECK
- EC2_INSTANCE_DETAILED_MONITORING_ENABLED
- EC2_INSTANCE_MANAGED_BY_SSM
- EC2_INSTANCE_MULTIPLE_ENI_CHECK
- EC2_INSTANCE_NO_PUBLIC_IP
- EC2_INSTANCE_PROFILE_ATTACHED

Palavras-chave de regras AWS Config gerenciadas suportadas

- EC2_LAST_BACKUP_RECOVERY_POINT_CREATED
- EC2_LAUNCH_TEMPLATE_PUBLIC_IP_DISABLED
- EC2_MANAGEDINSTANCE_APPLICATIONS_BLACKLISTED
- EC2_MANAGEDINSTANCE_APPLICATIONS_REQUIRED
- EC2_MANAGEDINSTANCE_ASSOCIATION_COMPLIANCE_STATUS_CHECK
- EC2_MANAGEDINSTANCE_INVENTORY_BLACKLISTED
- EC2_MANAGEDINSTANCE_PATCH_COMPLIANCE_STATUS_CHECK
- EC2_MANAGEDINSTANCE_PLATFORM_CHECK
- EC2_NO_AMAZON_KEY_PAR
- EC2_PARAVIRTUAL_INSTANCE_CHECK
- EC2_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- EC2_SECURITY_GROUP_ATTACHED_TO_ENI
- EC2_SECURITY_GROUP_ATTACHED_TO_ENI_PERIODIC
- EC2 _STOPPED_INSTANCE
- EC2 TOKEN_HOP_LIMIT_CHECK
- EC2_TRANSIT_GATEWAY_AUTO_VPC_ATTACH_DISABLED
- EC2_VOLUME_INUSE_CHECK
- ECR_PRIVATE_IMAGE_SCANNING_ENABLED
- ECR_PRIVATE_LIFECYCLE_POLICY_CONFIGURED
- ECR_PRIVATE_TAG_IMMUTABILITY_ENABLED
- ECS_ _HABILITADO AWSVPC_NETWORKING
- ECS_CONTAINER_INSIGHTS_ENABLED
- ECS_CONTAINERS_NONPRIVILEGED
- ECS_CONTAINERS_READONLY_ACCESS
- ECS_FARGATE_LATEST_PLATFORM_VERSION
- ECS_NO_ENVIRONMENT_SECRETS
- ECS_TASK_DEFINITION_LOG_CONFIGURATION
- ECS_TASK_DEFINITION_MEMORY_HARD_LIMIT
- ECS_TASK_DEFINITION_NONROOT_USER

Palavras-chave de regras AWS Config gerenciadas suportadas

- ECS_TASK_DEFINITION_PID_MODE_CHECK
- ECS_TASK_DEFINITION_USER_FOR_HOST_MODE_CHECK
- DIRETÓRIO EFS_ACCESS_POINT_ENFORCE_ROOT_
- EFS_ACCESS_POINT_ENFORCE_USER_IDENTITY
- EFS_ENCRYPTED_CHECK
- EFS_IN_BACKUP_PLAN
- EFS_LAST_BACKUP_RECOVERY_POINT_CREATED
- EFS_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- EIP_ATTACHED
- EKS_CLUSTER_LOGGING_ENABLED
- EKS_CLUSTER_OLDEST_SUPPORTED_VERSION
- EKS_CLUSTER_SUPPORTED_VERSION
- EKS_ENDPOINT_NO_PUBLIC_ACCESS
- EKS_SECRETS_ENCRYPTED
- ELASTIC_BEANSTALK_LOGS_TO_CLOUDWATCH
- ELASTIC_BEANSTALK_MANAGED_UPDATES_ENABLED
- ELASTICACHE_AUTO_MINOR_VERSION_UPGRADE_CHECK
- ELASTICACHE_RBAC_AUTH_ENABLED
- ELASTICACHE_REDIS_CLUSTER_AUTOMATIC_BACKUP_CHECK
- ELASTICACHE_REPL_GRP_AUTO_FAILOVER_ENABLED
- ELASTICACHE_REPL_GRP_ENCRYPTED_AT_REST
- ELASTICACHE_REPL_GRP_ENCRYPTED_IN_TRANSIT
- ELASTICACHE_REPL_GRP_REDIS_AUTH_ENABLED
- ELASTICACHE_SUBNET_GROUP_CHECK
- ELASTICACHE_SUPPORTED_ENGINE_VERSION
- ELASTICSEARCH_ENCRYPTED_AT_REST
- ELASTICSEARCH_IN_VPC_ONLY
- ELASTICSEARCH_LOGS_TO_CLOUDWATCH
- ELASTICSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK

Palavras-chave de regras AWS Config gerenciadas suportadas

- ELB_ACM_CERTIFICATE_REQUIRED
- ELB_CROSS_ZONE_LOAD_BALANCING_ENABLED
- ELB_CUSTOM_SECURITY_POLICY_SSL_CHECK
- ELB_DELETION_PROTECTION_ENABLED
- ELB_LOGGING_ENABLED
- ELB_PREDEFINED_SECURITY_POLICY_SSL_CHECK
- ELB_TLS_HTTPS_LISTENERS_ONLY
- ELBV2_ACM_CERTIFICATE_REQUIRED
- ELBV2_MULTIPLE_AZ
- EMR_KERBEROS_ENABLED
- EMR_MASTER_NO_PUBLIC_IP
- ENCRYPTED_VOLUMES
- FMS_SHIELD_RESOURCE_POLICY_CHECK
- FMS_WEBACL_RESOURCE_POLICY_CHECK
- FMS_WEBACL_RULEGROUP_ASSOCIATION_CHECK
- FSX_LAST_BACKUP_RECOVERY_POINT_CREATED
- FSX_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- GUARDDUTY_ENABLED_CENTRALIZED
- GUARDDUTY_NON_ARCHIVED_FINDINGS
- IAM_CUSTOMER_POLICY_BLOCKED_ACTIONS
- IAM_GROUP_HAS_USERS_CHECK
- IAM_INLINE_POLICY_BLOCKED_ACTIONS
- IAM_NO_INLINE_POLICY_CHECK
- IAM_PASSWORD_POLICY
- IAM_POLICY_BLACKLISTED_CHECK
- IAM_POLICY_IN_USE
- IAM_POLICY_NO_STATEMENTS_WITH_ADMIN_ACCESS
- IAM_POLICY_NO_STATEMENTS_WITH_FULL_ACCESS
- IAM_ROLE_MANAGED_POLICY_CHECK

Palavras-chave de regras AWS Config gerenciadas suportadas

- IAM_ROOT_ACCESS_KEY_CHECK
- IAM_USER_GROUP_MEMBERSHIP_CHECK
- IAM_USER_MFA_HABILITADO
- IAM_USER_NO_POLICIES_CHECK
- IAM_USER_UNUSED_CREDENTIALS_CHECK
- INCOMING_SSH_DISABLED
- INSTANCES_IN_VPC
- KINESIS_STREAM_ENCRYPTED
- INTERNET_GATEWAY_AUTHORIZED_VPC_ONLY
- KMS_CMK_NOT_SCHEDULED_FOR_DELETION
- LAMBDA_CONCURRENCY_CHECK
- LAMBDA_DLQ_CHECK
- LAMBDA_FUNCTION_PUBLIC_ACCESS_PROHIBITED
- LAMBDA_FUNCTION_SETTINGS_CHECK
- LAMBDA INSIDE_VPC
- LAMBDA_VPC_MULTI_AZ_CHECK
- MACIE_STATUS_CHECK
- MFA_ENABLED_FOR_IAM_CONSOLE_ACCESS
- MQ_AUTOMATIC_MINOR_VERSION_UPGRADE_ENABLED
- MQ_CLOUDWATCH_AUDIT_LOGGING_ENABLED
- MQ_NO_PUBLIC_ACCESS
- MULTI_REGION_CLOUD_TRAIL_ENABLED
- NACL_NO_UNRESTRICTED_SSH_RDP
- NETFW_LOGGING_ENABLED
- NETFW_MULTI_AZ_ENABLED
- NETFW_POLICY_DEFAULT_ACTION_FRAGMENT_PACKETS
- NETFW_POLICY_DEFAULT_ACTION_FULL_PACKETS
- NETFW_POLICY_RULE_GROUP_ASSOCIATED
- NETFW_STATELESS_RULE_GROUP_NOT_EMPTY

Palavras-chave de regras AWS Config gerenciadas suportadas

- NLB_CROSS_ZONE_LOAD_BALANCING_HABILITADO
- NO_UNRESTRICTED_ROUTE_TO_IGW
- OPENSEARCH_ACCESS_CONTROL_ENABLED
- OPENSEARCH_AUDIT_LOGGING_ENABLED
- OPENSEARCH_DATA_NODE_FAULT_TOLERANCE
- OPENSEARCH_ENCRYPTED_AT_REST
- OPENSEARCH_HTTPS_REQUIRED
- OPENSEARCH_IN_VPC_ONLY
- OPENSEARCH_LOGS_TO_CLOUDWATCH
- OPENSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK
- RDS_AUTOMATIC_MINOR_VERSION_UPGRADE_ENABLED
- RDS_CLUSTER_DEFAULT_ADMIN_CHECK
- RDS_CLUSTER_DELETION_PROTECTION_ENABLED
- RDS_CLUSTER_IAM_AUTHENTICATION_ENABLED
- RDS_CLUSTER_MULTI_AZ_ENABLED
- RDS_DB_SECURITY_GROUP_NOT_ALLOWED
- RDS_ENHANCED_MONITORING_ENABLED
- RDS_IN_BACKUP_PLAN
- RDS_INSTANCE_DEFAULT_ADMIN_CHECK
- RDS_INSTANCE_DELETION_PROTECTION_ENABLED
- RDS_INSTANCE_IAM_AUTHENTICATION_ENABLED
- RDS_INSTANCE_PUBLIC_ACCESS_CHECK
- RDS_LAST_BACKUP_RECOVERY_POINT_CREATED
- RDS_LOGGING_ENABLED
- RDS_MULTI_AZ_SUPPORT
- RDS_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- RDS_SNAPSHOT_ENCRYPTED
- RDS_SNAPSHOTS_PUBLIC_PROHIBITED
- RDS_STORAGE_ENCRYPTED

Palavras-chave de regras AWS Config gerenciadas suportadas

- REDSHIFT_BACKUP_ENABLED
- REDSHIFT_REQUIRE_TLS_SSL
- REDSHIFT_CLUSTER_CONFIGURATION_CHECK
- REDSHIFT_CLUSTER_MAINTENANCESETTINGS_CHECK
- REDSHIFT_CLUSTER_PUBLIC_ACCESS_CHECK
- REDSHIFT_AUDIT_LOGGING_ENABLED
- REDSHIFT_CLUSTER_KMS_ENABLED
- REDSHIFT_DEFAULT_ADMIN_CHECK
- REDSHIFT_DEFAULT_DB_NAME_CHECK
- REDSHIFT_ENHANCED_VPC_ROUTING_ENABLED
- REQUIRED_TAGS
- RESTRICTED_INCOMING_TRAFFIC
- ROOT_ACCOUNT_HARDWARE_MFA_ENABLED
- ROOT_ACCOUNT_MFA_ENABLED
- S3_ACCOUNT_LEVEL_PUBLIC_ACCESS_BLOCKS_PERIODIC
- S3_ACCOUNT_LEVEL_PUBLIC_ACCESS_BLOCKS
- S3_BUCKET_ACL_PROHIBITED
- S3_BUCKET_BLACKLISTED_ACTIONS_PROHIBITED
- S3_BUCKET_DEFAULT_LOCK_ENABLED
- S3_BUCKET_LEVEL_PUBLIC_ACCESS_PROHIBITED
- S3_BUCKET_LOGGING_ENABLED
- S3_BUCKET_POLICY_GRANTEE_CHECK
- S3_BUCKET_POLICY_NOT_MORE_PERMISSIVE
- S3_BUCKET_PUBLIC_READ_PROHIBITED
- S3_BUCKET_PUBLIC_WRITE_PROHIBITED
- S3_BUCKET_REPLICATION_ENABLED
- S3_BUCKET_SERVER_SIDE_ENCRYPTION_ENABLED
- S3_BUCKET_SSL_REQUESTS_ONLY
- S3_BUCKET_VERSIONING_ENABLED

Palavras-chave de regras AWS Config gerenciadas suportadas

- S3_DEFAULT_ENCRYPTION_KMS
- S3_EVENT_NOTIFICATIONS_ENABLED
- S3_LAST_BACKUP_RECOVERY_POINT_CREATED
- S3_LIFECYCLE_POLICY_CHECK
- S3_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- S3_VERSION_LIFECYCLE_POLICY_CHECK
- SAGEMAKER_ENDPOINT_CONFIGURATION_KMS_KEY_CONFIGURED
- SAGEMAKER_NOTEBOOK_INSTANCE_INSIDE_VPC
- SAGEMAKER_NOTEBOOK_INSTANCE_KMS_KEY_CONFIGURED
- SAGEMAKER_NOTEBOOK_INSTANCE_ROOT_ACCESS_CHECK
- SAGEMAKER_NOTEBOOK_NO_DIRECT_INTERNET_ACCESS
- SECRETSMANAGER_ROTATION_ENABLED_CHECK
- SECRETSMANAGER_SCHEDULED_ROTATION_SUCCESS_CHECK
- SECRETSMANAGER_SECRET_PERIODIC_ROTATION
- SECRETSMANAGER_SECRET_UNUSED
- SECRETSMANAGER_USING_CMK
- SECURITY_ACCOUNT_INFORMATION_PROVIDED
- SECURITYHUB_ENABLED
- SERVICE_VPC_ENDPOINT_ENABLED
- SES_MALWARE_SCANNING_ENABLED
- SHIELD_ADVANCED_ENABLED_AUTORENEW
- SHIELD_DRT_ACCESS
- SNS_ENCRYPTED_KMS
- SNS_TOPIC_MESSAGE_DELIVERY_NOTIFICATION_ENABLED
- SSM_DOCUMENT_NOT_PUBLIC
- STEP_FUNCTIONS_STATE_MACHINE_LOGGING_ENABLED
- GATEWAY_LAST_BACKUP_RECOVERY_POINT_CREATED
- STORAGEGATEWAY_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- SUBNET_AUTO_ASSIGN_PUBLIC_IP_DISABLED

Palavras-chave de regras AWS Config gerenciadas suportadas

- VIRTUALMACHINE_LAST_BACKUP_RECOVERY_POINT_CREATED
- VIRTUALMACHINE_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- VPC_DEFAULT_SECURITY_GROUP_CLOSED
- VPC_FLOW_LOGS_ENABLED
- VPC_NETWORK_ACL_UNUSED_CHECK
- VPC_PEERING_DNS_RESOLUTION_CHECK
- VPC_SG_OPEN_ONLY_TO_AUTHORIZED_PORTS
- VPC_VPN_2_TUNNELS_UP
- WAF_CLASSIC_LOGGING_ENABLED
- WAF_GLOBAL_RULEGROUP_NOT_EMPTY
- WAF_GLOBAL_RULE_NOT_EMPTY
- WAF_GLOBAL_WEBACL_NOT_EMPTY
- WAF_REGIONAL_RULEGROUP_NOT_EMPTY
- WAF_REGIONAL_RULE_NOT_EMPTY
- WAF_REGIONAL_WEBACL_NOT_EMPTY
- WAFV2_LOGGING_ENABLED
- WAFV2_RULEGROUP_NOT_EMPTY
- WAFV2_WEBACL_NOT_EMPTY

Usando regras AWS Config personalizadas com o Audit Manager

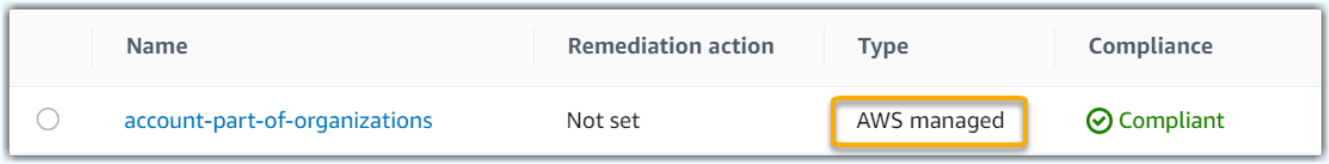
Agora você pode usar regras AWS Config personalizadas como fonte de dados para relatórios de auditoria. Quando um controle tem uma fonte de dados mapeada para uma AWS Config regra, o Audit Manager adiciona a avaliação criada pela AWS Config regra.

As regras personalizadas que você pode usar dependem das Conta da AWS que você usa para entrar no Audit Manager. Se você puder acessar uma regra personalizada no AWS Config, poderá usá-la como mapeamento da fonte de dados no Audit Manager.

- Para indivíduos Contas da AWS — você pode usar qualquer uma das regras personalizadas que você criou com sua conta.

- Para contas que fazem parte de uma organização, você também pode usar qualquer uma das suas regras personalizadas em nível de membro. Ou você pode usar qualquer uma das regras personalizadas em nível de organização que estão disponíveis para você no. AWS Config

Para obter instruções sobre como criar um controle que usa regras personalizadas como fonte de dados, consulte Criação de um novo controle do zero e Personalização de um controle existente.

> **Tip**
>
> Lembre-se de que as regras gerenciadas não são mostradas na lista suspensa de regras personalizadas no Audit Manager.
> Se quiser verificar se uma AWS Config regra é gerenciada ou personalizada, você pode fazer isso usando o AWS Config console. No menu de navegação à esquerda, escolha Regras e procure a regra na tabela. Se for uma regra gerenciada, a coluna Tipo mostrará AWS gerenciada.
>
> 
>
>
> Para mapear uma regra gerenciada como fonte de dados, você pode procurar a palavra-chave identificadora da regra gerenciada no Audit Manager na lista suspensa de regras gerenciadas. Para obter mais informações, consulte a seção Solução de problemasdeste guia.

Depois de mapear suas regras personalizadas como fonte de dados para um controle, você pode associar esse controle a uma estrutura personalizada no Audit Manager. Para obter instruções sobre como criar uma estrutura personalizada que usa seu controle personalizado, consulte como Criar uma nova estrutura do zero e Personalizar uma estrutura existente. Para obter instruções sobre como adicionar seu controle a uma estrutura personalizada existente, consulte Editar uma estrutura existente.

Para obter informações sobre como criar uma regra personalizada em AWS Config, consulte Desenvolvimento de uma regra personalizada para AWS Config no Guia doAWS Config desenvolvedor.

Solução de problemas AWS Config de integração com o Audit Manager

Para encontrar respostas para perguntas e problemas comuns, consulte a integraçãoAWS Config na seção Solução de problemas deste guia.

AWS Security Hub controles suportados por AWS Audit Manager

O Audit Manager permite que você relate os resultados das verificações de conformidade diretamente do Security Hub. Para fazer isso, você especifica um ou mais controles do Security Hub como mapeamento da fonte de dados ao configurar um controle personalizado no Audit Manager.

> **Note**
>
> - O Audit Manager não coleta evidências de AWS Config regras vinculadas a serviços criadas pelo Security Hub. Para obter mais informações, consulte a seção Solucionar problemasdeste guia.
> - Em 9 de novembro de 2022, o Security Hub lançou verificações de segurança automatizadas alinhadas aos requisitos do Center for Internet Security AWS Foundations Benchmark versão 1.4.0, níveis 1 e 2 (CIS v1.4.0). No Security Hub, o padrão CIS v1.4.0 é compatível além do padrão CIS v1.2.0.

Tópicos

- Usando controles do Security Hub com o Audit Manager
- Controles do Security Hub compatíveis

Usando controles do Security Hub com o Audit Manager

> **Tip**
>
> Recomendamos que você ative a configuração de descobertas de controle consolidadas no Security Hub, caso ela ainda não esteja ativada. Se você habilitar o Security Hub em ou após 23 de fevereiro de 2003, essa configuração será ativada por padrão.

Quando as descobertas consolidadas estão habilitadas, o Security Hub produz uma única descoberta para cada verificação de segurança (mesmo quando a mesma verificação se aplica

a vários padrões). Cada descoberta do Security Hub é coletada como uma avaliação de recurso exclusiva no Audit Manager. Como resultado, as descobertas consolidadas resultam em uma diminuição do total de avaliações exclusivas de atributos que o Audit Manager desempenha para as descobertas do Security Hub. Por esse motivo, o uso de descobertas consolidadas geralmente pode resultar em uma redução nos custos de uso do Audit Manager, sem sacrificar a qualidade e a disponibilidade das evidências. Para obter mais informações sobre precificação, consulte Precificação doAWS Audit Manager.

Exemplos de evidências quando as descobertas consolidadas são ativadas ou desativadas

Os exemplos a seguir mostram uma comparação de como o Audit Manager coleta e apresenta evidências, dependendo das configurações do Security Hub.

When consolidated findings is turned on

Digamos que você tenha habilitado os três padrões de segurança a seguir no Security Hub: AWS FSBP, PCI DSS e CIS Benchmark v1.2.0.

- Todos esses três padrões usam o mesmo controle (IAM.4) com a mesma AWS Config regra subjacente (iam-root-access-key-check).
- Como a configuração de descobertas de controle consolidadas está ativada, o Security Hub gera uma única descoberta para esse controle.
- O Security Hub envia a descoberta consolidada ao Audit Manager para esse controle.
- A descoberta consolidada conta como uma avaliação exclusiva de recursos no Audit Manager. Como resultado, uma única evidência é adicionada à sua avaliação.

Veja um exemplo de como essa evidência pode parecer:


```
{
    "SchemaVersion": "2018-10-08",
    "Id": "arn:aws:securityhub:us-west-2:111122223333:security-control/IAM.4/
finding/09876543-p0o9-i8u7-y6t5-098765432109",
    "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/securityhub",
    "ProductName": "Security Hub",
    "CompanyName": "AWS",
    "Region": "us-west-2",
    "GeneratorId": "security-control/IAM.4",
    "AwsAccountId": "111122223333",
    "Types": [
```

```
        "Software and Configuration Checks/Industry and Regulatory Standards"
    ],
    "FirstObservedAt": "2023-10-25T11:32:24.861Z",
    "LastObservedAt": "2023-11-02T11:59:19.546Z",
    "CreatedAt": "2023-10-25T11:32:24.861Z",
    "UpdatedAt": "2023-11-02T11:59:15.127Z",
    "Severity": {
        "Label": "INFORMATIONAL",
        "Normalized": 0,
        "Original": "INFORMATIONAL"
    },
    "Title": "IAM root user access key should not exist",
    "Description": "This AWS control checks whether the root user access key is
 available.",
    "Remediation": {
        "Recommendation": {
            "Text": "For information on how to correct this issue, consult the AWS
 Security Hub controls documentation.",
            "Url": "https://docs.aws.amazon.com/console/securityhub/IAM.4/
remediation"
        }
    },
    "ProductFields": {
        "RelatedAWSResources:0/name": "securityhub-iam-root-access-key-
check-000270f5",
        "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
        "aws/securityhub/ProductName": "Security Hub",
        "aws/securityhub/CompanyName": "AWS",
        "Resources:0/Id": "arn:aws:iam::111122223333:root",
        "aws/securityhub/FindingId": "arn:aws:securityhub:us-west-2::product/aws/
securityhub/arn:aws:securityhub:us-west-2:111122223333:security-control/IAM.4/
finding/09876543-p0o9-i8u7-y6t5-098765432109"
    },
    "Resources": [{
        "Type": "AwsAccount",
        "Id": "AWS::::Account:111122223333",
        "Partition": "aws",
        "Region": "us-west-2"
    }],
    "Compliance": {
        "Status": "PASSED",
        "RelatedRequirements": [
            "CIS AWS Foundations Benchmark v1.2.0/1.12"
        ],
```

```
        "SecurityControlId": "IAM.4",
        "AssociatedStandards": [{
                "StandardsId": "ruleset/cis-aws-foundations-benchmark/v/1.2.0"
            },
            {
                "StandardsId": "standards/aws-foundational-security-best-practices/
v/1.0.0"
            }
        ]
    },
    "WorkflowState": "NEW",
    "Workflow": {
        "Status": "RESOLVED"
    },
    "RecordState": "ACTIVE",
    "FindingProviderFields": {
        "Severity": {
            "Label": "INFORMATIONAL",
            "Original": "INFORMATIONAL"
        },
        "Types": [
            "Software and Configuration Checks/Industry and Regulatory Standards"
        ]
    },
    "ProcessedAt": "2023-11-02T11:59:20.980Z"
}
```


When consolidated findings is turned off

Digamos que você tenha habilitado os três padrões de segurança a seguir no Security Hub: AWS FSBP, PCI DSS e CIS Benchmark v1.2.0.

- Todos esses três padrões usam o mesmo controle (IAM.4) com a mesma AWS Config regra subjacente (iam-root-access-key-check).
- Como a configuração de descobertas consolidadas está desativada, o Security Hub gera uma descoberta separada por verificação de segurança para cada padrão habilitado (nesse caso, três descobertas).
- O Security Hub envia três descobertas separadas específicas do padrão ao Audit Manager para esse controle.
- As três descobertas contam como três avaliações de recursos exclusivas no Audit Manager. Como resultado, três evidências separadas são adicionadas à sua avaliação.

Veja a seguir um exemplo de como essa evidência pode parecer. Observe que, neste exemplo, cada uma das três cargas a seguir tem o mesmo ID de controle de segurança (*SecurityControlId":"IAM.4"*). Por esse motivo, o controle de avaliação que coleta essas evidências no Audit Manager (IAM.4) recebe três evidências separadas quando as seguintes descobertas chegam do Security Hub.

Evidências do IAM.4 (FSBP)


```
{
  "version":"0",
  "id":"12345678-1q2w-3e4r-5t6y-123456789012",
  "detail-type":"Security Hub Findings - Imported",
  "source":"aws.securityhub",
  "account":"111122223333",
  "time":"2023-10-27T18:55:59Z",
  "region":"us-west-2",
  "resources":[
     "arn:aws:securityhub:us-west-2::product/aws/securityhub/arn:aws:securityhub:us-
west-2:111122223333:subscription/aws-foundational-security-best-practices/v/1.0.0/
Lambda.1/finding/b5e68d5d-43c3-46c8-902d-51cb0d4da568"
  ],
  "detail":{
     "findings":[
        {
           "SchemaVersion":"2018-10-08",
           "Id":"arn:aws:securityhub:us-west-2:111122223333:subscription/aws-
foundational-security-best-practices/v/1.0.0/IAM.4/finding/8e2e05a2-4d50-4c2e-
a78f-3cbe9402d17d",
           "ProductArn":"arn:aws:securityhub:us-west-2::product/aws/securityhub",
           "ProductName":"Security Hub",
           "CompanyName":"AWS",
           "Region":"us-west-2",
           "GeneratorId":"aws-foundational-security-best-practices/v/1.0.0/IAM.4",
           "AwsAccountId":"111122223333",
           "Types":[
              "Software and Configuration Checks/Industry and Regulatory Standards/
AWS-Foundational-Security-Best-Practices"
           ],
           "FirstObservedAt":"2020-10-05T19:18:47.848Z",
           "LastObservedAt":"2023-11-01T14:12:04.106Z",
           "CreatedAt":"2020-10-05T19:18:47.848Z",
           "UpdatedAt":"2023-11-01T14:11:53.720Z",
           "Severity":{
```

```
            "Product":0,
            "Label":"INFORMATIONAL",
            "Normalized":0,
            "Original":"INFORMATIONAL"
         },
         "Title":"IAM.4 IAM root user access key should not exist",
         "Description":"This AWS control checks whether the root user access key
 is available.",
         "Remediation":{
            "Recommendation":{
               "Text":"For information on how to correct this issue, consult the
 AWS Security Hub controls documentation.",
               "Url":"https://docs.aws.amazon.com/console/securityhub/IAM.4/
remediation"
            }
         },
         "ProductFields":{
            "StandardsArn":"arn:aws:securityhub:::standards/aws-foundational-
security-best-practices/v/1.0.0",
            "StandardsSubscriptionArn":"arn:aws:securityhub:us-
west-2:111122223333:subscription/aws-foundational-security-best-practices/v/1.0.0",
            "ControlId":"IAM.4",
            "RecommendationUrl":"https://docs.aws.amazon.com/console/securityhub/
IAM.4/remediation",
            "RelatedAWSResources:0/name":"securityhub-iam-root-access-key-
check-67cbb1c4",
            "RelatedAWSResources:0/type":"AWS::Config::ConfigRule",
            "StandardsControlArn":"arn:aws:securityhub:us-
west-2:111122223333:control/aws-foundational-security-best-practices/v/1.0.0/IAM.4",
            "aws/securityhub/ProductName":"Security Hub",
            "aws/securityhub/CompanyName":"AWS",
            "Resources:0/Id":"arn:aws:iam::111122223333:root",
            "aws/securityhub/FindingId":"arn:aws:securityhub:us-west-2::product/
aws/securityhub/arn:aws:securityhub:us-west-2:111122223333:subscription/aws-
foundational-security-best-practices/v/1.0.0/IAM.4/finding/8e2e05a2-4d50-4c2e-
a78f-3cbe9402d17d"
         },
         "Resources":[
            {
               "Type":"AwsAccount",
               "Id":"AWS::::Account:111122223333",
               "Partition":"aws",
               "Region":"us-west-2"
            }
```

```
            ],
            "Compliance":{
               "Status":"PASSED",
               "SecurityControlId":"IAM.4",
               "AssociatedStandards":[
                  {
                     "StandardsId":"standards/aws-foundational-security-best-
practices/v/1.0.0"
                  }
               ]
            },
            "WorkflowState":"NEW",
            "Workflow":{
               "Status":"RESOLVED"
            },
            "RecordState":"ACTIVE",
            "FindingProviderFields":{
               "Severity":{
                  "Label":"INFORMATIONAL",
                  "Original":"INFORMATIONAL"
               },
               "Types":[
                  "Software and Configuration Checks/Industry and Regulatory
 Standards/AWS-Foundational-Security-Best-Practices"
               ]
            },
            "ProcessedAt":"2023-11-01T14:12:07.395Z"
         }
      ]
   }
}
```

Evidências do IAM.4 (CIS 1.2)

```
{
  "version":"0",
  "id":"12345678-1q2w-3e4r-5t6y-123456789012",
  "detail-type":"Security Hub Findings - Imported",
  "source":"aws.securityhub",
  "account":"111122223333",
  "time":"2023-10-27T18:55:59Z",
```

```
  "region":"us-west-2",
  "resources":[
     "arn:aws:securityhub:us-west-2::product/aws/securityhub/arn:aws:securityhub:us-
west-2:111122223333:subscription/aws-foundational-security-best-practices/v/1.0.0/
Lambda.1/finding/1dd8f2f8-cf1b-47c9-a875-8d7387fc9c23"
  ],
  "detail":{
     "findings":[
        {
           "SchemaVersion":"2018-10-08",
           "Id":"arn:aws:securityhub:us-west-2:111122223333:subscription/cis-aws-
foundations-benchmark/v/1.2.0/1.12/finding/1dd8f2f8-cf1b-47c9-a875-8d7387fc9c23",
           "ProductArn":"arn:aws:securityhub:us-west-2::product/aws/securityhub",
           "ProductName":"Security Hub",
           "CompanyName":"AWS",
           "Region":"us-west-2",
           "GeneratorId":"arn:aws:securityhub:::ruleset/cis-aws-foundations-
benchmark/v/1.2.0/rule/1.12",
           "AwsAccountId":"111122223333",
           "Types":[
              "Software and Configuration Checks/Industry and Regulatory Standards/
CIS AWS Foundations Benchmark"
           ],
           "FirstObservedAt":"2020-10-05T19:18:47.775Z",
           "LastObservedAt":"2023-11-01T14:12:07.989Z",
           "CreatedAt":"2020-10-05T19:18:47.775Z",
           "UpdatedAt":"2023-11-01T14:11:53.720Z",
           "Severity":{
              "Product":0,
              "Label":"INFORMATIONAL",
              "Normalized":0,
              "Original":"INFORMATIONAL"
           },
           "Title":"1.12 Ensure no root user access key exists",
           "Description":"The root user is the most privileged user in an AWS
 account. AWS Access Keys provide programmatic access to a given AWS account. It is
 recommended that all access keys associated with the root user be removed.",
           "Remediation":{
              "Recommendation":{
                 "Text":"For information on how to correct this issue, consult the
 AWS Security Hub controls documentation.",
                 "Url":"https://docs.aws.amazon.com/console/securityhub/IAM.4/
remediation"
              }
```

```
            },
            "ProductFields":{
               "StandardsGuideArn":"arn:aws:securityhub:::ruleset/cis-aws-
foundations-benchmark/v/1.2.0",
               "StandardsGuideSubscriptionArn":"arn:aws:securityhub:us-
west-2:111122223333:subscription/cis-aws-foundations-benchmark/v/1.2.0",
               "RuleId":"1.12",
               "RecommendationUrl":"https://docs.aws.amazon.com/console/securityhub/
IAM.4/remediation",
               "RelatedAWSResources:0/name":"securityhub-iam-root-access-key-
check-67cbb1c4",
               "RelatedAWSResources:0/type":"AWS::Config::ConfigRule",
               "StandardsControlArn":"arn:aws:securityhub:us-
west-2:111122223333:control/cis-aws-foundations-benchmark/v/1.2.0/1.12",
               "aws/securityhub/ProductName":"Security Hub",
               "aws/securityhub/CompanyName":"AWS",
               "Resources:0/Id":"arn:aws:iam::111122223333:root",
               "aws/securityhub/FindingId":"arn:aws:securityhub:us-west-2::product/
aws/securityhub/arn:aws:securityhub:us-west-2:111122223333:subscription/cis-aws-
foundations-benchmark/v/1.2.0/1.12/finding/1dd8f2f8-cf1b-47c9-a875-8d7387fc9c23"
            },
            "Resources":[
               {
                  "Type":"AwsAccount",
                  "Id":"AWS::::Account:111122223333",
                  "Partition":"aws",
                  "Region":"us-west-2"
               }
            ],
            "Compliance":{
               "Status":"PASSED",
               "SecurityControlId":"IAM.4",
               "AssociatedStandards":[
                  {
                     "StandardsId":"ruleset/cis-aws-foundations-benchmark/v/1.2.0"
                  }
               ]
            },
            "WorkflowState":"NEW",
            "Workflow":{
               "Status":"RESOLVED"
            },
            "RecordState":"ACTIVE",
            "FindingProviderFields":{
```

```
              "Severity":{
                 "Label":"INFORMATIONAL",
                 "Original":"INFORMATIONAL"
              },
              "Types":[
                 "Software and Configuration Checks/Industry and Regulatory
 Standards/CIS AWS Foundations Benchmark"
              ]
           },
           "ProcessedAt":"2023-11-01T14:12:13.436Z"
        }
     ]
  }
}
```

Evidências do PCI.IAM.1 (PCI DSS)

```
{
  "version":"0",
  "id":"12345678-1q2w-3e4r-5t6y-123456789012",
  "detail-type":"Security Hub Findings - Imported",
  "source":"aws.securityhub",
  "account":"111122223333",
  "time":"2023-10-27T18:55:59Z",
  "region":"us-west-2",
  "resources":[
     "arn:aws:securityhub:us-west-2::product/aws/securityhub/arn:aws:securityhub:us-
west-2:111122223333:subscription/aws-foundational-security-best-practices/v/1.0.0/
Lambda.1/finding/1dd8f2f8-cf1b-47c9-a875-8d7387fc9c23"
  ],
  "detail":{
     "findings":[
        {
           "SchemaVersion":"2018-10-08",
           "Id":"arn:aws:securityhub:us-west-2:111122223333:subscription/pci-dss/
v/3.2.1/PCI.IAM.1/finding/3c75f651-6e2e-44f4-8e22-297d5c2d0c8b",
           "ProductArn":"arn:aws:securityhub:us-west-2::product/aws/securityhub",
           "ProductName":"Security Hub",
           "CompanyName":"AWS",
           "Region":"us-west-2",
           "GeneratorId":"pci-dss/v/3.2.1/PCI.IAM.1",
           "AwsAccountId":"111122223333",
           "Types":[
```

```
            "Software and Configuration Checks/Industry and Regulatory Standards/
PCI-DSS"
         ],
         "FirstObservedAt":"2020-10-05T19:18:47.788Z",
         "LastObservedAt":"2023-11-01T14:12:02.413Z",
         "CreatedAt":"2020-10-05T19:18:47.788Z",
         "UpdatedAt":"2023-11-01T14:11:53.720Z",
         "Severity":{
            "Product":0,
            "Label":"INFORMATIONAL",
            "Normalized":0,
            "Original":"INFORMATIONAL"
         },
         "Title":"PCI.IAM.1 IAM root user access key should not exist",
         "Description":"This AWS control checks whether the root user access key
 is available.",
         "Remediation":{
            "Recommendation":{
               "Text":"For information on how to correct this issue, consult the
 AWS Security Hub controls documentation.",
               "Url":"https://docs.aws.amazon.com/console/securityhub/IAM.4/
remediation"
            }
         },
         "ProductFields":{
            "StandardsArn":"arn:aws:securityhub:::standards/pci-dss/v/3.2.1",
            "StandardsSubscriptionArn":"arn:aws:securityhub:us-
west-2:111122223333:subscription/pci-dss/v/3.2.1",
            "ControlId":"PCI.IAM.1",
            "RecommendationUrl":"https://docs.aws.amazon.com/console/securityhub/
IAM.4/remediation",
            "RelatedAWSResources:0/name":"securityhub-iam-root-access-key-
check-67cbb1c4",
            "RelatedAWSResources:0/type":"AWS::Config::ConfigRule",
            "StandardsControlArn":"arn:aws:securityhub:us-
west-2:111122223333:control/pci-dss/v/3.2.1/PCI.IAM.1",
            "aws/securityhub/ProductName":"Security Hub",
            "aws/securityhub/CompanyName":"AWS",
            "Resources:0/Id":"arn:aws:iam::111122223333:root",
            "aws/securityhub/FindingId":"arn:aws:securityhub:us-west-2::product/
aws/securityhub/arn:aws:securityhub:us-west-2:111122223333:subscription/pci-dss/
v/3.2.1/PCI.IAM.1/finding/3c75f651-6e2e-44f4-8e22-297d5c2d0c8b"
         },
         "Resources":[
```

```
            {
               "Type":"AwsAccount",
               "Id":"AWS::::Account:111122223333",
               "Partition":"aws",
               "Region":"us-west-2"
            }
         ],
         "Compliance":{
            "Status":"PASSED",
            "RelatedRequirements":[
               "PCI DSS 2.1",
               "PCI DSS 2.2",
               "PCI DSS 7.2.1"
            ],
            "SecurityControlId":"IAM.4",
            "AssociatedStandards":[
               {
                  "StandardsId":"standards/pci-dss/v/3.2.1"
               }
            ]
         },
         "WorkflowState":"NEW",
         "Workflow":{
            "Status":"RESOLVED"
         },
         "RecordState":"ACTIVE",
         "FindingProviderFields":{
            "Severity":{
               "Label":"INFORMATIONAL",
               "Original":"INFORMATIONAL"
            },
            "Types":[
               "Software and Configuration Checks/Industry and Regulatory
 Standards/PCI-DSS"
            ]
         },
         "ProcessedAt":"2023-11-01T14:12:05.950Z"
      }
   ]
  }
}
```

Controles do Security Hub compatíveis

Os seguintes controles do Security Hub são atualmente compatíveis com o Audit Manager. Você pode usar qualquer uma das seguintes palavras-chave de ID de controle específicas do padrão ao configurar uma fonte de dados para um controle personalizado.

Padrão de segurança	Palavra-chave compatíveis com o Audit Manager (ID de controle padrão no Security Hub)	Documentação de controle relacionada (ID de controle de segurança correspondente no Security Hub)
CIS v1.2.0	1.2	IAM.5
CIS v1.2.0	1.3	IAM.8
CIS v1.2.0	1.4	IAM.3
CIS v1.2.0	1.5	IAM.11
CIS v1.2.0	1.6	IAM 12
CIS v1.2.0	1,7	IAM.13
CIS v1.2.0	1.8	IAM.14
CIS v1.2.0	1.9	IAM.15
CIS v1.2.0	1.10	IAM.16
CIS v1.2.0	1.11	IAM.17
CIS v1.2.0	1.12	IAM.4
CIS v1.2.0	1.13	IAM.9
CIS v1.2.0	1.14	IAM.6

Padrão de segurança	Palavra-chave compatíveis com o Audit Manager (ID de controle padrão no Security Hub)	Documentação de controle relacionada (ID de controle de segurança correspondente no Security Hub)
CIS v1.2.0	1.16	IAM.2
CIS v1.2.0	1,20	IAM.18
CIS v1.2.0	1,22	IAM.1
CIS v1.2.0	2.1	CloudTrail.1
CIS v1.2.0	2.2	CloudTrail.4
CIS v1.2.0	2.3	CloudTrail.6
CIS v1.2.0	2.4	CloudTrail5.
CIS v1.2.0	2,5	Config.1
CIS v1.2.0	2.6	CloudTrail7.
CIS v1.2.0	2.7	CloudTrail.2
CIS v1.2.0	2.8	KMS.4
CIS v1.2.0	2.9	EC2.6
CIS v1.2.0	3.1	CloudWatch.2
CIS v1.2.0	3.2	CloudWatch.3
CIS v1.2.0	3.3	CloudWatch.1
CIS v1.2.0	3.4	CloudWatch.4

Padrão de segurança	Palavra-chave compatíveis com o Audit Manager (ID de controle padrão no Security Hub)	Documentação de controle relacionada (ID de controle de segurança correspondente no Security Hub)
CIS v1.2.0	3.5	CloudWatch5.
CIS v1.2.0	3.6	CloudWatch.6
CIS v1.2.0	3.7	CloudWatch7.
CIS v1.2.0	3.8	CloudWatch8.
CIS v1.2.0	3.9	CloudWatch9.
CIS v1.2.0	3.10	CloudWatch.10
CIS v1.2.0	3.11	CloudWatch1.1
CIS v1.2.0	3.12	CloudWatch1.2
CIS v1.2.0	3.13	CloudWatch1.3
CIS v1.2.0	3.14	CloudWatch1.4
CIS v1.2.0	4.1	EC2.13
CIS v1.2.0	4.2	EC2.14
CIS v1.2.0	4.3	EC2.2
PCI DSS	FOTO. AutoScaling.1	AutoScaling.1
PCI DSS	FOTO. CloudTrail.1	CloudTrail.1

Padrão de segurança	Palavra-chave compatíveis com o Audit Manager (ID de controle padrão no Security Hub)	Documentação de controle relacionada (ID de controle de segurança correspondente no Security Hub)
PCI DSS	FOTO. CloudTrail.2	CloudTrail.2
PCI DSS	FOTO. CloudTrail.3	CloudTrail.3
PCI DSS	FOTO. CloudTrail.4	CloudTrail.4
PCI DSS	FOTO. CodeBuild.1	CodeBuild.1
PCI DSS	FOTO. CodeBuild.2	CodeBuild.2
PCI DSS	PCI.Config.1	Config.1
PCI DSS	PCI.CW.1	CloudWatch.1
PCI DSS	PCI.DMS.1	DMS.1
PCI DSS	PCI.EC2.1	EC2.1
PCI DSS	PCI.EC2.2	EC2.2
PCI DSS	PCI.EC2.3	EC2.3
PCI DSS	PCI.EC2.4	EC2.12
PCI DSS	PCI.EC2.5	EC2.13

Padrão de segurança	Palavra-chave compatíveis com o Audit Manager (ID de controle padrão no Security Hub)	Documentação de controle relacionada (ID de controle de segurança correspondente no Security Hub)
PCI DSS	PCI.EC2.6	EC2.6
PCI DSS	PCI.ELB v2.1	ELB.1
PCI DSS	PCI.ES.1	ES.1
PCI DSS	PCI.ES.2	ES.2
PCI DSS	FOTO. GuardDuty.1	GuardDuty.1
PCI DSS	PCI.IAM.1	IAM.1
PCI DSS	PCI.IAM.2	IAM.2
PCI DSS	PCI.IAM.3	IAM.3
PCI DSS	PCI.IAM.4	IAM.4
PCI DSS	PCI.IAM.5	IAM.9
PCI DSS	PCI.IAM.6	IAM.6
PCI DSS	PCI.IAM.7	PCI.IAM.7
PCI DSS	PCI.IAM.8	PCI.IAM8.
PCI DSS	PCI.KMS.1	PCI. KMS.4
PCI DSS	PCI.Lambda.1	Lambda.1
PCI DSS	PCI.Lambda.2	Lambda.3

Padrão de segurança	Palavra-chave compatíveis com o Audit Manager (ID de controle padrão no Security Hub)	Documentação de controle relacionada (ID de controle de segurança correspondente no Security Hub)
PCI DSS	PCI.OpenSearch.1	Opensearch.1
PCI DSS	PCI.OpenSearch.2	Opensearch.2
PCI DSS	PCI.RDS.1	RDS.1
PCI DSS	PCI.RDS.2	RDS.2
PCI DSS	PCI.RedShift.1	Redshift.1
PCI DSS	PCI.S3.1	S3.1
PCI DSS	PCI.S3.2	S3.2
PCI DSS	PCI.S3.3	S3.3
PCI DSS	PCI.S3.4	S3.4
PCI DSS	PCIS.3.5	S3.5
PCI DSS	PCI.S3.6	S3.1
PCI DSS	FOTO. SageMaker.1	SageMaker.1
PCI DSS	PCI.SSM.1	SSM.1
PCI DSS	PCI.SSM.2	SSM.2
PCI DSS	PCI.SSM.3	SSM.3

Padrão de segurança	Palavra-chave compatíveis com o Audit Manager (ID de controle padrão no Security Hub)	Documentação de controle relacionada (ID de controle de segurança correspondente no Security Hub)
AWS Melhores práticas básicas de segurança	Account.1	Account.1
AWS Melhores práticas básicas de segurança	Conta 2	Conta 2
AWS Melhores práticas básicas de segurança	ACM.1	ACM.1
AWS Melhores práticas básicas de segurança	ACM.2	ACM.2
AWS Melhores práticas básicas de segurança	APIGateway.1	APIGateway.1
AWS Melhores práticas básicas de segurança	APIGateway.2	APIGateway.2
AWS Melhores práticas básicas de segurança	APIGateway.3	APIGateway.3
AWS Melhores práticas básicas de segurança	APIGateway.4	APIGateway.4
AWS Melhores práticas básicas de segurança	APIGateway.5	APIGateway.5
AWS Melhores práticas básicas de segurança	APIGateway.8	APIGateway.8

Padrão de segurança	Palavra-chave compatíveis com o Audit Manager (ID de controle padrão no Security Hub)	Documentação de controle relacionada (ID de controle de segurança correspondente no Security Hub)
AWS Melhores práticas básicas de segurança	APIGateway.9	APIGateway.9
AWS Melhores práticas básicas de segurança	AppSync.2	AppSync.2
AWS Melhores práticas básicas de segurança	AppSync5.	AppSync5.
AWS Melhores práticas básicas de segurança	Athena.1	Athena.1
AWS Melhores práticas básicas de segurança	AutoScaling.1	AutoScaling.1
AWS Melhores práticas básicas de segurança	AutoScaling.2	AutoScaling.2
AWS Melhores práticas básicas de segurança	AutoScaling.3	AutoScaling.3
AWS Melhores práticas básicas de segurança	AutoScaling.4	AutoScaling.4
AWS Melhores práticas básicas de segurança	Autoscaling.5	Autoscaling.5
AWS Melhores práticas básicas de segurança	AutoScaling.6	AutoScaling.6

Padrão de segurança	Palavra-chave compatíveis com o Audit Manager (ID de controle padrão no Security Hub)	Documentação de controle relacionada (ID de controle de segurança correspondente no Security Hub)
AWS Melhores práticas básicas de segurança	AutoScaling9.	AutoScaling9.
AWS Melhores práticas básicas de segurança	Backup.1	Backup.1
AWS Melhores práticas básicas de segurança	CloudFormation.1	CloudFormation.1
AWS Melhores práticas básicas de segurança	CloudFront.1	CloudFront.1
AWS Melhores práticas básicas de segurança	CloudFront.2	CloudFront.2
AWS Melhores práticas básicas de segurança	CloudFront.3	CloudFront.3
AWS Melhores práticas básicas de segurança	CloudFront.4	CloudFront.4
AWS Melhores práticas básicas de segurança	CloudFront5.	CloudFront5.
AWS Melhores práticas básicas de segurança	CloudFront.6	CloudFront.6
AWS Melhores práticas básicas de segurança	CloudFront7.	CloudFront7.

Padrão de segurança	Palavra-chave compatíveis com o Audit Manager (ID de controle padrão no Security Hub)	Documentação de controle relacionada (ID de controle de segurança correspondente no Security Hub)
AWS Melhores práticas básicas de segurança	CloudFront8.	CloudFront8.
AWS Melhores práticas básicas de segurança	CloudFront9.	CloudFront9.
AWS Melhores práticas básicas de segurança	CloudFront.10	CloudFront.10
AWS Melhores práticas básicas de segurança	CloudFront1.2	CloudFront1.2
AWS Melhores práticas básicas de segurança	CloudFront1.3	CloudFront1.3
AWS Melhores práticas básicas de segurança	CloudTrail.1	CloudTrail.1
AWS Melhores práticas básicas de segurança	CloudTrail.2	CloudTrail.2
AWS Melhores práticas básicas de segurança	CloudTrail.3	CloudTrail.3
AWS Melhores práticas básicas de segurança	CloudTrail.4	CloudTrail.4
AWS Melhores práticas básicas de segurança	CloudTrail5.	CloudTrail5.

Padrão de segurança	Palavra-chave compatíveis com o Audit Manager (ID de controle padrão no Security Hub)	Documentação de controle relacionada (ID de controle de segurança correspondente no Security Hub)
AWS Melhores práticas básicas de segurança	CloudTrail.6	CloudTrail.6
AWS Melhores práticas básicas de segurança	CloudTrail7.	CloudTrail7.
AWS Melhores práticas básicas de segurança	CloudWatch.1	CloudWatch.1
AWS Melhores práticas básicas de segurança	CloudWatch.2	CloudWatch.2
AWS Melhores práticas básicas de segurança	CloudWatch.3	CloudWatch.3
AWS Melhores práticas básicas de segurança	CloudWatch.4	CloudWatch.4
AWS Melhores práticas básicas de segurança	CloudWatch5.	CloudWatch5.
AWS Melhores práticas básicas de segurança	CloudWatch.6	CloudWatch.6
AWS Melhores práticas básicas de segurança	CloudWatch7.	CloudWatch7.
AWS Melhores práticas básicas de segurança	CloudWatch8.	CloudWatch8.

Padrão de segurança	Palavra-chave compatíveis com o Audit Manager (ID de controle padrão no Security Hub)	Documentação de controle relacionada (ID de controle de segurança correspondente no Security Hub)
AWS Melhores práticas básicas de segurança	CloudWatch9.	CloudWatch9.
AWS Melhores práticas básicas de segurança	CloudWatch.10	CloudWatch.10
AWS Melhores práticas básicas de segurança	CloudWatch1.1	CloudWatch1.1
AWS Melhores práticas básicas de segurança	CloudWatch1.2	CloudWatch1.2
AWS Melhores práticas básicas de segurança	CloudWatch1.3	CloudWatch1.3
AWS Melhores práticas básicas de segurança	CloudWatch1.4	CloudWatch1.4
AWS Melhores práticas básicas de segurança	CloudWatch1.5	CloudWatch1.5
AWS Melhores práticas básicas de segurança	CloudWatch1.6	CloudWatch1.6
AWS Melhores práticas básicas de segurança	CloudWatch1.7	CloudWatch1.7
AWS Melhores práticas básicas de segurança	CodeBuild.1	CodeBuild.1

Padrão de segurança	Palavra-chave compatíveis com o Audit Manager (ID de controle padrão no Security Hub)	Documentação de controle relacionada (ID de controle de segurança correspondente no Security Hub)
AWS Melhores práticas básicas de segurança	CodeBuild.2	CodeBuild.2
AWS Melhores práticas básicas de segurança	CodeBuild.3	CodeBuild.3
AWS Melhores práticas básicas de segurança	CodeBuild.4	CodeBuild.4
AWS Melhores práticas básicas de segurança	CodeBuild5.	CodeBuild5.
AWS Melhores práticas básicas de segurança	Config.1	Config.1
AWS Melhores práticas básicas de segurança	DMS.1	DMS.1
AWS Melhores práticas básicas de segurança	DMS.1	DMS.1
AWS Melhores práticas básicas de segurança	DMS.1	DMS.1
AWS Melhores práticas básicas de segurança	DMS.1	DMS.1
AWS Melhores práticas básicas de segurança	DMS.1	DMS.1

Padrão de segurança	Palavra-chave compatíveis com o Audit Manager (ID de controle padrão no Security Hub)	Documentação de controle relacionada (ID de controle de segurança correspondente no Security Hub)
AWS Melhores práticas básicas de segurança	DocumentDB	DocumentDB
AWS Melhores práticas básicas de segurança	DocumentDB	DocumentDB
AWS Melhores práticas básicas de segurança	DocumentDB	DocumentDB
AWS Melhores práticas básicas de segurança	DocumentDB	DocumentDB
AWS Melhores práticas básicas de segurança	DocumentDB	DocumentDB
AWS Melhores práticas básicas de segurança	DynamoDB.1	DynamoDB.1
AWS Melhores práticas básicas de segurança	DynamoDB.2	DynamoDB.2
AWS Melhores práticas básicas de segurança	DynamoDB.3	DynamoDB.3
AWS Melhores práticas básicas de segurança	DynamoDB.2	DynamoDB.2
AWS Melhores práticas básicas de segurança	DynamoDB.6	DynamoDB.6

Padrão de segurança	Palavra-chave compatíveis com o Audit Manager (ID de controle padrão no Security Hub)	Documentação de controle relacionada (ID de controle de segurança correspondente no Security Hub)
AWS Melhores práticas básicas de segurança	EC2.1	EC2.1
AWS Melhores práticas básicas de segurança	EC2.2	EC2.2
AWS Melhores práticas básicas de segurança	EC2.3	EC2.3
AWS Melhores práticas básicas de segurança	EC2.4	EC2.4
AWS Melhores práticas básicas de segurança	EC2.6	EC2.6
AWS Melhores práticas básicas de segurança	EC2.7	EC2.7
AWS Melhores práticas básicas de segurança	EC2.8	EC2.8
AWS Melhores práticas básicas de segurança	EC2.9	EC2.9
AWS Melhores práticas básicas de segurança	EC2.10	EC2.10
AWS Melhores práticas básicas de segurança	EC2.12	EC2.12

Padrão de segurança	Palavra-chave compatíveis com o Audit Manager (ID de controle padrão no Security Hub)	Documentação de controle relacionada (ID de controle de segurança correspondente no Security Hub)
AWS Melhores práticas básicas de segurança	EC2.13	EC2.13
AWS Melhores práticas básicas de segurança	EC2.14	EC2.14
AWS Melhores práticas básicas de segurança	EC2.15	EC2.15
AWS Melhores práticas básicas de segurança	EC2.16	EC2.16
AWS Melhores práticas básicas de segurança	EC2.17	EC2.17
AWS Melhores práticas básicas de segurança	EC2.18	EC2.18
AWS Melhores práticas básicas de segurança	EC2.19	EC2.19
AWS Melhores práticas básicas de segurança	EC2.20	EC2.20
AWS Melhores práticas básicas de segurança	EC2.21	EC2.21
AWS Melhores práticas básicas de segurança	EC2.22	EC2.22

Padrão de segurança	Palavra-chave compatíveis com o Audit Manager (ID de controle padrão no Security Hub)	Documentação de controle relacionada (ID de controle de segurança correspondente no Security Hub)
AWS Melhores práticas básicas de segurança	EC2.23	EC2.23
AWS Melhores práticas básicas de segurança	EC2.24	EC2.24
AWS Melhores práticas básicas de segurança	EC2.25	EC2.25
AWS Melhores práticas básicas de segurança	EC2.28	EC2.28
AWS Melhores práticas básicas de segurança	EC2.51	EC2.51
AWS Melhores práticas básicas de segurança	ECR.1	ECR.1
AWS Melhores práticas básicas de segurança	ECR.2	ECR.2
AWS Melhores práticas básicas de segurança	ECR.3	ECR.3
AWS Melhores práticas básicas de segurança	ECS.1	ECS.1
AWS Melhores práticas básicas de segurança	ECS.2	ECS.2

Padrão de segurança	Palavra-chave compatíveis com o Audit Manager (ID de controle padrão no Security Hub)	Documentação de controle relacionada (ID de controle de segurança correspondente no Security Hub)
AWS Melhores práticas básicas de segurança	ECS.3	ECS.3
AWS Melhores práticas básicas de segurança	ECS.4	ECS.4
AWS Melhores práticas básicas de segurança	ECS.5	ECS.5
AWS Melhores práticas básicas de segurança	ECS.8	ECS.8
AWS Melhores práticas básicas de segurança	ECS.12	ECS.12
AWS Melhores práticas básicas de segurança	ECS.10	ECS.10
AWS Melhores práticas básicas de segurança	ECS.12	ECS.12
AWS Melhores práticas básicas de segurança	EFS.1	EFS.1
AWS Melhores práticas básicas de segurança	EFS.2	EFS.2
AWS Melhores práticas básicas de segurança	EFS.3	EFS.3

Padrão de segurança	Palavra-chave compatíveis com o Audit Manager (ID de controle padrão no Security Hub)	Documentação de controle relacionada (ID de controle de segurança correspondente no Security Hub)
AWS Melhores práticas básicas de segurança	EFS.4	EFS.4
AWS Melhores práticas básicas de segurança	EKS.1	EKS.1
AWS Melhores práticas básicas de segurança	EKS.2	EKS.2
AWS Melhores práticas básicas de segurança	EKS.8	EKS.8
AWS Melhores práticas básicas de segurança	ElastiCache.1	ElastiCache.1
AWS Melhores práticas básicas de segurança	ElastiCache.2	ElastiCache.2
AWS Melhores práticas básicas de segurança	ElastiCache.3	ElastiCache.3
AWS Melhores práticas básicas de segurança	ElastiCache.4	ElastiCache.4
AWS Melhores práticas básicas de segurança	ElastiCache5.	ElastiCache5.
AWS Melhores práticas básicas de segurança	ElastiCache.6	ElastiCache.6

Padrão de segurança	Palavra-chave compatíveis com o Audit Manager (ID de controle padrão no Security Hub)	Documentação de controle relacionada (ID de controle de segurança correspondente no Security Hub)
AWS Melhores práticas básicas de segurança	ElastiCache7.	ElastiCache7.
AWS Melhores práticas básicas de segurança	ElasticBeanstalk.1	ElasticBeanstalk.1
AWS Melhores práticas básicas de segurança	ElasticBeanstalk.2	ElasticBeanstalk.2
AWS Melhores práticas básicas de segurança	ElasticBeanstalk.3	ElasticBeanstalk.3
AWS Melhores práticas básicas de segurança	ELB.1	ELB.1
AWS Melhores práticas básicas de segurança	ELB.2	ELB.2
AWS Melhores práticas básicas de segurança	ELB.3	ELB.3
AWS Melhores práticas básicas de segurança	ELB.4	ELB.4
AWS Melhores práticas básicas de segurança	ELB.5	ELB.5
AWS Melhores práticas básicas de segurança	ELB.6	ELB.6

Padrão de segurança	Palavra-chave compatíveis com o Audit Manager (ID de controle padrão no Security Hub)	Documentação de controle relacionada (ID de controle de segurança correspondente no Security Hub)
AWS Melhores práticas básicas de segurança	ELB.7	ELB.7
AWS Melhores práticas básicas de segurança	ELB.8	ELB.8
AWS Melhores práticas básicas de segurança	ELB.9	ELB.9
AWS Melhores práticas básicas de segurança	ELB.10	ELB.10
AWS Melhores práticas básicas de segurança	ELB.12	ELB.12
AWS Melhores práticas básicas de segurança	ELB.13	ELB.13
AWS Melhores práticas básicas de segurança	ELB.14	ELB.14
AWS Melhores práticas básicas de segurança	ELB.1	ELB.1
AWS Melhores práticas básicas de segurança	ELB v2.1	ELB.1
AWS Melhores práticas básicas de segurança	EMR.1	EMR.1

Padrão de segurança	Palavra-chave compatíveis com o Audit Manager (ID de controle padrão no Security Hub)	Documentação de controle relacionada (ID de controle de segurança correspondente no Security Hub)
AWS Melhores práticas básicas de segurança	EMR.2	EMR.2
AWS Melhores práticas básicas de segurança	ES.1	ES.1
AWS Melhores práticas básicas de segurança	ES.2	ES.2
AWS Melhores práticas básicas de segurança	ES.3	ES.3
AWS Melhores práticas básicas de segurança	ES.4	ES.4
AWS Melhores práticas básicas de segurança	ES.5	ES.5
AWS Melhores práticas básicas de segurança	ES.6	ES.6
AWS Melhores práticas básicas de segurança	ES.7	ES.7
AWS Melhores práticas básicas de segurança	ES.8	ES.8
AWS Melhores práticas básicas de segurança	EventBridge.3	EventBridge3.

Padrão de segurança	Palavra-chave compatíveis com o Audit Manager (ID de controle padrão no Security Hub)	Documentação de controle relacionada (ID de controle de segurança correspondente no Security Hub)
AWS Melhores práticas básicas de segurança	EventBridge.4	EventBridge.4
AWS Melhores práticas básicas de segurança	FSx.1	FSx.1
AWS Melhores práticas básicas de segurança	GuardDuty.1	GuardDuty.1
AWS Melhores práticas básicas de segurança	IAM.1	IAM.1
AWS Melhores práticas básicas de segurança	IAM.2	IAM.2
AWS Melhores práticas básicas de segurança	IAM.3	IAM.3
AWS Melhores práticas básicas de segurança	IAM.4	IAM.4
AWS Melhores práticas básicas de segurança	IAM.5	IAM.5
AWS Melhores práticas básicas de segurança	IAM.6	IAM.6
AWS Melhores práticas básicas de segurança	IAM.7	IAM.7

Padrão de segurança	Palavra-chave compatíveis com o Audit Manager (ID de controle padrão no Security Hub)	Documentação de controle relacionada (ID de controle de segurança correspondente no Security Hub)
AWS Melhores práticas básicas de segurança	IAM.8	IAM.8
AWS Melhores práticas básicas de segurança	IAM.9	IAM.9
AWS Melhores práticas básicas de segurança	IAM.10	IAM.10
AWS Melhores práticas básicas de segurança	IAM.11	IAM.11
AWS Melhores práticas básicas de segurança	IAM 12	IAM 12
AWS Melhores práticas básicas de segurança	IAM.13	IAM.13
AWS Melhores práticas básicas de segurança	IAM.14	IAM.14
AWS Melhores práticas básicas de segurança	IAM.15	IAM.15
AWS Melhores práticas básicas de segurança	IAM.16	IAM.16
AWS Melhores práticas básicas de segurança	IAM.17	IAM.17

Padrão de segurança	Palavra-chave compatíveis com o Audit Manager (ID de controle padrão no Security Hub)	Documentação de controle relacionada (ID de controle de segurança correspondente no Security Hub)
AWS Melhores práticas básicas de segurança	IAM.18	IAM.18
AWS Melhores práticas básicas de segurança	IAM.19	IAM.19
AWS Melhores práticas básicas de segurança	IAM.21	IAM.21
AWS Melhores práticas básicas de segurança	IAM.15	IAM.15
AWS Melhores práticas básicas de segurança	Kinesis.1	Kinesis.1
AWS Melhores práticas básicas de segurança	KMS.1	KMS.1
AWS Melhores práticas básicas de segurança	KMS.2	KMS.2
AWS Melhores práticas básicas de segurança	KMS.3	KMS.3
AWS Melhores práticas básicas de segurança	KMS.4	KMS.4
AWS Melhores práticas básicas de segurança	Lambda.1	Lambda.1

Padrão de segurança	Palavra-chave compatíveis com o Audit Manager (ID de controle padrão no Security Hub)	Documentação de controle relacionada (ID de controle de segurança correspondente no Security Hub)
AWS Melhores práticas básicas de segurança	Lambda.2	Lambda.2
AWS Melhores práticas básicas de segurança	Lambda.3	Lambda.3
AWS Melhores práticas básicas de segurança	Lambda.5	Lambda.5
AWS Melhores práticas básicas de segurança	Macie.1	Macie.1
AWS Melhores práticas básicas de segurança	MQ.5	MQ.5
AWS Melhores práticas básicas de segurança	MQ.5	MQ.5
AWS Melhores práticas básicas de segurança	MSK.1	MSK.1
AWS Melhores práticas básicas de segurança	MSK.2	MSK.2
AWS Melhores práticas básicas de segurança	Neptune.1	Neptune.1
AWS Melhores práticas básicas de segurança	Neptune.3	Neptune.3

Padrão de segurança	Palavra-chave compatíveis com o Audit Manager (ID de controle padrão no Security Hub)	Documentação de controle relacionada (ID de controle de segurança correspondente no Security Hub)
AWS Melhores práticas básicas de segurança	Neptune.3	Neptune.3
AWS Melhores práticas básicas de segurança	Neptune.3	Neptune.3
AWS Melhores práticas básicas de segurança	Neptune.3	Neptune.3
AWS Melhores práticas básicas de segurança	Neptune.3	Neptune.3
AWS Melhores práticas básicas de segurança	Neptune.3	Neptune.3
AWS Melhores práticas básicas de segurança	Neptune.3	Neptune.3
AWS Melhores práticas básicas de segurança	Neptune.9	Neptune.9
AWS Melhores práticas básicas de segurança	NetworkFirewall.1	NetworkFirewall.1
AWS Melhores práticas básicas de segurança	NetworkFirewall.2	NetworkFirewall.2
AWS Melhores práticas básicas de segurança	NetworkFirewall.3	NetworkFirewall.3

Padrão de segurança	Palavra-chave compatíveis com o Audit Manager (ID de controle padrão no Security Hub)	Documentação de controle relacionada (ID de controle de segurança correspondente no Security Hub)
AWS Melhores práticas básicas de segurança	NetworkFirewall.4	NetworkFirewall.4
AWS Melhores práticas básicas de segurança	NetworkFirewall5.	NetworkFirewall5.
AWS Melhores práticas básicas de segurança	NetworkFirewall.6	NetworkFirewall.6
AWS Melhores práticas básicas de segurança	NetworkFirewall9.	NetworkFirewall9.
AWS Melhores práticas básicas de segurança	Opensearch.1	Opensearch.1
AWS Melhores práticas básicas de segurança	Opensearch.2	Opensearch.2
AWS Melhores práticas básicas de segurança	Opensearch.3	Opensearch.3
AWS Melhores práticas básicas de segurança	Opensearch.4	Opensearch.4
AWS Melhores práticas básicas de segurança	Opensearch.5	Opensearch.5
AWS Melhores práticas básicas de segurança	Opensearch.6	Opensearch.6

Padrão de segurança	Palavra-chave compatíveis com o Audit Manager (ID de controle padrão no Security Hub)	Documentação de controle relacionada (ID de controle de segurança correspondente no Security Hub)
AWS Melhores práticas básicas de segurança	Opensearch.7	Opensearch.7
AWS Melhores práticas básicas de segurança	Opensearch.8	Opensearch.8
AWS Melhores práticas básicas de segurança	Opensearch.10	Opensearch.10
AWS Melhores práticas básicas de segurança	PCA.1	PCA.1
AWS Melhores práticas básicas de segurança	RDS.1	RDS.1
AWS Melhores práticas básicas de segurança	RDS.2	RDS 2
AWS Melhores práticas básicas de segurança	RDS.3	RDS.3
AWS Melhores práticas básicas de segurança	RDS.4	RDS.4
AWS Melhores práticas básicas de segurança	RDS.5	RDS.5
AWS Melhores práticas básicas de segurança	RDS.6	RDS.6

Padrão de segurança	Palavra-chave compatíveis com o Audit Manager (ID de controle padrão no Security Hub)	Documentação de controle relacionada (ID de controle de segurança correspondente no Security Hub)
AWS Melhores práticas básicas de segurança	RDS.7	RDS.7
AWS Melhores práticas básicas de segurança	RDS.8	RDS.8
AWS Melhores práticas básicas de segurança	RDS.9	RDS.9
AWS Melhores práticas básicas de segurança	RDS.10	RDS.10
AWS Melhores práticas básicas de segurança	RDS.11	RDS.11
AWS Melhores práticas básicas de segurança	RDS.12	RDS.12
AWS Melhores práticas básicas de segurança	RDS.13	RDS. 13
AWS Melhores práticas básicas de segurança	RDS.14	RDS.14
AWS Melhores práticas básicas de segurança	RDS.15	RDS.15
AWS Melhores práticas básicas de segurança	RDS.16	RDS.16

Padrão de segurança	Palavra-chave compatíveis com o Audit Manager (ID de controle padrão no Security Hub)	Documentação de controle relacionada (ID de controle de segurança correspondente no Security Hub)
AWS Melhores práticas básicas de segurança	RDS.17	RDS.17
AWS Melhores práticas básicas de segurança	RDS.18	RDS.18
AWS Melhores práticas básicas de segurança	RDS.19	RDS.19
AWS Melhores práticas básicas de segurança	RDS.20	RDS.20
AWS Melhores práticas básicas de segurança	RDS.21	RDS.21
AWS Melhores práticas básicas de segurança	RDS.22	RDS.22
AWS Melhores práticas básicas de segurança	RDS.23	RDS.23
AWS Melhores práticas básicas de segurança	RDS.24	RDS.24
AWS Melhores práticas básicas de segurança	RDS.25	RDS.25
AWS Melhores práticas básicas de segurança	RDS. 3	RDS. 3

Padrão de segurança	Palavra-chave compatíveis com o Audit Manager (ID de controle padrão no Security Hub)	Documentação de controle relacionada (ID de controle de segurança correspondente no Security Hub)
AWS Melhores práticas básicas de segurança	RDS. 3	RDS. 3
AWS Melhores práticas básicas de segurança	RDS. 3	RDS. 3
AWS Melhores práticas básicas de segurança	RDS. 3	RDS. 3
AWS Melhores práticas básicas de segurança	Redshift.1	Redshift.1
AWS Melhores práticas básicas de segurança	Redshift.2	Redshift.2
AWS Melhores práticas básicas de segurança	Redshift.3	Redshift.3
AWS Melhores práticas básicas de segurança	Redshift.4	Redshift.4
AWS Melhores práticas básicas de segurança	Redshift.6	Redshift.6
AWS Melhores práticas básicas de segurança	Redshift.7	Redshift.7
AWS Melhores práticas básicas de segurança	Redshift.8	Redshift.8

Padrão de segurança	Palavra-chave compatíveis com o Audit Manager (ID de controle padrão no Security Hub)	Documentação de controle relacionada (ID de controle de segurança correspondente no Security Hub)
AWS Melhores práticas básicas de segurança	Redshift.9	Redshift.9
AWS Melhores práticas básicas de segurança	Redshift.10	Redshift.10
AWS Melhores práticas básicas de segurança	Route53.2	Route53.2
AWS Melhores práticas básicas de segurança	S3.1	S3.1
AWS Melhores práticas básicas de segurança	S3.2	S3.2
AWS Melhores práticas básicas de segurança	S3.3	S3.3
AWS Melhores práticas básicas de segurança	S3.4	S3.4
AWS Melhores práticas básicas de segurança	S3.5	S3.5
AWS Melhores práticas básicas de segurança	3.6	S3.6
AWS Melhores práticas básicas de segurança	S3.7	S3.7

Padrão de segurança	Palavra-chave compatíveis com o Audit Manager (ID de controle padrão no Security Hub)	Documentação de controle relacionada (ID de controle de segurança correspondente no Security Hub)
AWS Melhores práticas básicas de segurança	S3.8	S3.8
AWS Melhores práticas básicas de segurança	S3.9	S3.9
AWS Melhores práticas básicas de segurança	S3.11	S3.11
AWS Melhores práticas básicas de segurança	S3.12	S3.12
AWS Melhores práticas básicas de segurança	S3.13	S3.13
AWS Melhores práticas básicas de segurança	S3.14	S3.14
AWS Melhores práticas básicas de segurança	S3.15	S3.15
AWS Melhores práticas básicas de segurança	S3.17	S3.17
AWS Melhores práticas básicas de segurança	S3.19	S3.19
AWS Melhores práticas básicas de segurança	S3.19	S3.20

Padrão de segurança	Palavra-chave compatíveis com o Audit Manager (ID de controle padrão no Security Hub)	Documentação de controle relacionada (ID de controle de segurança correspondente no Security Hub)
AWS Melhores práticas básicas de segurança	SageMaker.1	SageMaker.1
AWS Melhores práticas básicas de segurança	SageMaker.2	SageMaker.2
AWS Melhores práticas básicas de segurança	SageMaker.3	SageMaker.3
AWS Melhores práticas básicas de segurança	SecretsManager.1	SecretsManager.1
AWS Melhores práticas básicas de segurança	SecretsManager.2	SecretsManager.2
AWS Melhores práticas básicas de segurança	SecretsManager.3	SecretsManager.3
AWS Melhores práticas básicas de segurança	SecretsManager.4	SecretsManager.4
AWS Melhores práticas básicas de segurança	SNS.1	SNS.1
AWS Melhores práticas básicas de segurança	SNS.2	SNS.2
AWS Melhores práticas básicas de segurança	SQS.1	SQS.1

Padrão de segurança	Palavra-chave compatíveis com o Audit Manager (ID de controle padrão no Security Hub)	Documentação de controle relacionada (ID de controle de segurança correspondente no Security Hub)
AWS Melhores práticas básicas de segurança	SSM.1	SSM.1
AWS Melhores práticas básicas de segurança	SSM.2	SSM.2
AWS Melhores práticas básicas de segurança	SSM.3	SSM.3
AWS Melhores práticas básicas de segurança	SSM.4	SSM.4
AWS Melhores práticas básicas de segurança	StepFunctions.1	StepFunctions.1
AWS Melhores práticas básicas de segurança	WAF.1	WAF.1
AWS Melhores práticas básicas de segurança	WAF.2	WAF.2
AWS Melhores práticas básicas de segurança	WAF.3	WAF.3
AWS Melhores práticas básicas de segurança	WAF.4	WAF.4
AWS Melhores práticas básicas de segurança	WAF.6	WAF.6

Padrão de segurança	Palavra-chave compatíveis com o Audit Manager (ID de controle padrão no Security Hub)	Documentação de controle relacionada (ID de controle de segurança correspondente no Security Hub)
AWS Melhores práticas básicas de segurança	WAF.7	WAF.7
AWS Melhores práticas básicas de segurança	WAF.8	WAF.8
AWS Melhores práticas básicas de segurança	WAF.10	WAF.10
AWS Melhores práticas básicas de segurança	WAF.6	WAF.6
AWS Melhores práticas básicas de segurança	WAF.6	WAF.6

Chamadas de API suportadas por AWS Audit Manager

O Audit Manager faz chamadas de API Serviços da AWS para coletar um instantâneo dos detalhes de configuração de seus AWS recursos. Você pode especificar essas chamadas de API como um mapeamento da fonte de dados ao configurar um controle personalizado no Audit Manager.

Para cada recurso que está no escopo de uma chamada de API, o Audit Manager captura um snapshot da configuração e o converte em evidência. Isso resulta em uma evidência por recurso, em oposição a uma evidência por chamada de API.

Por exemplo, se a chamada de API `ec2_DescribeRouteTables` capturar snapshots de configuração de cinco tabelas de rotas, você obterá cinco evidências no total para uma única chamada de API. Cada evidência é um snapshot da configuração de uma tabela de rotas individual.

Nesta página

- Chamadas de API compatíveis com fontes de dados de controle personalizadas
- Chamadas de API paginadas
- Chamadas de API usadas na estrutura padrão AWS License Manager

Chamadas de API compatíveis com fontes de dados de controle personalizadas

Nos seus controles personalizados, você pode usar qualquer chamada de API a seguir como fonte de dados. O Audit Manager pode então usar essas chamadas de API para coletar evidências sobre seu AWS uso.

Chamada de API compatível	Como o Audit Manager usa essa API para coletar evidências
acm_ GetAccountConfiguration	Colete um snapshot das opções de configuração de conta associadas à sua Conta da AWS.
acm_ ListCertificates	Recupere uma lista de ARNs de certificados e nomes de domínio.
cloudtrail_ DescribeTrails	Colete um snapshot das configurações de uma ou mais trilhas associadas à região atual da sua Conta da AWS.
cloudwatch_ DescribeAlarms	Colete um snapshot da configuração dos alarmes que são usados para sua Conta da AWS.
configuração_ DescribeConfigRules	Recupere detalhes sobre suas AWS Config regras.
configuração_ DescribeDeliveryChannels	Colete um snapshot da configuração dos canais de entrega na sua Conta da AWS.
conexão direta_ DescribeDirectConnectGateways	Recupere uma lista de todos os seus AWS Direct Connect gateways.
conexão direta_ DescribeVirtualGateways	Recupere uma lista de gateways privados virtuais pertencentes à sua Conta da AWS.
docdb_ DescribeCertificates	Colete uma lista de certificados para sua Conta da AWS.

Chamada de API compatível	Como o Audit Manager usa essa API para coletar evidências
docdb_describeDB ClusterParameterGroups	Colete uma lista de descrições `DBClusterParameterGroup` para sua Conta da AWS.
docdb_DescribeDBInstances	Colete informações sobre instâncias provisionadas do Amazon DynamoDB para sua Conta da AWS.
dynamodb_ DescribeTable	Colete snapshots de configuração para as tabelas do DynamoDB na sua Conta da AWS. Ao usar essa API como fonte de dados, você não precisa fornecer o nome de uma tabela específica do DynamoDB. Em vez disso, o Audit Manager usa a operação `ListTables` para listar todas as suas tabelas. Para cada tabela listada, o Audit Manager executa a operação `DescribeTable` para gerar evidências para esse recurso.
dynamodb_ ListBackups	Recupere uma lista de backups do DynamoDB que estão associados à sua Conta da AWS.
dynamodb_ ListGlobalTables	Recupere uma lista de todas as tabelas globais que estão, atualmente, na sua Conta da AWS.
dynamodb_ ListTables	Recupere uma lista de todos os nomes de tabelas associados à sua Conta da AWS e ao seu endpoint atual.
ec2_ DescribeAddresses	Colete um snapshot dos seus endereços IP elásticos.
ec2_ DescribeCustomerGateways	Colete um snapshot dos seus gateways do cliente da VPN.
ec2_ DescribeEgressOnlyInternetGateways	Colete um snapshot dos seus gateways da Internet somente de saída.
ec2_ DescribeFlowLogs	Colete um snapshot dos seus logs de fluxo.
ec2_ DescribeInstances	Colete um snapshot das suas instâncias.

Chamada de API compatível	Como o Audit Manager usa essa API para coletar evidências
ec2_ DescribeInternetGateways	Colete um snapshot dos seus gateways da Internet.
ec2_ DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations	Colete uma descrição das associações entre os grupos de interface virtual e as tabelas de rotas do gateway local em seu Conta da AWS.
ec2_ DescribeLocalGateways	Colete um snapshot dos seus gateways locais.
ec2_ DescribeLocalGatewayVirtualInterfaces	Colete um snapshot das interfaces virtuais do gateway local.
ec2_ DescribeNatGateways	Colete um snapshot dos seus gateways NAT.
ec2_ DescribeNetworkAcls	Colete um snapshot das ACLs de rede.
ec2_ DescribeRouteTables	Colete um snapshot das suas tabelas de rotas.
ec2_ DescribeSecurityGroups	Colete um snapshot dos seus grupos de segurança.
ec2_ DescribeTransitGateways	Colete um snapshot dos seus gateways de trânsito.
ec2_ DescribeVolumes	Colete um snapshot dos seus endpoints da VPC.
ec2_ DescribeVpcs	Colete um snapshot das suas VPCs.
ec2_ DescribeVpcEndpoints	Colete um snapshot dos seus endpoints da VPC.
ec2_ DescribeVpcPeeringConnections	Colete um snapshot das suas conexões VPN.
ec2_ DescribeVpnConnections	Colete um snapshot das suas conexões VPN.
ec2_ DescribeVpnGateways	Colete um snapshot dos seus gateways privados virtuais.
ec2_ GetEbsDefaultKmsKeyId	Colete um instantâneo da criptografia padrão AWS KMS key do EBS para sua Conta da AWS região atual.

Chamada de API compatível	Como o Audit Manager usa essa API para coletar evidências
ec2_ GetEbsEncryptionBy Default	Descreve se a criptografia do EBS por padrão está habilitada para sua Conta da AWS na região atual.
ecs_ DescribeClusters	Colete um snapshot dos seus clusters do ECS.
eks_ DescribeAddonVersions	Colete um snapshot das suas versões de complementos.
elasticache_ DescribeC acheClusters	Colete um snapshot dos clusters provisionados.
elasticache_ DescribeS erviceUpdates	Colete um resumo das atualizações de serviços da Amazon ElastiCache.
sistema de arquivos elástico_ DescribeAccessPoints	Colete um snapshot dos pontos de acesso do Amazon EFS em seu Conta da AWS.
sistema de arquivos elástico_ DescribeFileSystems	Colete um snapshot dos seus sistemas de arquivos do Amazon EFS.
balanceamento de carga elástico v2_ DescribeL oadBalancers	Colete um instantâneo dos balanceadores de carga em seu. Conta da AWS
elasticloadbalancingv2_Desc ribeSSLPolicies	Colete um snapshot das políticas que você usa para negociação SSL.
balanceamento de carga elástico v2_ DescribeT argetGroups	Colete um snapshot dos seus grupos de destino de ELB.
elasticmareduce_ ListSecur ityConfigurations	Recupere uma lista das configurações de segurança que estão visíveis para sua Conta da AWS, junto com suas datas e horas de criação e seus nomes.
eventos_ ListConnections	Recupere uma lista das EventBridge conexões da Amazon em seu Conta da AWS.

Chamada de API compatível	Como o Audit Manager usa essa API para coletar evidências
eventos_ ListEventBuses	Recupere uma lista dos ônibus de EventBridge eventos da Amazon em seu Conta da AWS, incluindo o ônibus de eventos padrão, ônibus de eventos personalizados e ônibus de eventos de parceiros.
eventos_ ListEventSources	Recupere uma lista de fontes de eventos de parceiros que foram compartilhadas com sua Conta da AWS.
eventos_ ListRules	Recupere uma lista das suas EventBridge regras da Amazon.
mangueira de bombeiro_ ListDeliveryStreams	Recupere uma lista dos seus fluxos de entrega.
fsx_ DescribeFileSystems	Colete um snapshot dos sistemas de arquivos pertencentes à sua Conta da AWS.
guardião_ ListDetectors	Recupere uma lista dos recursos do `detectorIds` seu GuardDuty detector da Amazon.
eu sou _ GenerateCredential Report	Gere um relatório de credenciais para sua Conta da AWS.
eu sou _ GetAccoun tPasswordPolicy	Colete um snapshot da política de senhas para sua Conta da AWS.
eu sou _ GetAccoun tSummary	Colete um snapshot do uso da entidade do IAM e das cotas do IAM na sua Conta da AWS.
eu sou_ ListGroupPolicies	Recupere uma lista das políticas em linha que estão incorpora das em um grupo do IAM que está disponível em seu. Conta da AWS
eu sou_ ListGroups	Recupere uma lista dos grupos do IAM associados a um prefixo de caminho disponível em seu. Conta da AWS

Chamada de API compatível	Como o Audit Manager usa essa API para coletar evidências
iam_ ID ListOpen ConnectProviders	Recupere uma lista dos objetos de recurso de provedor OpenID Connect (OIDC) do IAM que são definidos na sua Conta da AWS.
eu sou_ ListPolicies	Recupere uma lista todas as políticas gerenciadas que estão disponíveis na sua Conta da AWS, incluindo suas próprias políticas gerenciadas definidas pelo cliente e todas as políticas gerenciadas pela AWS.
eu sou_ ListRoles	Recupere uma lista das funções do IAM associadas a um prefixo de caminho que está disponível em seu. Conta da AWS
iam_ListSAMLProviders	Recupere uma lista dos objetos de recurso do provedor SAML definidos no IAM na sua Conta da AWS.
eu sou_ ListUsers	Recupere uma lista dos usuários do IAM em seu Conta da AWS.
iam_ dispositivos MFA ListVirtual	Recupere uma lista dos dispositivos MFA virtuais que estão definidos na sua Conta da AWS.
kafka_ ListClusters	Recupere uma lista dos clusters do Amazon MSK em seu. Conta da AWS
kafka_ ListKafkaVersions	Recupere uma lista dos objetos da versão do Apache Kafka na sua Conta da AWS.
kinesis_ ListStreams	Recupere uma lista dos seus fluxos de dados do Kinesis.

Chamada de API compatível	Como o Audit Manager usa essa API para coletar evidências
kms_ GetKeyPolicy	O Audit Manager usa essa API para coletar um snapshot das políticas de chave para as AWS KMS keys na sua Conta da AWS. Ao usar essa API como fonte de dados, você não precisa fornecer o nome de uma API específica AWS KMS key. Em vez disso, o Audit Manager usa a operação `ListKeys` para listar todas as suas chaves do KMS. Para cada chave KMS listada, o Audit Manager executa a operação `GetKeyPolicy` para gerar evidências para esse recurso.
kms_ GetKeyRotationStatus	O Audit Manager usa essa API para coletar um instantâneo sobre se a rotação automática está habilitada para o AWS KMS keys em seu Conta da AWS. Ao usar essa API como fonte de dados, você não precisa fornecer o nome de uma API específica AWS KMS key. Em vez disso, o Audit Manager usa a operação `ListKeys` para listar todas as suas chaves do KMS. Para cada chave KMS listada, o Audit Manager executa a operação `GetKeyRotationStatus` para gerar evidências para esse recurso.
kms_ ListKeys	Recupere uma lista dos AWS KMS keys em seu Conta da AWS.
lambda_ ListFunctions	Recupere uma lista de funções do Lambda em Conta da AWSsua, com a configuração específica da versão de cada uma.
rds_DescribeDBClusters	Colete um snapshot dos clusters de banco de dados Amazon Aurora e dos clusters de banco de dados Multi-AZ existentes em seu. Conta da AWS
rds_DescribeDBInstances	Colete um instantâneo das instâncias provisionadas do RDS na sua Conta da AWS.
redshift_ DescribeClusters	Colete um snapshot dos clusters provisionados do Amazon Redshift na sua Conta da AWS.

Chamada de API compatível	Como o Audit Manager usa essa API para coletar evidências
s3_ GetBucketEncryption	Colete um snapshot que mostre a configuração de criptografia padrão para seus buckets do S3. Ao usar essa API como fonte de dados, você não precisa fornecer o nome de um bucket específico do S3. Em vez disso, o Audit Manager usa a operação `ListBuckets` para listar todos os seus buckets. Para cada bucket listado, o Audit Manager executa a operação `GetBucketEncryption` para gerar evidências para esse recurso. O Audit Manager só pode fornecer o status de criptografia para buckets que foram criados na Região da AWS mesma avaliação . Se você precisar ver o status de criptografia de todos os seus buckets do S3 em vários Regiões da AWS, recomendamos que você crie uma avaliação em cada um em Região da AWS que você tenha um bucket do S3.
s3_ ListBuckets	Recupere uma lista dos buckets S3 em seu. Conta da AWS
sns_ ListTopics	Recupere uma lista dos tópicos do SNS em seu. Conta da AWS
sqs_ ListQueues	Recupere uma lista das filas do SQS em seu. Conta da AWS

Chamadas de API paginadas

Muitos Serviços da AWS coletam e armazenam uma grande quantidade de dados. Como resultado, quando uma `list`, `describe` ou chamada de API `get` tenta retornar seus dados, pode haver muitos resultados. Se a quantidade de dados for muito grande para ser retornada em uma única resposta, os resultados podem ser divididos em partes mais gerenciáveis por meio do uso da paginação. Isso divide os resultados em “páginas” de dados, facilitando o manuseio das respostas.

Algumas das chamadas de API compatíveis com o Audit Manager são paginadas. Isso significa que eles retornam resultados parciais no início e exigem solicitações subsequentes para retornar todo o conjunto de resultados. Por exemplo, a operação DescribedBInstances do Amazon RDS retorna até 100 instâncias por vez, e solicitações subsequentes são necessárias para retornar a próxima página de resultados.

A partir de 08 de março de 2023, o Audit Manager oferece suporte a chamadas de API paginadas como fonte de dados para coleta de evidências. Anteriormente, se uma chamada de API paginada fosse usada como fonte de dados, somente um subconjunto dos seus recursos era devolvido na resposta da API (até 100 resultados). Agora, o Audit Manager chama a operação de API paginada várias vezes e obtém cada página de resultados até que todos os recursos sejam devolvidos. Para cada recurso, o Audit Manager captura um snapshot da configuração e o salva como evidência. Como seu conjunto completo de recursos agora está capturado na resposta da API, é provável que você perceba um aumento na quantidade de evidências coletadas.

O Audit Manager gerencia automaticamente a paginação de chamadas de API para você. Se você criar um controle personalizado que usa uma chamada de API paginada como fonte de dados, não precisa especificar nenhum parâmetro de paginação.

Chamadas de API usadas na estrutura padrão AWS License Manager

Na estrutura padrão AWS License Manager, o Audit Manager usa uma atividade personalizada chamada `GetLicenseManagerSummary` para coletar evidências. Essa atividade chama as três APIs do License Manager a seguir:

- ListLicenseConfigurations
- ListAssociationsForLicenseConfiguration
- ListUsageForLicenseConfiguration

Os dados que são retornados são então convertidos em evidências e anexados aos controles relevantes em sua avaliação.

Exemplo

Digamos que você use dois produtos licenciados (SQL Service 2017 e Oracle Database Enterprise Edition). Primeiro, a `GetLicenseManagerSummary` atividade chama a ListLicenseConfigurationsAPI, que fornece detalhes das configurações de licença em sua conta. Em seguida, ele adiciona dados contextuais adicionais para cada configuração de licença chamando ListUsageForLicenseConfiguratione. ListAssociationsForLicenseConfiguration Por fim, ele converte os dados de configuração da licença em evidência e os anexa aos respectivos controles no framework (4.5 - Licença gerenciada pelo cliente para o SQL Server 2017 e 3.0.4 - Licença gerenciada pelo cliente para o Oracle Database Enterprise Edition).

Se você estiver usando um produto licenciado que não esteja coberto por nenhum dos controles do framework, esses dados de configuração da licença serão anexados como evidência ao seguinte controle: 5.0 - Licença gerenciada pelo cliente para outras licenças.

AWS CloudTrail nomes de eventos suportados por AWS Audit Manager

Você pode capturar eventos AWS CloudTrail de gerenciamento e eventos de serviços globais como evidência no Audit Manager. Para fazer isso, você especifica o nome do CloudTrail evento como uma palavra-chave de mapeamento da fonte de dados ao criar um controle personalizado.

> **Note**
>
> O Audit Manager captura somente eventos de gerenciamento e eventos de serviços globais. Eventos de dados e eventos de insights não estão disponíveis como evidência. Para obter mais informações sobre os diferentes tipos de CloudTrail eventos, consulte CloudTrail os conceitos no GuiaAWS CloudTrail do usuário.

Como exceção ao acima exposto, os seguintes CloudTrail eventos não são suportados pelo Audit Manager:

- kms_ GenerateDataKey
- kms_Decrypt
- sts_ AssumeRole
- kinesisvideo_ GetDataEndpoint
- kinesisvideo_ GetSignalingChannelEndpoint
- kinesisvideo_ DescribeSignalingChannel
- kinesisvideo_ DescribeStream

A partir de 11 de maio de 2023, o Audit Manager não oferece mais suporte a CloudTrail eventos somente para leitura como palavras-chave para coleta de evidências. Removemos um total de 3.135 palavras-chave somente para leitura. Como os clientes e Serviços da AWS fazem chamadas de leitura para APIs, os eventos somente para leitura são ruidosos. Como resultado, palavras-chave somente para leitura coletam muitas evidências que não são confiáveis ou relevantes para auditorias. As palavras-chave somente para leitura incluem `ListDescribe`, e chamadas de `Get` API (por exemplo, GetObjecte ListBucketspara o Amazon S3). Se você estava usando uma

dessas palavras-chave para coleta de evidências, não será necessário executar nenhuma ação. As palavras-chave foram removidas automaticamente do console do Audit Manager e de suas avaliações, e as evidências não são mais coletadas para essas palavras-chave.

configurações AWS Audit Manager

É possível analisar e definir suas configurações AWS Audit Manager a qualquer momento.

Para acessar suas configurações

1. Abra o console do AWS Audit Manager em https://console.aws.amazon.com/auditmanager/home.
2. No painel de navegação a esquerda, escolha Configurações.

As seguintes configurações estão disponíveis:

- Configurações gerais
  - Permissões
  - Criptografia de dados
  - Administrador delegado (opcional)
  - AWS Config (opcional)
  - Security Hub (opcional)
  - Desabilitar AWS Audit Manager
- Configurações de avaliação
  - Proprietários de auditoria padrão (opcional)
  - Destino do relatório de avaliação (opcional)
  - Notificações (opcional)
- Configurações do localizador de evidências
  - Localizador de evidências (opcional)
  - Destino de exportação (opcional)

Configurações gerais

A guia de configurações Geral é a visualização padrão da página de configurações no console do Audit Manager. Use essa guia para analisar e atualizar suas configurações gerais do Audit Manager.

Tópicos

Permissões

AWS Audit Manager usa uma função vinculada ao serviço para conectar-se a fontes de dados em seu nome. Para obter mais informações, consulte Usando funções vinculadas a serviços para AWS Audit Manager.

Para analisar os detalhes da função vinculada ao serviço que o Audit Manager usa, escolha Visualizar permissão da função vinculada ao serviço do IAM.

Para obter mais informações sobre funções vinculadas a serviços, consulte Usando funções vinculadas a serviços no Guia do Usuário do IAM.

Criptografia de dados

O Audit Manager cria automaticamente um exclusivo Chave gerenciada pela AWS para o armazenamento seguro de seus dados. Por padrão, seus dados do Audit Manager são criptografados com essa chave KMS. Como alternativa, se quiser personalizar suas configurações de criptografia de dados, você pode especificar sua própria chave gerenciada pelo cliente com criptografia simétrica. Usar sua própria chave KMS traz mais flexibilidade, além da capacidade de criar, alternar e desabilitar chaves.

> **Important**
>
> Para gerar relatórios de avaliação e exportar os resultados da pesquisa do localizador de evidências com sucesso, sua chave gerenciada pelo cliente (caso forneça uma) deve estar na mesma Região da AWS que sua avaliação. Para ver a lista de Regiões Audit Manager, consulte AWS Audit Manager endpoints e cotas em Referência Geral Amazon Web Services.

Você pode atualizar suas configurações de criptografia de dados usando o console Audit Manager, o AWS Command Line Interface (AWS CLI), ou API Audit Manager.

Audit Manager console

Para atualizar suas configurações de criptografia de dados (console)

1. Na guia de configurações Geral, vá para a seção Criptografia de dados.
2. Para usar a chave KMS padrão fornecida pelo Audit Manager, desmarque a caixa de seleção Personalizar configurações de criptografia (avançado).
3. Para usar uma chave gerenciada pelo cliente, marque a caixa de seleção Personalizar as configurações de criptografia (avançado). É possível escolher um par de chaves KMS existente ou criar um novo.

AWS CLI

Para atualizar suas configurações de criptografia de dados (AWS CLI)

Execute o comando update-settings e use o parâmetro `--kms-key` para especificar sua própria chave gerenciada pelo cliente.

No exemplo a seguir, substitua o *`texto do espaço reservado`* por suas próprias informações.

```
aws auditmanager update-settings --kms-key arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab
```

Audit Manager API

Para atualizar suas configurações de criptografia de dados (API)

Chame o comando UpdateSettings e use o parâmetro kmsKey para especificar sua própria chave gerenciada pelo cliente.

Para obter mais informações, escolha um dos links anteriores na Referência de API Audit Manager. Isso inclui informações sobre como usar a operação e os parâmetros em um dos SDKs AWS específicos de idioma.

> **Note**
>
> Se você alterar as configurações de criptografia de dados do Audit Manager, essas alterações serão aplicadas a todas as novas avaliações criadas. Isso inclui quaisquer relatórios de avaliação e exportações do localizador de evidências que você criar a partir de suas novas avaliações.
>
> As alterações não se aplicam às avaliações existentes criadas antes de alterar suas configurações de criptografia. Isso inclui novos relatórios de avaliação e exportações de CSV a partir de avaliações existentes, além de relatórios de avaliação e exportações de CSV existentes. As avaliações existentes — e todos os respectivos relatórios de avaliação e exportações de CSV — continuam usando a antiga chave KMS.
>
> Se o identificador do IAM que gera o relatório de avaliação não puder usar a chave KMS antiga, conceda permissões no nível da política de chaves. Para obter instruções Permitir que usuários de outras contas usem uma chave do KMS no Guia do Desenvolvedor do AWS Key Management Service.

Para obter instruções sobre como criar chaves, consulte Criando chaves no Guia do UsuárioAWS Key Management Service.

Administrador delegado (opcional)

Se você usa AWS Organizations e deseja habilitar o suporte de várias contas para o Audit Manager, você pode designar uma conta membro em sua organização como administrador delegado do Audit Manager.

Pré-requisitos

- Sua conta deve ser membro de uma organização. Para obter mais informações, consulte Criando e gerenciando uma organização no Guia do UsuárioAWS Organizations.
- Antes de designar um administrador delegado, você deve ativar todos os atributos em sua organização. Você também deve definir as configurações do Security Hub da sua organização. Dessa forma, o Audit Manager pode coletar evidências do Security Hub de suas contas membro.
- A conta do administrador delegado deve ter acesso a chave KMS fornecida ao configurar o Audit Manager. Para analisar e alterar suas configurações de criptografia, consulteCriptografia de dados.

Considerações importantes para administradores delegados no Audit Manager

Observe os seguintes fatores que definem como o administrador delegado opera no Audit Manager:

Uso de conta de gerenciamento

Você não pode usar sua conta de gerenciamento do AWS Organizations como administrador delegado no Audit Manager.

Usando administradores delegados em vários Regiões da AWS

Se você quiser habilitar o Audit Manager em mais de uma Região da AWS, deverá designar uma conta de administrador delegada separadamente em cada região. Nas configurações do Audit Manager, você deve usar a mesma conta de administrador delegado em todas as regiões.

Tarefa de limpeza do localizador de evidências

Antes de usar sua conta de gerenciamento para remover ou alterar um administrador delegado, certifique-se de que a conta atual do administrador delegado faça login no Audit Manager e desabilite o localizador de evidências. A desativação do localizador de evidências exclui automaticamente o armazenamento de dados do evento criado na conta quando o localizador de evidências foi ativado.

Se essa tarefa não for concluída, o armazenamento de dados do evento permanecerá em sua conta. Nesse caso, recomendamos que o administrador delegado original use o CloudTrail Lake para excluir o armazenamento de dados do evento manualmente.

Essa tarefa de limpeza é necessária para garantir que você não acabe com vários armazenamentos de dados de eventos. O Audit Manager ignora um armazenamento de dados de eventos não utilizado depois que você remove ou altera uma conta de administrador delegado. No entanto, se você não excluir o armazenamento de dados de eventos não utilizado, o armazenamento de dados de eventos continuará incorrendo em custos de armazenamento do CloudTrail Lake.

Exclusão de dados

Quando você remove uma conta de administrador delegado do Audit Manager, os dados dessa conta não são excluídos. Se você quiser excluir dados de atributos de uma conta de administrador delegado, deverá executar essa tarefa separadamente antes de remover a conta. Você também pode fazer isso no console do Audit Manager. Ou usar uma das operações de exclusão da API fornecidas pelo Audit Manager. Para obter uma lista das operações de exclusão disponíveis, consulte Exclusão de dados do Audit Manager.

No momento, o Audit Manager não oferece a opção de excluir evidências de um administrador delegado específico. Em vez disso, quando sua conta de gerenciamento cancela o registro do Audit Manager, realizamos uma limpeza na conta atual do administrador delegado no momento do cancelamento.

Para soluções para problemas comuns do Organizations e administradores delegados no Audit Manager, consulte Solução de problemas de administradores delegados e do AWS Organizations.

Gerenciando a conta do seu administrador delegado para o Audit Manager

Você pode analisar e alterar as configurações da sua conta de administrador delegado da seguinte maneira:

Adicionar um administrador delegado

Você pode adicionar um administrador delegado usando o console do Audit Manager, o AWS Command Line Interface (AWS CLI) ou a API do Audit Manager.

> **Note**
>
> Depois de adicionar um administrador delegado nas configurações do Audit Manager, sua conta de gerenciamento não poderá mais criar avaliações adicionais no Audit Manager. Além disso, a coleta de evidências é interrompida para qualquer avaliação existente criada pela conta de gerenciamento. O Audit Manager coleta e anexa evidências à conta do administrador delegado, que é a conta principal destinada a gerenciar as avaliações da sua organização.

Audit Manager console

Como adicionar um administrador delegado (console)

1. Na guia de configurações Geral, vá para a seção Administrador delegado.
2. Em ID da conta de administrador delegado, insira o ID da conta do administrador delegado.
3. Escolha Delegar.

AWS CLI

Como adicionar um administrador delegado (AWS CLI)

Execute o comando register-organization-admin-account e use o parâmetro `--admin-account-id` para especificar o ID da conta do administrador delegado.

No exemplo a seguir, substitua o *texto do espaço reservado* por suas próprias informações.

```
aws auditmanager register-organization-admin-account --admin-account-id 111122223333
```

Audit Manager API

Como adicionar um administrador delegado (API)

Chame a operação RegisterOrganizationAdminAccount e use o parâmetro adminAccountId para especificar o ID da conta do administrador delegado.

Para obter mais informações, escolha um dos links anteriores na Referência de API Audit Manager. Isso inclui informações sobre como usar a operação e os parâmetros em um dos SDKs AWS específicos de idioma.

Alterar um administrador delegado

Você pode alterar um administrador delegado usando o console do Audit Manager, o AWS Command Line Interface (AWS CLI) ou a API do Audit Manager.

> **Warning**
>
> Ao alterar um administrador delegado, você continua a ter acesso às evidências coletadas anteriormente na antiga conta de administrador delegado. No entanto, o Audit Manager para de coletar e anexar evidências a antiga conta de administrador delegado.

Audit Manager console

Para alterar o administrador delegado atual (console)

1. (Opcional) Se o administrador delegado atual (conta A) habilitou o localizador de evidências, execute a seguinte tarefa de limpeza:

   - Antes de atribuir a conta B como novo administrador delegado, certifique-se de que a conta A entrou no Audit Manager e desabilitou o localizador de evidências.

A desativação do localizador de evidências exclui automaticamente o armazenamento de dados do evento criado quando a conta A habilitar o localizador de evidências. Se você não concluir essa etapa, a conta A deverá acessar o CloudTrail Lake e excluir o armazenamento de dados do evento manualmente. Caso contrário, o armazenamento de dados do evento permanecerá na conta A e continuará incorrendo em cobranças de armazenamento do CloudTrail Lake.

2. Na guia de configurações Geral, vá para a seção Administrador delegado e escolha Remover.
3. Na janela exibida, escolha Remover para confirmar.
4. Em ID da conta de administrador delegado, insira o ID da nova conta de administrador delegado.
5. Escolha Delegar.

AWS CLI

Antes de começar

Se o administrador delegado atual (conta A) habilitou o localizador de evidências, execute a seguinte tarefa de limpeza:

Antes de atribuir a conta B como novo administrador delegado, certifique-se de que a conta A entrou no Audit Manager e desabilitou o localizador de evidências.

A desativação do localizador de evidências exclui automaticamente o armazenamento de dados do evento criado quando a conta A habilitar o localizador de evidências. Se você não concluir essa etapa, a conta A deverá acessar o CloudTrail Lake e excluir o armazenamento de dados do evento manualmente. Caso contrário, o armazenamento de dados do evento permanecerá na conta A e continuará incorrendo em cobranças de armazenamento do CloudTrail Lake.

Para alterar o administrador delegado atual (AWS CLI)

Primeiro, execute o comando deregister-organization-admin-account usando o parâmetro `--admin-account-id` para especificar o ID da conta do administrador delegado atual.

No exemplo a seguir, substitua o *`texto do espaço reservado`* por suas próprias informações.

```
aws auditmanager deregister-organization-admin-account --admin-account-
id 111122223333
```

Primeiro, execute o comando register-organization-admin-account usando o parâmetro `--admin-account-id` para especificar o ID da conta do administrador delegado atual.

No exemplo a seguir, substitua o *texto do espaço reservado* por suas próprias informações.

```
aws auditmanager register-organization-admin-account --admin-account-id 444455556666
```

Audit Manager API

Antes de começar

Se o administrador delegado atual (conta A) habilitou o localizador de evidências, execute a seguinte tarefa de limpeza:

Antes de atribuir a conta B como novo administrador delegado, certifique-se de que a conta A entrou no Audit Manager e desabilitou o localizador de evidências.

A desativação do localizador de evidências exclui automaticamente o armazenamento de dados do evento criado quando a conta A habilitar o localizador de evidências. Se você não concluir essa etapa, a conta A deverá acessar o CloudTrail Lake e excluir o armazenamento de dados do evento manualmente. Caso contrário, o armazenamento de dados do evento permanecerá na conta A e continuará incorrendo em cobranças de armazenamento do CloudTrail Lake.

Para alterar o administrador delegado atual (API)

Primeiro, chame a operação DeregisterOrganizationAdminAccount e use o parâmetro adminAccountId para especificar o ID da conta do administrador delegado atual.

Em seguida, chame a operação RegisterOrganizationAdminAccount e use o parâmetro adminAccountId para especificar o ID da conta do administrador delegado.

Para obter mais informações, escolha um dos links anteriores na Referência de API Audit Manager. Isso inclui informações sobre como usar a operação e os parâmetros em um dos SDKs AWS específicos de idioma.

Para remover um administrador delegado

Você pode remover um administrador delegado usando o console do Audit Manager, o AWS Command Line Interface (AWS CLI) ou a API do Audit Manager.

> **Warning**
>
> Ao remover um administrador delegado, você continua a ter acesso às evidências coletadas anteriormente nessa conta de administrador delegado. No entanto, o Audit Manager para de coletar e anexar evidências a antiga conta de administrador delegado.

Audit Manager console

Para remover o administrador delegado atual (console)

1. Se o administrador delegado atual (conta A) habilitar o localizador de evidências, execute a seguinte tarefa de limpeza:

   - Certifique-se de que a conta atual do administrador delegado entre no Audit Manager e desabilite o localizador de evidências.

     A desativação do localizador de evidências exclui automaticamente o armazenamento de dados do evento criado na conta quando o localizador de evidências foi habilitado. Se essa etapa não for concluída, a conta do administrador delegado deverá usar o CloudTrail Lake para excluir o armazenamento de dados do evento manualmente. Caso contrário, o armazenamento de dados do evento permanecerá em sua conta e continuará incorrendo em cobranças de armazenamento do CloudTrail Lake.
2. Na guia de configurações Geral, vá para a seção Administrador delegado e escolha Remover.
3. Na janela exibida, escolha Remover para confirmar.

AWS CLI

Antes de começar

Se o administrador delegado atual tiver habilitado o localizador de evidências, execute a seguinte tarefa de limpeza:

Certifique-se de que a conta atual do administrador delegado entre no Audit Manager e desabilite o localizador de evidências.

A desativação do localizador de evidências exclui automaticamente o armazenamento de dados do evento criado na conta quando o localizador de evidências foi habilitado. Se essa etapa não for concluída, a conta do administrador delegado deverá usar o CloudTrail Lake para excluir o armazenamento de dados do evento manualmente. Caso contrário, o armazenamento de dados do evento permanecerá em sua conta e continuará incorrendo em cobranças de armazenamento do CloudTrail Lake.

Para remover o administrador delegado atual (AWS CLI)

Execute o comando deregister-organization-admin-account e use o parâmetro `--admin-account-id` para especificar o ID da conta do administrador delegado.

No exemplo a seguir, substitua o *`texto do espaço reservado`* por suas próprias informações.

```
aws auditmanager deregister-organization-admin-account --admin-account-
id 111122223333
```

Audit Manager API

Antes de começar

Se o administrador delegado atual tiver habilitado o localizador de evidências, execute a seguinte tarefa de limpeza:

Certifique-se de que a conta atual do administrador delegado entre no Audit Manager e desabilite o localizador de evidências.

A desativação do localizador de evidências exclui automaticamente o armazenamento de dados do evento criado na conta quando o localizador de evidências foi habilitado. Se essa etapa não for concluída, a conta do administrador delegado deverá usar o CloudTrail Lake para excluir o armazenamento de dados do evento manualmente. Caso contrário, o armazenamento de dados do evento permanecerá em sua conta e continuará incorrendo em cobranças de armazenamento do CloudTrail Lake.

Para remover o administrador delegado atual (API)

Chame a operação DeregisterOrganizationAdminAccount e use o parâmetro AdminAccountId para especificar o ID da conta do administrador delegado.

Para obter mais informações, escolha um dos links anteriores na Referência de API Audit Manager. Isso inclui informações sobre como usar a operação e os parâmetros em um dos SDKs AWS específicos de idioma.

AWS Config (opcional)

Você pode permitir que o Audit Manager colete descobertas de AWS Config. Quando AWS Config estiver ativado, o Audit Manager pode capturar telas de sua postura de segurança de atributos relatando os resultados das verificações de regras diretamente de AWS Config. Recomendamos que você ative AWS Config para obter uma experiência ideal no Audit Manager.

Para habilitar AWS Config, escolha Habilitar AWS Config para acessar esse serviço. Para obter instruções sobre como habilitar AWS Config, consulte ConfigurandoAWS Config no Guia do DesenvolvedorAWS Config.

Security Hub (opcional)

Essa etapa garante que o Audit Manager importará descobertas AWS Security Hub para todos os padrões de conformidade suportados. Quando o Security Hub estiver habilitado, o Audit Manager poderá capturar telas de sua postura de segurança de atributos relatando os resultados das verificações de segurança diretamente do Security Hub. Recomendamos que você ative Security Hub para obter uma experiência Ideal no Audit Manager.

Para habilitar o Security Hub, escolha Habilitar Security Hub para acessar esse serviço. Para obter instruções sobre como habilitar o Security Hub, consulte Configurando AWS Security Hub em Guia do Usuário Security Hub.

Desabilitar AWS Audit Manager

Você pode desabilitar o Audit Manager se não quiser mais usar o serviço. Ao desabilitar o Audit Manager, você também tem a opção de excluir todos os seus dados.

Por padrão, seus dados não são excluídos quando você desativa o Audit Manager. Seus dados de evidência são retidos por dois anos a partir do momento de sua criação. Seus outros atributos do Audit Manager (incluindo avaliações, controles personalizados e estruturas personalizadas) são

retidos indefinidamente e estarão disponíveis se você reativar o Audit Manager no futuro. Para obter mais informações sobre retenção de dados, consulte Proteção de Dados neste guia.

Se você optar por excluir seus dados, o Audit Manager excluirá todos os dados de evidências junto com todos os atributos do Audit Manager que você criou (incluindo avaliações, controles personalizados e estruturas personalizadas). Todos os seus dados são excluídos sete dias após a desativação do Audit Manager.

⚠ Warning

- Quando você desativa o Audit Manager, seu acesso é revogado e o serviço não coleta mais evidências de nenhuma avaliação existente. Você não pode acessar nada no serviço a menos que reabilite o Audit Manager.
- Excluir todos os dados é uma ação permanente. Se você decidir reativar o Audit Manager no futuro, seus dados não poderão ser recuperados.

Você pode desabilitar o Audit Manager usando o console do Audit Manager, o AWS Command Line Interface (AWS CLI) ou a API do Audit Manager.

Audit Manager console

Para desabilitar o Audit Manager (console)

1. Na guia de configurações Geral, vá para a seção Desabilitar AWS Audit Manager.
2. Escolha desabilitar.
3. Na janela, analise sua configuração atual de retenção de dados.
    a. Para continuar com sua seleção atual, escolha desabilitar Audit Manager.
    b. Para alterar sua seleção atual, execute as seguintes etapas:
        i. Escolha Cancelar para retornar a página de configurações.
        ii. Para usar a configuração padrão de retenção de dados, desative Excluir todos os dados. Essa seleção retém dados de evidências por dois anos a partir do momento de sua criação, além de outros atributos do Audit Manager, indefinidamente.
        iii. Para excluir seus dados, ative Excluir todos os dados.

iv. Escolha Desabilitar e, em seguida, escolha Desabilitar Audit Manager para confirmar sua escolha.

AWS CLI

Antes de começar

Antes de desabilitar o Audit Manager, você pode executar o comando update-settings para configurar sua política de retenção de dados preferida. Por padrão, o Audit Manager retém seus dados. Se você quiser solicitar a exclusão de seus dados, use o parâmetro `--deregistration-policy` com o valor `deleteResources` configurado como `ALL`.

```
aws auditmanager update-settings --deregistration-policy deleteResources=ALL
```

Para desabilitar o Audit Manager (AWS CLI)

Quando estiver pronto para desabilitar o Audit Manager, execute o comando deregister-account.

```
aws auditmanager deregister-account
```

Audit Manager API

Antes de começar

Antes de desabilitar o Audit Manager, você pode usar a operação da API UpdateSettings para configurar sua política de retenção de dados preferida. Por padrão, o Audit Manager retém seus dados. Se quiser excluir seus dados, você pode usar o atributo DeregistrationPolicy para solicitar a exclusão de seus dados.

Para desabilitar o Audit Manager (API)

Quando você estiver pronto para desabilitar o Audit Manager, chame a operação DeregisterAccount.

Para obter mais informações, escolha um dos links anteriores na Referência de API Audit Manager. Isso inclui informações sobre como usar essas operações e os parâmetros em um dos SDKs da AWS específicos do idioma.

Para reabilitar o Audit Manager depois de desabilitá-lo

Acesse a página inicial do serviço Audit Manager e siga as etapas para configurar o Audit Manager como um novo usuário. Para obter mais informações, consulte Configurar o AWS Audit Manager.

> **Tip**
>
> - Se você optou por excluir seus dados ao desabilitar o Audit Manager, deverá esperar até que seus dados sejam excluídos antes de poder reativar o serviço. Dependendo da quantidade de dados, isso pode levar até sete dias. No entanto, sinta-se à vontade para tentar reabilitar o Audit Manager antes disso. Em muitos casos, os dados são excluídos em menos de uma hora.
> - Se você optou por não excluir seus dados ao desabilitar o Audit Manager, suas avaliações existentes passaram para um estado inativo e, como resultado, interromperão a coleta de evidências. Para começar a coletar evidências novamente para uma avaliação preexistente, edite a avaliação e escolha Salvar sem fazer nenhuma alteração.

Configurações de avaliação

Use essa guia para analisar e atualizar suas configurações de avaliação.

Tópicos

Proprietários de auditoria padrão (opcional)

Você pode especificar os proprietários de auditoria padrão com acesso primário às suas avaliações no Audit Manager.

Você pode atualizar essa configuração usando o console Audit Manager, o AWS Command Line Interface (AWS CLI), ou API Audit Manager.

Audit Manager console

Você pode escolher entre os Contas da AWS listados na tabela ou usar a barra de pesquisa para procurar outros Contas da AWS.

Para atualizar suas configurações padrão de proprietários de auditoria (console)

1. Na guia de configurações Avaliação, vá até a seção Proprietários de auditoria padrão e escolha Editar.
2. Para adicionar um proprietário de auditoria padrão, marque a caixa de seleção ao lado do nome da conta em Proprietário da auditoria.
3. Para adicionar um proprietário de auditoria padrão, marque a caixa de seleção ao lado do nome da conta, em Proprietário da auditoria.
4. Quando terminar, escolha Salvar.

AWS CLI

Para atualizar suas configurações padrão de proprietário de auditoria (AWS CLI)

Execute o comando update-settings e use o parâmetro `--default-process-owners` para especificar um proprietário de auditoria.

No exemplo a seguir, substitua o *`texto do espaço reservado`* por suas próprias informações. Note que `roleType` só pode ser `PROCESS_OWNER`.

```
aws auditmanager update-settings --default-process-owners
 roleType=PROCESS_OWNER,roleArn=arn:aws:iam::111122223333:role/Administrator
```

Audit Manager API

Para atualizar suas configurações padrão de proprietário de auditoria (API)

Chame a operação UpdateSettings e use o parâmetro defaultProcessOwners para especificar os proprietários de auditoria padrão. Note que `roleType` só pode ser `PROCESS_OWNER`.

Para obter mais informações sobre proprietários de auditoria, consulte Proprietários de auditoria na seção Conceitos e terminologia deste guia.

Destino do relatório de avaliação (opcional)

Quando você gera um relatório de avaliação, o Audit Manager publica o relatório no bucket do S3 de sua preferência. Esse bucket do S3 é chamado de destino do relatório de avaliação. Você pode escolher o bucket do Amazon S3 no qual o Audit Manager armazenará seus relatórios de avaliação.

Você pode atualizar essa configuração usando o console Audit Manager, o AWS Command Line Interface (AWS CLI), ou API Audit Manager.

Audit Manager console

Para atualizar as configurações de destino do relatório de avaliação (console)

1. Na guia configurações Avaliação, vá para a seção Destino do relatório de avaliação
2. Para usar um bucket do Amazon S3 existente, selecione um nome de bucket no menu suspenso.
3. Para criar um novo bucket Amazon S3, escolha Criar um novo bucket.
4. Quando terminar, escolha Salvar.

AWS CLI

Para atualizar as configurações de destino do seu relatório de avaliação (AWS CLI)

Execute o comando update-settings e use o parâmetro `--default-assessment-reports-destination` para especificar um bucket do S3.

No exemplo a seguir, substitua o *`texto do espaço reservado`* por suas próprias informações.

```
aws auditmanager update-settings --default-assessment-reports-destination
 destinationType=S3,destination=s3://doc-example-destination-bucket
```

Audit Manager API

Para atualizar as configurações de destino do relatório de avaliação (API)

Chame a operação UpdateSettings e use o parâmetro defaultAssessmentReportsDestination para especificar um bucket S3.

Para obter mais informações sobre como criar um bucket do S3, consulte Criando um bucket, no Guia do Usuário Amazon S3.

Dicas de configuração para o destino do seu relatório de avaliação

Para garantir a geração bem-sucedida do seu relatório de avaliação, recomendamos que você verifique as seguintes configurações para o destino do relatório de avaliação.

Buckets de mesma Região

Recomendamos um bucket S3 no mesmo Região da AWS da sua avaliação. Quando você usa um repositório e uma avaliação de mesma Região, seu relatório de avaliação pode incluir até 22.000 itens de evidência. Por outro lado, quando você usa um intervalo e avaliação entre Regiões, somente 3.500 itens de evidência podem ser incluídos.

Região da AWS

A Região da AWS da sua chave gerenciada pelo cliente (caso tenha fornecido uma) deve corresponder a Região de sua avaliação e ao bucket S3 de destino do relatório de avaliação. Para obter instruções sobre como alterar a chave do KMS, consulte Configurações do AWS Audit Manager, criptografia de dados. Para obter instruções sobre como alterar o bucket do S3, consulte Configurações do AWS Audit Manager, destino do relatório de avaliação. Para ver a lista de Regiões Audit Manager suportadas, consulte AWS Audit Manager endpoints e cotas em Referência Geral Amazon Web Services.

criptografia do bucket do S3

Se o destino do seu relatório de avaliação tiver uma política de bucket que exija criptografia do lado do servidor (SSE) usando SSE-KMS, a chave KMS usada nessa política de bucket deverá corresponder a chave KMS definida nas configurações de criptografia de dados do Audit Manager. Se você não configurou uma chave KMS nas configurações do Audit Manager e sua política de bucket de destino do relatório de avaliação exige SSE, certifique-se de que a política de bucket permite SSE-S3. Para obter instruções sobre como configurar a chave KMS usada para criptografia de dados, consulte Configurações de criptografia de dados.

Buckets do S3 entre contas

O uso de um bucket S3 entre contas como destino do relatório de avaliação não é suportado no console do Audit Manager. É possível especificar um bucket entre contas como destino do relatório de avaliação usando o AWS CLI ou um dos SDKs AWS, mas, para simplificar, recomendamos que você não faça isso. Se você optar por usar um bucket S3 entre contas como destino do relatório de avaliação, considere os seguintes pontos:

- Por padrão, objetos S3 como relatórios de avaliação são de propriedade da Conta da AWS que carrega o objeto. Você pode usar a configuração Propriedade de Objeto S3 para alterar esse comportamento padrão, de maneira que todos os novos objetos gravados por contas com a lista de controle de acesso (ACL) padrão `bucket-owner-full-control` tornem-se automaticamente propriedade do proprietário do bucket.

Embora não seja obrigatório, recomendamos que você faça as seguintes alterações nas configurações entre contas do bucket. Fazer essas alterações garante que o proprietário do bucket tenha controle total sobre os relatórios de avaliação publicados por você no bucket dele.

- Configure a propriedade do objeto do bucket S3 como preferencial do proprietário do bucket, em vez do gravador de objeto padrão
- Adicione uma política de bucket para garantir que os objetos carregados para esse bucket tenham a ACL `bucket-owner-full-control`

- Para permitir que o Audit Manager publique relatórios em um bucket S3 entre contas, você deve adicionar a seguinte política de bucket do S3 ao destino do relatório de avaliação: Substitua o *espaço reservado de texto* por suas próprias informações. O elemento `Principal` dessa política é o usuário ou a função que possui a avaliação e cria o relatório de avaliação. `Resource` Especifica o bucket S3 entre contas onde o relatório é publicado.

```
{
  "Version": "2012-10-17",
  "Statement": [
      {
          "Sid": "Allow cross account assessment report publishing",
          "Effect": "Allow",
          "Principal": {
              "AWS":
 "arn:aws:iam::AssessmentOwnerAccountId:user/AssessmentOwnerUserName"
          },
          "Action": [
              "s3:ListBucket",
              "s3:PutObject",
              "s3:GetObject",
              "s3:GetBucketLocation",
              "s3:PutObjectAcl",
              "s3:DeleteObject"
          ],
          "Resource": [
              "arn:aws:s3:::CROSS-ACCOUNT-BUCKET",
              "arn:aws:s3:::CROSS-ACCOUNT-BUCKET/*"
          ]
      }
  ]
}
```

Notificações (opcional)

O Audit Manager pode enviar notificações para o tópico Amazon SNS especificado por você nessa configuração. Se você for assinante desse tópico do SNS, receberá notificações ao entrar no Audit Manager.

Você pode atualizar essa configuração usando o console Audit Manager, o AWS Command Line Interface (AWS CLI), ou API Audit Manager.

Audit Manager console

Para atualizar configurações de notificação (console)

1. Na guia de configurações Avaliação, vá para a seção Notificações.
2. Para usar um tópico do SNS existente, selecione o nome do tópico no menu suspenso.
3. Para criar um novo tópico do SNS, escolha Criar novo tópico.
4. Quando terminar, escolha Salvar.

AWS CLI

Para atualizar configurações de notificação (AWS CLI)

Execute o comando update-settings e use o parâmetro `--sns-topic` para especificar um tópico do SNS.

No exemplo a seguir, substitua o *`texto do espaço reservado`* por suas próprias informações.

```
aws auditmanager update-settings --sns-topic arn:aws:sns:us-east-1:111122223333:my-assessment-topic
```

Audit Manager API

Para atualizar suas configurações de notificação (API)

Chame a operação UpdateSettings e use o parâmetro snsStopic para especificar um tópico SNS.

> **Note**
>
> Você pode usar um tópico SNS padrão ou um tópico FIFO (first-in-first-out, ou primeiro entrar, primeiro a sair). Embora o Audit Manager suporte o envio de notificações para tópicos FIFO, a ordem na qual as mensagens serão enviadas não é garantida.
> Se você quiser usar um tópico do Amazon SNS do qual não seja o proprietário, configure sua política do (IAM) AWS Identity and Access Management. Mais especificamente, você deve configurá-lo para permitir a publicação a partir do Nome do Recurso da Amazon (ARN) do tópico. Para obter mais informações sobre IAM, consulte Identidade e gestão de acesso para AWS Audit Manager.

Para saber mais sobre a lista de ações que invocam notificações no Audit Manager, consulte Notificações em AWS Audit Manager.

Para obter instruções sobre como criar um tópico do Amazon SNS, consulte Criando um tópico do Amazon SNS do Guia do Usuário Amazon SNS.

Configurações do localizador de evidências

Use essa guia para analisar e atualizar suas configurações de localizador de evidências.

Tópicos

- Localizador de evidências (opcional)
- Destino de exportação (opcional)

Localizador de evidências (opcional)

É altamente recomendável habilitar o localizador de evidências. A ativação desse atributo é necessária se você quiser executar consultas de pesquisa sobre suas evidências.

Siga estas etapas para ativar, desabilitar ou verificar o status do localizador de evidências.

Habilite o localizador de evidências

Você deve habilitar o localizador de evidências em cada Região da AWS onde quiser pesquisar evidências. Se você for um administrador delegado do Audit Manager, habilite o localizador de evidências para pesquisar evidências para todas as contas membros em sua organização.

Permissões necessárias para habilitar o localizador de evidências

Para habilitar o localizador de evidências, você precisa de permissões para criar e gerenciar um armazenamento de dados de eventos no CloudTrail Lake. Para usar o atributo, você precisa de permissões para realizar consultas do CloudTrail Lake. Para ver um exemplo de política de permissão, consulte Permitir acesso total do administrador.

Se você precisar de ajuda com permissões, entre em contato com seu administrador AWS. Se você for administrador da AWS, poderá copiar a instrução de permissão necessária e anexá-la a uma política do IAM.

Solicitando ativação do localizador de evidências

Você pode completar essa tarefa usando o console Audit Manager, o AWS Command Line Interface (AWS CLI), ou API Audit Manager.

Audit Manager console

Para solicitar a ativação do localizador de evidências (console)

1. Abra o console do AWS Audit Manager em https://console.aws.amazon.com/auditmanager/home.
2. Na guia de configurações Localizador de evidências, vá para a seção Localizador de evidências.
3. Escolha Política de permissão necessária e, em seguida, Visualizar permissões do CloudTrail Lake para visualizar as permissões necessárias do localizador de evidências. Se você ainda não tem essas permissões, pode copiar essa declaração de política e anexar a uma política do IAM.
4. Escolha Habilitar.
5. Na janela, escolha Solicitar para habilitar.

AWS CLI

Para solicitar a ativação do localizador de evidências (AWS CLI)

Execute o comando update-settings com o parâmetro `--evidence-finder-enabled` .

```
aws auditmanager update-settings --evidence-finder-enabled
```

Audit Manager API

Para solicitar a habiltação do localizador de evidências (API)

Chame a operação UpdateSettings e use o parâmetro evidenceFinderEnabled.

Para obter mais informações, escolha um dos links anteriores na Referência de API Audit Manager. Isso inclui informações sobre como usar a operação e os parâmetros em um dos SDKs AWS específicos de idioma.

Confirme o status do localizador de evidências

Depois de enviar sua solicitação, são necessários até 10 minutos para ativar o localizador de evidências e criar um armazenamento de dados de eventos. Assim que o armazenamento de dados do evento é criado, todas as novas evidências serão ingeridas no armazenamento de dados do evento futuramente.

Quando o localizador de evidências é ativado e o armazenamento de dados do evento é criado, preenchemos o repositório de dados de eventos recém-criado com até dois anos de evidências anteriores. Esse processo acontece automaticamente e leva até sete dias para ser concluído.

Você pode verificar o status atual do localizador de evidências usando o console do Audit Manager, o AWS CLI ou a API do Audit Manager.

Audit Manager console

Para ver o status atual do localizador de evidências (console)

1. Abra o console do AWS Audit Manager em https://console.aws.amazon.com/auditmanager/home.
2. No painel de navegação à esquerda, escolha Configurações.
3. Em Habilitar localizador de evidências — opcional, analise o status atual.

   Cada status é definido da seguinte forma:

   - localizador de evidências não está ativado — Você ainda não habilitou com sucesso o localizador de evidências.
   - Você solicitou a desativação do localizador de evidências –- sua solicitação está pendente de armazenamento de dados de evento sendo criado.

- localizador de evidências está desativado — O armazenamento de dados do evento foi criado. Agora você pode usar o localizador de evidências.

  A depender da quantidade de evidências, serão necessários até sete dias para preencher o novo armazenamento de dados de eventos com seus dados de evidências anteriores. Um painel de informações azul indica que o preenchimento de dados está em andamento. Enquanto isso, sinta-se à vontade para começar a explorar o localizador de evidências. No entanto, lembre-se que nem todos os dados estarão disponíveis até que o preenchimento seja concluído.
- Você solicitou a desativação do localizador de evidências — Sua solicitação está pendente de exclusão de armazenamento de dados do evento.
- Localizador de evidências foi desativado — O localizador de evidências foi desativado permanentemente e o armazenamento de dados do evento, excluído.

AWS CLI

Para ver o status atual do localizador de evidências (AWS CLI)

Execute o comando get-settings com o parâmetro `--attribute` configurado para `EVIDENCE_FINDER_ENABLEMENT`.

```
aws auditmanager get-settings --attribute EVIDENCE_FINDER_ENABLEMENT
```

Este procedimento retorna as informações a seguir:

enablementStatus

Esse atributo mostra o status atual do localizador de evidência.

- `ENABLE_IN_PROGRESS` — Você solicitou a ativação do localizador de evidências. Atualmente, um armazenamento de dados de eventos está sendo criado para dar suporte às consultas de localizador de evidência.
- `ENABLED` — Um armazenamento de dados de eventos foi criado e o localizador de evidências está ativado. Recomendamos esperar sete dias até que o armazenamento de dados do evento seja preenchido com seus dados de evidências anteriores. Enquanto isso, você pode usar o localizador de evidências, mas nem todos os dados estarão disponíveis até que o preenchimento seja concluído.

- `DISABLE_IN_PROGRESS` — Você solicitou a desativação do localizador de evidências e sua solicitação está pendente de exclusão do armazenamento de dados do evento.
- `DISABLED` — Você desabilitou permanentemente o localizador de evidências e o armazenamento de dados do evento é excluído. Você não pode reativar o localizador de evidências após esse ponto.

backfillStatus

Esse atributo mostra o status atual do preenchimento dos dados de evidência.

- `NOT_STARTED` — O preenchimento ainda não começou.
- `IN_PROGRESS` — O preenchimento está em andamento. Isso leva até sete dias para ser concluído, de acordo com a quantidade de dados de evidência.
- `COMPLETED` — O preenchimento está completo. Todas as suas evidências anteriores agora podem ser consultadas.

Audit Manager API

Para ver o status atual do localizador de evidências (API)

Chame a operação GetSettings com o `attribute` parâmetro configurado para `EVIDENCE_FINDER_ENABLEMENT`. Este procedimento retorna as informações a seguir:

enablementStatus

Esse atributo mostra o status atual do localizador de evidência.

- `ENABLE_IN_PROGRESS` - Você solicitou a ativação do localizador de evidências. Atualmente, um armazenamento de dados de eventos está sendo criado para dar suporte às consultas de localizador de evidência.
- `ENABLED` - Um armazenamento de dados de eventos foi criado e o localizador de evidências está ativado. Recomendamos esperar sete dias até que o armazenamento de dados do evento seja preenchido com seus dados de evidências anteriores. Enquanto isso, você pode usar o localizador de evidências, mas nem todos os dados estarão disponíveis até que o preenchimento seja concluído.
- `DISABLE_IN_PROGRESS` - Você solicitou a desativação do localizador de evidências e sua solicitação está pendente de exclusão do armazenamento de dados do evento.

- `DISABLED` - Você deshabilitou permanentemente o localizador de evidências e o armazenamento de dados do evento foi excluído. Você não pode reativar o localizador de evidências após esse ponto.

backfillStatus

Esse atributo mostra o status atual do preenchimento dos dados de evidência.

- `NOT_STARTED` significa que o preenchimento ainda não começou.
- `IN_PROGRESS` significa que o preenchimento está em andamento. Isso leva até sete dias para ser concluído, de acordo com a quantidade de dados de evidência.
- `COMPLETED` significa que o preenchimento está completo. Todas as suas evidências anteriores agora podem ser consultadas.

Para obter mais informações, consulte evidenceFinderEnablement na Referência de API Audit Manager.

Desativar o localizador de evidências

Se não quiser mais usar o localizador de evidências, você pode desabilitar esse atributo a qualquer momento.

> **Warning**
>
> A desativação do localizador de evidências exclui o armazenamento de dados de eventos do CloudTrail Lake criado pelo Audit Manager. Consequentemente, não é possível reativar o atributo. Para reutilizar o localizador de evidências depois de desativá-lo, você deve desabilitar AWS Audit Manager e então reativar completamente o serviço.

Permissões necessárias para desabilitar o localizador de evidências

Para desabilitar o localizador de evidências, você precisa de permissões para excluir um armazenamento de dados de eventos no CloudTrail Lake. Para um exemplo de política, consulte Permissões para desabilitar o localizador de evidências.

Se você precisar de ajuda com permissões, entre em contato com seu administrador AWS. Se você for administrador AWS, poderá anexar a declaração de permissão necessária a uma política do IAM.

Desativando o localizador de evidências

Você pode completar essa tarefa usando o console Audit Manager, o AWS Command Line Interface (AWS CLI), ou API Audit Manager.

Audit Manager console

Para desabilitar o localizador de evidências (console)

1. Na seção Localizador de evidências da página de configurações do Audit Manager, escolha desabilitar.
2. Na janela pop-up, insira **`Yes`** para confirmar sua decisão.
3. Escolha Solicite para desabilitar.

AWS CLI

Para desabilitar o localizador de evidências (AWS CLI)

Execute o comando update-settings com o parâmetro `--no-evidence-finder-enabled`.

```
aws auditmanager update-settings --no-evidence-finder-enabled
```

Audit Manager API

Para desabilitar o localizador de evidências (API)

Chame a operação UpdateSettings e use o parâmetro evidenceFinderEnabled.

Para obter mais informações, escolha um dos links anteriores na Referência de API Audit Manager. Isso inclui informações sobre como usar a operação e os parâmetros em um dos SDKs AWS específicos de idioma.

Destino de exportação (opcional)

Ao executar consultas no localizador de evidências, você pode exportar os resultados da pesquisa para um arquivo de valores separados por vírgula (CSV). Use essa configuração para escolher o bucket padrão do S3 onde o Audit Manager salvará seus arquivos exportados.

Você pode atualizar essa configuração usando o console Audit Manager, o AWS Command Line Interface (AWS CLI), ou API Audit Manager.

> **Important**
>
> Seu bucket do S3 deve ter a política de permissões exigida para permitir que o CloudTrail grave os arquivos de exportação nele. Mais especificamente, a política do bucket deve incluir uma ação `s3:PutObject` e o ARN do bucket, além de listar o CloudTrail como entidade principal do serviço. Fornecemos um exemplo de política de permissão que você pode usar. Para obter instruções sobre como anexar essa política ao seu bucket do S3, consulte Adicionando uma política de bucket usando o console do Amazon S3.
> Para obter mais dicas, consulte dicas de configuração para seu destino de exportação nesta página.

Audit Manager console

Para atualizar suas configurações de destino de exportação (console)

1. Na guia de configurações do Localizador de evidências, vá para a seção Destino da exportação.
2. Escolha uma das seguintes opções:
   - Se você quiser remover o bucket atual do S3, escolha Remover para limpar suas configurações.
   - Se você quiser salvar um bucket padrão do S3 pela primeira vez, vá para a etapa 3.
3. Especifique o bucket do S3 no qual deseja armazenar seus arquivos exportados.
   - Escolha Navegar S3 para escolher em uma lista de buckets.
   - Como alternativa, você pode inserir o URI do bucket nesse formato: **`s3://bucketname/prefix`**

> **Tip**
>
> Para manter seu bucket de destino organizado, você pode criar uma pasta opcional para suas exportações de CSV. Para fazer isso, acrescente uma barra (**`/`**) e um prefixo ao valor na caixa URI de Atributo (por exemplo, **`/evidenceFinderCSVExports`**). Em seguida, o Audit Manager incluirá esse prefixo ao adicionar o arquivo CSV ao bucket e o Amazon S3 irá gerar o caminho especificado pelo prefixo. Para obter mais informações sobre prefixos de objeto e

pastas no Amazon S3, consulte Organizando objetos no console do Amazon S3 no Guia do Usuário Amazon Simple Storage Service.

4. Quando terminar, escolha Salvar.

Para obter mais informações sobre como criar um bucket do S3, consulte Criando um bucket, no Guia do Usuário Amazon S3.

AWS CLI

Para atualizar suas configurações de destino de exportação (AWS CLI)

Execute o comando update-settings e use o parâmetro `--default-export-destination` para especificar um bucket do S3.

No exemplo a seguir, substitua o *`texto do espaço reservado`* por suas próprias informações.

```
aws auditmanager update-settings --default-export-destination
 destinationType=S3,destination=s3://doc-example-destination-bucket
```

Para obter instruções sobre como criar um bucket do S3, consulte create-bucket na AWS CLI Referência de Comando.

Audit Manager API

Para atualizar suas configurações de destino de exportação (API)

Chame a operação UpdateSettings e use o parâmetro defaultExportDestination para especificar um bucket S3.

Para obter instruções sobre como criar um bucket do S3, consulte CreateBucket na Referência de API Amazon S3.

Dicas de configuração para seu destino de exportação

Para garantir uma exportação de arquivo bem-sucedida, recomendamos que você verifique as seguintes configurações para seu destino de exportação:

Região da AWS

A Região da AWS da sua chave gerenciada pelo cliente (caso tenha fornecido uma) deve corresponder a Região de sua avaliação. Para obter instruções sobre como alterar a chave do KMS, consulte Configurações de criptografia de dados Audit Manager.

Buckets do S3 entre contas

O uso de um bucket S3 entre contas como destino de exportação não é suportado no console do Audit Manager. É possível especificar um bucket entre contas usando o AWS CLI ou um dos SDKs AWS; para simplificar, recomendamos que não faça isso. Se você optar por usar um bucket S3 entre contas como destino de exportação, considere os seguintes pontos.

- Por padrão, objetos S3 –- como exportações CSV –- são de propriedade da Conta da AWS que carrega o objeto. Você pode usar a configuração Propriedade de Objeto S3 para alterar esse comportamento padrão, o que permite que novos objetos gravados por contas com a lista de controle de acesso (ACL) padrão `bucket-owner-full-control` tornem-se automaticamente propriedade do proprietário do bucket.

  Embora não seja obrigatório, recomendamos que você faça as seguintes alterações nas configurações entre contas do bucket. Fazer essas alterações garante que o proprietário do bucket terá controle total dos arquivos exportados publicados por você no bucket dele.

  - Configure a propriedade do objeto do bucket S3 como preferencial do proprietário do bucket, em vez do gravador de objeto padrão
  - Adicione uma política de bucket para garantir que os objetos carregados para esse bucket tenham a ACL `bucket-owner-full-control`
- Para permitir que o Audit Manager exporte arquivos para um bucket S3 entre contas, você deve adicionar a seguinte política de bucket S3 ao seu destino de exportação do bucket. Substitua o *`espaço reservado de texto`* por suas próprias informações. O elemento `Principal` dessa política é o usuário ou a função que possui a avaliação e exporta o arquivo. `Resource` Especifica o bucket S3 entre contas para onde o arquivo é exportado.

```
{
  "Version": "2012-10-17",
  "Statement": [
      {
          "Sid": "Allow cross account file exports",
          "Effect": "Allow",
          "Principal": {
```

```
                "AWS":
 "arn:aws:iam::AssessmentOwnerAccountId:user/AssessmentOwnerUserName"
            },
            "Action": [
                "s3:ListBucket",
                "s3:PutObject",
                "s3:GetObject",
                "s3:GetBucketLocation",
                "s3:PutObjectAcl",
                "s3:DeleteObject"
            ],
            "Resource": [
                "arn:aws:s3:::CROSS-ACCOUNT-BUCKET",
                "arn:aws:s3:::CROSS-ACCOUNT-BUCKET/*"
            ]
        }
    ]
}
```

Notificações em AWS Audit Manager

AWS Audit Manager pode notificar você sobre ações de usuários por meio do Amazon Simple Notification Service (Amazon SNS).

O Audit Manager envia notificações quando um dos seguintes eventos ocorre:

- O responsável pela auditoria delega um conjunto de controles para análise.
- Um delegado envia um conjunto de controles analisado de volta ao responsável pela auditoria.
- O responsável pela auditoria conclui a análise de um conjunto de controles.

Pré-requisitos

Antes de configurar notificações do Amazon SNS no Audit Manager, certifique-se de ter concluído as etapas a seguir.

1. Crie um tópico do Amazon SNS, se ainda não tiver um. Para obter instruções, consulte Criação de um tópico do Amazon SNS no Guia do Desenvolvedor do Amazon Simple Notification Service.
2. Inscreva pelo menos um endpoint para o tópico. Por exemplo, se quiser receber notificações por mensagem de texto, inscreva um endpoint de SMS, (ou seja, um número de telefone celular) para o tópico. Um endpoint de SMS é um número de telefone celular. Para receber notificações por e-mail, inscreva um endpoint de e-mail para o tópico. Um endpoint de e-mail é um endereço de e-mail..

   Para obter mais informações, consulte Conceitos básicos no Guia do Desenvolvedor do Amazon Simple Notification Service.
3. (Opcional) Se seu tópico usarAWS Key Management Service (AWS KMS) para criptografia do lado do servidor (SSE), será necessário adicionar permissões à política do AWS KMS key. Para um exemplo de política que você pode usar, consulte Permissões para chave KMS anexada a um tópico SNS.

Configurar notificações no AWS Audit Manager

Siga estas etapas para configurar suas notificações no AWS Audit Manager.

Para configurar notificações em AWS Audit Manager

1. Abra o console do AWS Audit Manager em https://console.aws.amazon.com/auditmanager/home.
2. No painel de navegação à esquerda, escolha Configurações.
3. Em Notificações - opcional, especifique o tópico SNS que você deseja usar para receber notificações.
   - Para escolher um tópico existente, selecione o nome do tópico no menu suspenso.
   - Para criar um novo tópico, escolha Criar novo tópico. Isso leva ao console do Amazon SNS, onde você pode criar um tópico.
4. Quando terminar, selecione Salvar.

> **Observações**
>
> - Você pode usar um tópico SNS padrão ou um tópico FIFO (first-in-first-out, ou primeiro entrar, primeiro a sair). O Audit Manager é compatível com o envio de notificações para tópicos FIFO. No entanto, a ordem que essas mensagens são processadas não é garantida.
> - Se quiser usar um tópico do Amazon SNS pelo qual não é o responsável, configure sua política do AWS Identity and Access Management (IAM). Mais especificamente, você deve configurar sua política para permitir a publicação a partir do Nome do Recurso da Amazon (ARN) do tópico. Para obter mais informações, consulte Gerenciamento de identidade e acesso do AWS Audit Manager.

Solução de problemas

Para encontrar respostas para perguntas e problemas comuns, consulte Solução de problemas na seção Solução de problemas deste guia.

Solucão de problemas no AWS Audit Manager

Você pode usar as informações a seguir para solucionar problemas encontrados ao trabalhar com o AWS Audit Manager.

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 o AWS Support.

Tópicos

Solução de problemas de avaliação e coleta de evidências

Você pode usar as informações desta página para resolver problemas comuns de avaliação e coleta de evidências no Audit Manager.

Tópicos

- Minha avaliação não está coletando evidências de outro AWS service (Serviço da AWS)
- Minhas evidências são geradas em intervalos diferentes e não tenho certeza sobre a frequência de coleta
- O que acontece se eu remover uma conta do escopo da minha organização?
- Não consigo editar os serviços no escopo da minha avaliação
- Qual é a diferença entre um serviço no escopo e um tipo de fonte de dados?
- Ocorreu uma falha na criação da minha avaliação
- Eu desativei e reativei o Audit Manager. Agora, minhas avaliações preexistentes não estão mais coletando evidências

Eu criei uma avaliação, mas ainda não consigo ver nenhuma evidência

Se você não consegue ver nenhuma evidência, é provável que não tenha esperado pelo menos 24 horas depois de criar a avaliação ou que haja um erro de configuração.

Recomendamos verificar o seguinte:

1. Certifique-se de que passaram 24 horas desde que você criou a avaliação. As evidências automatizadas ficam disponíveis 24 horas após a criação da avaliação.
2. Certifique-se de usar o Audit Manager na mesma Região da AWS do AWS service (Serviço da AWS) que você espera ver evidências.
3. Se você espera ver evidências de verificação de conformidade do AWS Config e do AWS Security Hub, certifique-se de que os consoles do AWS Config e do Security Hub exibam os resultados dessas verificações. Os resultados do AWS Config e do Security Hub devem ser exibidos na mesma Região da AWS em que você usa o Audit Manager.

Se você ainda não consegue ver evidências em sua avaliação e o motivo não é nenhum desses problemas, verifique as outras possíveis causas descritas nesta página.

Minha avaliação não está coletando evidências de verificação de conformidade do AWS Security Hub

Se você não encontrar evidências de verificação de conformidade para um controle do AWS Security Hub, o motivo pode ser um dos problemas a seguir.

Falta de configuração no AWS Security Hub

Esse problema pode ser causado se você perdeu algumas etapas de configuração ao habilitar o AWS Security Hub.

Verifique se você ativou o Security Hub e definiu suas configurações conforme a seguir.

Confirmação de suas configurações do Security Hub para uma única Conta da AWS

Caso esteja usando uma única Conta da AWS, confira o seguinte:

- Confirme se você habilitou AWS Config e configurou a gravação de atributos para sua conta.
- Confirme se você ativou o padrão de segurança PCI DSS para sua conta.
- Confirme se você ativou a configuração de descobertas de controle consolidadas no Security Hub.

Confirmar as configurações do Security Hub para uma organização

Caso esteja usando o Organizations, confira o seguinte:

- Confirme se você ativou o AWS Config e configurou a gravação de atributos para sua conta.
- Confirme se você ativou o padrão de segurança PCI DSS para cada conta-membro da organização.
- Confirme se você ativou a configuração de descobertas de controle consolidadas no Security Hub.
- Confirme se a conta de administrador delegado que você usa no Security Hub é a mesma utilizada no Audit Manager.
- Confirme se você habilitou as contas da sua organização como contas-membro do Security Hub.

Um nome de controle do Security Hub foi inserido incorretamente em sua **`ControlMappingSource`**

Ao usar a API do Audit Manager para criar um controle personalizado, você pode especificar um controle do Security Hub como um mapeamento de fonte de dados para coleta de evidências. Para fazer isso, você insere uma ID de controle como o `keywordValue`.

Se você não encontrar evidências de verificação de conformidade para um controle do Security Hub, talvez o `keywordValue` tenha sido inserido incorretamente na sua `ControlMappingSource`. O `keywordValue` diferencia maiúsculas de minúsculas. Se você inseri-lo incorretamente, o Audit Manager poderá não reconhecer essa regra.

Consequentemente, você não poderá coletar evidências de verificação de conformidade para esse controle, conforme esperado.

Para corrigir esse problema, atualize o controle personalizado e revise o `keywordValue`. O formato correto de uma palavra-chave do Security Hub varia. Para fins de precisão, consulte a lista de palavras-chave de controle do Security Hub compatíveis.

Falta a regra **`AuditManagerSecurityHubFindingsReceiver`** do Amazon EventBridge

Quando você ativa o Audit Manager, uma regra chamada `AuditManagerSecurityHubFindingsReceiver` é automaticamente criada e habilitada no Amazon EventBridge. Essa regra permite que o Audit Manager colete as descobertas do Security Hub como evidência.

Se essa regra não estiver listada e habilitada na Região da AWS onde você usa o Security Hub, o Audit Manager não poderá coletar as descobertas do Security Hub para essa Região.

Para resolver esse problema, acesse o console do EventBridge e confirme se a regra `AuditManagerSecurityHubFindingsReceiver` existe na sua Conta da AWS. Se a regra não existir, recomendamos que você desative o Audit Manager e reative o serviço. Se essa ação não resolver o problema ou se desativar o Audit Manager não for uma opção, entre em contato com AWS Support para obter ajuda.

Regras do AWS Config vinculadas a serviços criadas pelo Security Hub

Lembre-se de que o Audit Manager não coleta evidências das regras do AWS Config vinculadas ao serviço que o Security Hub cria. Esse é um tipo específico de regra gerenciada do AWS Config que é habilitada e controlada pelo serviço Security Hub. O Security Hub cria instâncias dessas regras vinculadas ao serviço no seu ambiente AWS, mesmo se outras instâncias das mesmas regras já existirem. Como resultado, para evitar a duplicação de evidências, o Audit Manager não oferece suporte à coleta de evidências a partir das regras vinculadas ao serviço.

Minha avaliação não está coletando evidências de verificação de conformidade do AWS Config

Se você não vir evidências de verificação de conformidade de uma regra do AWS Config, isso pode ser devido a um dos seguintes problemas.

O identificador da regra foi inserido incorretamente na sua **`ControlMappingSource`**

Ao usar a API do Audit Manager para criar um controle personalizado, você pode especificar uma regra do AWS Config como um mapeamento de fonte de dados para coleta de evidências. O `keywordValue` que você especifica depende do tipo de regra.

Se você não encontrar evidências de verificação de conformidade para uma regra do AWS Config, talvez o `keywordValue` tenha sido inserido incorretamente no seu `ControlMappingSource`. O `keywordValue` diferencia maiúsculas de minúsculas. Se você inseri-lo incorretamente, o Audit Manager poderá não reconhecer a regra. Consequentemente, você não poderá coletar evidências de verificação de conformidade para essa regra, conforme esperado.

Para corrigir esse problema, atualize o controle personalizado e revise o `keywordValue`.

- Para regras personalizadas, verifique se o `keywordValue` tem o prefixo `Custom_` seguido pelo nome da regra personalizada. O formato do nome da regra personalizada pode variar. Para fins de precisão, visite o console do AWS Config para verificar os nomes das regras personalizadas.
- Para regras gerenciadas, certifique-se de que o `keywordValue` seja o identificador da regra em `ALL_CAPS_WITH_UNDERSCORES`. Por exemplo, `CLOUDWATCH_LOG_GROUP_ENCRYPTED`. Para fins de precisão, consulte a lista de palavras-chave compatíveis para regras gerenciadas.

> **Note**
>
> Para algumas regras gerenciadas, o identificador da regra é diferente do nome. Por exemplo, o identificador de regra para restricted-ssh é `INCOMING_SSH_DISABLED`. Certifique-se de usar o identificador da regra, não o nome. Para encontrar um identificador, escolha uma regra na lista de regras gerenciadas e procure seu valor Identificador.

A regra é uma regra do AWS Config vinculada ao serviço

Você pode usar regras gerenciadas e regras personalizadas como mapeamento da fonte de dados para coleta de evidências. No entanto, o Audit Manager não coleta evidências da maioria das regras vinculadas a serviços.

Há apenas dois tipos de regras vinculadas a serviços cujas evidências o Audit Manager coleta:

- Regras vinculadas a serviços nos pacotes de conformidade

- Regras vinculadas a serviços do AWS Organizations

  O Audit Manager não coleta evidências de outras regras vinculadas a serviços, especificamente de quaisquer regras com um nome do atributo da Amazon (ARN) contendo o seguinte prefixo: `arn:aws:config:*:*:config-rule/aws-service-rule/...`

  O motivo pelo qual o Audit Manager não coleta evidências da maioria das regras do AWS Config vinculadas a serviços é para evitar evidências duplicadas em suas avaliações. Uma regra vinculada ao serviço é um tipo específico de regra gerenciada que permite que outros Serviços da AWS criem regras do AWS Config em sua conta. Por exemplo, alguns controles do Security Hub usam uma regra vinculada ao serviço do AWS Config para executar verificações de segurança. Para cada controle do Security Hub que usa uma regra do AWS Config vinculada ao serviço, o Security Hub cria uma instância da regra do AWS Config necessária em seu ambiente AWS. Isso acontece mesmo se a regra original já existir na conta. Portanto, para evitar a coleta da mesma evidência da mesma regra duas vezes, o Audit Manager ignora a regra vinculada ao serviço e não coleta evidências dela.

O AWS Config não está habilitado e incluído como um serviço no escopo

O AWS Config deve estar ativado na sua Conta da AWS. Ele também deve ser incluído como um serviço no escopo de sua avaliação. Depois de configurar o AWS Config dessa forma, o Audit Manager coleta evidências sempre que a avaliação de uma regra do AWS Config ocorre.

Primeiro, certifique-se de que você habilitou o AWS Config na sua Conta da AWS. Para obter instruções, consulte Habilitar e configurar o AWS Config.

Em seguida, certifique-se de incluir o AWS Config como serviço no escopo de sua avaliação. Para revisar os serviços atuais no escopo de sua avaliação, consulte Analisar uma avaliação, guia Serviços da AWS. Para editar a lista de serviços no escopo de uma avaliação, consulte Editar Serviços da AWS no escopo.

A regra do AWS Config avaliou a configuração de um atributo antes de você configurar sua avaliação

Se sua regra do AWS Config estiver configurada para avaliar as alterações de configuração de um atributo específico, você poderá ver uma incompatibilidade entre a avaliação no AWS Config e a evidência no Audit Manager. Isso acontece se a avaliação da regra ocorreu antes de configurar o controle em sua avaliação do Audit Manager. Nesse caso, o Audit Manager não gera evidências até que o atributo subjacente mude de estado novamente e acione uma reavaliação da regra.

Como solução alternativa, você pode navegar até o console do AWS Config e reavaliar a regra manualmente. Isso invoca uma nova avaliação de todos os atributos que pertencerem a essa regra.

Minha avaliação não está coletando evidências de atividades dos usuários do AWS CloudTrail

Ao usar a API do Audit Manager para criar um controle personalizado, você pode especificar um nome de evento do CloudTrail como um mapeamento de fonte de dados para coleta de evidências. Para fazer isso, você insere o nome do evento como o `keywordValue`.

Se você não visualizar evidências de atividades dos usuários em um evento do CloudTrail, talvez o `keywordValue` tenha sido inserido incorretamente na sua `ControlMappingSource`. O `keywordValue` diferencia maiúsculas de minúsculas. Se você inseri-lo incorretamente, o Audit Manager poderá não reconhecer o nome do evento. Como resultado, você pode não coletar evidências das atividades dos usuários para esse evento conforme pretendido.

Para corrigir esse problema, atualize o controle personalizado e revise o `keywordValue`. Certifique-se de que o evento esteja escrito como `serviceprefix_ActionName`. Por exemplo, `cloudtrail_StartLogging`. Para fins de precisão, analise o prefixo AWS service (Serviço da AWS) e os nomes das ações na Referência de autorização do serviço.

Minha avaliação não está coletando evidências de dados de configuração para uma chamada de API da AWS

Ao usar a API do Audit Manager para criar um controle personalizado, você pode especificar uma chamada de API da AWS como um mapeamento de fonte de dados para coleta de evidências. Para fazer isso, você insere a chamada de API como o `keywordValue`.

Se você não vir evidências de dados de configuração para uma chamada de API da AWS, pode ser que o `keywordValue` tenha sido inserido incorretamente no seu `ControlMappingSource`. O `keywordValue` diferencia maiúsculas de minúsculas. Se você inseri-lo incorretamente, o Audit Manager poderá não reconhecer a chamada de API. Como resultado, talvez você não colete evidências de dados de configuração para essa chamada de API conforme pretendido.

Para corrigir esse problema, atualize o controle personalizado e revise o `keywordValue`. Certifique-se de que a chamada de API esteja escrito como `serviceprefix_ActionName`. Por exemplo, `iam_ListGroups`. Para fins de precisão, consulte a lista de Chamadas de API compatíveis.

Minha avaliação não está coletando evidências de outro AWS service (Serviço da AWS)

Se um AWS service (Serviço da AWS) não for selecionado como escopo para sua avaliação, o Audit Manager não coletará evidências de atributos relacionados a esse serviço. Esse também é o caso se um AWS service (Serviço da AWS) estiver selecionado mas você não tiver habilitado-o em seu ambiente.

Se você criou sua avaliação a partir de um framework personalizada, poderá editar os serviços no escopo de sua avaliação. Em seguida, você pode especificar outros Serviços da AWS dos quais deseja coletar evidências. Depois de adicionar esses serviços, as evidências ficarão disponíveis após 24 horas.

> **Note**
>
> Se você criou sua avaliação a partir de um framework padrão, a lista de Serviços da AWS no escopo é pré-selecionada e não pode ser editada. Isso ocorre porque, ao criar uma avaliação a partir de um framework padrão, o Audit Manager mapeia e seleciona automaticamente as fontes de dados e os serviços relevantes para seu caso. A seleção é feita com base nos requisitos do framework padrão. Observe que, para frameworks padrão contendo somente controles manuais, nenhum Serviços da AWS está no escopo.
>
> A solução alternativa para editar os Serviços da AWS no escopo e, ao mesmo tempo, criar uma avaliação com base em um framework padrão é personalizar o framework padrão. Com essa solução alternativa, você pode usar o framework que personalizou para criar uma nova avaliação. Nessa avaliação, você pode especificar quais Serviços da AWS estão no escopo.

Minhas evidências são geradas em intervalos diferentes e não tenho certeza sobre a frequência de coleta

Os controles nas avaliações do Audit Manager são mapeados para várias fontes de dados. Cada fonte de dados tem uma frequência diferente de coleta de evidências. Como resultado, não há uma resposta única para a frequência com que as evidências são coletadas. Algumas fontes de dados avaliam a conformidade, enquanto outras apenas capturam o estado dos atributos e alteram os dados sem determinação da conformidade.

Veja a seguir um resumo dos diferentes tipos de fontes de dados e da frequência com que coletam evidências.

Tipo de fonte de dado	Descrição	Frequência das coletas de evidências	Quando esse controle estiver ativo em uma avaliação
AWS CloudTrail	Rastreia uma atividade específica do usuário.	Contínuo	O Audit Manager filtra seus logs do CloudTrail com base na palavra-chave que você escolher. Os logs processados são importados como evidência de Atividade do usuário.
AWS Security Hub	Captura um snapshot da sua postura de segurança de recursos relatando as descobertas do Security Hub.	Com base no cronograma da verificação do Security Hub (normalmente a cada 12 horas)	O Audit Manager recupera a descoberta de segurança diretamente do Security Hub. A descoberta é importada como evidência de Verificação de conformidade.
AWS Config	Captura um snapshot da sua postura de segurança de recursos relatando as descobertas do AWS Config.	Com base nas configurações definidas na regra do AWS Config	O Audit Manager recupera a avaliação da regra diretamente do AWS Config. A avaliação é importada como evidência de Verificação de conformidade.
Chamadas de API da AWS	Tira um snapshot da configuração do seu recurso diretamente por meio de uma chamada de API para o AWS service	Diária, semanal ou mensalmente	O Audit Manager faz a chamada de API com base na frequência que você especifica. A resposta é importada como evidência de Dados de configuração.

Tipo de fonte de dado	Descrição	Frequência das coletas de evidências	Quando esse controle estiver ativo em uma avaliação
	(Serviço da AWS) especificado.		

Independente da frequência da coleta de evidências, novas evidências são coletadas automaticamente enquanto a avaliação estiver ativa. Para obter mais informações, consulte Frequência da coleta de evidências.

Para saber mais, consulte Fontes de dados de controle compatíveis para evidências automatizadas e Alteração da frequência de coleta de evidências para um controle.

O que acontece se eu remover uma conta do escopo da minha organização?

Quando uma conta do escopo é removida da sua organização, o Audit Manager não coleta mais evidências dessa conta. No entanto, a conta continua sendo exibida em sua avaliação na guia Contas da AWS. Para remover a conta da lista de contas no escopo, edite a avaliação. A conta removida não aparece mais na lista durante a edição e você pode salvar suas alterações sem que essa conta esteja no escopo.

Não consigo editar os serviços no escopo da minha avaliação

Quando você usa o console do Audit Manager para criar uma avaliação a partir de um framework padrão, a lista de Serviços da AWS no escopo é selecionada por padrão. Essa lista não pode ser editada. Isso ocorre porque o Audit Manager mapeia e seleciona automaticamente as fontes de dados e os serviços para você. Essa seleção é feita de acordo com os requisitos do framework padrão. Se a estrutura padrão que você selecionou contiver somente controles manuais, nenhum Serviços da AWS estará no escopo da sua avaliação e não será possível adicionar nenhum serviço à sua avaliação.

Se você precisar editar a lista de serviços no escopo, use a operação da API UpdateAssessment fornecida pelo Audit Manager. Como alternativa, você pode personalizar o framework padrão e, em seguida, criar uma avaliação a partir do framework personalizado.

Qual é a diferença entre um serviço no escopo e um tipo de fonte de dados?

Um serviço no escopo é um AWS service (Serviço da AWS) especificado como parte de sua avaliação. Quando um serviço está no escopo, o Audit Manager coleta evidências sobre o uso desse serviço e de seus atributos.

Um tipo de fonte de dados indica de onde exatamente a evidência é coletada. Se você carregar sua própria evidência, o tipo de fonte de dados será Manual. Se o Audit Manager coletar as evidências, a fonte de dados poderá ser de um dos quatro tipos.

1. AWS Security Hub – Captura um snapshot da sua postura de segurança de recursos relatando as descobertas do Security Hub.
2. AWS Config – Captura de tela da sua postura de segurança de atributos relatando as descobertas do AWS Config.
3. AWS CloudTrail – Rastreia uma atividade específica do usuário para um atributo.
4. Chamadas de API da AWS – Obtém uma captura de tela da configuração do seu atributo diretamente por meio de uma chamada de API para um AWS service (Serviço da AWS) especificado.

Confira a seguir dois exemplos para ilustrar a diferença entre um serviço no escopo e um tipo de fonte de dado.

Exemplo 1

Digamos que você queira coletar evidências para um controle chamado 4.1.2 – Proibir o acesso público de gravação aos buckets do S3. Esse controle verifica os níveis de acesso das suas políticas de bucket S3. Para esse controle, o Audit Manager usa uma regra específica do AWS Config (s3-bucket-public-write-prohibited) para procurar uma avaliação de seus buckets do S3. Neste exemplo, o seguinte é verdadeiro:

- O serviço no escopo é o Amazon S3
- Os atributos que estão sendo avaliados são seus buckets do S3
- O tipo da fonte de dados é AWS Config
- O mapeamento da fonte de dados é uma regra AWS Config específica (`s3-bucket-public-write-prohibited`)

Exemplo 2

Digamos que você queira coletar evidências para um controle HIPAA chamado 164.308(a)(5)(ii)(C). Esse controle requer um procedimento de monitoramento para detectar logins inadequados. Para esse controle, o Audit Manager usa os logs do CloudTrail para procurar todos os eventos de login do Console de Gerenciamento da AWS. Neste exemplo, o seguinte é verdadeiro:

- O serviço no escopo é IAM
- Os atributos que estão sendo avaliados são seus usuários
- O tipo de fonte de dado é CloudTrail
- O mapeamento da fonte de dados é um evento específico do CloudTrail (`ConsoleLogin`)

Ocorreu uma falha na criação da minha avaliação

Se a criação da avaliação falhar, talvez seja porque você selecionou muitas Contas da AWS no escopo da avaliação. Se estiver usando o AWS Organizations, o Audit Manager pode suportar até aproximadamente 150 contas-membro no escopo de uma única avaliação. Se exceder esse número, a criação da avaliação poderá falhar. Como solução alternativa, você pode executar várias avaliações com contas diferentes no escopo de cada avaliação.

Eu desativei e reativei o Audit Manager. Agora, minhas avaliações preexistentes não estão mais coletando evidências

Quando você desativa o Audit Manager e opta por não excluir seus dados, suas avaliações existentes entram em um estado inativo e param de coletar evidências. Ou seja, quando você reativa o Audit Manager, as avaliações que criou anteriormente permanecem disponíveis. No entanto, elas não retomam automaticamente a coleta de evidências.

Para começar a coletar evidências novamente para uma avaliação preexistente, edite a avaliação e escolha Salvar sem fazer nenhuma alteração.

Solução de problemas de relatórios de avaliação

Você pode usar as informações nesta página para resolver problemas comuns de relatórios de avaliação no Audit Manager.

Tópicos

Ocorreu uma falha na geração do meu relatório de avaliação

Seu relatório de avaliação pode não ter sido gerado por vários motivos. Você pode começar a solucionar esse problema verificando as causas mais frequentes. Use a lista de verificação a seguir para começar.

1. Verifique se alguma das informações da sua Região da AWS não coincide:
   a. A Região da AWS da chave gerenciada pelo cliente corresponde à Região da AWS da sua avaliação?

      Se você forneceu sua própria chave do KMS para a criptografia de dados do Audit Manager, a chave deve estar na mesma Região da AWS da sua avaliação. Para resolver esse problema, altere a chave do KMS para uma que esteja na mesma região da sua avaliação. Para obter instruções sobre como alterar a chave do KMS, consulte Configurações do AWS Audit Manager, criptografia de dados.

   b. A Região da AWS da chave gerenciada pelo cliente corresponde à Região da AWS do bucket do S3?

      Se você forneceu sua própria chave do KMS para criptografia de dados do Audit Manager, a chave deverá estar na mesma Região da AWS do bucket S3 usado como destino do relatório de avaliação. Para resolver esse problema, você pode alterar a chave do KMS ou o bucket do S3 para que ambos estejam na mesma região da sua avaliação. Para obter instruções sobre como alterar a chave do KMS, consulte Configurações do AWS Audit Manager, criptografia de dados. Para obter instruções sobre como alterar o bucket do S3, consulte Configurações do AWS Audit Manager, destino do relatório de avaliação.

2. Verifique as permissões do bucket do S3 que você está usando como destino do relatório de avaliação:

   a. A entidade do IAM gerando o relatório de avaliação tem as permissões necessárias para o bucket do S3?

      A entidade do IAM deve ter as permissões de bucket do S3 necessárias para publicar relatórios nesse bucket. Fornecemos uma política de exemplo que você pode usar. Para obter instruções sobre como especificar um bucket S3 diferente, consulte Configurações do AWS Audit Manager, destino do relatório de avaliação.

   b. O bucket do S3 tem uma política de bucket que exige criptografia do lado do servidor (SSE) usando SSE-KMS?

      Se tiver, a chave do KMS usada nessa política de bucket deve corresponder à chave do KMS especificada nas configurações de criptografia de dados do Audit Manager. Se você não configurou uma chave do KMS nas configurações do Audit Manager e sua política de bucket do S3 exige SSE, certifique-se de que a política de bucket permita SSE-S3. Para obter instruções sobre como alterar a chave do KMS, consulte Configurações do AWS Audit Manager, criptografia de dados. Para obter instruções sobre como alterar o bucket do S3, consulte Configurações do AWS Audit Manager, destino do relatório de avaliação.

Se você ainda não conseguir gerar um relatório de avaliação com sucesso, analise os problemas a seguir nesta página.

Segui a lista de verificação acima e a geração do meu relatório de avaliação falhou mesmo assim

O Audit Manager limita a quantidade de evidências que você pode adicionar a um relatório de avaliação. O limite é baseado na Região da AWS da sua avaliação, na região do bucket do S3 que é usada como destino do relatório de avaliação e se sua avaliação usa uma AWS KMS key gerenciada pelo cliente.

1. O limite é 22.000 para relatórios da mesma região (onde o bucket do S3 e a avaliação estão na mesma Região da AWS)
2. O limite é 3.500 para relatórios de diferentes regiões (onde o bucket do S3 e a avaliação estão em Regiões da AWS diferentes)
3. O limite será 3.500 se a avaliação usar uma chave do KMS gerenciada pelo cliente

Se tentar gerar um relatório que contenha mais evidências do que isso, a operação poderá falhar.

Como solução alternativa, você pode gerar vários relatórios de avaliação em vez de um relatório de avaliação maior. Ao fazê-lo, você pode exportar evidências de sua avaliação para lotes de tamanho mais gerenciável.

Recebo um erro de acesso negado quando tento gerar um relatório

Você receberá um erro de `access denied` se sua avaliação tiver sido criada por uma conta de administrador delegado à qual a chave do KMS especificada nas configurações do Audit Manager não pertence. Para evitar esse erro, ao designar um administrador delegado para o Audit Manager, certifique-se de que a conta do administrador delegado tenha acesso à chave do KMS que você forneceu ao configurar o Audit Manager.

Você também pode receber um erro de `access denied` se não tiver permissões de gravação para o bucket do S3 que está usando como destino do relatório de avaliação.

Se você receber um erro `access denied`, certifique-se de atender aos seguintes requisitos:

- Sua chave do KMS nas configurações do Audit Manager dá permissões ao administrador delegado. Você pode configurar isso seguindo as instruções em Permitir que usuários de outras contas usem uma chave do KMS no Guia do Desenvolvedor do AWS Key Management Service. Para obter instruções sobre como analisar e alterar suas configurações de criptografia no Audit Manager, consulte Criptografia de dados.
- Você tem uma política de permissões que concede acesso de gravação para o bucket do S3 que está usando como destino do relatório de avaliação. Mais especificamente, sua política de permissões contém uma ação `s3:PutObject`, especifica o ARN do bucket do S3 e inclui a chave do KMS usada para criptografar seus relatórios de avaliação. Para ver um exemplo de política que você pode usar, consulte Exemplos de políticas baseadas em identidade para o AWS Audit Manager.

> **Note**
>
> Se você alterar as configurações de criptografia de dados do Audit Manager, essas alterações se aplicarão às novas avaliações que forem criadas daqui para frente. Isso inclui todos os relatórios de avaliação criados a partir de suas novas avaliações.
> As alterações não se aplicam às avaliações existentes criadas antes de alterar suas configurações de criptografia. Isso inclui novos relatórios de avaliação criados a partir de

avaliações existentes, além dos relatórios de avaliação existentes. As avaliações existentes – e todos os seus relatórios de avaliação – continuam usando a antiga chave do KMS. Se a identidade do IAM que está gerando o relatório de avaliação não tiver permissões para usar a antiga chave do KMS, você poderá conceder permissões no nível da política de chaves.

Não consigo descompactar o relatório de avaliação

Se você não conseguir descompactar o relatório de avaliação no Windows, é provável que o Windows Explorer não esteja conseguindo extraí-lo porque o caminho do arquivo tem várias pastas aninhadas ou nomes longos. Isso ocorre porque, no sistema de nomenclatura de arquivos do Windows, o caminho da pasta, o nome do arquivo e a extensão do arquivo não podem exceder 259 caracteres. Caso contrário, isso resultará em um erro de `Destination Path Too Long`.

Para resolver esse problema, tente mover o arquivo .zip para a pasta principal de seu local atual. Em seguida, você pode tentar descompactá-lo novamente a partir daí. Como alternativa, você também pode tentar encurtar o nome do arquivo .zip, ou extraí-lo para um local diferente que tenha um caminho de arquivo mais curto.

Quando escolho o nome de uma evidência em um relatório, não sou redirecionado para os detalhes da mesma

Esse problema pode ocorrer se você estiver interagindo com o relatório de avaliação em um navegador, ou usando o leitor de PDF padrão instalado em seu sistema operacional. Alguns leitores de PDF padrão do navegador e do sistema não permitem a abertura de links relacionados. Isso significa que, embora os hiperlinks possam funcionar no PDF de resumo do relatório de avaliação (como nomes de controle com hiperlinks no índice), os hiperlinks são ignorados quando você tenta migrar do PDF do resumo da avaliação para um PDF separado de detalhes de evidências.

Se você encontrar esse problema, recomendamos usar um leitor de PDF exclusivo para interagir com seus relatórios de avaliação. Para obter uma experiência confiável, recomendamos que você instale e use o Adobe Acrobat Reader, que pode ser baixado no site da Adobe. Outros leitores de PDF também estão disponíveis, mas foi comprovado que o Adobe Acrobat Reader funciona de forma consistente e confiável com os relatórios de avaliação do Audit Manager.

A geração do meu relatório de avaliação está no status Em andamento e tenho dúvidas se isso afeta meu faturamento

A geração do relatório de avaliação não impacta no faturamento. A cobrança ocorre apenas com base nas evidências que suas avaliações coletam. Para obter mais informações sobre precificação, consulte Precificação do AWS Audit Manager.

Consulte também

As páginas a seguir contêm orientações para solução de problemas sobre a geração de um relatório de avaliação a partir do localizador de evidências:

- Não consigo gerar vários relatórios de avaliação a partir dos meus resultados de pesquisa
- Não consigo adicionar resultados de pesquisa individuais a um relatório de avaliação
- Nem todos os resultados do meu localizador de evidências estão incluídos no relatório de avaliação
- Quero gerar um relatório de avaliação a partir dos resultados da minha pesquisa, mas ocorre uma falha na minha instrução de consulta

Solução de problemas de controle e conjunto de controles

Você pode usar as informações desta página para resolver problemas comuns com controles no Audit Manager.

Problemas gerais

- Não consigo ver nenhum controle ou conjuntos de controles na minha avaliação
- Não consigo carregar evidências manuais para um controle

Problemas de integração com AWS Config

- Preciso usar várias regras do AWS Config como fonte de dados para um único controle
- A opção de regra personalizada não está disponível quando configuro uma fonte de dados de controle
- A opção de regra personalizada está disponível, mas nenhuma aparece na lista suspensa
- Algumas regras personalizadas estão disponíveis, mas não consigo ver a que quero usar

- Não consigo ver a regra gerenciada que quero usar
- Quero compartilhar um framework personalizado, mas ele tem controles que usam regras personalizadas do AWS Config como fonte de dados. O destinatário pode coletar evidências para esses controles?
- O que acontece quando uma regra personalizada é atualizada no AWS Config? Preciso desempenhar alguma ação no Audit Manager?

Não consigo ver nenhum controle ou conjuntos de controles na minha avaliação

Em resumo, para visualizar os controles de uma avaliação, você deve ser designado como responsável pela auditoria para essa avaliação. Além disso, você precisa das permissões necessárias do IAM para visualizar e gerenciar os atributos relacionados do Audit Manager.

Se precisar acessar os controles em uma avaliação, peça a um dos responsáveis pela auditoria que defina você como responsável pela auditoria. Você pode especificar os responsáveis pela auditoria ao criar ou editar uma avaliação.

Certifique-se de que também tem as permissões necessárias para gerenciar a avaliação. Recomendamos que os proprietários da auditoria usem a política AWSAuditManagerAdministratorAccess. Se você precisar de ajuda com as permissões do IAM, entre em contato com seu administrador ou com o Suporte da AWS. Para obter mais informações sobre como anexar uma política a uma identidade do IAM, consulte Adicionar permissões a um usuário e Adicionar e remover permissões de identidade do IAM no Guia do Usuário do IAM.

Não consigo carregar evidências manuais para um controle

Se você não conseguir carregar evidências manualmente para um controle, é provável que o status do controle esteja Inativo.

Para fazer upload de evidências manuais para um controle, primeiro você deve alterar o status do controle para Em análise ou Analisado. Para ver mais informações, consulte Atualizar status de controle.

> **Important**
>
> Cada Conta da AWS só pode carregar manualmente até 100 arquivos de evidências para um controle por dia. Exceder essa cota diária faz com que qualquer carregamento

manual adicional falhe nesse controle. Se você precisar carregar uma grande quantidade de evidências manuais em um único controle, carregue as evidências em lotes ao longo de vários dias.

Preciso usar várias regras do AWS Config como fonte de dados para um único controle

Você pode usar uma combinação de regras gerenciadas e personalizadas para um único controle. Para fazer isso, configure várias fontes de dados para o controle e selecione seu tipo de regra preferido para cada uma delas. Você pode definir até dez fontes de dados para um único controle personalizado.

A opção de regra personalizada não está disponível quando configuro uma fonte de dados de controle

Isso significa que você não tem permissões para visualizar regras personalizadas para sua Conta da AWS ou organização. Mais especificamente, você não tem permissões para executar a operação DescribeConfigRules no console do Audit Manager.

Para resolver esse problema, entre em contato com seu administrador da AWS para obter ajuda. Se você for administrador da AWS, poderá fornecer permissões para seus usuários ou grupos gerenciando suas políticas do IAM.

A opção de regra personalizada está disponível, mas nenhuma aparece na lista suspensa

Isso significa que nenhuma regra personalizada está habilitada e disponível para uso em sua Conta da AWS ou organização.

Caso ainda não tenha nenhuma regra personalizada no AWS Config, você pode criar uma. Para obter instruções, consulte Regras personalizadas do AWS Config no Guia do Desenvolvedor do AWS Config.

Se você espera ver uma regra personalizada, verifique o item de solução de problemas a seguir.

Algumas regras personalizadas estão disponíveis, mas não consigo ver a que quero usar

Se você não consegue ver a regra personalizada que espera encontrar, o motivo pode um dos problemas a seguir.

Sua conta foi excluída da regra

É possível que a conta de administrador delegado que você está usando esteja excluída da regra.

A conta de gerenciamento da sua organização (ou uma das contas de administrador delegado do AWS Config) pode criar regras de organização personalizadas usando o AWS Command Line Interface (AWS CLI). Ao fazer isso, é possível especificar uma lista de contas a serem excluídas da regra. Caso sua conta esteja nessa lista, a regra não estará disponível no Audit Manager.

Para resolver esse problema, entre em contato com seu administrador da AWS Config para obter ajuda. Se você for administrador do AWS Config, poderá atualizar a lista de contas excluídas executando o comando put-organization-config-rule.

A regra não foi criada e habilitada com sucesso no AWS Config

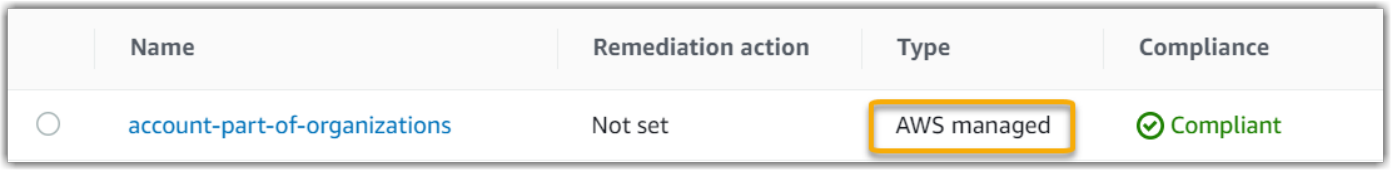
Também é possível que a regra personalizada não tenha sido criada e ativada com êxito. Se um erro ocorreu ao criar a regra ou se a regra não estiver ativada, ela não aparecerá na lista de regras disponíveis no Audit Manager.

Para obter ajuda relacionada a esse problema, recomendamos entrar em contato com seu administrador do AWS Config.

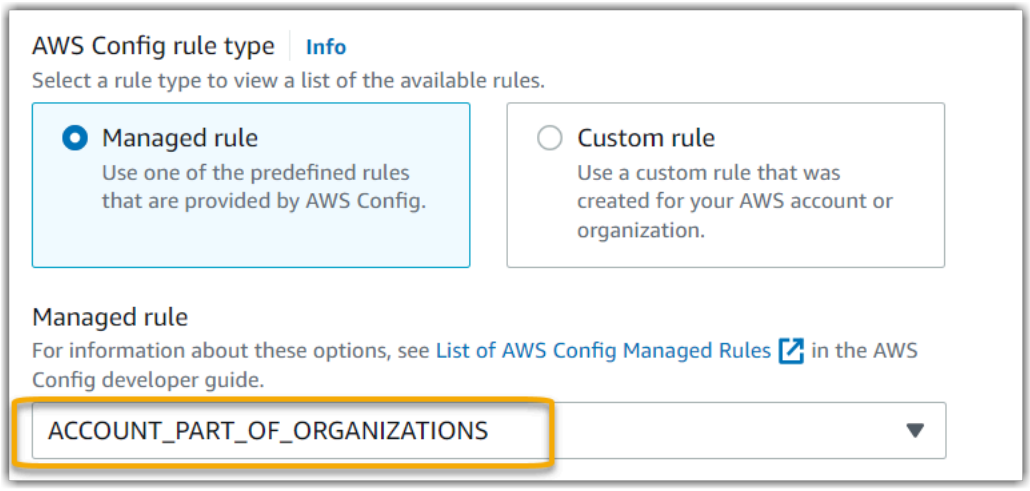
A regra é gerenciada

Se você não conseguir encontrar a regra que está procurando na lista suspensa de regras personalizadas, é possível que ela seja gerenciada.

Você pode usar o console do AWS Config para verificar se uma regra é gerenciada. Para fazer isso, escolha Regras no menu de navegação à esquerda e procure pela regra na tabela. Se a regra for gerenciada, a coluna Tipo mostrará AWS gerenciada.

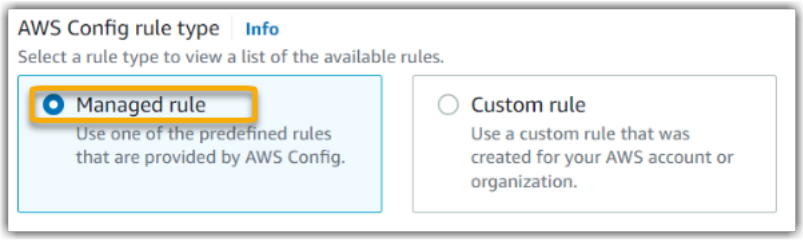


Depois de confirmar que é uma regra gerenciada, retorne ao Audit Manager e selecione Regra gerenciada como o tipo de regra. Em seguida, procure a palavra-chave identificadora de regra gerenciada na lista suspensa de regras gerenciadas.



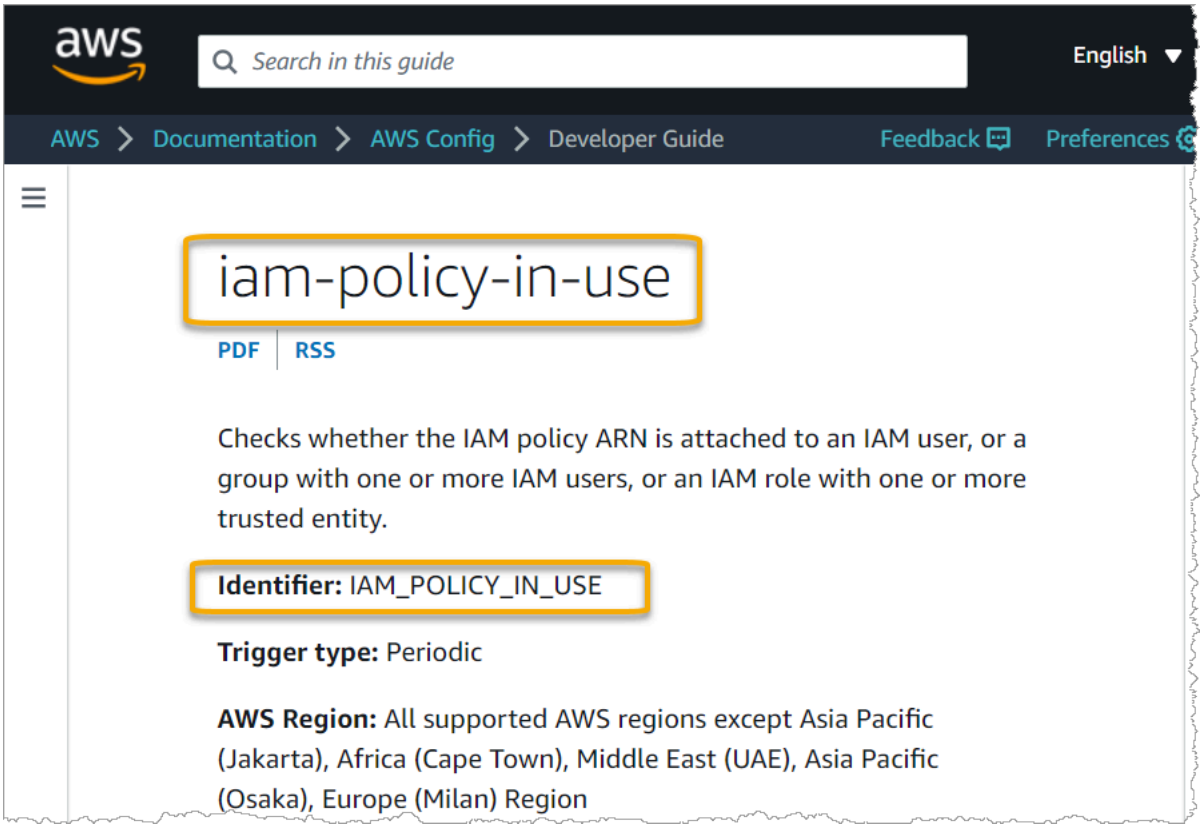
Não consigo ver a regra gerenciada que quero usar

Antes de selecionar uma regra na lista suspensa no console do Audit Manager, certifique-se de selecionar Regra gerenciada como o tipo de regra.

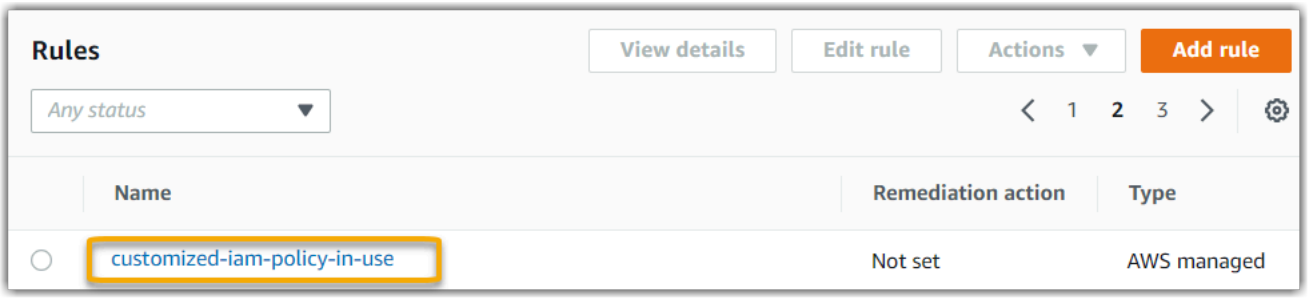


Se ainda não conseguiu ver a regra gerenciada que esperava encontrar, é possível que esteja procurando o nome da regra. Em vez disso, você deve procurar o identificador da regra.

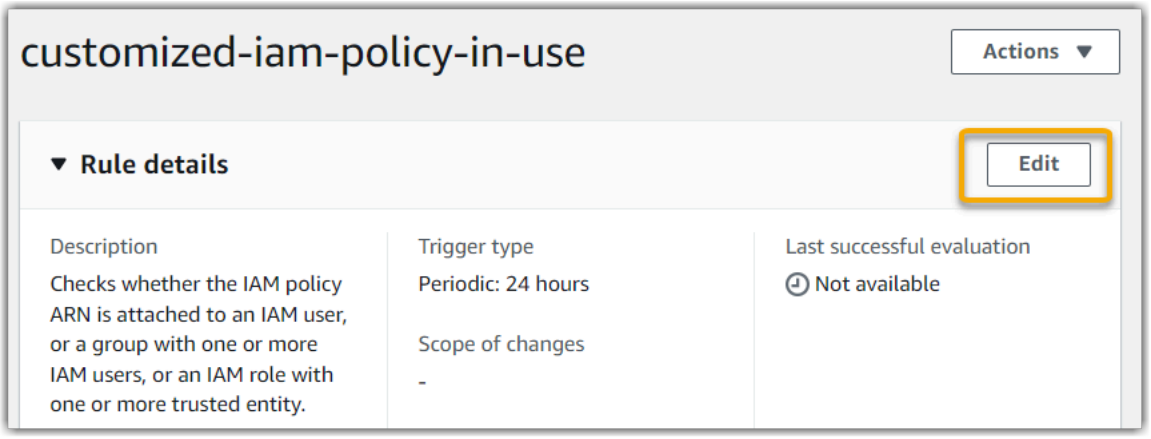
Se você estiver usando uma regra gerenciada padrão, o nome e o identificador serão semelhantes. O nome está em letras minúsculas e inclui traços (por exemplo, `iam-policy-in-use`). O identificador está em maiúsculas e inclui sublinhados (por exemplo, `IAM_POLICY_IN_USE`). Para encontrar o identificador de uma regra gerenciada padrão, analise a lista de palavras-chave compatíveis para regras gerenciadas do AWS Config e siga o link da regra que você deseja usar. Isso leva você à documentação do AWS Config referente a essa regra gerenciada. A partir daqui, você pode ver o nome e o identificador. Procure a palavra-chave identificadora na lista suspensa do Audit Manager.



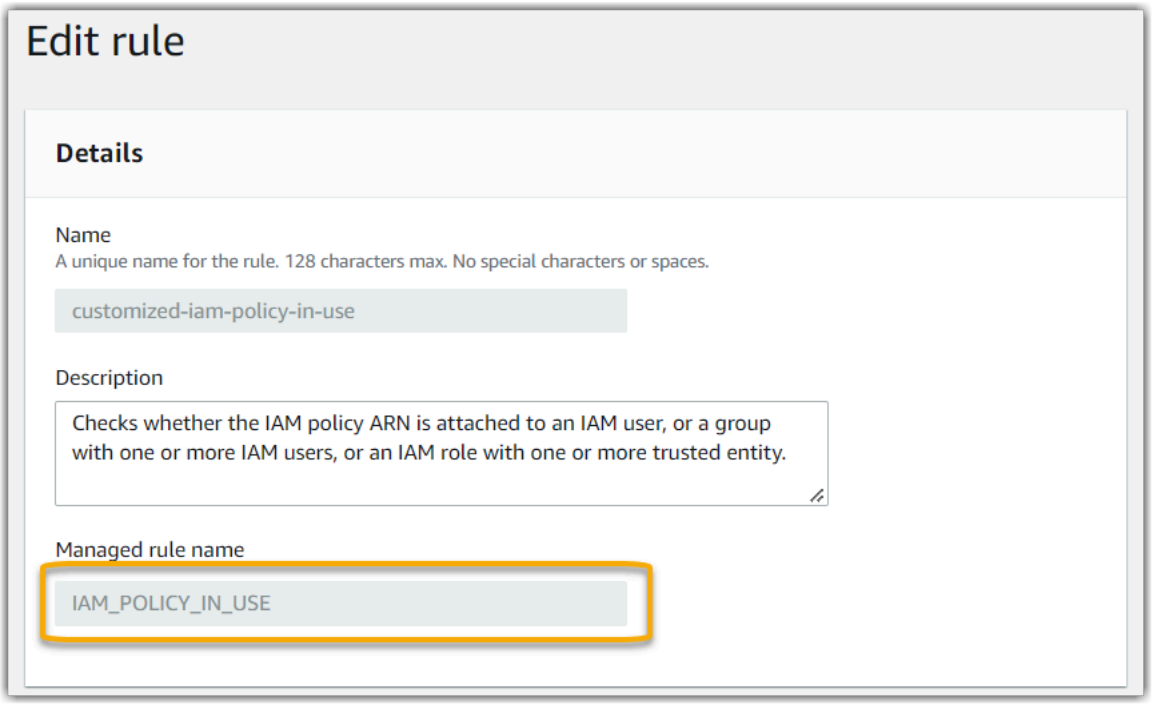
Se você estiver usando uma regra gerenciada personalizada, poderá usar o console do AWS Config para encontrar o identificador da regra. Por exemplo, digamos que você deseja usar a regra gerenciada `customized-iam-policy-in-use`. Para encontrar o identificador dessa regra, acesse o console do AWS Config, escolha Regras no menu de navegação à esquerda e selecione a regra na tabela.



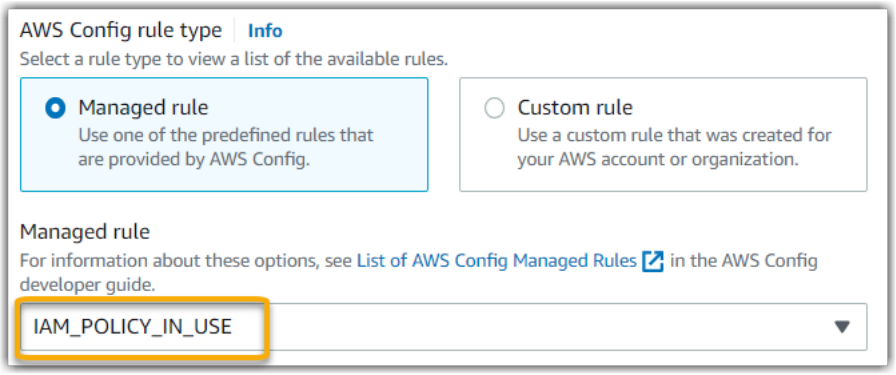
Escolha Editar para abrir detalhes sobre a regra gerenciada.



Na seção Detalhes, você encontra o identificador de origem a partir do qual a regra gerenciada foi criada (`IAM_POLICY_IN_USE`).



Agora você pode retornar ao console do Audit Manager e selecionar a mesma palavra-chave identificadora na lista suspensa.



Quero compartilhar um framework personalizado, mas ele tem controles que usam regras personalizadas do AWS Config como fonte de dados. O destinatário pode coletar evidências para esses controles?

Sim, o destinatário pode coletar evidências para esses controles, mas é preciso concluir algumas etapas.

Para que o Audit Manager colete evidências usando uma regra do AWS Config como mapeamento da fonte de dados, o seguinte deve ser verdadeiro. Isso se aplica às regras gerenciadas e personalizadas.

1. A regra deve existir no ambiente da AWS do destinatário
2. A regra deve estar habilitada no ambiente AWS do destinatário.

Lembre-se de que as regras personalizadas do AWS Config em sua conta provavelmente ainda não existem no ambiente da AWS do destinatário. Além disso, quando o destinatário aceita a solicitação de compartilhamento, o Audit Manager não recria nenhuma de suas regras personalizadas na conta. Para que o destinatário colete evidências usando suas regras personalizadas como mapeamento da fonte de dados, ele deve criar as mesmas regras personalizadas em sua instância do AWS Config. Depois que o destinatário cria e habilitada as regras, o Audit Manager pode coletar evidências dessa fonte de dados.

Recomendamos que você se comunique com o destinatário para informá-lo se alguma regra personalizada precisa ser criada em sua instância do AWS Config.

O que acontece quando uma regra personalizada é atualizada no AWS Config? Preciso desempenhar alguma ação no Audit Manager?

Para atualizações de regras em seu ambiente da AWS

Se você atualizar uma regra personalizada em seu ambiente da AWS, nenhuma ação será necessária no Audit Manager. O Audit Manager detecta e gerencia as atualizações de regras, conforme descrito na tabela a seguir. O Audit Manager não notifica quando uma atualização de regra é detectada.

Cenário	O que o Audit Manager faz	O que você precisa fazer
Uma regra personalizada é atualizada na sua instância do AWS Config.	O Audit Manager continua relatando as descobert as dessa regra ao usar a definição de regra atualizada.	Nenhuma ação é necessária.
Uma regra personalizada é excluída na sua instância do AWS Config.	O Audit Manager interrompe a notificação das descobertas da regra excluída.	Nenhuma ação é necessária. Se quiser, você pode editar os controles personalizados que usaram a regra excluída como mapeamento da fonte de dados. Isso ajuda a limpar as configurações da fonte de dados ao remover a regra excluída. Caso contrário, o nome da regra excluída permanecerá como um mapeamento de fonte de dados não utilizado.

Para atualizações de regras fora de seu ambiente AWS

Se uma regra personalizada for atualizada fora do seu ambiente da AWS, o Audit Manager não detectará a atualização da regra. Você deve considerar essa possibilidade se usa estruturas personalizadas compartilhadas. Isso ocorre porque, nesse cenário, o remetente e o destinatário

trabalham em ambientes separados da AWS. A tabela a seguir fornece ações recomendadas para esse cenário.

Sua função	Cenário	Ação recomendada
Remete	• Você compartilhou um framework que usa regras personalizadas como mapeamento de fonte de dados. • Depois de compartilhar o framework, você atualizou ou excluiu uma dessas regras no AWS Config.	Informe o destinatário sobre sua atualização. Dessa forma, ele pode aplicar a mesma atualização e continuar a par da definição de regra mais recente.
Destina rio	• Você aceitou uma estrutura compartil hada que usa regras personalizadas como mapeamento de fonte de dados. • Depois de recriar as regras personali zadas na sua instância do AWS Config, o remetente atualizou ou excluiu uma dessas regras.	Faça a atualização da regra correspon dente em sua própria instância do AWS Config.

Solução de problemas no painel

Você pode usar as informações nesta página para resolver problemas comuns do painel no Audit Manager.

Tópicos

Não há dados no meu painel

Se os números no widget de captura de tela diária exibirem um hífen (-), isso indica que nenhum dado está disponível. Você deve ter pelo menos uma avaliação ativa para visualizar os dados no painel. Para começar, crie uma avaliação. Após um período de 24 horas, os dados da sua avaliação começarão a aparecer no painel.

> **Note**
>
> Se os números no widget de captura de tela diária exibirem zero (0), isso indica que suas avaliações ativas (ou a avaliação selecionada) não têm evidências de não conformidade.

A opção de download de CSV não está disponível

Essa opção está disponível somente para avaliações individuais. Certifique-se de ter um the section called “Filtro de avaliação” aplicado ao painel e tente novamente. Lembre-se de que você só pode baixar um arquivo CSV por vez.

Não vejo o arquivo baixado ao tentar baixar um arquivo CSV

Se um domínio de controle possuir um grande número de controles, pode haver um pequeno atraso enquanto o Audit Manager gera o arquivo CSV. Depois que o arquivo for gerado, ele é baixado automaticamente.

Se você ainda não visualizar o arquivo baixado, verifique se sua conexão com a Internet está funcionando normalmente e se está usando a versão mais recente do seu navegador. Além disso, verifique sua pasta de downloads recentes. Os arquivos são baixados no local padrão determinado pelo seu navegador. Se isso não resolver o problema, tente baixar o arquivo usando um navegador diferente.

Não há um controle ou domínio de controle específico no painel

Isso provavelmente significa que suas avaliações ativas (ou avaliações especificadas) não têm dados relevantes para esse controle ou domínio de controle.

Um domínio de controle será exibido no painel somente se os dois critérios a seguir forem atendidos:

- Suas avaliações ativas (ou avaliação especificada) contêm pelo menos um controle relacionado a esse domínio

- Pelo menos um controle dentro desse domínio coletou evidências na data indicada na parte superior do painel

Um controle será exibido em um domínio somente se tiver coletado evidências na data na parte superior do painel.

A captura de tela diária mostra quantidades variáveis de evidências a cada dia. Isto é normal?

Nem todas as evidências são coletadas diariamente. Os controles nas avaliações do Audit Manager são mapeados para diferentes fontes de dados e cada um deles pode ter um cronograma de coleta de evidências diferente. Como resultado, espera-se que a captura de tela diária exiba uma quantidade variável de evidências a cada dia. Para obter mais informações sobre a frequência de coleta de evidências, consulte Como o AWS Audit Manager coleta evidências.

Solução de problemas de administradores delegados e do AWS Organizations

Você pode usar as informações nesta página para resolver problemas comuns de administradores delegados no Audit Manager.

Tópicos

Não consigo configurar o Audit Manager com minha conta de administrador delegado

Embora haja suporte para vários administradores delegados no AWS Organizations, o Audit Manager permite somente um administrador delegado. Se você tentar designar vários administradores delegados no Audit Manager, receberá a seguinte mensagem de erro:

- Console: `You have exceeded the allowed number of delegated administrators for the delegated service`
- CLI: `An error occurred (ValidationException) when calling the RegisterAccount operation: Cannot change delegated Admin for an active account 11111111111 from 2222222222222 to 333333333333`

Escolha a conta individual que você deseja usar como administrador delegado no Audit Manager. Primeiramente, certifique-se de registrar a conta de administrador delegado no Organizations e, em seguida, adicione a mesma conta como administrador delegado no Audit Manager.

Quando eu crio uma avaliação, não consigo ver as contas da minha organização em Contas no escopo

Se você quiser que sua avaliação do Audit Manager inclua várias contas da sua organização, deve especificar um administrador delegado.

Certifique-se de configurar uma conta de administrador delegado para o Audit Manager. Para obter instruções, consulte Configurando administrador delegado.

Algumas questões a serem levadas em consideração:

- Você não pode usar sua conta de gerenciamento do AWS Organizations como administrador delegado no Audit Manager.
- Se você quiser habilitar o Audit Manager em mais de uma Região da AWS, deverá designar uma conta de administrador delegada separadamente em cada região. Nas configurações do Audit Manager, designe a mesma conta de administrador delegado para todas as regiões.
- Ao designar um administrador delegado, certifique-se de que a conta do administrador delegado tenha acesso à chave do KMS fornecida ao configurar o Audit Manager. Para saber como analisar e alterar suas configurações de criptografia, consulte Criptografia de dados.

Recebo uma mensagem de erro de acesso negado quando tento gerar um relatório de avaliação usando minha conta de administrador delegado

Você receberá um erro de `access denied` se sua avaliação tiver sido criada por uma conta de administrador delegado à qual a chave do KMS especificada nas configurações do Audit Manager não pertence. Para evitar esse erro, ao designar um administrador delegado para o Audit Manager, certifique-se de que a conta do administrador delegado tenha acesso à chave do KMS que você forneceu ao configurar o Audit Manager.

Você também pode receber um erro de `access denied` se não tiver permissões de gravação para o bucket do S3 que está usando como destino do relatório de avaliação.

Se você receber um erro `access denied`, certifique-se de atender aos seguintes requisitos:

- Sua chave do KMS nas configurações do Audit Manager dá permissões ao administrador delegado. Você pode configurar isso seguindo as instruções em Permitir que usuários de outras contas usem uma chave do KMS no Guia do Desenvolvedor do AWS Key Management Service. Para obter instruções sobre como analisar e alterar suas configurações de criptografia no Audit Manager, consulte Criptografia de dados.
- Você tem uma política de permissões que lhe concede acesso de gravação para o destino do relatório de avaliação. Mais especificamente, sua política de permissões contém uma ação `s3:PutObject`, especifica o ARN do bucket do S3 e inclui a chave do KMS usada para criptografar seus relatórios de avaliação. Para ver um exemplo de política que você pode usar, consulte Exemplos de políticas baseadas em identidade para o AWS Audit Manager.

> **Note**
>
> Se você alterar as configurações de criptografia de dados do Audit Manager, essas alterações se aplicarão às novas avaliações que forem criadas daqui para frente. Isso inclui todos os relatórios de avaliação criados a partir de suas novas avaliações.
> As alterações não se aplicam às avaliações existentes criadas antes de alterar suas configurações de criptografia. Isso inclui novos relatórios de avaliação criados a partir de avaliações existentes, além dos relatórios de avaliação existentes. As avaliações existentes – e todos os seus relatórios de avaliação – continuam usando a antiga chave do KMS. Se a identidade do IAM que está gerando o relatório de avaliação não tiver permissões para usar a antiga chave do KMS, você poderá conceder permissões no nível da política de chaves.

O que acontece no Audit Manager se eu desvincular uma conta-membro da minha organização?

Quando você desvincula uma conta-membro de uma organização, o Audit Manager recebe uma notificação sobre esse evento. Em seguida, o Audit Manager remove automaticamente essa Conta da AWS das listas de contas no escopo de suas avaliações existentes. Quando você especifica o escopo de novas avaliações daqui em diante, a conta desvinculada não aparece mais na lista de Contas da AWS elegíveis.

Quando o Audit Manager remove uma conta-membro desvinculada das listas de contas no escopo de suas avaliações, você não é notificado sobre essa alteração. Além disso, a conta-membro desvinculada não é notificada de que o Audit Manager não está mais ativado em sua conta.

O que acontece se eu vincular novamente uma conta-membro à minha organização?

Quando você revincula uma conta-membro à sua organização, essa conta não é adicionada automaticamente ao escopo de suas avaliações existentes do Audit Manager. No entanto, a conta-membro vinculada novamente agora aparece como Conta da AWS elegível quando você especifica as contas no escopo de suas avaliações.

- Para avaliações existentes, você pode editar manualmente o escopo da avaliação a fim de adicionar a conta-membro vinculada novamente. Para obter instruções, consulte Editar Contas da AWS no escopo.
- Para novas avaliações, você pode adicionar a conta vinculada novamente durante a configuração da avaliação. Para obter instruções, consulte Especificar Contas da AWS no escopo.

O que acontece se eu migrar uma conta-membro de uma organização para outra?

Se uma conta-membro tiver o Audit Manager habilitado na organização 1 e, em seguida, migrar para a organização 2, o Audit Manager não será habilitado para a organização 2 como resultado da migração.

Solução de problemas de localizador de evidências

Use as informações nesta página para resolver problemas comuns do localizador de evidências no Audit Manager.

Problemas gerais do localizador de evidências

- Não consigo habilitar o localizador de evidências
- Eu habilitei o localizador de evidências, mas não vejo evidências anteriores nos resultados da minha pesquisa
- Não consigo desabilitar o localizador de evidências
- Ocorre uma falha na minha consulta de pesquisa

Problemas no relatório de avaliação do localizador de evidências

- Não consigo gerar vários relatórios de avaliação a partir dos meus resultados de pesquisa
- Não consigo incluir evidências específicas nos resultados da minha pesquisa
- Nem todos os resultados do meu localizador de evidências estão incluídos no relatório de avaliação
- Quero gerar um relatório de avaliação a partir dos resultados da minha pesquisa, mas ocorre uma falha na minha instrução de consulta
- Mais atributos

Problemas de exportação de CSV do localizador de evidências

- Ocorreu uma falha na minha exportação do CSV
- Não consigo exportar evidências específicas dos meus resultados de pesquisa
- Não consigo exportar vários arquivos CSV de uma vez

Não consigo habilitar o localizador de evidências

Os motivos comuns pelos quais você não pode habilitar o localizador de evidências incluem as seguintes situações:

Não há permissões suficientes

Se você estiver tentando ativar o localizador de evidências pela primeira vez, verifique se tem as permissões necessárias. Essas permissões possibilitam a criação e a gestão de um armazenamento de dados de eventos no CloudTrail Lake, o que é necessário para respaldar as consultas de pesquisa do localizador de evidências. As permissões também viabilizam a execução de consultas de pesquisa no localizador de evidências.

Se você precisar de ajuda com permissões, entre em contato com seu administrador AWS. Se você for administrador da AWS, poderá copiar a instrução de permissão necessária e anexá-la a uma política do IAM.

Você está usando a conta de gerenciamento do Organizations

Lembre-se de que não usar a conta de gerenciamento para habilitar o localizador de evidências. Faça login com a conta de administrador delegado e tente novamente.

Você desativou o localizador de evidências anteriormente

A reativação do localizador de evidências não é suportada no momento. Se você desativou o localizador de evidências anteriormente, não poderá reativá-lo.

Eu habilitei o localizador de evidências, mas não vejo evidências anteriores nos resultados da minha pesquisa

Quando você ativa o localizador de evidências, leva até sete dias para que todos os seus dados de evidências anteriores estejam disponíveis.

Durante esse período de sete dias, um armazenamento de dados de eventos é preenchido com os dados de evidências dos últimos dois anos. Isso significa que, se usar o localizador de evidências imediatamente após ativá-lo, nem todos os resultados estarão disponíveis até que o preenchimento seja concluído.

Para obter instruções sobre como verificar o status do preenchimento de dados, consulte Confirmando status do localizador de evidências.

Não consigo desabilitar o localizador de evidências

Isso pode ser causado por um dos seguintes motivos.

Não há permissões suficientes

Se você estiver tentando desabilitar o localizador de evidências, você precisa ter as permissões necessárias. Essas permissões permitem atualizar e excluir um armazenamento de dados de eventos no CloudTrail Lake, o que é necessário para desabilitar o localizador de evidências.

Se você precisar de ajuda com permissões, entre em contato com seu administrador AWS. Se você for administrador da AWS, poderá copiar a instrução de permissão necessária e anexá-la a uma política do IAM.

Uma solicitação para habilitar o localizador de evidências ainda está em andamento

Quando você solicita a ativação do localizador de evidências, criamos um armazenamento de dados de eventos para respaldar as consultas do localizador de evidências. Você não pode desativar o localizador de evidências enquanto o armazenamento de dados de eventos está sendo criado.

Para continuar, aguarde até que o armazenamento de dados de eventos seja criado e tente novamente. Para obter mais informações, consulte Confirmando status do localizador de evidências.

Você já solicitou a desabilitação do localizador de evidências

Quando você solicita a desativação do localizador de evidências, excluímos o armazenamento de dados de eventos usado para consultas do localizador de evidências. Se você tentar novamente desativar o localizador de evidências enquanto o armazenamento de dados de eventos estiver sendo excluído, receberá uma mensagem de erro.

Nesse caso, nenhuma ação é necessária. Aguarde até que o armazenamento de dados de eventos seja excluído. Assim que essa ação for concluída, o localizador de evidências será desativado. Para obter mais informações, consulte Confirmando status do localizador de evidências.

Ocorre uma falha na minha consulta de pesquisa

A falha em uma consulta de pesquisa pode ser causada por um dos motivos a seguir.

Não há permissões suficientes

Verifique se o usuário tem as permissões necessárias para executar consultas de pesquisa e acessar os respectivos resultados. Mais especificamente, você precisa de permissões para as seguintes ações do CloudTrail:

- StartQuery
- DescribeQuery
- CancelQuery
- GetQueryResults

Se você precisar de ajuda com permissões, entre em contato com seu administrador AWS. Se você for administrador da AWS, poderá copiar a instrução de permissão necessária e anexá-la a uma política do IAM.

Você está executando o número máximo de consultas

Você pode executar até cinco consultas por vez. Se você estiver executando o número máximo de consultas simultâneas, isso resultará em um erro de `MaxConcurrentQueriesException`. Se você receber essa mensagem de erro, aguarde um minuto até que algumas consultas sejam concluídas e execute a consulta novamente.

Sua instrução de consulta tem um erro de validação

Se você estiver usando a API ou a CLI para executar a operação StartQuery do CloudTrail Lake, verifique se o seu `queryStatement` é válido. Se a instrução de consulta tiver erros de validação, sintaxe incorreta ou palavras-chave incompatíveis, isso resultará em um `InvalidQueryStatementException`.

Para obter mais informações sobre como redigir uma consulta, confira Criar ou editar uma consulta no Guia do Usuário do AWS CloudTrail.

Para obter exemplos de sintaxe válida, analise os seguintes exemplos de instruções de consulta usados para consultar um armazenamento de dados de eventos do Audit Manager.

Exemplo 1: investigar evidências e seu status de conformidade

Este exemplo localiza evidências com qualquer status de conformidade em todas as avaliações da conta, dentro de um intervalo de datas especificado.

```
SELECT eventData.evidenceId, eventData.resourceArn,
 eventData.resourceComplianceCheck FROM $EDS_ID WHERE eventTime > '2022-11-02
 00:00:00.000' AND eventTime < '2022-11-03 00:00:00.000'
```

Exemplo 2: determinar evidências de não conformidade de um controle

Este exemplo localiza todas as evidências de não conformidade em um intervalo de datas determinado para uma avaliação e um controle específicos.

```
SELECT * FROM $EDS_ID WHERE eventData.assessmentId = '11aa33bb-55cc-77dd-99ee-
ff22gg44hh66' AND eventTime > '2022-10-27 22:05:00.000' AND eventTime
 < '2022-11-03 22:05:00.000' AND eventData.resourceComplianceCheck IN
 ('NON_COMPLIANT','FAILED','WARNING') AND eventData.controlId IN ('aa11bb22-cc33-
dd44-ee55-ff66gg77hh88')
```

Exemplo 3: contar as evidências por nome

Este exemplo lista o total de evidências de uma avaliação em um intervalo de datas especificado, agrupadas por nome e ordenadas pela contagem de evidências.

```
SELECT eventData.eventName as eventName, COUNT(*) as totalEvidence FROM  $EDS_ID
 WHERE eventData.assessmentId = '11aa33bb-55cc-77dd-99ee-ff22gg44hh66' AND eventTime
 > '2022-10-27 22:05:00.000' AND eventTime < '2022-11-03 22:05:00.000' GROUP BY
 eventData.eventName ORDER BY totalEvidence DESC
```

Exemplo 4: explorar evidências por fonte de dados e serviço

Este exemplo encontra todas as evidências em um intervalo de datas determinado para uma fonte de dados e um serviço específicos.

```
SELECT * FROM $EDS_ID WHERE eventTime > '2022-10-27 22:05:00.000' AND eventTime
 < '2022-11-03 22:05:00.000' AND eventData.service IN ('dynamodb') AND
 eventData.dataSource IN ('AWS API calls')
```

Exemplo 5: explorar evidências de conformidade por fonte de dados e domínio de controle

Este exemplo localiza evidências de conformidade provenientes de uma fonte de dados diferente do AWS Config para domínios de controle específicos.

```
 SELECT * FROM $EDS_ID WHERE eventData.resourceComplianceCheck IN
 ('PASSED','COMPLIANT') AND eventData.controlDomainName IN ('Logging and
```

```
monitoring','Data security and privacy') AND eventData.dataSource NOT IN ('AWS
Config')
```

Outras exceções de API

A API StartQuery pode falhar por vários outros motivos. Para obter uma lista completa dos possíveis erros e descrições, consulte Erros StartQuery na Referência de API AWS CloudTrail.

Não consigo gerar vários relatórios de avaliação a partir dos meus resultados de pesquisa

Esse erro é causado pela execução de muitas consultas do CloudTrail Lake ao mesmo tempo.

Esse erro poderá ocorrer se você agrupar os resultados da pesquisa e tentar gerar imediatamente relatórios de avaliação para cada item de linha nos resultados agrupados. Quando você obtém os resultados da pesquisa e gera um relatório de avaliação, cada ação invoca uma consulta. Você pode executar até cinco consultas por vez. Se você estiver executando o número máximo de consultas simultâneas, um erro `MaxConcurrentQueriesException` será retornado.

Para evitar esse erro, verifique se você não está gerando muitos relatórios de avaliação ao mesmo tempo. Se você estiver executando o número máximo de consultas simultâneas, um erro `MaxConcurrentQueriesException` será retornado. Se você receber essa mensagem de erro, aguarde alguns minutos até que seus relatórios de avaliação em andamento sejam concluídos.

Você pode verificar o status dos seus relatórios de avaliação na página da central de downloads no console do Audit Manager. Depois que seus relatórios forem concluídos, retorne aos resultados agrupados no localizador de evidências. Em seguida, você pode continuar obtendo os resultados e gerar um relatório de avaliação para cada item de linha.

Não consigo incluir evidências específicas nos resultados da minha pesquisa

Todos os resultados da sua pesquisa estão inclusos no relatório de avaliação. Você não pode adicionar seletivamente linhas individuais do seu conjunto de resultados de pesquisa.

Se você quiser incluir apenas resultados de pesquisa específicos no relatório de avaliação, recomendamos que edite seus filtros de pesquisa atuais. Dessa forma, você pode restringir seus resultados para direcionar apenas as evidências que deseja incluir no relatório.

Nem todos os resultados do meu localizador de evidências estão incluídos no relatório de avaliação

Quando você gera um relatório de avaliação, há limites para a quantidade de evidências que pode adicionar. O limite é baseado na Região da AWS da sua avaliação, na região do bucket do S3 que é usada como destino do relatório de avaliação e se sua avaliação usa uma AWS KMS key gerenciada pelo cliente.

1. O limite é 22.000 para relatórios da mesma região (onde o bucket do S3 e a avaliação estão na mesma Região da AWS)
2. O limite é 3.500 para relatórios de diferentes regiões (onde o bucket do S3 e a avaliação estão em Regiões da AWS diferentes)
3. O limite será 3.500 se a avaliação usar uma chave do KMS gerenciada pelo cliente

Se você exceder esse limite, o relatório ainda será criado. No entanto, o Audit Manager adiciona somente os primeiros 3.500 ou 22.000 itens de evidência ao relatório.

Para evitar esse problema, recomendamos que você edite seus filtros de pesquisa atuais. Dessa forma, você pode reduzir seus resultados de pesquisa visando a uma quantidade menor de evidências. Se necessário, você pode repetir esse método e gerar vários relatórios de avaliação em vez de um relatório maior.

Quero gerar um relatório de avaliação a partir dos resultados da minha pesquisa, mas ocorre uma falha na minha instrução de consulta

Se você estiver usando a API CreateAssessmentReport e sua instrução de consulta retornar uma exceção de validação, confira a tabela abaixo para obter orientação sobre como corrigi-la.

> **Note**
>
> Mesmo que uma instrução de consulta funcione no CloudTrail, a mesma consulta poderá não ser válida para a geração de relatórios de avaliação no Audit Manager. Isso ocorre devido a algumas diferenças na validação de consultas entre os dois serviços.

Cláusul	Problema	Solução	Observações
`SELECT`	A cláusula `SELECT` contém um nome de coluna	Remova a cláusula `SELECT` e substitua por `SELECT eventJson .`	Somente `SELECT eventJson` é suportado. Essa validação é processada pelo Audit Manager.
`FROM`	A cláusula `FROM` contém uma ID de armazenamento de dados de eventos inválida ou A ID do armazenamento de dados de eventos fornecida não corresponde à ID do armazenamento de dados de eventos nas configurações do Audit Manager	Remova a cláusula `FROM` e substitua por `FROM edsID`, em que o valor de `edsID` corresponde à ID do armazenamento de dados de eventos especificada nas configurações do Audit Manager. Você pode recuperar o ARN do armazenamento de dados de eventos nas configurações do Audit Manager. Para obter mais informações, consulte GetSettings na Referência de API AWS Audit Manager.	Essa validação é processada pelo Audit Manager.
`GROUP BY`	Uma cláusula `GROUP BY` está presente na consulta	Remova a cláusula `GROUP BY`.	Essa validação é processada pelo Audit Manager.
`HAVING`	Uma cláusula `HAVING` está presente na consulta	Remova a cláusula `HAVING`.	Essa validação é processada pelo Audit Manager.
`LIMIT`	A cláusula `LIMIT` contém um valor que excede o limite máximo permitido	Se a cláusula `LIMIT` existir, certifique-se de que seu valor seja igual ou menor que o limite máximo compatível:	No console, não há limite para o número de resultados de evidências que podem ser retornados. No entanto,

Cláusul	Problema	Solução	Observações
		• Para relatórios de mesma Região, o limite é 22.000 • Para relatórios entre Regiões, o limite é 3.500 • Para relatórios em que a avaliação relacionada usa uma AWS KMS key gerenciada pelo cliente, o limite é 3.500	ao gerar um relatório de avaliação, um limite se aplica à quantidade de evidências que você pode incluir. Se nenhum valor `LIMIT` for fornecido em sua instrução de consulta, os limites máximos padrão serão aplicados. Essa validação é processada pelo Audit Manager.
`ORDER BY`	A cláusula `ORDER BY` contém perfis agregados ou Apelidos que não estão presentes na cláusula `SELECT`	Certifique-se de que a cláusula `ORDER BY` não contenha nenhuma condição usando perfis agregados ou aliases.	Essa validação é processada pela API StartQuery do CloudTrail.

Cláusul	Problema	Solução	Observações
`WHERE`	A cláusula `WHERE` contém mais de uma `assessmentId` ou A cláusula `WHERE` contém uma `assessmentId` que não corresponde à `assessmentId` da sua solicitação `createAssessmentReport` ou A cláusula `WHERE` contém um nome de coluna não suportado	Certifique-se de que somente uma assessmentID seja especificada e que corresponda ao parâmetro assessmentId que você especificou na solicitação da API `createAssessmentReport` . Remova nomes de coluna não compatíveis.	Essa validação é processada pela API StartQuery do CloudTrail.

Exemplos

Os exemplos a seguir mostram como você pode usar o parâmetro `queryStatement` ao chamar a operação CreateAssessmentReport. Antes de usar essas consultas, substitua o *`texto do espaço reservado`* pelo seus valores `edsId` e `assessmentId`.

Exemplo 1: criar um relatório (aplica-se o limite para a mesma região)

Este exemplo cria um relatório que inclui resultados para buckets do S3 criados entre 22 e 23 de janeiro de 2022.

```
SELECT eventJson FROM 12345678-abcd-1234-abcd-123456789012 WHERE eventData.assessmentId
 = '11aa33bb-55cc-77dd-99ee-ff22gg44hh66' AND eventTime > '2022-01-22 00:00:00.000' AND
 eventTime < '2022-01-23 00:00:00.000' AND eventName='CreateBucket' LIMIT 22000
```

Exemplo 2: criar um relatório (aplica-se o limite para diferentes regiões)

Este exemplo cria um relatório que inclui todos os resultados para o armazenamento de dados de eventos e a avaliação especificados, sem nenhum intervalo de datas determinado.

```
SELECT eventJson FROM 12345678-abcd-1234-abcd-123456789012 WHERE eventData.assessmentId
 = '11aa33bb-55cc-77dd-99ee-ff22gg44hh66' LIMIT 7000
```

Exemplo 3: criar um relatório (abaixo do limite padrão)

Este exemplo cria um relatório que inclui todos os resultados do armazenamento e avaliação de dados de eventos especificados, com um limite abaixo do máximo padrão.

```
SELECT eventJson FROM 12345678-abcd-1234-abcd-123456789012 WHERE eventData.assessmentId
 = '11aa33bb-55cc-77dd-99ee-ff22gg44hh66' LIMIT 2000
```

Mais atributos

As páginas a seguir contêm orientações para solução de problemas gerais sobre relatórios de avaliação:

- Solução de problemas de relatórios de avaliação

Ocorreu uma falha na minha exportação do CSV

A exportação do CSV pode falhar por vários motivos. Você pode solucionar esse problema verificando as causas mais frequentes.

Primeiro, certifique-se de que os pré-requisitos sejam atendidos para o uso do atributo de exportação de CSV:

Você habilitou com sucesso o localizador de evidências

> Se você não tiver ativado o localizador de evidências, não poderá executar uma consulta de pesquisa nem exportar os resultados da pesquisa.

O preenchimento do seu armazenamento de dados de eventos está concluído

Se você usar o localizador de evidências imediatamente após ativá-lo e o preenchimento de evidências ainda estiver em andamento, alguns resultados poderão não estar disponíveis. Para verificar o status do preenchimento, consulte Confirmação do status do localizador de evidências.

Sua consulta de pesquisa teve êxito

O Audit Manager não pode exportar os resultados de uma consulta na qual ocorreu uma falha. Para solucionar uma falha na consulta, confira Ocorre uma falha na minha consulta de pesquisa.

Depois de confirmar que você atende aos pré-requisitos, use a lista de verificação a seguir para verificar possíveis problemas:

1. Verifique o status da sua consulta de pesquisa:
   a. A consulta foi cancelada? O localizador de evidências exibe resultados parciais que foram processados antes do cancelamento da consulta. No entanto, o Audit Manager não exporta resultados parciais para seu bucket do S3 ou para a central de downloads.
   b. A consulta está sendo executada há mais de uma hora? Consultas executadas por mais de uma hora podem expirar. O localizador de evidências exibe resultados parciais que foram processados antes do tempo limite da consulta esgotar. No entanto, o Audit Manager não exporta resultados parciais. Para evitar tempo limite, você pode reduzir a quantidade de evidências digitalizadas editando sua consulta de pesquisa, para especificar um intervalo mais restrito.
2. Verifique o nome e o URI do seu bucket do S3 de destino de exportação:
   a. O bucket especificado existe? Se você inseriu manualmente um URI do bucket, certifique-se de não cometido erros de digitação. Um erro de digitação ou um URI incorreto pode resultar em um erro `RESOURCE_NOT_FOUND` quando o Audit Manager tenta exportar o arquivo CSV para o Amazon S3.
3. Verifique as permissões do seu bucket do S3 de destino de exportação:
   a. Você tem permissões de gravação para o bucket S3? Você deve ter acesso de gravação ao bucket do S3 usado como destino de exportação. Mais especificamente, a política de permissões do IAM deve incluir uma ação `s3:PutObject` e o ARN do bucket, além de listar o CloudTrail como entidade principal do serviço. Fornecemos uma política de exemplo que você pode usar. Para obter instruções sobre como usar um bucket S3 diferente, consulte Exportar configurações de destino.
4. Verifique se alguma das informações da sua Região da AWS não coincide:

a. A Região da AWS da chave gerenciada pelo cliente corresponde à Região da AWS da sua avaliação? Se você forneceu uma chave gerenciada pelo cliente para criptografia de dados, ela deverá ser da mesma Região da AWS que a sua avaliação. Para obter instruções sobre como alterar a chave do KMS, consulte Configurações de criptografia de dados.

5. Verifique as permissões da sua conta de administrador delegado:

a. A chave gerenciada pelo cliente nas configurações do Audit Manager concede permissões ao administrador delegado? Se você estiver usando uma conta de administrador delegado e tiver especificado uma chave gerenciada pelo cliente para criptografia de dados, certifique-se de que o administrador delegado tenha acesso a essa chave do KMS. Para obter instruções Permitir que usuários de outras contas usem uma chave do KMS no Guia do Desenvolvedor do AWS Key Management Service. Para analisar e alterar suas configurações de criptografia no Audit Manager, consulte Configurações de criptografia de dados.

> **Note**
>
> Se você alterar as configurações de criptografia de dados do Audit Manager, essas alterações se aplicarão às novas avaliações que você criar daqui para frente. Isso inclui todos os arquivos CSV exportados de suas novas avaliações.
> As alterações não se aplicam às avaliações existentes criadas antes de alterar suas configurações de criptografia. Isso inclui novas exportações de CSV de avaliações existentes, além das exportações de CSV. As avaliações existentes — e todas as suas exportações CSV — continuam a usar a antiga chave do KMS. Se a identidade do IAM que está exportando o arquivo CSV não tiver permissões para usar a chave do KMS antiga, você poderá conceder permissões no nível da política de chaves.

Não consigo exportar evidências específicas dos meus resultados de pesquisa

Todos os resultados da sua pesquisa estão incluídos nos resultados.

Se desejar incluir apenas evidências específicas no arquivo CSV, recomendamos que você edite seus filtros de pesquisa atuais. Dessa forma, você pode restringir seus resultados para direcionar apenas as evidências que deseja exportar.

Não consigo exportar vários arquivos CSV de uma vez

Esse erro é causado pela execução de muitas consultas do CloudTrail Lake ao mesmo tempo.

Isso pode acontecer se você agrupar os resultados da pesquisa e tentar exportar imediatamente um arquivo CSV para cada item de linha nos resultados agrupados. Quando você obtém os resultados da pesquisa e exporta um arquivo CSV, cada uma dessas ações invoca uma consulta. Você pode executar até cinco consultas por vez. Se você estiver executando o número máximo de consultas simultâneas, um erro `MaxConcurrentQueriesException` será retornado.

Para evitar esse erro, verifique se você não está exportando muitos arquivos CSV ao mesmo tempo.

Para resolver esse erro, aguarde a conclusão das exportações de CSV em andamento. A maioria das exportações leva alguns minutos. No entanto, se estiver exportando uma quantidade muito grande de dados, a exportação pode levar até uma hora para ser concluída. Sinta-se à vontade para sair do localizador de evidências enquanto a exportação estiver em andamento.

Você pode verificar o status da exportação na central de downloads no console do Audit Manager. Depois que os arquivos exportados estiverem prontos, retorne aos resultados agrupados no localizador de evidências. Em seguida, você pode continuar a obter os resultados e exportar um arquivo CSV para cada item de linha.

Solução de problemas de compartilhamento de framework

Você pode usar as informações nesta página para resolver problemas comuns de compartilhamento de estrutura no Audit Manager.

Tópicos

O status da minha solicitação de compartilhamento enviada foi exibido como Falha

Se você tentar compartilhar uma estrutura personalizada e a operação falhar, recomendamos que verifique o seguinte:

1. Certifique-se de que o Audit Manager esteja ativado na Conta da AWS do destinatário e na região especificada. Para obter uma lista de regiões do AWS Audit Manager compatíveis, consulte Endpoints e cotas do AWS Audit Manager na Referência geral da Amazon Web Services.
2. Verifique se você inseriu a ID correta da Conta da AWS ao especificar a conta do destinatário.
3. Verifique se você não especificou uma conta de gerenciamento do AWS Organizations como destinatária. Você pode compartilhar uma estrutura personalizada com um administrador delegado, mas se tentar compartilhar uma estrutura personalizada com uma conta de gerenciamento, ocorrerá uma falha.
4. Se você usar uma chave gerenciada pelo cliente para criptografar seus dados do Audit Manager, certifique-se de que sua chave do KMS esteja ativada. Se sua chave do KMS estiver desativada e você tentar compartilhar um framework personalizada, ocorrerá uma falha. Para obter instruções sobre como ativar uma chave do KMS desativada, consulte Ativação e desativação de chaves no Guia do Desenvolvedor do AWS Key Management Service.

Minha solicitação de compartilhamento tem um ponto azul ao lado. O que isso significa?

Uma notificação de ponto azul indica que uma solicitação de compartilhamento precisa de sua atenção.

Notificações com pontos azuis para remetentes

Um ponto de notificação azul aparece ao lado das solicitações de compartilhamento enviadas com status Expirando. O Audit Manager exibe a notificação com pontos azuis para que você possa lembrar o destinatário de agir em relação à solicitação de compartilhamento antes que ela expire.

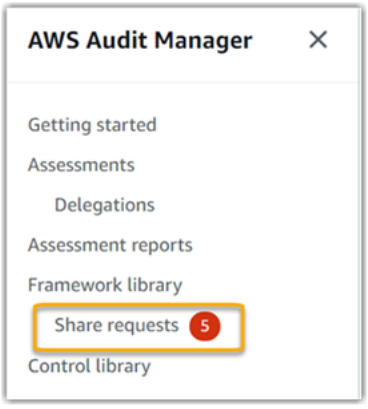
Para que o ponto azul da notificação desapareça, o destinatário deve aceitar ou recusar a solicitação. O ponto azul também desaparece se você revogar a solicitação de compartilhamento.

Você pode usar o procedimento a seguir para verificar se há solicitações de compartilhamento expiradas e enviar um lembrete opcional para que o destinatário desempenhe uma ação.

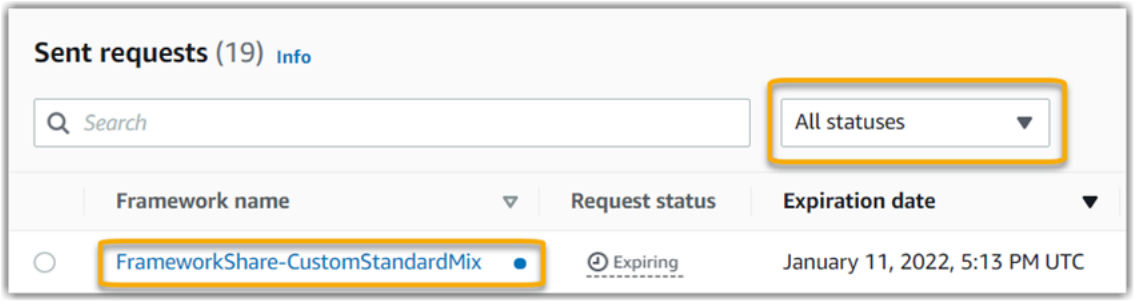
Para notificações de solicitações enviadas

1. Abra o console do AWS Audit Manager em https://console.aws.amazon.com/auditmanager/home.
2. Se você tiver uma notificação de solicitação de compartilhamento, o Audit Manager exibirá um ponto vermelho ao lado do ícone do menu de navegação.

3. Expanda o painel de navegação e veja ao lado de Solicitações de compartilhamento. Um selo de notificação indica o número de solicitações de compartilhamento que precisam de sua atenção.



4. Escolha Compartilhar solicitações e, em seguida, a guia Solicitações enviadas.
5. Procure o ponto azul para identificar as solicitações de compartilhamento que expiram nos próximos 30 dias. Como alternativa, você também pode visualizar as solicitações de compartilhamento expirando ao selecionar Expirando no menu suspenso do filtro Todos os status.



6. (Opcional) Lembre ao destinatário que ele precisa agir em relação à solicitação de compartilhamento antes que ela expire. Essa etapa é opcional, pois o Audit Manager envia uma notificação no console para informar ao destinatário quando uma solicitação de

compartilhamento está ativa ou expirando. No entanto, você também pode enviar seu próprio lembrete ao destinatário usando seu canal de comunicação preferido.

Notificações com pontos azuis para destinatários

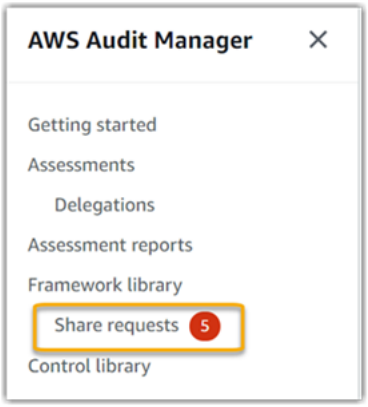
Um ponto de notificação azul aparece próximo às solicitações de compartilhamento recebidas com status Ativo ou Expirando. O Audit Manager exibe a notificação de ponto azul para lembrá-lo de tomar medidas em relação à solicitação de compartilhamento antes que ela expire. Para que o ponto azul da notificação desapareça, você deve aceitar ou recusar a solicitação. O ponto azul também desaparece se o remetente revogar a solicitação de compartilhamento.

Você pode usar o procedimento a seguir para verificar solicitações de compartilhamento ativas e expirando.

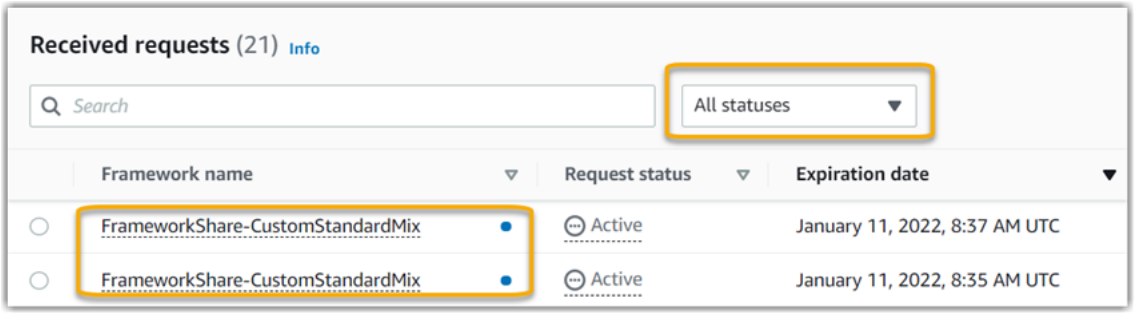
Para ver notificações de solicitações recebidas

1. Abra o console do AWS Audit Manager em https://console.aws.amazon.com/auditmanager/home.
2. Se você tiver uma notificação de solicitação de compartilhamento, o Audit Manager exibirá um ponto vermelho ao lado do ícone do menu de navegação.

3. Expanda o painel de navegação e veja ao lado de Solicitações de compartilhamento. Um selo de notificação indica o número de solicitações de compartilhamento que precisam de atenção.



4. Escolha Solicitações de compartilhamento. Por padrão, essa página é aberta na guia Solicitações recebidas.
5. Identifique as solicitações de compartilhamento que precisem de ação procurando itens com um ponto azul.



6. (Opcional) Para visualizar somente as solicitações que expiram nos próximos 30 dias, localize a lista suspensa Todos os status e selecione Expirando.

Meu framework compartilhado tem controles que usam regras personalizadas do AWS Config como fonte de dados. O destinatário pode coletar evidências para esses controles?

Sim, o seu destinatário pode recolher provas para estes controlos, mas são necessárias algumas etapas para o conseguir.

Para que o Audit Manager colete evidências usando uma regra do AWS Config como mapeamento da fonte de dados, o seguinte deve ser verdadeiro. Esses critérios se aplicam tanto às regras gerenciadas quanto personalizadas.

- A regra deve existir no ambiente AWS do destinatário.
- A regra deve estar habilitada no ambiente AWS do destinatário.

Lembre-se de que as regras do AWS Config em sua conta provavelmente ainda não existem no ambiente AWS do destinatário. Além disso, quando o destinatário aceita a solicitação de compartilhamento, o Audit Manager não recria nenhuma de suas regras personalizadas na conta. Para que o destinatário colete evidências usando suas regras personalizadas como mapeamento da fonte de dados, ele deve criar as mesmas regras personalizadas em sua instância do AWS Config. Depois que o destinatário cria e depois habilita as regras no AWS Config, o Audit Manager pode coletar evidências dessa fonte de dados.

Recomendamos que você se comunique com o destinatário para informá-lo se alguma regra personalizada do AWS Config precisa ser criada em sua instância do AWS Config.

Atualizei uma regra personalizada usada em um framework compartilhado. Preciso desempenhar alguma ação?

Para atualizações de regras em seu ambiente da AWS

Se você atualizar uma regra personalizada em seu ambiente AWS, nenhuma ação será necessária no Audit Manager. O Audit Manager detecta e trata atualizações de regras da maneira descrita na tabela a seguir. O Audit Manager não notifica quando uma atualização de regra é detectada.

Cenário	O que o Audit Manager faz	O que você precisa fazer
Uma regra personalizada é atualizada na sua instância do AWS Config.	O Audit Manager continua relatando as descobert as dessa regra ao usar a definição de regra atualizada.	Nenhuma ação é necessária.
Uma regra personalizada é excluída na sua instância do AWS Config.	O Audit Manager interrompe a notificação das descobertas da regra excluída.	Nenhuma ação é necessária. Se quiser, você pode editar os controles personalizados que usaram a regra excluída como mapeamento da fonte de dados. Em seguida, você pode remover a regra excluída para limpar as configura ções da fonte de dados do seu controle. Caso contrário , o nome da regra excluída permanecerá como um mapeamento de fonte de dados não utilizado.

Para atualizações de regras fora de seu ambiente AWS

No ambiente da AWS do destinatário, o Audit Manager não detecta a atualização da regra. Isso ocorre porque remetentes e destinatários trabalham em ambientes AWS separados. A tabela a seguir fornece ações recomendadas para esse cenário.

Sua função	Cenário	Ação recomendada
Remete	• Você compartilhou um framework que usa regras personalizadas como mapeamento de fonte de dados. • Depois de compartilhar o framework, você atualizou ou excluiu uma dessas regras no AWS Config.	Entre em contato com o destinatário para informá-lo sobre a atualização. Dessa forma, ele pode fazer a mesma atualização e ficar sincronizado com a definição de regras mais recente.
Destina rio	• Você aceitou uma estrutura compartil hada que usa regras personalizadas como mapeamento de fonte de dados. • Depois de recriar as regras personali zadas na sua instância do AWS Config, o remetente atualizou ou excluiu uma dessas regras.	Faça a atualização da regra correspon dente em sua própria instância do AWS Config.

Solução de problemas de notificação

Você pode usar as informações nesta página para resolver problemas comuns de notificação no Audit Manager.

Tópicos

- Eu especifiquei um tópico do Amazon SNS no Audit Manager, mas não estou recebendo nenhuma notificação
- Especifiquei um tópico FIFO mas não estou recebendo notificações na ordem esperada

Eu especifiquei um tópico do Amazon SNS no Audit Manager, mas não estou recebendo nenhuma notificação

Se o tópico do Amazon SNS usar o AWS KMS para criptografia do lado do servidor (SSE), talvez você não tenha as permissões necessárias para a política de chave do AWS KMS. Você também poderá deixar de receber notificações se não tiver inscrito um endpoint em seu tópico.

Caso não esteja recebendo notificações, certifique-se de ter feito o seguinte:

- Você anexou a política de permissões necessária para sua chave do KMS. Há um exemplo de política disponível na página Notificações deste guia.
- Você inscreveu um endpoint no tópico através do qual as notificações são enviadas. Ao enviar um endpoint de e-mail em um tópico, você recebe um e-mail solicitando a confirmação da inscrição. Você deve confirmar sua assinatura para começar a receber notificações por e-mail. Para obter mais informações, consulte Conceitos básicos no Guia do Desenvolvedor do Amazon SNS.

Especifiquei um tópico FIFO mas não estou recebendo notificações na ordem esperada

O Audit Manager suporta o envio de notificações para tópicos FIFO do SNS. No entanto, a ordem na qual o Audit Manager envia notificações para seus tópicos FIFO não é garantida.

Solução de problemas de permissão e acesso

Você pode usar as informações nesta página para resolver problemas comuns de permissão no Audit Manager.

Tópicos

Segui o procedimento de configuração do Audit Manager mas não tenho privilégios suficientes do IAM

O usuário, função ou grupo usado para acessar o Audit Manager deve ter as permissões necessárias. Além disso, sua política baseada em identidade não deve ser muito restritiva. Caso

contrário, o console não funcionará conforme esperado. O procedimento Configuração neste guia fornece uma política que concede as permissões mínimas necessárias para configurar o Audit Manager. Dependendo do seu caso de uso, você poderá precisar de permissões mais amplas e menos restritivas. Por exemplo, recomendamos que os responsáveis pela auditoria tenham acesso de administrador. Dessa forma, eles poderão modificar as configurações do Audit Manager e gerenciar atributos como avaliações, estruturas, controles e relatórios de avaliação. Outros usuários, como delegados, talvez precisem apenas de acesso de gerenciamento ou acesso somente leitura.

Certifique-se de adicionar as permissões apropriadas para seu usuário, função ou grupo. Para proprietários de auditoria, a política recomendada é AWSAuditManagerAdministratorAccess. Para delegados, você pode usar este exemplo disponível na página de exemplos de políticas do IAM. A partir desses exemplos de políticas, você pode fazer as alterações necessárias para atender às suas necessidades.

Recomendamos que você reserve um tempo para personalizar suas permissões a fim de atender aos seus requisitos específicos. Se você precisar de ajuda com as permissões do IAM, entre em contato com seu administrador ou com o Suporte da AWS.

Eu especifiquei outra pessoa como responsável pela auditoria, mas ela pessoa ainda não tem acesso total à avaliação. Por que isso acontece??

Especificar outra pessoa como responsável pela auditoria, por si só, não fornece acesso total a uma avaliação. Os responsáveis pela auditoria também devem ter as permissões necessárias do IAM para acessar e gerenciar os atributos do Audit Manager. Ou seja, além de especificar um usuário como responsável pela auditoria, você também deve anexar as políticas do IAM necessárias para esse usuário. A justificativa para tal procedimento é que, com ambas as exigências, o Audit Manager garante que você tenha controle total sobre todas as especificidades de cada avaliação.

> **Note**
>
> Para proprietários de auditoria, recomendamos usar a política AWSAuditManagerAdministratorAccess. Para obter mais informações, consulte Políticas recomendadas para personas de usuários no Audit Manager.

Não consigo desempenhar uma ação no Audit Manager

Se você não tiver as permissões necessárias para usar o console do AWS Audit Manager ou as operações da API do Audit Manager, provavelmente encontrará um erro `AccessDeniedException`.

Para resolver esse problema, entre em contato com o administrador para obter assistência. Caso seu administrador seja a pessoa que forneceu suas credenciais de início de sessão.

Quero permitir que pessoas fora da minha Conta da AWS acessem os atributos do meu Audit Manager

Você pode criar uma função que os usuários de outras contas ou pessoas fora da sua organização podem usar para acessar seus recursos. Você pode especificar quem é confiável para assumir a função. Para serviços que oferecem suporte a 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 Audit Manager oferece suporte a esses atributos, consulte Como AWS Audit Manager funciona com o IAM.
- Para saber como conceder acesso a seus recursos em todas as Contas da AWS pertencentes a você, consulte Fornecimento de acesso a um usuário do IAM em outra Conta da AWS pertencente a você no Guia de usuário do IAM.
- Para saber como conceder acesso a seus recursos para terceiros Contas da AWS, consulte Fornecimento de acesso a Contas da AWS pertencentes 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 perfis e políticas baseadas em recursos para acesso entre contas, consulte Como os perfis do IAM diferem de políticas baseadas em recursos no Guia do usuário do IAM.

Consulte também

As páginas a seguir contêm orientações de solução de outros problemas que podem ser causados pela falta de permissões:

- Não consigo ver nenhum controle ou conjuntos de controles na minha avaliação
- A opção de regra personalizada não está disponível quando configuro uma fonte de dados de controle
- Recebo um erro de acesso negado quando tento gerar um relatório de avaliação
- Recebo uma mensagem de erro de acesso negado quando tento gerar um relatório de avaliação usando minha conta de administrador delegado
- Não consigo habilitar o localizador de evidências
- Não consigo desabilitar o localizador de evidências
- Ocorre uma falha da minha consulta no localizador de evidências
- Eu especifiquei um tópico do Amazon SNS no Audit Manager, mas não estou recebendo nenhuma notificação

Cotas e restrições para AWS Audit Manager

Sua Conta da AWS tem cotas padrão, anteriormente chamadas de limites, para cada AWS service (Serviço da AWS). A menos que especificado de outra forma, cada cota é específica da Região. Você pode solicitar aumentos para algumas cotas; outras não podem ser aumentadas.

Grande parte das cotas do Audit Manager, mas não todas, estão listadas no AWS Audit Manager namespace do console do Service Quotas. Para saber mais sobre como solicitar um aumento da cota, consulte Gerenciando suas cotas Audit Manager.

Cotas padrão Audit Manager

As seguintes cotas AWS Audit Manager são por Conta da AWS por Região.

Avaliações

- Número de avaliações ativas por conta: 100

Relatórios de avaliação

- Número de itens de evidência que você pode adicionar a um relatório de avaliação:
  - Para relatórios da mesma Região (onde a avaliação e o bucket S3 de destino do relatório de avaliação estiverem no mesmo Região da AWS lugar): 22.000
  - Para relatórios entre Regiões (onde a avaliação e o bucket S3 de destino do relatório de avaliação estão em Regiões da AWS diferentes): 3.500
  - Para relatórios cuja avaliação relacionada usa um cliente gerenciadoAWS KMS key: 3.500

Controles

- Número de controles personalizados por conta: 500

Evidência

- Tamanho máximo de um único arquivo de evidência manual: 100 MB
- Número de carregamentos diários de evidências manuais por controle: 100

> **Tip**
>
> Se precisar carregar uma grande quantidade de evidências manuais em um único controle, carregue as evidências em lotes ao longo de vários dias.

Frameworks

- Número de frameworks personalizados por conta: 100

> **Note**
>
> As cotas de framework se aplicam a todos os frameworks personalizados compartilhados em sua biblioteca de framework, independente de quem o tenha criado.

Destinatários da framework personalizado compartilhado

- Número de contas de destinatários ativas: 100

Acesso à API

- Número de Transações por Segundo (TPS) em todas as APIs: 20 TPS

Gerenciando suas cotas Audit Manager

AWS Audit Manager é integrado às Service Quotas, AWS service (Serviço da AWS) que permitem visualizar e gerenciar cotas de um local central. Para obter mais informações, consulte O que são Service Quotas? no Guia do Usuário de Service Quotas. Service Quotas simplificam a pesquisa do valor das cotas do Amazon ECS.

Para ver as service quotas do Audit Manager usando o console

1. Abra o console Service Quotas em https://console.aws.amazon.com/servicequotas/.
2. No painel de navegação, escolha Serviços da AWS.
3. Na lista Serviços da AWS, procure e selecione AWS Audit Manager.

4. Na lista Service Quotas é possível ver o nome da service quota, o valor aplicado (se disponível), o valor da cota padrão AWS e se o valor da cota é ajustável.
5. Para visualizar informações adicionais sobre uma service quota, como descrição, escolha o nome da cota.
6. (Opcional) Para solicitar um aumento de cota, selecione a cota que deseja aumentar, selecione Solicitar Aumento de Cota, insira ou selecione as informações necessárias e, por fim, selecione Solicitar.

Para obter mais informações, consulte Solicitando um Aumento de Cota no Guia do Usuário do Service Quotas.

Segurança em AWS Audit 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 a segurança da nuvem e segurança na nuvem:

- Segurança da nuvem — AWS é responsável por proteger a infraestrutura que executa AWS os serviços na AWS nuvem. 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 que se aplicam AWS Audit Manager, consulte AWS Serviços no escopo do programa de conformidadeAWS .
- 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 ajuda você a entender como aplicar o modelo de responsabilidade compartilhada ao usar AWS Audit Manager. Os tópicos a seguir mostram como configurar o Audit Manager para atender aos seus objetivos de segurança e conformidade. Você também aprenderá a usar outros AWS serviços que ajudam a monitorar e proteger seus recursos do Audit Manager.

Tópicos

Proteção de dados em AWS Audit Manager

O modelo de responsabilidade AWS compartilhada modelo se aplica à proteção de dados em AWS Audit 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 ter mais informações sobre a privacidade de dados, consulte as Perguntas frequentes sobre privacidade de dados. Para ter mais informações sobre a proteção de dados na Europa, consulte a publicação no blog AWS Shared Responsibility Model and GDPR no Blog de segurança daAWS .

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, 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 Audit Manager ou outro Serviços da AWS usando o console, a API ou AWS os SDKs. AWS CLIQuaisquer 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 URL para um servidor externo, recomendemos fortemente que não sejam incluídas informações de credenciais na URL para validar a solicitação a esse servidor.

Além da recomendação acima, recomendamos especificamente que os clientes do Audit Manager não incluam informações confidenciais de identificação em campos de formato livre ao criarem avaliações, controles personalizados, estruturas personalizadas e comentários de delegação.

Exclusão dos dados do Audit Manager

Existem diversas maneiras de excluir os dados do Audit Manager.

Exclusão de dados ao desativar o Audit Manager

Ao desativar o Audit Manager, você pode decidir se deseja excluir todos os dados do Audit Manager. Se você optar por excluir seus dados, eles serão excluídos até 7 dias após a desativação do Audit Manager. Depois que seus dados forem excluídos, você não poderá recuperá-los.

Exclusão de dados automática

Alguns dados do Audit Manager são excluídos automaticamente após um período específico. O Audit Manager retém os dados do cliente da seguinte forma:

Tipo de dados	Período de retenção de dados	Observações
Evidências	Os dados são retidos por 2 anos a partir do momento da criação	Inclui evidências automatizadas e evidências manuais
Recursos criados pelo cliente	Os dados são retidos indefinidamente	Inclui avaliações, relatórios de avaliação, controles personalizados e estruturas personalizadas

Exclusão manual de dados

É possível excluir recursos individuais do Audit Manager a qualquer momento. Para obter instruções, consulte:

- Como excluir uma avaliação
  - Veja também: DeleteAssessmentna Referência daAWS Audit Manager API
- Como excluir um framework personalizado
  - Veja também: DeleteAssessmentFrameworkna Referência daAWS Audit Manager API
- Como excluir uma solicitação de compartilhamento
  - Veja também: DeleteAssessmentFrameworkSharena Referência daAWS Audit Manager API
- Como excluir um relatório de avaliação
  - Veja também: DeleteAssessmentReportna Referência daAWS Audit Manager API
- Como excluir um controle personalizado
  - Veja também: DeleteControlna Referência daAWS Audit Manager API

Para excluir outros dados de recursos que você possa ter criado ao usar o Audit Manager, veja o seguinte:

- Excluir um armazenamento de dados de eventos no AWS CloudTrail Guia do Usuário
- Deletando um bucket no Guia do Usuário Amazon Simple Storage Service (Amazon S3)

Criptografia inativa

Para criptografar dados em repouso, o Audit Manager usa criptografia do lado do servidor Chaves gerenciadas pela AWS para todos os seus repositórios de dados e registros.

Seus dados são criptografados sob uma chave gerenciada pelo cliente ou uma Chave pertencente à AWS, dependendo das configurações selecionadas. Se você não fornecer uma chave gerenciada pelo cliente, o Audit Manager usa uma Chave pertencente à AWS para criptografar seu conteúdo. Todos os metadados de serviço no DynamoDB e no Amazon S3 no Audit Manager são criptografados usando um Chave pertencente à AWS.

O Audit Manager criptografa os dados da seguinte forma:

- Os metadados do serviço armazenados no Amazon S3 são criptografados Chave pertencente à AWS usando SSE-KMS.
- Os metadados de serviço armazenados no DynamoDB são criptografados no lado do servidor usando KMS e um Chave pertencente à AWS.

- Seu conteúdo armazenado no DynamoDB é criptografado do lado do cliente usando uma chave gerenciada pelo cliente ou Chave pertencente à AWS. A chave KMS é baseada nas configurações escolhidas.
- Seu conteúdo armazenado no Amazon S3 no Audit Manager é criptografado usando SSE-KMS. A chave KMS é baseada na sua seleção e pode ser uma chave gerenciada pelo cliente ou Chave pertencente à AWS.
- Os relatórios de avaliação publicados em seu bucket do S3 são criptografados da seguinte forma:
  - Se você forneceu uma chave gerenciada pelo cliente, seus dados serão criptografados usando o SSE-KMS.
  - Se você usou o Chave pertencente à AWS, seus dados são criptografados usando SSE-S3.

Criptografia em trânsito

O Audit Manager fornece endpoints seguros e privados para criptografar dados em trânsito. Os endpoints seguros e privados permitem proteger AWS a integridade das solicitações de API ao Audit Manager.

Trânsito entre serviços

Por padrão, todas as comunicações entre serviços são protegidas pelo uso da criptografia Transport Layer Security (TLS).

Gerenciamento de chaves

O Audit Manager suporta chaves gerenciadas Chaves pertencentes à AWS tanto pelo cliente quanto pelo cliente para criptografar todos os recursos do Audit Manager (avaliações, controles, estruturas, evidências e relatórios de avaliação salvos nos buckets do S3 em suas contas).

Recomendamos usar uma chave gerenciada pelo cliente. Ao fazer isso, você pode visualizar e gerenciar as chaves de criptografia que protegem seus dados, inclusive a visualização de logs de seu uso em AWS CloudTrail. Ao escolher uma chave gerenciada pelo cliente, o Audit Manager cria uma concessão para a chave do KMS para que ela possa ser usada para criptografar o conteúdo.

> **Warning**
>
> Depois que uma chave do KMS é excluída, não é mais possível descriptografar os dados que foram criptografados com ela, o que significa que os dados são irrecuperáveis.

> Excluir uma chave KMS em AWS Key Management Service (AWS KMS) é destrutivo e potencialmente perigoso. Para obter mais informações sobre a exclusão de chaves KMS, consulte Deletando AWS KMS keys em AWS Key Management Service Guia de Usuário.

Você pode especificar suas configurações de criptografia ao ativar o Audit Manager usando a AWS Management Console, a API do Audit Manager ou a AWS Command Line Interface (AWS CLI). Para obter instruções, consulte Habilitar AWS Audit Manager.

Você pode revisar e alterar suas configurações de criptografia a qualquer momento. Para obter instruções, consulte Criptografia de dados.

Para obter mais informações sobre como configurar chaves gerenciadas pelo cliente, consulte Criando chaves no AWS Key Management Service Guia do Usuário.

Gerenciamento de identidade e acesso para AWS Audit 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 recursos do ACM. O IAM é um AWS service (Serviço da AWS) que você pode usar sem custo adicional.

Tópicos

Público

A forma como você usa AWS Identity and Access Management (IAM) difere, dependendo do trabalho que você faz no Audit Manager.

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

Administrador do serviço – Se você for o responsável pelos recursos do Audit Manager na sua empresa, provavelmente terá acesso total ao Audit Manager. Cabe a você determinar quais funcionalidades e recursos do Audit 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 Audit Manager, consulte Como AWS Audit Manager funciona com o IAM.

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

Autenticando com identidades

A autenticação é 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 uma 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 AWS, consulte Como fazer login Conta da AWSno Guia doInício 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.

Independentemente 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 GuiaAWS IAM Identity Center do usuário. Usar 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 pode 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 acessam 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 doAWS IAM Identity Center .

Grupos e usuários 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 depender de 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 atribuir 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 uma função) 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. Ela é semelhante a um usuário do IAM, mas não está associada 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 Usar perfis do IAM no Guia do usuário do IAM.

Perfis 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 IAM Identity Center, configure um conjunto de permissões. Para controlar o que suas identidades podem acessar após a autenticação, o IAM Identity Center 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 doAWS IAM Identity Center .
- Permissões temporárias para usuários do IAM: um usuário ou um perfil do IAM pode assumir 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 recurso para acesso entre contas, consulte Como os perfis do IAM diferem das políticas baseadas em recurso 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 aplicações 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 uma função vinculada ao serviço.
  - Sessões de acesso direto (FAS) — Quando você usa um usuário ou uma função do IAM para realizar ações AWS, você é considerado 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.
  - Perfil 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 assumir 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 pode editar as permissões para perfis vinculados 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 obter mais informações, consulte Usar uma função 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 as funções do IAM, consulte Quando criar um perfil do IAM (em vez de um usuário) no Guia do usuário do IAM.

Gerenciamento do 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 permissão para executar ações nos recursos de que eles precisam, um administrador do IAM pode criar políticas do IAM. O administrador pode então adicionar as políticas do IAM a perfis, e os usuários podem assumir os perfis.

As políticas do IAM definem permissões para uma ação, independentemente 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 um usuário do IAM, grupo de usuários ou função 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 Criação de política do IAM no Guia do usuário do IAM.

As políticas baseadas em identidade podem ser categorizadas ainda mais 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 recurso

Políticas baseadas em recurso 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 compatíveis com 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 uma entidade principal especificada 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 que estão 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 às 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 WAFPara 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 e dos seus limites de permissões. As políticas baseadas em recurso que especificam o usuário ou a função 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 Organizations e SCPs, consulte Como os SCPs funcionam no Guia do usuário doAWS 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 recurso. 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 Audit Manager funciona com o IAM

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

Recursos do IAM que você pode usar com AWS Audit Manager

Atributos do IAM	Suporte do Audit Manager
Políticas baseadas em identidade	Sim
Políticas baseadas em recursos	Não
Ações de políticas	Sim
Recursos de políticas	Sim
Chaves de condição de políticas	Parcial
ACLs	Não
ABAC (tags em políticas)	Sim
Credenciais temporárias	Sim
Sessões de acesso direto (FAS)	Sim
Perfis de serviço	Não
Funções vinculadas ao serviço	Sim

Para ter uma visão de alto nível de como AWS Audit 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.

Políticas baseadas em identidade para AWS Audit Manager

É compatível com 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 Criar 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, bem 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 função à 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.

AWS Audit Manager cria uma política gerenciada nomeada `AWSAuditManagerAdministratorAccess` para administradores do Audit Manager. Essa política concede acesso total a administração no Audit Manager. Os administradores podem anexar essa política a qualquer função ou usuário existente, ou criar uma nova função com essa política.

Políticas recomendadas para personas de usuários em AWS Audit Manager

AWS Audit Manager permite que você mantenha a segregação de tarefas entre diferentes usuários e para diferentes auditorias usando diferentes políticas do IAM. As duas personas no Audit Manager e suas políticas recomendadas são definidas da seguinte forma:

Pessoa	Descrição e política recomendada
Proprietário da auditoria	• Essa pessoa deve ter as permissões necessárias para gerenciar as avaliações em. AWS Audit Manager

Pessoa	Descrição e política recomendada
	• A política recomendada a ser usada para essa pessoa é a política gerenciada chamada AWSAuditManagerAdministratorAccess. Você pode usar essa política como um ponto de partida e definir o escopo dessas permissões conforme necessário para atender às suas necessidades.
Delegar	• Essa pessoa pode acessar os conjuntos de controle delegados em uma avaliação. Eles podem atualizar o status do controle, adicionar comentários, enviar um conjunto de controles para análise e adicionar evidências ao relatório de avaliação. • A política recomendada a ser usada para essa persona é o seguinte exemplo: Permita que os usuários tenham acesso total do administrador ao AWS Audit Manager. A partir dessas políticas, você pode fazer as alterações necessárias para atender às suas necessidades.

Exemplos de políticas baseadas em identidade para AWS Audit Manager

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

Políticas baseadas em recursos dentro AWS Audit Manager

Oferece suporte a políticas baseadas em recursos	Não

Políticas baseadas em recurso 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 compatíveis com 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 uma entidade principal especificada 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 recurso. Adicionar um 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 um principal na mesma conta, nenhuma política baseada em identidade adicional será necessária. Para obter mais informações, consulte Como os perfis do IAM diferem de políticas baseadas em recursos no Guia do usuário do IAM.

Ações políticas para AWS Audit Manager

Oferece suporte a 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. Há também algumas operações que 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 de AWS Audit Manager ações, consulte Ações definidas pelo AWS Audit Manager na Referência de Autorização de Serviço.

As ações de política AWS Audit Manager usam o seguinte prefixo antes da ação.

```
auditmanager
```

Para especificar várias ações em uma única instrução, separe-as com vírgulas.

```
"Action": [
      "auditmanager:GetEvidenceDetails",
```

```
      "auditmanager:GetEvidenceEventDetails"
         ]
```

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

```
"Action": "auditmanager:Get*"
```

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

Recursos políticos para AWS Audit Manager

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

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

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

Para ver uma lista dos tipos de AWS Audit Manager recursos e seus ARNs, consulte Recursos definidos pelo AWS Audit Manager na Referência de Autorização de Serviço. Para saber com quais ações é possível especificar o ARN de cada recurso, consulte Ações definidas por AWS Audit Manager.

Uma avaliação do Audit Manager tem o seguinte formato do Amazon Resource Name (ARN):

```
arn:${Partition}:auditmanager:${Region}:${Account}:assessment/${assessmentId}
```

Um conjunto de controles do Audit Manager tem o seguinte formato ARN:

```
arn:${Partition}:auditmanager:${Region}:${Account}:assessment/
${assessmentId}controlSet/${controlSetId}
```

Um controle do Audit Manager tem o seguinte formato ARN:

```
arn:${Partition}:auditmanager:${Region}:${Account}:control/${controlId}
```

Para obter mais informações sobre o formato de ARNs, consulte Nomes de recursos da Amazon (ARNs).

Por exemplo, para especificar a avaliação `i-1234567890abcdef0` em sua declaração, use o seguinte ARN:

```
"Resource": "arn:aws:auditmanager:us-east-1:123456789012:assessment/
i-1234567890abcdef0"
```

Para especificar todas as instâncias que pertencem a uma conta específica, use o caractere curinga (*).

```
"Resource": "arn:aws:auditmanager:us-east-1:123456789012:assessment/*"
```

Algumas ações do Audit Manager, como as ações para a criação de recursos, não podem ser executadas em um recurso específico. Nesses casos, você deve utilizar o caractere curinga (*).

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

Muitas ações de API do Many Audit Manager envolvem vários recursos. Por exemplo, `ListAssessments` retorna uma lista de metadados de avaliação que pode ser acessada por quem está conectado no momento. Conta da AWSPortanto, um usuário deve ter permissões para visualizar as avaliações. Para especificar vários recursos em uma única instrução, separe os ARNs com vírgulas.

```
"Resource": [
```

```
      "resource1",
      "resource2"
```

Para ver uma lista dos tipos de recursos do Audit Manager e seus ARNs, consulte Recursos Definidos por AWS Audit Manager no Guia do Usuário do IAM. Para saber com quais ações você pode especificar o ARN de cada recurso, consulte Ações definidas pelo AWS Audit Manager.

Algumas ações da API do Audit Manager oferecem suporte a vários recursos. Por exemplo, `GetChangeLogs` acessa um `assessmentID`, `controlID` e `controlSetId`, portanto, uma entidade principal deve ter permissões para acessar cada um desses recursos. Para especificar vários recursos em uma única instrução, separe os ARNs com vírgulas.

```
"Resource": [
      "assessmentId",
      "controlId",
      "controlSetId"
```

Chaves de condição de política para AWS Audit Manager

Suporta chaves de condição de política específicas do serviço	Parcial

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 de `Condition`) permite que você especifique condições nas quais uma instrução está em vigor. O elemento `Condition` é opcional. É possível criar expressões condicionais que usam atendentes 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 elemento `Condition`, 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 para que as permissões da instrução sejam concedidas.

Quando a entidade principal em uma declaração de política chave é uma AWS entidade principal de serviço, recomendamos usar `aws:SourceArn` ou as chaves de condição globais

`aws:SourceAccount` na política. Você pode usar essas chaves de contexto de condição global para ajudar a evitar o cenário de "confused deputy". O exemplo a seguir mostra como usar as chaves de contexto de condição globais `aws:SourceArn` e `aws:SourceAccount` mo Audit Manager para evitar o problema "confused deputy."

- Exemplo de política para um tópico do SNS usado para notificações do Audit Manager
- Exemplo de política para uma chave KMS usada com um tópico do SNS

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

Audit Manager não fornece nenhuma chave de condição específica ao serviço, mas sim suporte ao uso de algumas chaves de condição globais. Para ver todas as chaves de condição AWS globais, consulte as chaves de contexto de condiçãoAWS global no Guia do usuário do IAM.

Listas de controle de acesso (ACLs) em AWS Audit Manager

Oferece suporte a 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 às políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

Controle de acesso baseado em atributos (ABAC) com AWS Audit Manager

Oferece suporte a ABAC (tags em políticas)	Sim

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 recursos 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 está tentando acessar.

O ABAC é útil em ambientes que estão crescendo rapidamente e ajuda em situações em que 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 `aws:TagKeys` chaves de condição.

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 Usar controle de acesso baseado em atributos (ABAC) no Guia do usuário do IAM.

Para obter mais informações sobre a marcação de AWS Audit Manager recursos, consulteMarcando atributos AWS Audit Manager.

Usando credenciais temporárias com AWS Audit Manager

Oferece suporte a 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 trabalhar 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 perfis, consulte Alternar para uma função (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 obter mais informações, consulte Credenciais de segurança temporárias no IAM.

Sessões de acesso direto para AWS Audit 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 AWS, você é considerado 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 Encaminhamento de sessões de acesso.

Funções de serviço para AWS Audit Manager

Oferece suporte a perfis de serviço	Não

A função 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 AWS Audit Manager . Só edite os perfis de serviço quando o Audit Manager orientar você a fazê-lo.

Funções vinculadas a serviços para AWS Audit Manager

Oferece suporte a funções vinculadas 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 assumir 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 pode editar as permissões para perfis vinculados ao serviço.

Para obter detalhes sobre funções vinculadas a serviços para AWS Audit Manager, consulte. Usando funções vinculadas a serviços para AWS Audit Manager

Exemplos de políticas baseadas em identidade para AWS Audit Manager

Por padrão, usuários e funções não têm permissão para criar ou modificar recursos do Audit 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 permissões para executar ações nos recursos de 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 assumir 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 recurso definidos pelo AWS Audit Manager, inclusive o formato dos ARNs para cada tipo de recurso, consulte Ações, recursos e chaves de condição para AWS Audit Manager em Referência de autorização de serviço.

Tópicos

- Práticas recomendadas de políticas
- Permita as permissões mínimas necessárias para ativar o Audit Manager
- Permita que os usuários tenham acesso total do administrador ao AWS Audit Manager
- Permita que o gerenciamento de usuários acesse AWS Audit Manager
- Permita que os usuários tenham acesso somente para leitura ao AWS Audit Manager
- Permitir que os usuários visualizem suas próprias permissões
- AWS Audit Manager Permitir o envio de notificações para tópicos do Amazon SNS
- Permitir que os usuários executem consultas de pesquisa no localizador de evidências

Práticas recomendadas de políticas

As políticas baseadas em identidade determinam se alguém pode criar, acessar ou excluir recursos do Audit Manager em sua conta. Essas ações podem incorrer em custos para a 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 políticasAWS 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 pelaAWS ou Políticas gerenciadas pelaAWS para perfis 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 recursos 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 escrever 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 de política JSON do IAM: Condition no Manual 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 ajudar você 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 AWSa MFA para obter segurança adicional. Para exigir a 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.

Permita as permissões mínimas necessárias para ativar o Audit Manager

Este exemplo mostra como você pode permitir que contas sem uma função de administrador sejam habilitadas. AWS Audit Manager

> **Note**
>
> O que fornecemos aqui é uma política básica, que concede as permissões mínimas necessárias para habilitar o Audit Manager. Todas as permissões na política a seguir são necessárias. Se você omitir qualquer parte dessa política, não poderá habilitar Audit Manager.
>
> Recomendamos que você reserve um tempo para personalizar suas permissões, a fim de atender aos seus requisitos específicos. Se precisar de ajuda, entre em contato com seu administrador ou AWS Support.

Para conceder o acesso mínimo necessário para ativar o Audit Manager, use as seguintes permissões:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "auditmanager:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "auditmanager.amazonaws.com"
                }
            }
        },
        {
```

```
            "Sid": "CreateEventsAccess",
            "Effect": "Allow",
            "Action": [
                "events:PutRule"
            ],
            "Resource": "*",
            "Condition": {
                "ForAllValues:StringEquals": {
                    "events:source": [
                        "aws.securityhub"
                   ]
                }
            }
        },
        {
            "Sid": "EventsAccess",
            "Effect": "Allow",
            "Action": [
                "events:PutTargets"
            ],
            "Resource": "arn:aws:events:*:*:rule/
AuditManagerSecurityHubFindingsReceiver"
        },
        {
            "Effect": "Allow",
            "Action": "kms:ListAliases",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "auditmanager.amazonaws.com"
                }
            }
        }
    ]
}
```

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 às ações que corresponderem a operação da API que você estiver tentando executar.

Permita que os usuários tenham acesso total do administrador ao AWS Audit Manager

O exemplo de políticas a seguir concede acesso total ao administrador AWS Audit Managera.

- Exemplo 1 (política gerenciada, `AWSAuditManagerAdministratorAccess`)
- Exemplo 2 (permissões de destino do relatório de avaliação)
- Exemplo 3 (permissões de destino de exportação)
- Exemplo 4 (permissões para ativar o localizador de evidências)
- Exemplo 5 (permissões para desativar o localizador de evidências)

Exemplo 1 (política gerenciada, **`AWSAuditManagerAdministratorAccess`**)

Essa política do exemplo é a política gerenciada, `AWSAuditManagerAdministratorAccess`. Essa política inclui a capacidade de ativar e desativar o Audit Manager, a capacidade de alterar as configurações do Audit Manager e a capacidade de gerenciar todos os recursos do Audit Manager, como avaliações, estruturas, controles e relatórios de avaliação.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AuditManagerAccess",
            "Effect": "Allow",
            "Action": [
                "auditmanager:*"
            ],
            "Resource": "*"
        },
        {
            "Sid": "OrganizationsAccess",
            "Effect": "Allow",
            "Action": [
                "organizations:ListAccountsForParent",
                "organizations:ListAccounts",
                "organizations:DescribeOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribeAccount",
                "organizations:ListParents",
                "organizations:ListChildren"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowOnlyAuditManagerIntegration",
            "Effect": "Allow",
```

```
            "Action": [
                "organizations:RegisterDelegatedAdministrator",
                "organizations:DeregisterDelegatedAdministrator",
                "organizations:EnableAWSServiceAccess"
            ],
            "Resource": "*",
            "Condition": {
                "StringLikeIfExists": {
                    "organizations:ServicePrincipal": [
                        "auditmanager.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Sid": "IAMAccess",
            "Effect": "Allow",
            "Action": [
                "iam:GetUser",
                "iam:ListUsers",
                "iam:ListRoles"
            ],
            "Resource": "*"
        },
        {
            "Sid": "IAMAccessCreateSLR",
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/
auditmanager.amazonaws.com/AWSServiceRoleForAuditManager*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "auditmanager.amazonaws.com"
                }
            }
        },
        {
            "Sid": "IAMAccessManageSLR",
            "Effect": "Allow",
            "Action": [
                "iam:DeleteServiceLinkedRole",
                "iam:UpdateRoleDescription",
                "iam:GetServiceLinkedRoleDeletionStatus"
            ],
```

```
            "Resource": "arn:aws:iam::*:role/aws-service-role/
auditmanager.amazonaws.com/AWSServiceRoleForAuditManager*"
        },
        {
            "Sid": "S3Access",
            "Effect": "Allow",
            "Action": [
                "s3:ListAllMyBuckets"
            ],
            "Resource": "*"
        },
        {
            "Sid": "KmsAccess",
            "Effect": "Allow",
            "Action": [
                "kms:DescribeKey",
                "kms:ListKeys",
                "kms:ListAliases"
            ],
            "Resource": "*"
        },
        {
            "Sid": "KmsCreateGrantAccess",
            "Effect": "Allow",
            "Action": [
                "kms:CreateGrant"
            ],
            "Resource": "*",
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": "true"
                },
                "StringLike": {
                    "kms:ViaService": "auditmanager.*.amazonaws.com"
                }
            }
        },
        {
            "Sid": "SNSAccess",
            "Effect": "Allow",
            "Action": [
                "sns:ListTopics"
            ],
            "Resource": "*"
```

```
        },
        {
            "Sid": "CreateEventsAccess",
            "Effect": "Allow",
            "Action": [
                "events:PutRule"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "events:detail-type": "Security Hub Findings - Imported"
                },
                "ForAllValues:StringEquals": {
                    "events:source": [
                        "aws.securityhub"
                    ]
                }
            }
        },
        {
            "Sid": "EventsAccess",
            "Effect": "Allow",
            "Action": [
                "events:DeleteRule",
                "events:DescribeRule",
                "events:EnableRule",
                "events:DisableRule",
                "events:ListTargetsByRule",
                "events:PutTargets",
                "events:RemoveTargets"
            ],
            "Resource": "arn:aws:events:*:*:rule/
AuditManagerSecurityHubFindingsReceiver"
        },
        {
            "Sid": "TagAccess",
            "Effect": "Allow",
            "Action": [
                "tag:GetResources"
            ],
            "Resource": "*"
        }
    ]
```

```
}
```

Exemplo 2 (permissões de destino do relatório de avaliação)

Essa política concede permissão para acessar um bucket específico do S3, para adicionar e excluir arquivos dele. Isso permite que você use o bucket especificado como destino do relatório de avaliação no Audit Manager.

Substitua o *espaço reservado de texto* por suas próprias informações. Inclua o bucket do S3 que você usa como destino do relatório de avaliação e a chave KMS que você usa para criptografar seus relatórios de avaliação.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
               "s3:PutObject",
               "s3:GetObject",
               "s3:ListBucket",
               "s3:DeleteObject",
               "s3:GetBucketLocation",
               "s3:PutObjectAcl"
            ],
            "Resource": "arn:aws:s3:::DOC-EXAMPLE-DESTINATION-BUCKET/*"
        }
    ]
},
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt",
                "kms:Encrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ]
```

```
}
```

Exemplo 3 (permissões de destino de exportação)

A política a seguir permite CloudTrail fornecer os resultados da consulta do localizador de evidências para o bucket S3 especificado. Como prática recomendada de segurança, a chave de condição global do IAM `aws:SourceArn` ajuda a garantir que as CloudTrail gravações no bucket do S3 sejam gravadas somente para o armazenamento de dados do evento.

Substitua o *`texto do espaço reservado`* por suas próprias informações, da seguinte forma:

- Substitua *`DOC-EXAMPLE-DESTINATION-BUCKET`* pelo bucket do S3 que você usa como destino de exportação.
- Substitua a *`myQueryRunningregião`* Região da AWS pela apropriada para sua configuração.
- Substitua *`myAccountID`* pela Conta da AWS ID usada para. CloudTrail Talvez não seja a mesma ID Conta da AWS do bucket do S3. Se for um armazenamento de dados de eventos da organização, você deverá usar o Conta da AWS para a conta de gerenciamento.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action": [
                "s3:PutObject*",
                "s3:Abort*"
            ],
            "Resource": [
                "arn:aws:s3:::DOC-EXAMPLE-DESTINATION-BUCKET",
                "arn:aws:s3:::DOC-EXAMPLE-DESTINATION-BUCKET/*"
            ],
            "Condition": {
                "StringEquals": {
                    "AWS:SourceArn":
 "arn:aws:cloudtrail:myQueryRunningRegion:myAccountID:eventdatastore/*"
                }
            }
        },
```

```
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::DOC-EXAMPLE-DESTINATION-BUCKET",
            "Condition": {
                "StringEquals": {
                    "AWS:SourceArn":
 "arn:aws:cloudtrail:myQueryRunningRegion:myAccountID:eventdatastore/*"
                }
            }
        },
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action": [
                "kms:Decrypt*",
                "kms:GenerateDataKey*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "s3.amazonaws.com"
            },
            "Action": [
                "kms:Decrypt*",
                "kms:GenerateDataKey*"
            ],
            "Resource": "*"
        }
    ]
}
```

Exemplo 4 (permissões para ativar o localizador de evidências)

A política de permissão a seguir é necessária se você quiser ativar e usar o atributo de busca de evidências. Essa declaração de política permite que o Audit Manager crie um armazenamento de dados de eventos do CloudTrail Lake e execute consultas de pesquisa.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
           "Sid": "ManageCloudTrailLakeQueryAccess",
           "Effect": "Allow",
           "Action": [
               "cloudtrail:StartQuery",
               "cloudtrail:DescribeQuery",
               "cloudtrail:GetQueryResults",
               "cloudtrail:CancelQuery"
           ],
           "Resource": "arn:aws:cloudtrail:*:*:eventdatastore/*"
        },
        {
           "Sid": "ManageCloudTrailLakeAccess",
           "Effect": "Allow",
           "Action": [
                "cloudtrail:CreateEventDataStore"
           ],
           "Resource": "arn:aws:cloudtrail:*:*:eventdatastore/*"
         }
    ]
}
```

Exemplo 5 (permissões para desativar o localizador de evidências)

Este exemplo de política concede permissão para desativar o atributo de localização de evidências no Audit Manager. Isso envolve a exclusão do armazenamento de dados de eventos criado quando você ativou o atributo pela primeira vez.

Antes de usar esta política, substitua o *texto do espaço reservado* por suas próprias informações. Você deve especificar o UUID do armazenamento de dados do evento criado quando você ativou o localizador de evidências. Você pode recuperar o ARN do armazenamento de dados de eventos nas configurações do Audit Manager. Para obter mais informações, consulte GetSettings na Referência da API doAWS Audit Manager .

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
               "cloudtrail:DeleteEventDataStore",
               "cloudtrail:UpdateEventDataStore"
            ],
            "Resource": "arn:aws:cloudtrail:::event-data-store-UUID"
        }
    ]
}
```

Permita que o gerenciamento de usuários acesse AWS Audit Manager

Este exemplo mostra como você pode permitir o acesso de gerenciamento não administrativo ao AWS Audit Manager.

Essa política concede a capacidade de gerenciar todos os recursos do Audit Manager (avaliações, estruturas e controles), mas não permite ativar ou desativar o Audit Manager nem modificar suas configurações.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AuditManagerAccess",
            "Effect": "Allow",
            "Action": [
                "auditmanager:GetAccountStatus",
                "auditmanager:ListAssessmentFrameworks",
                "auditmanager:CreateAssessmentFramework",
                "auditmanager:GetAssessmentFramework",
                "auditmanager:UpdateAssessmentFramework",
                "auditmanager:DeleteAssessmentFramework",
                "auditmanager:ListAssessmentReports",
                "auditmanager:ListAssessments",
                "auditmanager:CreateAssessment",
                "auditmanager:ListControls",
                "auditmanager:CreateControl",
                "auditmanager:GetControl",
```

```
                "auditmanager:UpdateControl",
                "auditmanager:DeleteControl",
                "auditmanager:ListKeywordsForDataSource",
                "auditmanager:GetDelegations",
                "auditmanager:ValidateAssessmentReportIntegrity",
                "auditmanager:ListNotifications",
                "auditmanager:GetServicesInScope",
                "auditmanager:GetSettings",
                "auditmanager:ListTagsForResource",
                "auditmanager:TagResource",
                "auditmanager:UntagResource"
            ],
            "Resource": "*"
        },
        {
            "Sid": "OrganizationsAccess",
            "Effect": "Allow",
            "Action": [
                "organizations:ListAccountsForParent",
                "organizations:ListAccounts",
                "organizations:DescribeOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribeAccount",
                "organizations:ListParents",
                "organizations:ListChildren"
            ],
            "Resource": "*"
        },
        {
            "Sid": "IAMAccess",
            "Effect": "Allow",
            "Action": [
                "iam:GetUser",
                "iam:ListUsers",
                "iam:ListRoles"
            ],
            "Resource": "*"
        },
        {
            "Sid": "S3Access",
            "Effect": "Allow",
            "Action": [
                "s3:ListAllMyBuckets"
            ],
```

```
            "Resource": "*"
        },
        {
            "Sid": "KmsAccess",
            "Effect": "Allow",
            "Action": [
                "kms:DescribeKey",
                "kms:ListKeys",
                "kms:ListAliases"
            ],
            "Resource": "*"
        },
        {
            "Sid": "SNSAccess",
            "Effect": "Allow",
            "Action": [
                "sns:ListTopics"
            ],
            "Resource": "*"
        },
        {
            "Sid": "TagAccess",
            "Effect": "Allow",
            "Action": [
                "tag:GetResources"
            ],
            "Resource": "*"
        }
    ]
}
```

Permita que os usuários tenham acesso somente para leitura ao AWS Audit Manager

Essa política concede acesso somente para leitura a AWS Audit Manager recursos, como avaliações, estruturas e controles.

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

```
                "auditmanager:Get*",
                "auditmanager:List*"
            ],
            "Resource": "*"
        }
    ]
}
```

Permitir que os usuários visualizem suas próprias permissões

Este exemplo mostra como você pode criar uma política que permite 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": "*"
        }
    ]
}
```

AWS Audit Manager Permitir o envio de notificações para tópicos do Amazon SNS

As políticas deste exemplo concedem ao Audit Manager permissões para enviar notificações para um tópico existente do Amazon SNS.

- Exemplo 1 — Se você quiser receber notificações do Audit Manager, use este exemplo para adicionar permissões a sua política de acesso a tópicos do SNS.
- Exemplo 2 — Se o tópico do SNS usa AWS Key Management Service (AWS KMS) para criptografia do lado do servidor (SSE), use esse exemplo para adicionar permissões à política de acesso à chave KMS.

No exemplo de política de chaves a seguir, a entidade principal que obtém as permissões é a entidade principal do serviço, `auditmanager.amazonaws.com`. Quando a entidade principal em uma declaração de política chave é uma AWS entidade principal de serviço, recomendamos usar `aws:SourceArn` ou as chaves de condição globais `aws:SourceAccount` na política. Você pode usar essas chaves de contexto de condição global para ajudar a evitar o cenário de "confused deputy".

Exemplo 1 (permissões para o tópico SNS)

Essa política permite que o Audit Manager publique eventos em um tópico SNS específico. Qualquer solicitação de publicação no tópico do SNS especificado deve atender às condições da política.

Antes de usar esta política, substitua o *`texto do espaço reservado`* por suas próprias informações. Observe o seguinte:

- Se você usar a chave de condição `aws:SourceArn` nessa política, o valor deverá ser o ARN do recurso do Audit Manager de onde vem a notificação. No exemplo abaixo, `aws:SourceArn` usa um caractere curinga (`*`) para a ID do recurso. Isso permite que todas as solicitações provenientes do Audit Manager estejam em todos os recursos do Audit Manager. Com a chave de condição global `aws:SourceArn`, você pode usar o operador de condição `StringLike` ou a condição `ArnLike`. Como prática recomendada, sugerimos que você use `ArnLike`.

- Se você usar a chave de condição `aws:SourceAccount`, poderá usar o operador de condição `StringEquals` ou `StringLike`. Como prática recomendada, sugerimos que você use `StringEquals` para implementar o privilégio mínimo.
- Se usar `aws:SourceAccount` e `aws:SourceArn`, os valores da conta deverão mostrar a mesma ID da conta.

```
{
  "Version": "2012-10-17",
  "Statement": {
      "Sid": "AllowAuditManagerToUseSNSTopic",
      "Effect": "Allow",
      "Principal": {
        "Service": "auditmanager.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:region:accountID:topicName",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "accountID"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:auditmanager:region:accountID:*"
        }
      }
    }
}
```

O exemplo alternativo a seguir usa apenas a chave de condição `aws:SourceArn`, com o operador de condição `StringLike`:

```
      "Condition": {
        "StringLike": {
          "aws:SourceArn": "arn:aws:auditmanager:region:accountID:*"
        }
      }
```

O exemplo alternativo a seguir usa apenas a chave de condição `aws:SourceAccount`, com o operador de condição `StringLike`:

```
    "Condition": {
```

```
      "StringLike": {
        "aws:SourceAccount": "accountID"
       }
     }
```

Exemplo 2 (permissões para a chave KMS anexada ao tópico do SNS)

A declaração de política permite que o CloudTrail use a chave do KMS para gerar a chave de dados usada para criptografar uma trilha. Qualquer solicitação para usar a chave do KMS para a operação especificada deve atender às duas condições.

Antes de usar esta política, substitua o *texto do espaço reservado* por suas próprias informações. Observe o seguinte:

- Se você usar a chave de condição `aws:SourceArn` nessa política, o valor deverá ser o ARN do recurso sendo criptografado. Por exemplo, nesse caso, o tópico do SNS na sua conta. Defina o valor como o ARN ou um padrão de ARN com caracteres curinga (*). Você pode usar o operador de condição `StringLike` ou o operador de condição `ArnLike` com a chave de condição`aws:SourceArn`. Como prática recomendada, sugerimos que você use `ArnLike`.
- Se você usar a chave de condição `aws:SourceAccount`, poderá usar o operador de condição `StringEquals` ou `StringLike`. Como prática recomendada, sugerimos que você use `StringEquals` para implementar o privilégio mínimo. Você pode usar o `aws:SourceAccount` se não souber o ARN do tópico do SNS.
- Se usar `aws:SourceAccount` e `aws:SourceArn`, os valores da conta deverão mostrar a mesma ID da conta.

```
{
     "Version": "2012-10-17",
     "Statement": {
       "Sid": "AllowAuditManagerToUseKMSKey",
       "Effect": "Allow",
       "Principal": {
           "Service": "auditmanager.amazonaws.com"
       },
       "Action": [
           "kms:Decrypt",
           "kms:GenerateDataKey"
       ],
       "Resource": "arn:aws:kms:region:accountID:key/*",
```

```
        "Condition": {
            "StringEquals": {
                "aws:SourceAccount": "accountID"
             }
             "ArnLike": {
                  "aws:SourceArn": "arn:aws:sns:region:accountID:topicName"
             }
       }
     }
  ]
}
```

O exemplo alternativo a seguir usa apenas a chave de condição `aws:SourceArn`, com o operador de condição `StringLike`:

```
      "Condition": {
        "StringLike": {
          "aws:SourceArn": "arn:aws:sns:region:accountID:topicName"
        }
      }
```

O exemplo alternativo a seguir usa apenas a chave de condição `aws:SourceAccount`, com o operador de condição `StringLike`:

```
   "Condition": {
     "StringLike": {
       "aws:SourceAccount": "accountID"
      }
    }
```

Permitir que os usuários executem consultas de pesquisa no localizador de evidências

A política a seguir concede permissões para realizar consultas em um armazenamento de dados de eventos do CloudTrail Lake. Essa política de permissão é obrigatória se quiser usar o atributo de busca de evidências.

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

```
            "Effect": "Allow",
            "Action": [
                "cloudtrail:StartQuery",
                "cloudtrail:DescribeQuery",
                "cloudtrail:GetQueryResults",
                "cloudtrail:CancelQuery"
            ],
            "Resource": "*"
        }
    ]
}
```

Prevenção contra o ataque “confused deputy” em todos os serviços

‘Confused deputy’ é um problema de segurança em que uma entidade que não tem permissão para executar uma ação pode coagir uma entidade com mais privilégios a executá-la. Em AWS, a falsificação de identidade entre serviços pode resultar no problema confuso do deputado. A imitação entre serviços pode ocorrer quando um serviço (o serviço de chamada) chama outro serviço (o serviço chamado). O serviço de chamada pode ser manipulado de modo a usar suas permissões para atuar nos recursos de outro cliente, de uma forma que não deveria ter permissão para acessar. Para evitar isso, o Amazon Web Services fornece ferramentas que ajudam a proteger seus dados para todos os serviços, com entidades principais de serviço que receberem acesso aos recursos em sua conta.

Recomendamos usar `aws:SourceArn`as chaves de contexto de condição `aws:SourceAccount`global nas políticas de recursos para limitar as permissões AWS Audit Manager concedidas a outro serviço para acessar seus recursos.

- Use `aws:SourceArn` se quiser que apenas um recurso seja associado ao acesso entre serviços. Você também pode usar `aws:SourceArn` com um curinga (`*`) se quiser especificar vários recursos.

  Por exemplo, você pode usar um tópico do Amazon SNS para receber notificações de atividade do Audit Manager. Nesse caso, em sua política de acesso a tópicos do SNS, o valor do ARN de `aws:SourceArn` é o recurso do Audit Manager de onde vem a notificação. Como é provável que você tenha vários recursos do Audit Manager, recomendamos que você use `aws:SourceArn` com um caractere curinga. Isso permite que você especifique todos os recursos do Audit Manager em sua política de acesso a tópicos do SNS.

- Use `aws:SourceAccount` se quiser permitir que qualquer recurso nessa conta seja associado ao uso entre serviços.
- Se o valor `aws:SourceArn` não contiver a ID da conta, como um ARN de bucket do Amazon S3, você deve usar ambas as chaves de contexto de condição global para limitar as permissões.
- Se utilizar ambas as condições e o valor `aws:SourceArn` contiver a ID da conta, o valor `aws:SourceAccount` e a conta no valor `aws:SourceArn` deverão utilizar a mesma ID de conta quando na mesma instrução de política.
- A maneira mais eficaz de proteger-se contra o problema “confused deputy” é usar a chave de contexto de condição global `aws:SourceArn` com o ARN completo do recurso. Se você não souber o nome completo do recurso da Amazon Resource Name (ARN) ou estiver especificando vários recursos, use a chave de condição de contexto global `aws:SourceArn` com caracteres curingas (*) para as partes desconhecidas do ARN. Por exemplo, `arn:aws:`*`servicename`*`:*:`*`123456789012`*`:*`.

Suporte Audit Manager a “confused deputy”

O Audit Manager fornece suporte a “confused deputy” nos seguintes cenários: O exemplo a seguir mostra como é possível usar as chaves de condição `aws:SourceArn` e `aws:SourceAccount` para evitar o problema “confused deputy.”

- Exemplo de política: o tópico do SNS que você usa para receber notificações do Audit Manager
- Exemplo de política: a chave KMS que você usa para criptografar seu tópico do SNS

O Audit Manager não fornece suporte a “confused deputy” para a chave gerenciada pelo cliente fornecida por você nas configurações Criptografia de dados do Audit Manager. Se você forneceu sua própria chave gerenciada pelo cliente, não poderá usar as condições `aws:SourceAccount` ou `aws:SourceArn` dessa política de chaves do KMS.

AWS políticas gerenciadas para AWS Audit 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 elas estão disponíveis para uso de todos os

AWS clientes. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo cliente 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) for lançada ou novas operações de API forem disponibilizadas para serviços existentes.

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

Tópicos

- AWS política gerenciada: AWSAuditManagerAdministratorAccess
- AWS política gerenciada: AWSAuditManagerServiceRolePolicy
- AWS Audit Manager atualizações nas políticas AWS gerenciadas

AWS política gerenciada: AWSAuditManagerAdministratorAccess

É possível anexar a política `AWSAuditManagerAdministratorAccess` a suas identidades do IAM.

Essa política concede permissões administrativas que permitem acesso total da administração AWS Audit Managera. Esse acesso inclui a capacidade de ativar e desativar AWS Audit Manager, alterar configurações e gerenciar todos os recursos do Audit Manager, como avaliações, estruturas, controles e relatórios de avaliação. AWS Audit Manager

AWS Audit Manager requer amplas permissões em vários AWS serviços. Isso ocorre porque AWS Audit Manager se integra a vários AWS serviços para coletar evidências automaticamente dos serviços Conta da AWS e serviços no escopo de uma avaliação.

Detalhes de permissão

Esta política inclui as seguintes permissões:

- `Audit Manager` — Concede às entidades principais permissões completas sobre os recursos AWS Audit Manager .
- `Organizations` — Concede às entidades principais permissão para listarem contas e unidades organizacionais, para registrar ou cancelar o registro de um administrador delegado. Isso é necessário para que você possa ativar o suporte a várias contas e permitir AWS Audit Manager a

execução de avaliações em várias contas e consolidar evidências em uma conta de administrador delegado.

- `iam` — Permite que entidades principais obtenham e listem usuários no IAM criando uma função vinculada ao serviço. Isso é necessário para designar proprietários e delegados de auditoria para uma avaliação. Essa política também permite que entidades principais excluam a função vinculada ao serviço e recuperem o status da exclusão. Isso é necessário para que você AWS Audit Manager possa limpar recursos e excluir a função vinculada ao serviço quando você optar por desativar o serviço no. AWS Management Console
- `s3` — Permite que as entidades principais listem buckets do Amazon Simple Storage Service (Amazon S3) disponíveis. Esse recurso é necessário para que você possa designar o bucket S3 no qual deseja armazenar relatórios de evidências ou carregar evidências manuais.
- `kms` — Permite que entidades principais listem e descrevam chaves, listem apelidos e criem doações. Isso é necessário para que você possa escolher chaves gerenciadas pelo cliente para criptografia de dados.
- `sns` — Permite que entidades principais listem tópicos de assinatura no Amazon SNS. Isso é necessário para especificar para qual tópico do SNS você quer que AWS Audit Manager envie notificações.
- `events`— Permite que os diretores listem e gerenciem cheques de AWS Security Hub. Isso é necessário para que AWS Audit Manager possa coletar automaticamente AWS Security Hub as descobertas dos AWS serviços que são monitorados pelo AWS Security Hub. Em seguida, ele pode converter esses dados em evidências para incluí-las em suas avaliações AWS Audit Manager .
- `tag` — Permite que entidades principais recuperem recursos taggeados. Isso é necessário para que você possa usar tags como filtro de pesquisa ao navegar por estruturas, controles e avaliações em AWS Audit Manager.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AuditManagerAccess",
            "Effect": "Allow",
            "Action": [
                "auditmanager:*"
            ],
            "Resource": "*"
```

```
        },
        {
            "Sid": "OrganizationsAccess",
            "Effect": "Allow",
            "Action": [
                "organizations:ListAccountsForParent",
                "organizations:ListAccounts",
                "organizations:DescribeOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribeAccount",
                "organizations:ListParents",
                "organizations:ListChildren"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowOnlyAuditManagerIntegration",
            "Effect": "Allow",
            "Action": [
                "organizations:RegisterDelegatedAdministrator",
                "organizations:DeregisterDelegatedAdministrator",
                "organizations:EnableAWSServiceAccess"
            ],
            "Resource": "*",
            "Condition": {
                "StringLikeIfExists": {
                    "organizations:ServicePrincipal": [
                        "auditmanager.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Sid": "IAMAccess",
            "Effect": "Allow",
            "Action": [
                "iam:GetUser",
                "iam:ListUsers",
                "iam:ListRoles"
            ],
            "Resource": "*"
        },
        {
            "Sid": "IAMAccessCreateSLR",
```

```
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/
auditmanager.amazonaws.com/AWSServiceRoleForAuditManager*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "auditmanager.amazonaws.com"
                }
            }
        },
        {
            "Sid": "IAMAccessManageSLR",
            "Effect": "Allow",
            "Action": [
                "iam:DeleteServiceLinkedRole",
                "iam:UpdateRoleDescription",
                "iam:GetServiceLinkedRoleDeletionStatus"
            ],
            "Resource": "arn:aws:iam::*:role/aws-service-role/
auditmanager.amazonaws.com/AWSServiceRoleForAuditManager*"
        },
        {
            "Sid": "S3Access",
            "Effect": "Allow",
            "Action": [
                "s3:ListAllMyBuckets"
            ],
            "Resource": "*"
        },
        {
            "Sid": "KmsAccess",
            "Effect": "Allow",
            "Action": [
                "kms:DescribeKey",
                "kms:ListKeys",
                "kms:ListAliases"
            ],
            "Resource": "*"
        },
        {
            "Sid": "KmsCreateGrantAccess",
            "Effect": "Allow",
            "Action": [
                "kms:CreateGrant"
```

```
            ],
            "Resource": "*",
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": "true"
                },
                "StringLike": {
                    "kms:ViaService": "auditmanager.*.amazonaws.com"
                }
            }
        },
        {
            "Sid": "SNSAccess",
            "Effect": "Allow",
            "Action": [
                "sns:ListTopics"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CreateEventsAccess",
            "Effect": "Allow",
            "Action": [
                "events:PutRule"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "events:detail-type": "Security Hub Findings - Imported"
                },
                "ForAllValues:StringEquals": {
                    "events:source": [
                        "aws.securityhub"
                    ]
                }
            }
        },
        {
            "Sid": "EventsAccess",
            "Effect": "Allow",
            "Action": [
                "events:DeleteRule",
                "events:DescribeRule",
                "events:EnableRule",
```

```
                "events:DisableRule",
                "events:ListTargetsByRule",
                "events:PutTargets",
                "events:RemoveTargets"
            ],
            "Resource": "arn:aws:events:*:*:rule/
AuditManagerSecurityHubFindingsReceiver"
        },
        {
            "Sid": "TagAccess",
            "Effect": "Allow",
            "Action": [
                "tag:GetResources"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS política gerenciada: AWSAuditManagerServiceRolePolicy

Não é possível anexar `AWSAuditManagerServiceRolePolicy` às entidades do IAM. Essa política está vinculada a uma função vinculada ao serviço,`AWSServiceRoleForAuditManager`, que permite AWS Audit Manager realizar ações em seu nome. Para obter mais informações, consulte Usando funções vinculadas a serviço para AWS Audit Manager.

A política de permissões de função `AWSAuditManagerServiceRolePolicy` permite que AWS Audit Manager colete evidências automatizadas fazendo o seguinte em seu nome:

- Colete dados das seguintes fontes de dados:
  - Eventos de gerenciamento de AWS CloudTrail
  - Verificações de conformidade de Regras do AWS Config
  - Verificações de conformidade de AWS Security Hub
- Use chamadas de API para descrever suas configurações de recursos para o Serviços da AWSseguinte.

> **Tip**
>
> Para obter mais informações sobre as chamadas de API que o Audit Manager usa para coletar evidências desses serviços, consulte Chamadas de API compatíveis com fontes de dados de controle personalizadas neste guia.

- AWS Certificate Manager
- AWS Backup
- Amazon Bedrock
- AWS CloudTrail
- Amazon CloudWatch
- CloudWatch Registros da Amazon
- Grupos de usuários do Amazon Cognito
- AWS Config
- AWS Direct Connect
- Amazon DynamoDB
- Amazon EC2
- Amazon Elastic Container Service
- Amazon Elastic File System
- Amazon Elastic Kubernetes Service
- Amazon ElastiCache
- Elastic Load Balancing
- Amazon EMR
- Amazon EventBridge
- Amazon Data Firehose
- Amazon FSx
- Amazon GuardDuty
- AWS Identity and Access Management (IAM)
- Amazon Kinesis
- AWS KMS

- AWS Lambda
- AWS License Manager
- Amazon Managed Streaming for Apache Kafka
- AWS Organizations
- Amazon Relational Database Service
- Amazon Redshift
- Amazon Route 53
- Amazon S3
- AWS Security Hub
- Amazon Simple Notification Service
- Amazon Simple Queue Service
- AWS WAF

Detalhes da permissão

`AWSAuditManagerServiceRolePolicy`permite AWS Audit Manager concluir as seguintes ações nos recursos especificados:

- `acm:GetAccountConfiguration`
- `acm:ListCertificates`
- `backup:ListRecoveryPointsByResource`
- `bedrock:GetCustomModel`
- `bedrock:GetFoundationModel`
- `bedrock:GetModelCustomizationJob`
- `bedrock:GetModelInvocationLoggingConfiguration`
- `bedrock:ListCustomModels`
- `bedrock:ListFoundationModels`
- `bedrock:ListModelCustomizationJobs`
- `cloudtrail:DescribeTrails`
- `cloudtrail:LookupEvents`
- `cloudwatch:DescribeAlarms`
- `cloudwatch:DescribeAlarmsForMetric`

- cloudwatch:GetMetricStatistics
- cloudwatch:ListMetrics
- cognito-idp:DescribeUserPool
- config:DescribeConfigRules
- config:DescribeDeliveryChannels
- config:ListDiscoveredResources
- directconnect:DescribeDirectConnectGateways
- directconnect:DescribeVirtualGateways
- dynamodb:DescribeTable
- dynamodb:ListBackups
- dynamodb:ListGlobalTables
- dynamodb:ListTables
- ec2:DescribeAddresses
- ec2:DescribeCustomerGateways
- ec2:DescribeEgressOnlyInternetGateways
- ec2:DescribeFlowLogs
- ec2:DescribeInstances
- ec2:DescribeInternetGateways
- ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations
- ec2:DescribeLocalGateways
- ec2:DescribeLocalGatewayVirtualInterfaces
- ec2:DescribeNatGateways
- ec2:DescribeNetworkAcls
- ec2:DescribeRouteTables
- ec2:DescribeSecurityGroups
- ec2:DescribeSnapshots
- ec2:DescribeTransitGateways
- ec2:DescribeVolumes
- ec2:DescribeVpcEndpoints
- ec2:DescribeVpcPeeringConnections

- ec2:DescribeVpcs
- ec2:DescribeVpnConnections
- ec2:DescribeVpnGateways
- ec2:GetEbsDefaultKmsKeyId
- ec2:GetEbsEncryptionByDefault
- ecs:DescribeClusters
- eks:DescribeAddonVersions
- elasticache:DescribeCacheClusters
- elasticache:DescribeServiceUpdates
- elasticfilesystem:DescribeAccessPoints
- elasticfilesystem:DescribeFileSystems
- elasticloadbalancing:DescribeLoadBalancers
- elasticloadbalancing:DescribeSslPolicies
- elasticloadbalancing:DescribeTargetGroups
- elasticmapreduce:ListClusters
- elasticmapreduce:ListSecurityConfigurations
- events:DeleteRule
- events:DescribeRule
- events:DisableRule
- events:EnableRule
- events:ListConnections
- events:ListEventBuses
- events:ListEventSources
- events:ListRules
- events:ListTargetsByRule
- events:PutRule
- events:PutTargets
- events:RemoveTargets
- firehose:ListDeliveryStreams

- fsx:DescribeFileSystems
- guardduty:ListDetectors
- iam:GenerateCredentialReport
- iam:GetAccountAuthorizationDetails
- iam:GetAccountPasswordPolicy
- iam:GetAccountSummary
- iam:GetCredentialReport
- iam:ListEntitiesForPolicy
- iam:ListGroupPolicies
- iam:ListGroups
- iam:ListOpenIdConnectProviders
- iam:ListPolicies
- iam:ListRolePolicies
- iam:ListRoles
- iam:ListSamlProviders
- iam:ListUserPolicies
- iam:ListUsers
- iam:ListVirtualMFADevices
- kafka:ListClusters
- kafka:ListKafkaVersions
- kinesis:ListStreams
- kms:DescribeKey
- kms:GetKeyPolicy
- kms:GetKeyRotationStatus
- kms:ListGrants
- kms:ListKeyPolicies
- kms:ListKeys
- lambda:ListFunctions
- license-manager:ListAssociationsForLicenseConfiguration
- license-manager:ListLicenseConfigurations

- `license-manager:ListUsageForLicenseConfiguration`
- `logs:DescribeDestinations`
- `logs:DescribeExportTasks`
- `logs:DescribeLogGroups`
- `logs:DescribeMetricFilters`
- `logs:DescribeResourcePolicies`
- `logs:FilterLogEvents`
- `organizations:DescribeOrganization`
- `organizations:DescribePolicy`
- `rds:DescribeCertificates`
- `rds:DescribeDbClusterEndpoints`
- `rds:DescribeDbClusterParameterGroups`
- `rds:DescribeDbClusters`
- `rds:DescribeDBInstances`
- `rds:DescribeDbSecurityGroups`
- `redshift:DescribeClusters`
- `route53:GetQueryLoggingConfig`
- `s3:GetBucketPolicy`
  - Essa ação de API opera dentro do escopo de Conta da AWS onde service-linked-role está disponível. Ela não pode acessar políticas de bucket entre contas.
- `s3:GetBucketPublicAccessBlock`
- `s3:GetBucketVersioning`
- `s3:GetEncryptionConfiguration`
- `s3:GetLifecycleConfiguration`
- `s3:ListAllMyBuckets`
- `securityhub:DescribeStandards`
- `sns:ListTopics`
- `sqs:ListQueues`
- `waf-regional:GetLoggingConfiguration`
- `waf-regional:ListRuleGroups`

- waf-regional:ListSubscribedRuleGroups
- waf-regional:ListWebACLs
- waf:ListActivatedRulesInRuleGroup

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "acm:GetAccountConfiguration",
    "acm:ListCertificates",
    "backup:ListRecoveryPointsByResource",
    "bedrock:GetCustomModel",
    "bedrock:GetFoundationModel",
    "bedrock:GetModelCustomizationJob",
    "bedrock:GetModelInvocationLoggingConfiguration",
    "bedrock:ListCustomModels",
    "bedrock:ListFoundationModels",
    "bedrock:ListModelCustomizationJobs",
    "cloudtrail:DescribeTrails",
    "cloudtrail:LookupEvents",
    "cloudwatch:DescribeAlarms",
    "cloudwatch:DescribeAlarmsForMetric",
    "cloudwatch:GetMetricStatistics",
    "cloudwatch:ListMetrics",
    "cognito-idp:DescribeUserPool",
    "config:DescribeConfigRules",
    "config:DescribeDeliveryChannels",
    "config:ListDiscoveredResources",
    "directconnect:DescribeDirectConnectGateways",
    "directconnect:DescribeVirtualGateways",
    "dynamodb:DescribeTable",
    "dynamodb:ListBackups",
    "dynamodb:ListGlobalTables",
    "dynamodb:ListTables",
    "ec2:DescribeAddresses",
    "ec2:DescribeCustomerGateways",
    "ec2:DescribeEgressOnlyInternetGateways",
    "ec2:DescribeFlowLogs",
    "ec2:DescribeInstances",
    "ec2:DescribeInternetGateways",
```

```
    "ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations",
    "ec2:DescribeLocalGateways",
    "ec2:DescribeLocalGatewayVirtualInterfaces",
    "ec2:DescribeNatGateways",
    "ec2:DescribeNetworkAcls",
    "ec2:DescribeRouteTables",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSnapshots",
    "ec2:DescribeTransitGateways",
    "ec2:DescribeVolumes",
    "ec2:DescribeVpcEndpoints",
    "ec2:DescribeVpcPeeringConnections",
    "ec2:DescribeVpcs",
    "ec2:DescribeVpnConnections",
    "ec2:DescribeVpnGateways",
    "ec2:GetEbsDefaultKmsKeyId",
    "ec2:GetEbsEncryptionByDefault",
    "ecs:DescribeClusters",
    "eks:DescribeAddonVersions",
    "elasticache:DescribeCacheClusters",
    "elasticache:DescribeServiceUpdates",
    "elasticfilesystem:DescribeAccessPoints",
    "elasticfilesystem:DescribeFileSystems",
    "elasticloadbalancing:DescribeLoadBalancers",
    "elasticloadbalancing:DescribeSslPolicies",
    "elasticloadbalancing:DescribeTargetGroups",
    "elasticmapreduce:ListClusters",
    "elasticmapreduce:ListSecurityConfigurations",
    "events:DescribeRule",
    "events:ListConnections",
    "events:ListEventBuses",
    "events:ListEventSources",
    "events:ListRules",
    "firehose:ListDeliveryStreams",
    "fsx:DescribeFileSystems",
    "guardduty:ListDetectors",
    "iam:GenerateCredentialReport",
    "iam:GetAccountAuthorizationDetails",
    "iam:GetAccountPasswordPolicy",
    "iam:GetAccountSummary",
    "iam:GetCredentialReport",
    "iam:ListEntitiesForPolicy",
    "iam:ListGroupPolicies",
    "iam:ListGroups",
```

```
    "iam:ListOpenIdConnectProviders",
    "iam:ListPolicies",
    "iam:ListRolePolicies",
    "iam:ListRoles",
    "iam:ListSamlProviders",
    "iam:ListUserPolicies",
    "iam:ListUsers",
    "iam:ListVirtualMFADevices",
    "kafka:ListClusters",
    "kafka:ListKafkaVersions",
    "kinesis:ListStreams",
    "kms:DescribeKey",
    "kms:GetKeyPolicy",
    "kms:GetKeyRotationStatus",
    "kms:ListGrants",
    "kms:ListKeyPolicies",
    "kms:ListKeys",
    "lambda:ListFunctions",
    "license-manager:ListAssociationsForLicenseConfiguration",
    "license-manager:ListLicenseConfigurations",
    "license-manager:ListUsageForLicenseConfiguration",
    "logs:DescribeDestinations",
    "logs:DescribeExportTasks",
    "logs:DescribeLogGroups",
    "logs:DescribeMetricFilters",
    "logs:DescribeResourcePolicies",
    "logs:FilterLogEvents",
    "organizations:DescribeOrganization",
    "organizations:DescribePolicy",
    "rds:DescribeCertificates",
    "rds:DescribeDbClusterEndpoints",
    "rds:DescribeDbClusterParameterGroups",
    "rds:DescribeDbClusters",
    "rds:DescribeDBInstances",
    "rds:DescribeDbSecurityGroups",
    "redshift:DescribeClusters",
    "route53:GetQueryLoggingConfig",
    "s3:GetBucketPublicAccessBlock",
    "s3:GetBucketVersioning",
    "s3:GetEncryptionConfiguration",
    "s3:GetLifecycleConfiguration",
    "s3:ListAllMyBuckets",
    "securityhub:DescribeStandards",
    "sns:ListTopics",
```

```
    "sqs:ListQueues",
    "waf-regional:GetLoggingConfiguration",
    "waf-regional:ListRuleGroups",
    "waf-regional:ListSubscribedRuleGroups",
    "waf-regional:ListWebACLs",
    "waf:ListActivatedRulesInRuleGroup"
   ],
   "Resource": "*",
   "Sid": "AuditManagerAPICallAccess"
  },
  {
   "Sid": "AuditManagerS3GetBucketPolicyAccess",
   "Effect": "Allow",
   "Action": [
    "s3:GetBucketPolicy"
   ],
   "Resource": "*",
   "Condition": {
    "StringEquals": {
     "aws:ResourceAccount": [
      "${aws:PrincipalAccount}"
     ]
    }
   }
  },
  {
   "Sid": "CreateEventsAccess",
   "Effect": "Allow",
   "Action": [
    "events:PutRule"
   ],
   "Resource": "arn:aws:events:*:*:rule/AuditManagerSecurityHubFindingsReceiver",
   "Condition": {
    "StringEquals": {
     "events:detail-type": "Security Hub Findings - Imported"
    },
    "Null": {
     "events:source": "false"
    },
    "ForAllValues:StringEquals": {
     "events:source": [
      "aws.securityhub"
     ]
    }
```

```
    }
   },
   {
    "Sid": "EventsAccess",
    "Effect": "Allow",
    "Action": [
     "events:DeleteRule",
     "events:DescribeRule",
     "events:EnableRule",
     "events:DisableRule",
     "events:ListTargetsByRule",
     "events:PutTargets",
     "events:RemoveTargets"
    ],
    "Resource": "arn:aws:events:*:*:rule/AuditManagerSecurityHubFindingsReceiver"
   }
  ]
}
```

AWS Audit Manager atualizações nas políticas AWS gerenciadas

Veja detalhes sobre as atualizações das políticas AWS gerenciadas AWS Audit Manager desde que esse serviço começou a rastrear essas alterações. Para receber alertas automáticos sobre alterações nessa página, assine o feed RSS na página Histórico do AWS Audit Manager documento.

Alteração	Descrição	Data
AWSAuditManagerServiceRolePolicy – Atualizar para uma política existente	A função vinculada ao serviço agora permite realizar AWS Audit Manager a ação `s3:GetBucketPolicy` . Essa ação de API é necessária para dar suporte ao framework de práticas recomendadas de IA generativa daAWS v1. Ela permite que o Audit Manager colete evidências automatizadas sobre as restrições de política que estão em vigor para conjuntos de dados de treinamento de dados do modelo de IA generativa.	12/06/2023

Alteração	Descrição	Data
	A `GetBucketPolicy` ação opera dentro do escopo do Conta da AWS onde service-linked-role está disponível. Ela não pode acessar políticas de bucket entre contas.	

Alteração	Descrição	Data
AWSAuditManagerServiceRolePolicy – Atualizar para uma política existente	Adicionamos as seguintes permissões aoAWSAuditManagerServiceRolePolicy . AWS Audit Manager agora pode realizar as seguintes ações para coletar evidências automatizadas sobre os recursos em seu Conta da AWS. • acm:GetAccountConfiguration • acm:ListCertificates • backup:ListRecoveryPointsByResource • bedrock:GetCustomModel • bedrock:GetFoundationModel • bedrock:GetModelCustomizationJob • bedrock:GetModelInvocationLoggingConfiguration • bedrock:ListCustomModels • bedrock:ListFoundationModels • bedrock:ListModelCustomizationJobs • cloudtrail:LookupEvents • cloudwatch:DescribeAlarmsForMetric • cloudwatch:GetMetricStatistics • cloudwatch:ListMetrics • directconnect:DescribeDirectConnectGateways • directconnect:DescribeVirtualGateways • dynamodb:ListBackups	11/06/2023

Alteração	Descrição	Data
	• dynamodb:ListGlobalTables • ec2:DescribeAddresses • ec2:DescribeCustomerGateways • ec2:DescribeEgressOnlyInternetGateways • ec2:DescribeInternetGateways • ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations • ec2:DescribeLocalGateways • ec2:DescribeLocalGatewayVirtualInterfaces • ec2:DescribeNatGateways • ec2:DescribeTransitGateways • ec2:DescribeVpcPeeringConnections • ec2:DescribeVpnConnections • ec2:DescribeVpnGateways • ec2:GetEbsDefaultKmsKeyId • ec2:GetEbsEncryptionByDefault • ecs:DescribeClusters • eks:DescribeAddonVersions • elasticache:DescribeCacheClusters • elasticache:DescribeServiceUpdates • elasticfilesystem:DescribeAccessPoints • elasticloadbalancing:DescribeLoadBalancers	

Alteração	Descrição	Data
	• elasticloadbalancing:DescribeSslPolicies • elasticloadbalancing:DescribeTargetGroups • elasticmapreduce:ListClusters • elasticmapreduce:ListSecurityConfigurations • events:ListConnections • events:ListEventBuses • events:ListEventSources • events:ListRules • firehose:ListDeliveryStreams • fsx:DescribeFileSystems • iam:GetAccountPasswordPolicy • iam:GetCredentialReport • iam:ListOpenIdConnectProviders • iam:ListSamlProviders • iam:ListVirtualMFADevices • kafka:ListClusters • kafka:ListKafkaVersions • kinesis:ListStreams • lambda:ListFunctions • logs:DescribeDestinations • logs:DescribeExportTasks • logs:DescribeLogGroups • logs:DescribeMetricFilters • logs:DescribeResourcePolicies • logs:FilterLogEvents • rds:DescribeCertificates	

Alteração	Descrição	Data
	• rds:DescribeDbClusterEndpoints • rds:DescribeDbClusterParameterGroups • rds:DescribeDbClusters • rds:DescribeDbSecurityGroups • redshift:DescribeClusters • s3:GetBucketPublicAccessBlock • s3:GetBucketVersioning • sns:ListTopics • sqs:ListQueues • waf-regional:GetLoggingConfiguration • waf-regional:ListRuleGroups • waf-regional:ListSubscribedRuleGroups • waf-regional:ListWebACLs	
AWSAuditManagerServiceRolePolicy – Atualizar para uma política existente	Adicionamos a seguinte permissão a AWSAuditManagerServiceRolePolicy : • dynamodb:DescribeTable • dynamodb:ListTables • ec2:DescribeVolumes • kms:GetKeyPolicy • kms:GetKeyRotationStatus • kms:ListKeyPolicies • rds:DescribeDBInstances • redshift:DescribeClusters • s3:GetEncryptionConfiguration • s3:ListAllMyBuckets	07/07/2022

Alteração	Descrição	Data
AWSAuditManagerServiceRolePolicy: atualização para uma política existente	A função vinculada ao serviço agora permite realizar AWS Audit Manager a açãoorganizations:DescribeOrganization . Também reduzimos o escopo do recurso CreateEventsAccess de um curinga (*) para um tipo específico de recurso (arn:aws:events:*:*:rule/AuditManagerSecurityHubFindingsReceiver). Por fim, adicionamos um operador de condição Null para a chave de condição events:source , para confirmar que existe um valor de origem e que ele não é nulo.	20/05/2022
AWSAuditManagerAdministratorAccess: atualização para uma política existente	Atualizamos a política de condição chave para events:source refletir que trata-se de uma chave de vários valores.	29/04/2022
AWSAuditManagerServiceRolePolicy: atualização para uma política existente	Atualizamos a política de condição chave para events:source refletir que trata-se de uma chave de vários valores.	16/03/2022
AWS Audit Manager começou a rastrear alterações	AWS Audit Manager começou a rastrear as mudanças em suas políticas AWS gerenciadas.	05/06/2021

Solução de problemas AWS Audit Manager de identidade e acesso

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

Tópicos

- Não estou autorizado a realizar uma ação em AWS Audit Manager

- Não estou autorizado a realizar iam: PassRole
- Quero permitir que pessoas fora da minha Conta da AWS acessem meus AWS Audit Manager recursos

Não estou autorizado a realizar uma ação em AWS Audit Manager

O `AccessDeniedException` erro aparece quando um usuário não tem permissão para usar AWS Audit Manager as operações da API Audit Manager.

Nesse caso, o administrador do usuário precisa atualizar a política para permitir o acesso do mesmo.

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 Audit 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 fazê-lo, um usuário deve ter permissões para passar o perfil para o serviço.

O erro do exemplo a seguir ocorre quando um usuário do IAM chamado `marymajor` tenta usar o console para executar uma ação no Audit Management. No entanto, a ação exige que o serviço tenha permissões concedidas por um perfil de serviço. Mary não tem permissões para passar a função 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 da AWS acessem meus AWS Audit Manager recursos

Você pode criar um perfil que os usuários de outras contas ou pessoas fora da organização podem usar para acessar seus recursos. Você pode especificar quem é confiável para assumir o perfil. Para

serviços que oferecem suporte a 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 Audit Manager oferece suporte a esses atributos, consulte Como AWS Audit 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 perfis e políticas baseadas em recursos para acesso entre contas, consulte Como os perfis do IAM diferem de políticas baseadas em recursos no Guia do usuário do IAM.

Usando funções vinculadas a serviços para AWS Audit Manager

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

Uma função vinculada ao serviço facilita a configuração AWS Audit Manager porque você não precisa adicionar manualmente as permissões necessárias. O Audit Manager define as permissões das funções vinculadas ao serviço e, a menos que definido de outra forma, somente o Audit Manager pode presumir suas funções. As permissões definidas incluem a política de confiança e a política de permissões, que não pode ser anexada a nenhuma outra entidade do IAM.

Para obter informações sobre outros serviços compatíveis com funções vinculadas a serviços, consulte Serviços daAWS compatíveis com o IAM e procure serviços que tenham Sim na coluna função vinculada ao serviço. Escolha um Sim com um link para visualizar a documentação do perfil vinculado a esse serviço.

Permissões de função vinculadas ao serviço para AWS Audit Manager

O Audit Manager usa a função vinculada ao serviço chamada**`AWSServiceRoleForAuditManager`**, que permite o acesso aos serviços e recursos da AWS usados ou gerenciados por. AWS Audit Manager

A função vinculada ao serviço `AWSServiceRoleForAuditManager` confia no serviço `auditmanager.amazonaws.com` para presumir a função.

A política de permissões de função, `AWSAuditManagerServiceRolePolicy`, permite que o Audit Manager colete evidências automatizadas sobre seu AWS uso. Mais especificamente, ele pode realizar as seguintes ações em seu nome:

- O Audit Manager pode ser usado AWS Security Hub para coletar evidências de verificação de conformidade. Nesse caso, o Audit Manager usa a seguinte permissão para relatar os resultados das verificações de segurança diretamente de AWS Security Hub. Em seguida, ele anexa os resultados aos controles de avaliação relevantes como evidência.
  - `securityhub:DescribeStandards`

  > **Note**
  >
  > Para obter mais informações sobre quais controles específicos do Security Hub o Audit Manager pode descrever, consulte AWS Security Hub controles suportados por AWS Audit Manager.

- O Audit Manager pode ser usado AWS Config para coletar evidências de verificação de conformidade. Nesse caso, o Audit Manager usa as seguintes permissões para relatar os resultados das avaliações de AWS Config regras diretamente de AWS Config. Em seguida, ele anexa os resultados aos controles de avaliação relevantes como evidência.
  - `config:DescribeConfigRules`
  - `config:DescribeDeliveryChannels`
  - `config:ListDiscoveredResources`

  > **Note**
  >
  > Para obter mais informações sobre quais AWS Config regras específicas o Audit Manager pode descrever, consulte AWS Config Regras suportadas por AWS Audit Manager.

- O Audit Manager pode ser usado AWS CloudTrail para coletar evidências de atividades do usuário. Nesse caso, o Audit Manager usa as seguintes permissões para capturar a atividade do usuário CloudTrail nos registros. Em seguida, ele anexa a atividade aos controles de avaliação relevantes como evidência.
  - `cloudtrail:DescribeTrails`
  - `cloudtrail:LookupEvents`

  > **Note**
  >
  > Para obter mais informações sobre quais CloudTrail eventos específicos o Audit Manager pode descrever, consulte nomes deAWS CloudTrail eventos suportados por AWS Audit Manager.

- O Audit Manager pode usar chamadas de AWS API para coletar evidências de configuração de recursos. Nesse caso, o Audit Manager usa as seguintes permissões para chamar APIs somente para leitura que descrevem suas configurações de recursos para o seguinte Serviços da AWS. Em seguida, ele anexa os resultados API aos controles de avaliação relevantes como evidência.
  - `acm:GetAccountConfiguration`
  - `acm:ListCertificates`
  - `backup:ListRecoveryPointsByResource`
  - `bedrock:GetCustomModel`
  - `bedrock:GetFoundationModel`
  - `bedrock:GetModelCustomizationJob`
  - `bedrock:GetModelInvocationLoggingConfiguration`
  - `bedrock:ListCustomModels`
  - `bedrock:ListFoundationModels`
  - `bedrock:ListModelCustomizationJobs`
  - `cloudwatch:DescribeAlarms`
  - `cloudwatch:DescribeAlarmsForMetric`
  - `cloudwatch:GetMetricStatistics`
  - `cloudwatch:ListMetrics`
  - `cognito-idp:DescribeUserPool`
  - `directconnect:DescribeDirectConnectGateways`

- directconnect:DescribeVirtualGateways
- dynamodb:DescribeTable
- dynamodb:ListBackups
- dynamodb:ListGlobalTables
- dynamodb:ListTables
- ec2:DescribeAddresses
- ec2:DescribeCustomerGateways
- ec2:DescribeEgressOnlyInternetGateways
- ec2:DescribeFlowLogs
- ec2:DescribeInstances
- ec2:DescribeInternetGateways
- ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations
- ec2:DescribeLocalGateways
- ec2:DescribeLocalGatewayVirtualInterfaces
- ec2:DescribeNatGateways
- ec2:DescribeNetworkAcls
- ec2:DescribeRouteTables
- ec2:DescribeSecurityGroups
- ec2:DescribeSnapshots
- ec2:DescribeTransitGateways
- ec2:DescribeVolumes
- ec2:DescribeVpcEndpoints
- ec2:DescribeVpcPeeringConnections
- ec2:DescribeVpcs
- ec2:DescribeVpnConnections
- ec2:DescribeVpnGateways
- ec2:GetEbsDefaultKmsKeyId
- ec2:GetEbsEncryptionByDefault
- ecs:DescribeClusters
- eks:DescribeAddonVersions

- elasticache:DescribeCacheClusters
- elasticache:DescribeServiceUpdates
- elasticfilesystem:DescribeAccessPoints
- elasticfilesystem:DescribeFileSystems
- elasticloadbalancing:DescribeLoadBalancers
- elasticloadbalancing:DescribeSslPolicies
- elasticloadbalancing:DescribeTargetGroups
- elasticmapreduce:ListClusters
- elasticmapreduce:ListSecurityConfigurations
- events:DeleteRule
- events:DescribeRule
- events:DisableRule
- events:EnableRule
- events:ListConnections
- events:ListEventBuses
- events:ListEventSources
- events:ListRules
- events:ListTargetsByRule
- events:PutRule
- events:PutTargets
- events:RemoveTargets
- firehose:ListDeliveryStreams
- fsx:DescribeFileSystems
- guardduty:ListDetectors
- iam:GenerateCredentialReport
- iam:GetAccountAuthorizationDetails
- iam:GetAccountPasswordPolicy
- iam:GetAccountSummary
- iam:GetCredentialReport
- iam:ListEntitiesForPolicy

- iam:ListGroupPolicies
- iam:ListGroups
- iam:ListOpenIdConnectProviders
- iam:ListPolicies
- iam:ListRolePolicies
- iam:ListRoles
- iam:ListSamlProviders
- iam:ListUserPolicies
- iam:ListUsers
- iam:ListVirtualMFADevices
- kafka:ListClusters
- kafka:ListKafkaVersions
- kinesis:ListStreams
- kms:DescribeKey
- kms:GetKeyPolicy
- kms:GetKeyRotationStatus
- kms:ListGrants
- kms:ListKeyPolicies
- kms:ListKeys
- lambda:ListFunctions
- license-manager:ListAssociationsForLicenseConfiguration
- license-manager:ListLicenseConfigurations
- license-manager:ListUsageForLicenseConfiguration
- logs:DescribeDestinations
- logs:DescribeExportTasks
- logs:DescribeLogGroups
- logs:DescribeMetricFilters
- logs:DescribeResourcePolicies
- logs:FilterLogEvents
- organizations:DescribeOrganization

- `organizations:DescribePolicy`
- `rds:DescribeCertificates`
- `rds:DescribeDbClusterEndpoints`
- `rds:DescribeDbClusterParameterGroups`
- `rds:DescribeDbClusters`
- `rds:DescribeDBInstances`
- `rds:DescribeDbSecurityGroups`
- `redshift:DescribeClusters`
- `route53:GetQueryLoggingConfig`
- `s3:GetBucketPolicy`
  - Essa ação de API opera dentro do escopo de Conta da AWS onde service-linked-role está disponível. Ela não pode acessar políticas de bucket entre contas.
- `s3:GetBucketPublicAccessBlock`
- `s3:GetBucketVersioning`
- `s3:GetEncryptionConfiguration`
- `s3:GetLifecycleConfiguration`
- `s3:ListAllMyBuckets`
- `sns:ListTopics`
- `sqs:ListQueues`
- `waf-regional:GetLoggingConfiguration`
- `waf-regional:ListRuleGroups`
- `waf-regional:ListSubscribedRuleGroups`
- `waf-regional:ListWebACLs`
- `waf:ListActivatedRulesInRuleGroup`

> **Note**
>
> Para obter mais informações sobre as chamadas de API específicas que o Audit Manager pode descrever, consulte Chamadas de API compatíveis com fontes de dados de controle personalizadas.

Para ver os detalhes completos das permissões da função vinculada ao serviço`AWSServiceRoleForAuditManager`, consulte o Guia `AWSAuditManagerServiceRolePolicy`de referência de políticasAWS gerenciadas.

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

Criando a função AWS Audit Manager vinculada ao serviço

Não é necessário criar manualmente um perfil vinculado ao serviço. Quando você ativa AWS Audit Manager, o serviço cria automaticamente a função vinculada ao serviço para você. Você pode ativar o Audit Manager na página de integração do AWS Management Console, ou por meio da API ou AWS CLI. Para obter mais informações, consulte Habilitar AWS Audit Manager no guia de usuário.

Se excluir esse perfil vinculado ao serviço e precisar criá-lo novamente, você poderá usar esse mesmo processo para recriar o perfil em sua conta.

Editando a função AWS Audit Manager vinculada ao serviço

AWS Audit Manager não permite que você edite a função `AWSServiceRoleForAuditManager` 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 uma função vinculada a serviço no Guia do Usuário do IAM.

Permite que uma entidade IAM edite a descrição da função vinculada ao serviço **`AWSServiceRoleForAuditManager`**

Adicione a seguinte declaração a política de permissões da entidade do IAM para a qual precise editar a descrição de uma função vinculada ao serviço.

```
{
    "Effect": "Allow",
    "Action": [
        "iam:UpdateRoleDescription"
    ],
    "Resource": "arn:aws:iam::*:role/aws-service-role/auditmanager.amazonaws.com/
AWSServiceRoleForAuditManager*",
    "Condition": {"StringLike": {"iam:AWSServiceName": "auditmanager.amazonaws.com"}}
```

```
}
```

Excluindo a função vinculada ao AWS Audit Manager serviço

Se você não precisa mais usar o Audit Manager, recomendamos que exclua a função vinculada a serviço `AWSServiceRoleForAuditManager`. Dessa forma, você não terá uma entidade não utilizada e não monitorada ativamente ou mantida. No entanto, você deve limpar sua função vinculada ao serviço antes de excluí-la.

Limpando a função vinculada ao serviço

Antes que possa usar o IAM para excluir uma função vinculada ao Audit Manager, você deve primeiro confirmar que a função não tem sessões ativas e remover quaisquer recursos usados pela função. Para fazer isso, certifique-se de que o registro do Audit Manager seja cancelado em todos. Regiões da AWSDepois de cancelar o registro, o Audit Manager não usará mais a função vinculada ao serviço.

Para obter instruções sobre como cancelar o Audit Manager, consulte os recursos a seguir:

- Desabilitar AWS Audit Manager neste guia
- DeregisterAccount na Referência de API doAWS Audit Manager
- cancelar o registro da conta na Referência paraAWS CLI AWS Audit Manager

Para obter instruções sobre como excluir recursos do Audit Manager manualmente, consulte Exclusão de dados do Audit Manager nesta guia.

Excluindo uma função vinculada ao serviço

Você também pode deletar a função vinculada ao serviço usando o console IAM, AWS Command Line Interface (AWS CLI) ou a API do IAM.

IAM console

Siga estas etapas para excluir o perfil vinculado ao serviço no console do IAM:

Para excluir uma função vinculada ao serviço (console)

1. Faça login AWS Management Console e abra o console do IAM em https://console.aws.amazon.com/iam/.

2. No painel de navegação do console do IAM, escolha Perfis. Marque a caixa de seleção ao lado de `AWSServiceRoleForAuditManager`, não o nome ou a linha em si.
3. Em Ações da função na parte superior da página, escolha Excluir.
4. Na caixa de diálogo de confirmação, analise as informações acessadas por último, que mostram quando cada uma das funções selecionadas foi acessada pela última vez um AWS service (Serviço da AWS). Isso ajuda a confirmar se a função está ativa no momento. Se quiser continuar, insira **`AWSServiceRoleForAuditManager`** no campo de texto e selecione Excluir para enviar a função vinculada ao serviço para eliminação.
5. Monitore as notificações do console do IAM para progresso da exclusão da função vinculada ao serviço. Como a exclusão da função vinculada ao serviço do IAM é assíncrona, depois de enviar a função para exclusão, a tarefa pode ou não ser bem-sucedida. Se a tarefa obtiver êxito, a função será removida da lista e uma notificação de êxito será exibida na parte superior da página.

AWS CLI

Você pode usar os comandos do IAM do AWS CLI para excluir uma função vinculada ao serviço.

Para excluir uma função vinculada ao serviço (AWS CLI)

1. Insira o comando a seguir para listar a função na sua conta:

```
aws iam get-role --role-name AWSServiceRoleForAuditManager
```

2. Como uma função vinculada ao serviço não pode ser excluída se estiver sendo usada ou possuir recursos associados, você deve enviar uma solicitação de exclusão. Essa solicitação pode ser negada se essas condições não forem atendidas. Você deve capturar o `deletion-task-id` da resposta para verificar o status da tarefa de exclusão.

   Insira o seguinte comando para enviar uma solicitação de exclusão de função vinculada ao serviço:

```
aws iam delete-service-linked-role --role-name AWSServiceRoleForAuditManager
```

3. Use o seguinte comando para verificar o status da tarefa de exclusão:

```
aws iam get-service-linked-role-deletion-status --deletion-task-id deletion-task-id
```

O status da tarefa de exclusão pode ser `NOT_STARTED`, `IN_PROGRESS`, `SUCCEEDED`, ou `FAILED`. Se a exclusão falhar, a chamada informará o motivo de falha para que você possa solucionar o problema.

IAM API

Você pode usar a API do IAM para excluir uma função vinculada ao serviço.

Para excluir uma função vinculada ao serviço (API)

1. Ligue GetRolepara listar a função em sua conta. Na solicitação, especifique `AWSServiceRoleForAuditManager` como `RoleName`.
2. Como uma função vinculada ao serviço não pode ser excluída se estiver sendo usada ou possuir recursos associados, você deve enviar uma solicitação de exclusão. Essa solicitação pode ser negada se essas condições não forem atendidas. Você deve capturar o `DeletionTaskId` da resposta para verificar o status da tarefa de exclusão.

   Para enviar uma solicitação de exclusão de um roll vinculada ao serviço, chame DeleteServiceLinkedRole. Na solicitação, especifique `AWSServiceRoleForAuditManager` como `RoleName`.
3. Para verificar o status da exclusão, chame GetServiceLinkedRoleDeletionStatus. Na solicitação, especifique o `DeletionTaskId`.

   O status da tarefa de exclusão pode ser `NOT_STARTED`, `IN_PROGRESS`, `SUCCEEDED`, ou `FAILED`. Se a exclusão falhar, a chamada informará o motivo de falha para que você possa solucionar o problema.

> **Tip**
>
> A exclusão falhará se o serviço Audit Manager estiver usando a função ou possuir recursos associados. Isso só acontecerá se você ainda estiver registrado no Audit Manager em um ou mais Regiões da AWS. Depois de cancelar o registro, o Audit Manager deixará de usar a função vinculada ao serviço.
> Para resolver um problema de exclusão com falha, primeiro certifique-se de cancelar o registro do Audit Manager em Regiões da AWS todos os lugares em que você usou o serviço. Em seguida, tente novamente seguir as etapas do procedimento anterior.

Regiões suportadas para funções vinculadas a AWS Audit Manager serviços

AWS Audit Manager suporta o uso de funções vinculadas ao serviço em todos os lugares em Regiões da AWS que o serviço está disponível. Para obter mais informações, consulte Endpoints de serviço daAWS.

Validação de conformidade para AWS Audit Manager

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 ConformidadeServiços da AWS e escolha o programa de conformidade em que você está interessado. Para obter informações gerais, consulte Programas de AWS conformidade ProgramasAWS 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 regulamentos 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 doAWS 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.
- 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 Audit 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 aplicações e bancos de dados que automaticamente executam o failover entre as zonas sem interrupção. As zonas de disponibilidade são mais altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de datacenter tradicionais.

Para obter mais informações sobre AWS regiões e zonas de disponibilidade, consulte InfraestruturaAWS global.

Segurança da infraestrutura em AWS Audit Manager

Como um serviço gerenciado, o AWS Audit 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 AWS Audit Manager pela rede. Os clientes precisam oferecer suporte para:

- Transport Layer Security (TLS). Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Conjuntos de criptografia com sigilo de encaminhamento perfeito (perfect forward secrecy, ou PFS) como DHE (Ephemeral Diffie-Hellman, ou Efêmero Diffie-Hellman) ou ECDHE (Ephemeral Elliptic Curve Diffie-Hellman, ou Curva elíptica efêmera Diffie-Hellman). A maioria dos sistemas modernos, como Java 7 e versões posteriores, comporta esses modos.

Além disso, as solicitações devem ser assinadas utilizando um ID da chave de acesso e uma chave de acesso secreta associada a uma entidade principal do IAM. Ou é possível usar o AWS Security Token Service (AWS STS) para gerar credenciais de segurança temporárias para assinar solicitações.

Você pode chamar essas operações de API de qualquer local de rede, mas AWS Audit Manager oferece suporte a políticas de acesso baseadas em recursos, que podem incluir restrições com base no endereço IP de origem. Você também pode usar políticas do IAM para controlar o acesso de endpoints específicos da Amazon Virtual Private Cloud (Amazon VPC) ou VPCs específicas. Efetivamente, isso isola o acesso à rede a um determinado recurso do Audit Manager somente da VPC específica dentro da AWS rede.

AWS Audit Manager e endpoints VPC de interface ()AWS PrivateLink

Você pode estabelecer uma conexão privada entre sua VPC e criar uma AWS Audit Manager interface VPC endpoint. Os endpoints de interface são habilitados por AWS PrivateLink, uma tecnologia que permite acessar de forma privada as APIs do Audit Manager sem um gateway da internet, dispositivo NAT, conexão VPN, ou conexão Direct Connect AWS . As instâncias na seu VPC não demandam comunicação de endereços IP públicos com APIs do Audit Manager. O tráfego entre sua VPC e AWS Audit Manager o tráfego não sai da AWS rede.

Cada endpoint de interface é representado por uma ou mais Interfaces de Rede Elástica nas sub-redes.

Para obter mais informações, consulte Endpoints da VPC da interface (AWS PrivateLink) no Manual do Usuário do Amazon VPC.

Considerações sobre AWS Audit Manager VPC endpoints

Antes de configurar uma interface para o VPC endpoint AWS Audit Manager, certifique-se de revisar as propriedades e limitações do endpoint da interface no Guia do usuário do Amazon VPC.

AWS Audit Manager suporta fazer chamadas para todas as suas ações de API a partir de sua VPC.

Criar um endpoint da VPC de interface para o AWS Audit Manager

Você pode criar um VPC endpoint para o AWS Audit Manager serviço usando o console Amazon VPC ou o (). AWS Command Line Interface AWS CLIPara obter mais informações, consulte Criar um endpoint da interface no Guia do usuário da Amazon VPC.

Crie um VPC endpoint para AWS Audit Manager usar o seguinte nome de serviço:

- `com.amazonaws.region.auditmanager`

Se você habilitar o DNS privado para o endpoint, poderá fazer solicitações de API AWS Audit Manager usando seu nome DNS padrão para a região, por exemplo,. `auditmanager.us-east-1.amazonaws.com`

Para obter mais informações, consulte Acessar um serviço por um endpoint de interface no Guia do usuário da Amazon VPC.

Criação de uma política de VPC endpoint para AWS Audit Manager

É possível anexar uma política de endpoint ao endpoint da VPC que controla o acesso ao AWS Audit Manager. Essa política especifica as seguintes informações:

- A entidade principal que pode executar ações.
- As ações que podem ser executadas.
- Os recursos sobre os quais as ações podem ser realizadas.

Para obter mais informações, consulte Controlar o acesso a serviços com endpoints da VPC no Guia do usuário da Amazon VPC.

Exemplo: política de VPC endpoint para ações AWS Audit Manager

Veja a seguir um exemplo de uma política de endpoint para AWS Audit Manager. Quando anexada a um endpoint, essa política concede acesso às ações Audit Manager indicadas para todas as entidades principais, em todos os recursos.

```
{
   "Statement":[
      {
         "Principal":"*",
         "Effect":"Allow",
         "Action":[
            "auditmanager:GetAssessments",
            "auditmanager:GetServicesInScope",
            "auditmanager:ListNotifications"
         ],
         "Resource":"*"
      }
   ]
}
```

Registro e monitoramento em AWS Audit Manager

O monitoramento é uma parte importante da manutenção da confiabilidade, disponibilidade e desempenho do Audit Manager e de suas outras AWS soluções. AWS fornece as seguintes ferramentas de monitoramento para monitorar o Audit Manager, relatar quando algo está errado e realizar ações automáticas quando apropriado:

- O AWS CloudTrail captura chamadas de API e eventos relacionados feitos por sua conta da Conta da AWS ou em nome dela e entrega os arquivos de log a um bucket do Amazon S3 que você especificar. Você pode identificar quais usuários e contas chamaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. Para obter mais informações, consulte o AWS CloudTrail Guia do Usuário.
- EventBridgeA Amazon é um serviço de ônibus de eventos sem servidor que facilita a conexão de seus aplicativos com dados de várias fontes. EventBridge fornece um fluxo de dados em tempo real de seus próprios aplicativos, aplicativos S oftware-as-a -Service (SaaS) AWS e serviços e encaminha esses dados para destinos como o Lambda. Isso permite monitorar eventos que ocorram em serviços e criem arquiteturas orientadas a eventos. Para obter mais informações, consulte o Guia EventBridge do usuário da Amazon.

Monitoramento AWS Audit Manager com a Amazon EventBridge

EventBridge A Amazon ajuda você a automatizar Serviços da AWS e responder automaticamente a eventos do sistema, como problemas de disponibilidade de aplicativos ou alterações de recursos.

Você pode usar EventBridge regras para detectar e reagir aos eventos do Audit Manager. Com base nas regras que você cria, EventBridge invoca uma ou mais ações de destino quando um evento corresponde aos valores que você especifica em uma regra. A depender do tipo de evento, convém enviar notificações, capturar informações, tomar medidas corretivas, iniciar eventos ou tomar outras ações.

Por exemplo, você pode detectar sempre que os seguintes eventos do Audit Manager ocorrerem na sua conta:

- Um proprietário de auditoria cria, atualiza ou exclui uma avaliação
- Um proprietário de auditoria delega um conjunto de controles para análise
- Um encarregado conclui sua análise e envia o conjunto de controles analisado de volta ao proprietário da auditoria
- Um proprietário Audit atualiza o status de um controle de avaliação

Ações que podem ser automaticamente acionadas incluem:

- Use uma AWS Lambda função para passar uma notificação para um canal do Slack.
- Enviar dados sobre a verificação para um Amazon Kinesis Data Streams para oferecer monitoramento de suporte abrangente e em tempo real.
- Envie um tópico Amazon Simple Notification Service (Amazon SNS) para o seu email.
- Seja notificado com uma ação de CloudWatch alarme da Amazon.

> **Note**
>
> O Audit Manager entrega eventos de forma duradoura. Isso significa que o Audit Manager tentará entregar eventos com sucesso pelo EventBridge menos uma vez. Nos casos em que os eventos não puderem ser entregues devido a uma interrupção do EventBridge serviço, eles serão repetidos posteriormente pelo Audit Manager por até 24 horas.

EventBridge formato de exemplo para Audit Manager

O código JSON a seguir mostra um exemplo de criação de avaliação no Audit Manager. Para obter informações sobre qualquer um dos campos desse evento, consulte Referência de estrutura de evento.

```
{
    "version": "0",
    "id": "55c5a6f3-6183-3989-49ec-a3c998857644",
    "detail-type": "Assessment Created",
    "source": "aws.auditmanager",
    "account": "111122223333",
    "time": "2023-07-27T00:38:33Z",
    "region": "us-west-2",
    "resources":
        [
            "arn:aws:auditmanager:us-west-2:111122223333:assessment/a1b2c3d4-e5f6-g7h8-
i9j0-k1l2m3n4o5p6"
        ],
    "detail":
    {
        "eventID": "4e939b2f-9429-3141-beec-d640d83ef68e",
        "author": "arn:aws:sts::111122223333:assumed-role/roleName/role-session-name",
        "assessmentTenantId": "111122223333",
        "assessmentName": "myAssessment",
        "eventTime": 1690418289068,
        "eventName": "CREATE",
        "eventType": "ASSESSMENT",
        "assessmentID": "a1b2c3d4-e5f6-g7h8-i9j0-k1l2m3n4o5p6"
    }
}
```

Pré-requisitos para criar uma regra EventBridge

Antes de criar regras para eventos Audit Manager, recomendamos o seguinte:

- Familiarize-se com eventos, regras e metas em EventBridge. Para obter mais informações, consulte O que é a Amazon EventBridge? no Guia do EventBridge usuário da Amazon.
- Crie um destino para usar em sua regra de evento. Por exemplo, é possível criar um tópico Amazon SNS de maneira que, sempre que uma análise de conjunto de controles for concluída,

você receba uma mensagem de texto ou email. Para obter mais informações, consulte EventBridge alvos.

Criação de uma EventBridge regra para o Audit Manager

Siga estas etapas para criar uma EventBridge regra que é acionada em um evento emitido pelo Audit Manager. Os eventos são emitidos com base no melhor esforço.

Para criar uma EventBridge regra para o Audit Manager

1. Abra o EventBridge console da Amazon em https://console.aws.amazon.com/events/.
2. No painel de navegação, escolha Regras.
3. Selecione Criar regra.
4. Na página Definir detalhe de regra, insira um nome e uma descrição para a regra.
5. Mantenha os valores padrão do Barramento de eventos e Tipo de regra e, depois, escolha Próximo.
6. Na página Criar padrão de evento, em Origem do evento, escolha AWS eventos ou eventos de EventBridge parceiros.
7. Para Método de criação, escolha Padrão personalizado (editor JSON).
8. Em Padrão de evento, registre um padrão de evento em JSON e especifique os campos que deseja usar para correspondência.

   Para corresponder a um evento do Audit Manager, você pode usar o seguinte padrão simples:

   ```
   {
     "detail-type": ["Event"]
   }
   ```

   Substitua *Evento* por um dos seguintes valores suportados:

   a. Insira `Assessment Created` para receber notificações quando uma avaliação for criada.

   b. Insira `Assessment Updated` para receber notificações quando uma avaliação for atualizada.

   c. Insira `Assessment Deleted` para receber notificações quando uma avaliação for excluída.

d. Insira `Assessment ControlSet Delegation Created` para receber notificações quando um conjunto de controles for delegado para análise.

e. Insira `Assessment ControlSet Reviewed` para receber notificações quando um conjunto de controles de avaliação for analisado.

f. Insira `Assessment Control Reviewed` para receber notificações quando um controle de avaliação for analisado.

> **Tip**
>
> Adicione mais campos ao seu padrão de eventos conforme necessário. Para obter mais informações sobre os campos disponíveis, consulte os padrões de EventBridge eventos da Amazon.

9. Escolha Próximo.
10. Na página Selecionar Destino(s), escolha o tipo de destino criado para essa regra e, em seguida, configure quaisquer opções adicionais necessárias a esse tipo. Por exemplo, se escolher o Amazon SNS, verifique se o tópico do SNS está configurado corretamente para ser notificado por email ou SMS.

> **Tip**
>
> Os campos exibidos variam de acordo com o serviço selecionado. Para obter mais informações sobre os alvos disponíveis, consulte Destinos disponíveis no EventBridge console.

11. Para muitos tipos de alvo, EventBridge precisa de permissões para enviar eventos ao alvo. Nesses casos, EventBridge você pode criar a função do IAM necessária para que sua regra seja executada.

    a. Para criar um perfil do IAM automaticamente, escolha Criar novo perfil para este recurso específico.

    b. Para usar um perfil do IAM criado anteriormente, escolha Usar função existente

12. (Opcional) Selecione Adicionar outro destino para adicionar outro destino a essa regra.
13. Escolha Next (Próximo).
14. (Opcional) Na página Configurar tags, adicione tags e escolha Próximo.

15. Na página Analisar e criar, analise a configuração da regra garantindo que ela atenda aos requisitos de monitoramento de eventos.
16. Escolha Criar regra. Sua regra agora irá monitorar eventos Audit Manager e, em seguida, enviá-los ao destino que você especificou.

Registrando chamadas de AWS Audit Manager API com CloudTrail

O Audit Manager é integrado com CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, função ou um AWS service (Serviço da AWS) no Audit Manager. CloudTrail captura todas as chamadas de API para o Audit Manager como eventos. As chamadas capturadas incluem chamadas do console Audit Manager e chamadas de código para as operações da API do Audit Manager.

Se você criar uma trilha, poderá habilitar a entrega contínua de CloudTrail eventos para um bucket do Amazon S3, incluindo eventos para o Audit Manager. Se você não configurar uma trilha, ainda poderá ver os eventos mais recentes no CloudTrail console no Histórico de eventos.

Usando as informações coletadas por CloudTrail, você pode determinar a solicitação que foi feita ao Audit Manager, o endereço IP do qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita e detalhes adicionais.

Para saber mais sobre isso CloudTrail, consulte o GuiaAWS CloudTrail do usuário.

Informações do Audit Manager em CloudTrail

CloudTrail é ativado no seu Conta da AWS quando você cria a conta. Quando a atividade ocorre no Audit Manager, essa atividade é registrada em um CloudTrail evento junto com outros AWS service (Serviço da AWS) eventos no histórico de eventos.

Você pode visualizar, pesquisar e baixar eventos recentes no seu Conta da AWS. Para obter mais informações, consulte Visualizar eventos com o histórico de eventos do CloudTrail .

Para um registro contínuo dos eventos em seu Conta da AWS, incluindo eventos para o Audit Manager, crie uma trilha. Uma trilha permite CloudTrail entregar arquivos de log para 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 eventos de todas as regiões na AWS partição e entrega os arquivos de log ao bucket do Amazon S3 que você especificar.

Além disso, você pode configurar outros Serviços da AWS para analisar e agir com base nos dados do evento coletados nos CloudTrail registros. Para mais informações, consulte:

- Visão Geral para Criar uma Trilha
- CloudTrail Serviços e integrações compatíveis
- Configurando notificações do Amazon SNS para CloudTrail
- Recebendo arquivos de CloudTrail log de várias regiões e recebendo arquivos de CloudTrail log de várias contas

Todas as ações do Audit Manager são registradas CloudTrail e documentadas na Referência daAWS Audit Manager API. Por exemplo, chamadas para o`CreateCustomControl`, `DeleteControl` e operações de `UpdateAssessmentTemplate` API geram entradas nos arquivos de CloudTrail log.

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.
- 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 AWS service (Serviço da AWS).

Para obter mais informações, consulte Elemento userIdentity do CloudTrail .

Entendendo entradas de arquivo de log Audit Manager

Uma trilha é uma configuração que permite a entrega de eventos como arquivos de log para um bucket do Amazon S3 que você especificar. CloudTrail os arquivos de log 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 da solicitação e assim por diante. CloudTrail os arquivos de log não são um rastreamento de pilha ordenado das chamadas públicas de API, portanto, eles não aparecem em nenhuma ordem específica.

O exemplo a seguir mostra uma entrada de CloudTrail registro que demonstra a `CreateAssessment`ação.

```
{
      eventVersion:"1.05",
      userIdentity:{
        type:"IAMUser",
        principalId:"principalId",
        arn:"arn:aws:iam::accountId:user/userName",
```

```
        accountId:"111122223333",
        accessKeyId:"accessKeyId",
        userName:"userName",
        sessionContext:{
          sessionIssuer:{
          },
          webIdFederationData:{
          },
          attributes:{
            mfaAuthenticated:"false",
            creationDate:"2020-11-19T07:32:06Z"
          }
        }
      },
      eventTime:"2020-11-19T07:32:36Z",
      eventSource:"auditmanager.amazonaws.com",
      eventName:"CreateAssessment",
      awsRegion:"us-west-2",
      sourceIPAddress:"sourceIPAddress",
      userAgent:"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
      requestParameters:{
        frameworkId:"frameworkId",
        assessmentReportsDestination:{
          destination:"***",
          destinationType:"S3"
        },
        clientToken:"***",
        scope:{
          awsServices:[
            {
              serviceName:"license-manager"
            }
          ],
          awsAccounts:"***"
        },
        roles:"***",
        name:"***",
        description:"***",
        tags:"***"
      },
      responseElements:{
        assessment:"***"
      },
```

```
    requestID:"0d950f8c-5211-40db-8c37-2ed38ffcc894",
    eventID:"a782029a-959e-4549-81df-9f6596775cb0",
    readOnly:false,
    eventType:"AwsApiCall",
    recipientAccountId:"recipientAccountId"
  }
```

Análise de configuração e vulnerabilidade em AWS Audit 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.

Marcando atributos AWS Audit Manager

Uma tag é um rótulo de metadados que você ou AWS atribuem a um atributo da AWS. Cada tag consiste em uma chave e um valor. Em tags atribuídas por você, você mesmo define a chave e o valor. Por exemplo, você pode definir a chave como `stage` e o valor de um atributo como `test`.

As tags ajudam a:

- Localizar facilmente seus atributos Audit Manager. Você pode usar tags como critérios de pesquisa ao navegar na biblioteca de framework e de controle.
- Associe seu atributo a um tipo de conformidade. Você pode marcar vários atributos com uma tag específica de conformidade para associá-los a um framework específico.
- Identificar e organizar seus atributos AWS. Muitos Serviços da AWS são compatíveis com marcação e permitem que você atribua a mesma tag a atributos de diferentes serviços, para indicar que estes atributos estão relacionados.
- Monitorar seus custos AWS. Você pode ativar essas tags no painel AWS Billing and Cost Management. AWS usa tags para categorizar seus custos e entregar um relatório mensal de alocação de custos a você. Para obter mais informações, consulte Usar etiquetas de alocação de custos no Guia do UsuárioAWS Billing and Cost Management.

As seções a seguir fornecem mais informações sobre tags para AWS Audit Manager.

Atributos suportados no Audit Manager

Os seguintes atributos Audit Manager oferecem suporte à marcação:

- Avaliações
- Controles
- Frameworks

Restrições de tag

As restrições básicas a seguir se aplicam às tags nos atributos do Audit Manager

- Número máximo de tags que você pode atribuir a um atributo — 50

- Comprimento máximo da chave — 128 caracteres Unicode
- Comprimento máximo de valor — 256 caracteres Unicode
- Caracteres válidos de chave e valor — a-z, A-Z, 0-9, espaço, e os seguintes caracteres: _ . : / = + - e @
- As chaves e os valores diferenciam letras maiúsculas de minúsculas
- Não use `aws:` como um prefixo para chaves, pois ele é reservado para uso da AWS

Gerenciando tags

Você pode configurar tags como propriedades ao criar uma avaliação, framework ou controle. Você pode adicionar, editar e excluir tags por meio do console Audit Manager, do AWS Command Line Interface (AWS CLI) e da API Audit Manager. Para obter mais informações, consulte os seguintes links.

- Para avaliações:
  - Como criar uma avaliação e Como editar uma avaliação na seção Avaliações deste guia
  - Guia Tags na seção Analisar uma avaliação deste guia
  - CreateAssessment and UpdateAssessment na Referência de API AWS Audit Manager
  - TagResource e UntagResource na Referência de API AWS Audit Manager
- Para estruturas:
  - Criando criar um framework personalizado e Como editar um framework personalizado na seção Biblioteca de framework deste guia
  - Guia Tags na seção Exibir detalhes de framework deste guia
  - CreateAssessmentFramework e UpdateAssessmentFramework na Referência de API AWS Audit Manager
  - TagResource e UntagResource na Referência de API AWS Audit Manager
- Para controles:
  - Criar um controle personalizado e Editar um controle personalizado na seção Biblioteca de controle deste guia
  - Guia Tags na seção Exibir detalhes do controle deste guia
  - CreateControl e UpdateControl na Referência de API AWS Audit Manager
  - TagResource e UntagResource na Referência de API AWS Audit Manager

Criando atributos AWS Audit Manager com AWS CloudFormation

AWS Audit Manager está integrado a AWS CloudFormation, um serviço que ajuda a modelar e configurar seus atributos AWS para que você possa gastar menos tempo criando e gerenciando seus atributos e infraestrutura. Você cria um modelo que descreve todos os atributos AWS desejados (como avaliações), e o AWS CloudFormation provisiona e configura esses recursos para você.

Quando você usa AWS CloudFormation, é possível reutilizar seu modelo para configurar seus atributos do Audit Manager repetidamente e de forma consistente. Descreva seus atributos uma vez e, em seguida, provisione os mesmos recursos repetidamente, em várias contas e regiões da AWS.

Audit Manager e modelos AWS CloudFormation

Para provisionar e configurar atributos para o Audit Manager e serviços relacionados, você deve entender os modelosAWS CloudFormation. Os modelos são arquivos de texto formatados em JSON ou YAML. Esses modelos descrevem os atributos que você deseja provisionar nas suas pilhas AWS CloudFormation. Se não estiver familiarizado com JSON ou YAML, você pode usar AWS CloudFormation Designer para ajudá-lo a começar a usar os modelos AWS CloudFormation. Para obter mais informações, consulte O que é Designer AWS CloudFormation? no Guia do UsuárioAWS CloudFormation.

O Audit Manager suporta a criação de avaliações no AWS CloudFormation. Para obter mais informações, como exemplos de modelos JSON e YAML para esses atributos, consulte Referência de tipo de atributoAWS Audit Manager no Guia do UsuárioAWS CloudFormation.

Saiba mais sobre AWS CloudFormation

Para mais sobre o AWS CloudFormation, consulte os seguintes atributos:

- AWS CloudFormation
- Guia do UsuárioAWS CloudFormation
- Referência de API AWS CloudFormation
- Guia do Usuário da Interface de Linha de ComandoAWS CloudFormation

Histórico de documento do Guia do Usuário AWS Audit Manager

A tabela a seguir descreve as alterações importantes em cada versão do Guia do Usuário AWS Audit Manager, de 8 de dezembro de 2020 em diante.

Alteração	Descrição	Data
Novo framework compatível: PCI DSS V4.0	Um novo framework de fábrica está disponível em AWS Audit Manager. Para obter mais informações, consulte PCI DSS.V4.0.	19 de dezembro de 2023
Suporte para chamadas de API da AWS adicionais	Agora, você pode usar chamadas de API da AWS adicionais como fonte de dados para controles personalizados no Audit Manager. Para obter mais informações, consulte Chamadas de API compatíveis com fontes de dados de controle personalizadas.	7 de dezembro de 2023
Política gerenciada atualizada AWS	AWS Audit Manager atualizou AWSauditManagerServiceRolePolicy. Para obter mais informações, consulte Políticas gerenciadas AWS para AWS Audit Manager.	6 de dezembro de 2023
Suporte para descobertas de controle consolidadas AWS Security Hub	O Audit Manager agora oferece suporte a controles consolidados em AWS Security Hub. Para obter	16 de novembro de 2023

	mais informações, consulte Controles suportados AWS Security Hub por AWS Audit Manager.	
Integração com MetricStream	Agora você pode ingerir evidências do Audit Manager no MetricStream. Para obter mais informações, consulte Integrações com produtos GRC de terceiros.	14 de novembro de 2023
Novo framework suportado: práticas recomendadas de IA generativa AWS	Um novo framework de fábrica está disponível em AWS Audit Manager. Para obter mais informações, consulte Práticas recomendadas da AWS para IA generativa do framework v1.	8 de novembro de 2023
Política gerenciada atualizada AWS	AWS Audit Manager atualizou AWSauditManagerServiceRolePolicy. Para obter mais informações, consulte Políticas gerenciadas AWS para AWS Audit Manager.	6 de novembro de 2023
Integração com o Amazon Eventbridge	Agora você pode monitorar eventos que acontecem no AWS Audit Manager e usar esses eventos como parte de sua arquitetura orientada a eventos. Para obter mais informações, consulte Monitoramento do AWS Audit Manager com o Amazon EventBridge.	18 de agosto de 2023

Suporte para avaliações de risco e novas opções de evidências manuais	Agora você pode usar o fluxo de trabalho de criação de controle personalizado para fornecer suporte às avaliações de risco. Um controle pode representar uma pergunta de avaliação de risco e você pode fornecer uma resposta carregando um arquivo ou inserindo texto como prova manual. Para obter mais informações, consulte Criar um controle personalizado e Adicionar evidência manual.	12 de junho de 2023
Suporte para exportações CSV	Agora você pode exportar os resultados da pesquisa do localizador de evidências no formato CSV. Para obter mais informações, consulte Exportação dos resultados da pesquisa.	9 de junho de 2023
Novo framework suportado: Manual de Segurança da Informação do Centro de Segurança Cibernética Australiano (ACSC)	Um novo framework de fábrica está disponível em AWS Audit Manager. Para obter mais informações, consulte o Manual de Segurança da Informação do Centro de Segurança Cibernética Australiano (ACSC).	24 de março de 2023

Relatórios de avaliação aprimorados	Fizemos melhorias no formato e conteúdo dos relatórios de avaliação do Audit Manager. Para obter mais informaçõ es sobre como navegar e entender os relatórios de avaliação, consulte Relatórios de avaliação.	23 de março de 2023
Suporte para chamadas de API paginadas	AWS Audit Manager agora oferece suporte a chamadas de API paginadas como fonte de dados para coleta de evidências. Para obter mais informações, consulte Chamadas de API paginadas.	8 de março de 2023
Novo framework suportado : Regra Final de Segurança Geral da HIPAA de 2013	Um novo framework de fábrica está disponível em AWS Audit Manager. Para obter mais informações, consulte Regra final de segurança geral da HIPAA de 2013. Para fins de diferenciação, o framework HIPAA existente (anterior mente chamado de HIPAA na biblioteca do framework) agora se chama Regra de Segurança HIPAA de 2003.	8 de março de 2023

Suporte para chamadas de API da AWS adicionais	Agora você pode usar mais nove chamadas de API da AWS como fonte de dados para seus controles personalizados no Audit Manager. Para obter mais informações, consulte Chamadas de API compatíveis com fontes de dados de controle personalizadas.	3 de março de 2023
Guia atualizado para alinhamento com as práticas recomendadas do IAM	Guia atualizado para alinhamento com as práticas recomendadas do IAM. Para obter mais informações, consulte Práticas recomendadas de segurança no IAM.	6 de janeiro de 2023
Nova configuração de retenção de dados	Agora você pode especificar se deseja excluir todos os seus dados ao desativar o Audit Manager. Para obter mais informações, consulte Desativar AWS Audit Manager e Exclusão de dados do Audit Manager.	6 de janeiro de 2023
Suporte para localizador de evidências	Agora você pode usar o localizador de evidências para realizar consultas de pesquisa em seus dados de evidência. Para obter mais informações, consulte Localizador de evidência.	18 de novembro de 2022

Novo framework suportado : Essential Eight do Centro Australiano de Segurança Cibernética (ACSC)	Um novo framework de fábrica está disponível em AWS Audit Manager. Para obter mais informações, consulte Essential Eight do Centro Australiano de Segurança Cibernética (ACSC).	24 de agosto de 2022
Política gerenciada atualizada AWS	AWS Audit Manager atualizou AWSauditManagerServiceRolePolicy. Para obter mais informações, consulte Políticas gerenciadas AWS para AWS Audit Manager.	7 de julho de 2022
Política gerenciada atualizada AWS	AWS Audit Manager atualizou AWSauditManagerServiceRolePolicy. Para obter mais informações, consulte Políticas gerenciadas AWS para AWS Audit Manager.	20 de maio de 2022
Novo framework suportado : perfil de controle de nuvem médio do Centro Canadense de Segurança Cibernética	Um novo framework de fábrica está disponível em AWS Audit Manager. Para obter mais informações, consulte Perfil de controle de nuvem médio do Centro Canadense de Segurança Cibernética.	6 de maio de 2022
Política gerenciada atualizada AWS	AWS Audit Manager atualizou a política AWSauditManagerAdministratorAccess. Para obter mais informações, consulte Políticas gerenciadas AWS para AWS Audit Manager.	29 de abril de 2022

Suporte para regras AWS Config gerenciadas adicionais	Agora você pode usar 91 regras gerenciadas adicionais AWS Config como fonte de dados para seus controles personalizados no Audit Manager. Para obter mais informações, consulte Como usar regras AWS Config gerenciadas com o AWS Audit Manager.	27 de abril de 2022
Suporte para regras AWS Config personalizadas	Agora você pode usar regras personalizadas AWS Config como fonte de dados para seus controles personalizados no Audit Manager. Para obter mais informações, consulte Como usar regras AWS Config personalizadas com o AWS Audit Manager.	27 de abril de 2022
Novo framework suportado: ISO/IEC 27001:2013 Anexo A	Um novo framework de fábrica está disponível em AWS Audit Manager. Para obter mais informações, consulte o ISO/IEC 27001:2013 Anexo A.	7 de abril de 2022
Política gerenciada atualizada AWS	AWS Audit Manager atualizou AWSauditManagerServiceRolePolicy. Para obter mais informações, consulte Políticas gerenciadas AWS para AWS Audit Manager.	16 de março de 2022

Novos frameworks suportados: CIS Benchmark para CIS Amazon Web Services Foundations Benchmark v1.4	Dois novos frameworks de fábrica estão disponíveis no AWS Audit Manager: CIS Benchmark para CIS Amazon Web Services Foundations Benchmark v1.4, Nível 1 e CIS Benchmark para CIS Amazon Web Services Foundations Benchmark v1.4, Níveis 1 e 2. Para obter mais informações, consulte CIS Benchmark para CIS AWS Audit Manager Foundations Benchmark v1.4.0.	2 de março de 2022
Novo framework suportado: CIS Controls v8 IG1	Um novo framework de fábrica está disponível em AWS Audit Manager. Para obter mais informações, consulte CIS Controls v8 IG1.	2 de março de 2022
Painel AWS Audit Manager	Agora você pode usar o painel do Audit Manager para monitorar suas avaliações ativas e identificar rapidamente evidências que não estejam em conformidade. Para obter mais informações, consulte Usando o painel do Audit Manager.	18 de novembro de 2021

Compartilhamento de framework personalizado	Agora você pode compartilhar seus frameworks personalizados do Audit Manager com outra Conta da AWS ou replicá-los em outra Região da AWS usando sua própria conta. Para obter mais informações, consulte Compartilhamento framework personalizado.	22 de outubro de 2021
Novos exemplos de controles AWS Audit Manager	Agora você pode analisar exemplos de controles e aprender como o Audit Manager ajuda a alinhar seu ambiente da AWS com seus requisitos. Para obter mais informações, consulte Exemplos de controles AWS Audit Manager.	21 de setembro de 2021
Novo framework suportado : Lei Gramm-Leach-Bliley (GLBA)	Um novo framework de fábrica está disponível em AWS Audit Manager. Para obter mais informações, consulte a Lei Gramm-Leach-Bliley (GLBA).	2 de setembro de 2021
Novo capítulo de solução de problemas	Um novo capítulo de solução de problemas já está disponível. Para obter mais informações, consulte Solução de problemas em AWS Audit Manager.	23 de agosto de 2021

Novo capítulo e tutorial de delegação	Expandimos nossa documentação de delegação em um novo capítulo. Para obter mais informações, consulte Delegações em AWS Audit Manager. Também adicionamos um novo tutorial destinado aos delegados que estiverem analisando um conjunto de controles pela primeira vez em AWS Audit Manager. Para obter mais informações, consulte Tutorial para delegados: analisando um conjunto de controles.	25 de junho de 2021
Novo framework suportado: NIST SP 800-171 Rev. 2	Um novo framework de fábrica está disponível em AWS Audit Manager. Para obter mais informações, consulte NIST SP 800-171 Rev. 2..	17 de junho de 2021
Relatórios de avaliação aprimorados	Fizemos melhorias no formato e conteúdo dos relatórios de avaliação AWS Audit Manager. Para obter mais informações sobre como navegar e entender os novos relatórios de avaliação, consulte Relatórios de avaliação.	8 de junho de 2021

Novas políticas gerenciadas pela AWS	AWS Audit Manager começou a monitorar as alterações nas políticas gerenciadas. Para obter mais informações, consulte Políticas gerenciadas AWS para AWS Audit Manager.	6 de maio de 2021
Novo framework suportado: NIST Cybersecurity Framework versão 1.1	Um novo framework de fábrica está disponível em AWS Audit Manager. Para obter mais informações, consulte NIST Cybersecurity Framework versão 1.1.	5 de maio de 2021
Novo framework suportado: AWS Well-Architected	Um novo framework de fábrica está disponível em AWS Audit Manager. Para obter mais informações, consulte AWS Well-Architected.	5 de maio de 2021
Novo framework suportado: práticas recomendadas de segurança básica AWS	Um novo framework de fábrica está disponível em AWS Audit Manager. Para obter mais informações, consulte Práticas recomendadas de segurança básica AWS.	5 de maio de 2021
Novo framework suportado: Anexo 11 da GxP EU	Um novo framework de fábrica está disponível em AWS Audit Manager. Para obter mais informações, consulte Anexo 11 da GxP EU.	28 de abril de 2021

Novo framework suportado: NIST 800-53 (Rev. 5) Baixo-Moderado-Alto	Um novo framework de fábrica está disponível em AWS Audit Manager. Para obter mais informações, consulte NIST 800-53 (Rev. 5) Baixo-Moderado-Alto.	25 de março de 2021
Novos frameworks suportados: CIS Benchmark para CIS AWS Audit Manager Foundations Benchmark v1.3	Dois novos frameworks de fábrica já estão disponíveis no AWS Audit Manager: CIS Benchmark para CIS AWS Audit Manager Foundations Benchmark v1.3.0, Level 1, e CIS Benchmark para CIS AWS Audit Manager Foundations Benchmark v1.3.0, Level 1 e 2. Para obter mais informações, consulte CIS Benchmark para CIS AWS Audit Manager Foundations Benchmark v1.3.0.	22 de março de 2021
Lançamento inicial	Lançamento inicial do Guia do Usuário e Referência de API AWS Audit Manager.	8 de dezembro de 2020

Glossário do AWS

Para obter a terminologia mais recente da AWS, consulte o glossário da AWS na Referência do Glossário da AWS.

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.