Informações de segurança

AWSCatálogo de controle

AWSCatálogo de controle: Informações de segurança

Table of Contents

O que é o AWS Control Catalog?

Bem-vindo ao guia de informações de segurança do AWS Control Catalog. O Catálogo de Controle faz parte do AWS Control Tower, que lista controles para vários AWS serviços. É um catálogo consolidado de AWS controles. Você não precisa configurar AWS Control Tower para usar o Catálogo de Controle.

Com o Catálogo de Controle, você pode visualizar os controles de acordo com casos de uso comuns, incluindo segurança, custo, durabilidade e operações.

Neste documento, você pode encontrar informações de segurança e conformidade que precisa conhecer, ao usar as APIs fornecidas pelo AWS Control Catalog.

O Catálogo de Controle incorpora uma Ontologia de Controle, que é um sistema de classificação padrão para controles.

Visão geral da ontologia

AWS desenvolveu um sistema de classificação padrão para ajudar a classificar, organizar e criar mapeamentos entre os controles. Essa ontologia pode ser usada para mapear controles para padrões regulatórios novos e existentes, incluindo 24 estruturas, bem como padrões regulatórios comoPCI,HIPAA, e outros. Também mapeamos os padrões do setor, como NIST eISO, e para estruturas específicas da Amazon, incluindo a estrutura Well-Architected.

A ontologia tem quatro aspectos principais

- Classificação dos controles por domínio de controle, objetivo de controle e controles comuns. A ontologia ajuda a organizar e agrupar os controles relacionados em três níveis—
  - L1: Domínio de controle,
  - L2: Objetivo de controle,
  - L3: Controle comum.

  Esses níveis têm uma relação hierárquica estrita. Ou seja, cada domínio tem vários objetivos de controle, mas cada objetivo de controle deve ter um único domínio principal. Cada objetivo de controle tem vários controles comuns, mas cada controle comum tem um único objetivo principal.
- Mapeamento de acordo com os padrões regulatórios. A ontologia tem um conceito chamado controle padrão (L4) que representa um requisito específico dentro de um padrão regulatório ou

industrial. Esses controles padrão são mapeados para controles comuns que ajudam a atender a esses requisitos específicos.

Por exemplo, PCI- DSS v3.2.1. ID 4.1 Use protocolos fortes de criptografia e segurança para proteger dados confidenciais do titular do cartão durante a transmissão em redes públicas abertas. NIST 800.53.r5 ID SC-16 A transmissão de atributos de segurança e privacidade são dois controles padrão, ambos mapeados para o controle comum de criptografia de dados em trânsito.

- Implementações de controle e evidências de controle. A ontologia tem um conceito de implementações de controle (L6) que pode representar uma implementação de controle específica em AWS, por exemplo, um AWS Control Tower controle, um AWS Security Hub cheque, um AWS Config regra, etc., ou uma implementação não técnica externa AWS, como orientação de processos. Um conceito separado de evidência de controle (L7) representa fontes de dados que podem ser usadas como evidência para controles por AWS Audit Manager, ferramentas de terceiros ou os próprios clientes. Essas fontes de evidência podem ser AWS fontes como AWS CloudTrail eventos, registros de API chamadas e AWS Config resultados da avaliação da regra. Ou podem ser fontes externas, como documentação do cliente.
- O conceito de controle central (L5). O controle central é uma camada de mapeamento que consolida todas as implementações de controle (L6), fontes de evidência correspondentes (L7), controles padrão relacionados (L4) e controles comuns (L3) em um único objeto holístico. O controle principal é mais um documento de mapeamento do que um controle em si. Isso ajuda a responder à pergunta de me mostrar todas as informações relacionadas ao controle X. Cada controle central pode ter várias implementações de controle (L6) e várias fontes de evidência (L7).

Em resumo, o AWS a ontologia do catálogo de controle contém sete camadas. Três são camadas de classificação hierárquica (domínios de controle, objetivos de controle, controles comuns). Outra camada (controles padrão) descreve os requisitos regulatórios ou padrões do setor. Uma camada de mapeamento (controle principal) descreve um resultado de controle para um determinado tipo de recurso. Duas camadas (implementações de controle, evidências de controle) descrevem as implementações de controle específicas e as fontes de evidências.

Essa ontologia foi projetada por um AWS equipe de auditores certificados, com base em sua experiência trabalhando com centenas de clientes em auditorias de conformidade. Os conceitos de domínios de controle, objetivos de controle, controles comuns e controles padrão (L1-L4) são usados em todo o setor. Eles correspondem aos padrões e NIST recomendações comuns do setor. As três camadas restantes (L5-L7) foram projetadas com base nas existentes AWS conceitos, como tipos de recursos e controles gerenciados.

Acesso ao catálogo AWS de controle

AWSO Control Catalog está disponível por meio do console e da interface de programação do aplicativo AWS Control Catalog (API). Isso API fornece uma maneira programática de identificar e filtrar os controles comuns e os metadados relacionados que estão disponíveis para você como AWS cliente. Para obter mais informações, consulte a APIReferência do Catálogo de AWS Controle.

Catálogo de segurança no AWS controle

Segurança na nuvem em AWS é a maior prioridade. Como um 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 AWS e você. O modelo de responsabilidade compartilhada descreve isso como segurança da nuvem e segurança na nuvem:

- Segurança da nuvem — AWS é responsável por proteger a infraestrutura que funciona Serviços da AWS no Nuvem AWS. AWS também fornece serviços que você pode usar com segurança. Auditores terceirizados testam e verificam regularmente a eficácia de nossa segurança como parte do AWS Programas de conformidade . Para saber mais sobre os programas de conformidade que se aplicam ao AWS Control Catalog, consulte AWS Serviços no escopo do Programa de Conformidade .
- Segurança na nuvem — Sua responsabilidade é determinada pelo AWS service (Serviço da AWS) 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 o Catálogo AWS de Controle. Os tópicos a seguir mostram como configurar o Catálogo AWS de Controle para atender aos seus objetivos de segurança e conformidade. Você também aprende a usar outros Serviços da AWS que ajudam você a monitorar e proteger seus recursos do Catálogo de AWS Controle.

Tópicos

Proteção de dados no AWS Control Catalog

A ferramenta AWS modelo de responsabilidade compartilhada modelo se aplica à proteção de dados no Catálogo AWS de Controle. Conforme descrito neste modelo, AWS é responsável por proteger a infraestrutura global que executa todas as Nuvem AWS. Você é responsável por manter o controle sobre o conteúdo hospedado nessa infraestrutura. Você também é responsável pelas tarefas de configuração e gerenciamento de segurança do Serviços da AWS que você usa. Para obter mais informações sobre privacidade de dados, consulte Privacidade de dados FAQ. Para obter informações sobre proteção de dados na Europa, consulte AWS Modelo de responsabilidade compartilhada e postagem no GDPR blog sobre o AWS Blog de segurança.

Para fins de proteção de dados, recomendamos que você proteja Conta da AWS 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 a autenticação multifator (MFA) com cada conta.
- UseSSL/TLSpara se comunicar com AWS recursos. Exigimos TLS 1,2 e recomendamos TLS 1,3.
- Configure API e registre as atividades do usuário com AWS CloudTrail. Para obter informações sobre o uso de CloudTrail trilhas para capturar AWS atividades, consulte Trabalhando com CloudTrail trilhas no AWS CloudTrail Guia do usuário.
- Use AWS soluções de criptografia, junto com todos os controles de segurança padrão dentro 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 FIPS 140-3 módulos criptográficos validados ao acessar AWS por meio de uma interface de linha de comando ou umaAPI, use um FIPS endpoint. Para obter mais informações sobre os FIPS endpoints disponíveis, consulte Federal Information Processing Standard (FIPS) 140-3.

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 AWS Control Catalog ou outro Serviços da AWS usando o consoleAPI, AWS CLI, ou AWS SDKs. Quaisquer dados inseridos em tags ou campos de texto de formato livre usados para nomes podem ser usados para logs de faturamento ou

de diagnóstico. Se você fornecer um URL para um servidor externo, é altamente recomendável que você não inclua informações de credenciais no URL para validar sua solicitação para esse servidor.

Criptografia de dados

AWS O Control Catalog não armazena nenhum dado do cliente.

Criptografia em repouso

AWS O Control Catalog não criptografa os dados do cliente. Porque nenhum dado do cliente é mantido ou retido pelo AWS Catálogo de controle, não há diretrizes específicas para criptografia em repouso.

Criptografia em trânsito

AWS O Control Catalog não criptografa os dados do cliente. Porque nenhum dado confidencial é trocado ou persistido por AWS Catálogo de controle, não há diretrizes específicas para criptografia em trânsito.

Gerenciamento de chaves

O gerenciamento de chaves de criptografia não se aplica a AWS Catálogo de controle.

Privacidade do tráfego entre redes

A privacidade do tráfego entre redes não se aplica a AWS Catálogo de controle.

Gerenciamento de identidade e acesso para o AWS Control Catalog

AWS Identity and Access Management (IAM) é um AWS service (Serviço da AWS) que ajuda o administrador a controlar com segurança o acesso ao AWS recursos. IAMos administradores controlam quem pode ser autenticado (conectado) e autorizado (tem permissões) a usar os recursos do Catálogo AWS de Controle. IAMé um AWS service (Serviço da AWS) que você pode usar sem custo adicional.

Tópicos

- Gerenciando acesso usando políticas
- Como o AWS Control Catalog funciona com IAM
- Exemplos de políticas baseadas em identidade para AWS o Control Catalog
- Solução de problemas AWS de identidade e acesso ao Control Catalog

Público

Como você usa AWS Identity and Access Management (IAM) difere, dependendo do trabalho que você faz no Catálogo AWS de Controle.

Usuário do serviço — Se você usar o serviço AWS Control Catalog para fazer seu trabalho, seu administrador fornecerá as credenciais e as permissões de que você precisa. À medida que você usa mais recursos do Catálogo de AWS Controle para fazer seu trabalho, talvez precise de permissões adicionais. Entender como o acesso é gerenciado pode ajudar você a solicitar as permissões corretas ao seu administrador. Se você não conseguir acessar um recurso no Catálogo AWS de Controle, consulteSolução de problemas AWS de identidade e acesso ao Control Catalog.

Administrador de serviços — Se você é responsável pelos recursos do AWS Control Catalog em sua empresa, provavelmente tem acesso total ao AWS Control Catalog. É seu trabalho determinar quais recursos e recursos do AWS Control Catalog seus usuários do serviço devem acessar. Em seguida, você deve enviar solicitações ao IAM administrador para alterar as permissões dos usuários do serviço. Revise as informações nesta página para entender os conceitos básicos doIAM. Para saber mais sobre como sua empresa pode usar o IAM AWS Control Catalog, consulteComo o AWS Control Catalog funciona com IAM.

IAMadministrador — Se você for IAM administrador, talvez queira saber detalhes sobre como criar políticas para gerenciar o acesso ao Catálogo AWS de Controle. Para ver exemplos AWS de políticas baseadas em identidade do Catálogo de Controle que você pode usar emIAM, consulte. Exemplos de políticas baseadas em identidade para AWS o Control Catalog

Autenticando com identidades

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

Você pode entrar em AWS como uma identidade federada usando credenciais fornecidas por meio de uma fonte de identidade. AWS IAM Identity Center Os usuários (do 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 entra como uma identidade federada, seu administrador configurou previamente a federação de identidades usando IAM funções. Quando você acessa AWS ao usar a federação, você está assumindo indiretamente uma função.

Dependendo do tipo de usuário que você é, você pode entrar no AWS Management Console ou o AWS portal de acesso. Para obter mais informações sobre como fazer login no AWS, veja Como fazer login no seu Conta da AWS no Início de Sessão da AWS Guia do 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 você mesmo assinar solicitações, consulte Assinatura AWS APIsolicitações no Guia do IAM usuário.

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

Conta da AWS usuário raiz

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

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, um provedor de identidade da web, o AWS Directory Service, o diretório do Identity Center ou qualquer usuário que acesse Serviços da AWS usando credenciais fornecidas por meio de uma fonte de identidade.

Quando as identidades federadas acessam Contas da AWS, eles assumem funções, e as funções fornecem credenciais temporárias.

Para gerenciamento de acesso centralizado, recomendamos que você use 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 todas as suas Contas da AWS e aplicativos. Para obter informações sobre o IAM Identity Center, consulte O que é o IAM Identity Center? no AWS IAM Identity Center Guia do usuário.

Grupos e usuários do IAM

Um IAMusuário é uma identidade dentro do seu Conta da AWS que tem permissões específicas para uma única pessoa ou aplicativo. Sempre que possível, recomendamos confiar em credenciais temporárias em vez de criar IAM usuários que tenham 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 IAM os usuários, recomendamos que você alterne as chaves de acesso. Para obter mais informações, consulte Alterne as chaves de acesso regularmente para casos de uso que exigem credenciais de longo prazo no Guia do IAMusuário.

Um IAMgrupo é uma identidade que especifica uma coleção de IAM usuários. 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 IAMAdminse conceder a esse grupo permissões para administrar IAM recursos.

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 IAM usuário (em vez de uma função) no Guia do IAM usuário.

IAMfunções

Um IAMpapel é uma identidade dentro de você Conta da AWS que tem permissões específicas. É semelhante a um IAM usuário, mas não está associado a uma pessoa específica. Você pode assumir temporariamente uma IAM função no AWS Management Console trocando de papéis. Você pode assumir uma função chamando um AWS CLI ou AWS APIoperação ou usando um personalizadoURL. Para obter mais informações sobre métodos de uso de funções, consulte Usando IAM funções no Guia IAM do usuário.

IAMfunções 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 informações sobre funções para federação, consulte Criação de uma função para um provedor de identidade terceirizado no Guia IAM do usuário. Se você usa o IAM Identity Center, configura 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 uma função em. IAM Para obter informações sobre conjuntos de permissões, consulte Conjuntos de permissões no AWS IAM Identity Center Guia do usuário.
- Permissões temporárias IAM de IAM usuário — Um usuário ou função pode assumir uma IAM função para assumir temporariamente permissões diferentes para uma tarefa específica.
- Acesso entre contas — Você pode usar uma IAM função para permitir que alguém (um diretor confiável) em uma conta diferente acesse recursos em sua conta. Os perfis são a principal forma de conceder acesso entre contas. No entanto, com alguns Serviços da AWS, você pode anexar uma política diretamente a um recurso (em vez de usar uma função como proxy). Para saber a diferença entre funções e políticas baseadas em recursos para acesso entre contas, consulte Acesso a recursos entre contas IAM no Guia do IAM usuário.
- Acesso entre serviços — Alguns Serviços da AWS use recursos em outros Serviços da AWS. Por exemplo, quando você faz uma chamada em um serviço, é comum que esse serviço execute aplicativos na Amazon EC2 ou armazene objetos no Amazon S3. Um serviço pode fazer isso usando as permissões do principal de chamada, usando um perfil de serviço ou um perfil vinculado a serviço.
  - Sessões de acesso direto (FAS) — Quando você usa um IAM usuário ou função para realizar ações no AWS, você é considerado um diretor. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. FASusa as permissões do diretor chamando um AWS service (Serviço da AWS), combinado com a solicitação AWS service (Serviço da AWS) para fazer solicitações para serviços posteriores. FASas solicitações são feitas somente quando um serviço recebe uma solicitação que requer interações com outros Serviços da AWS ou recursos para concluir. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer FAS solicitações, consulte Encaminhar sessões de acesso.
  - Função de serviço — Uma função de serviço é uma IAMfunção que um serviço assume para realizar ações em seu nome. Um IAM administrador pode criar, modificar e excluir uma função de serviço internamenteIAM. Para obter mais informações, consulte Criação de uma função para delegar permissões a um AWS service (Serviço da AWS) no IAM Guia do usuário.

  - Função vinculada a serviços — Uma função vinculada a serviços é um tipo de função de serviço vinculada a um AWS service (Serviço da AWS). O serviço pode assumir a função de realizar uma ação em seu nome. As funções vinculadas ao serviço aparecem em seu Conta da AWS e são de propriedade do serviço. Um IAM administrador pode visualizar, mas não editar, as permissões das funções vinculadas ao serviço.
- Aplicativos em execução na Amazon EC2 — Você pode usar uma IAM função para gerenciar credenciais temporárias para aplicativos que estão sendo executados em uma EC2 instância e fazendo AWS CLI ou AWS APIsolicitações. Isso é preferível ao armazenamento de chaves de acesso na EC2 instância. Para atribuir um AWS Ao atribuir a uma EC2 instância e disponibilizá-la para todos os seus aplicativos, você cria um perfil de instância que é anexado à instância. Um perfil de instância contém a função e permite que programas em execução na EC2 instância recebam credenciais temporárias. Para obter mais informações, consulte Como usar uma IAM função para conceder permissões a aplicativos executados em EC2 instâncias da Amazon no Guia IAM do usuário.

Para saber se usar IAM funções ou IAM usuários, consulte Quando criar uma IAM função (em vez de um usuário) no Guia do IAM usuário.

Gerenciando acesso usando políticas

Você controla o acesso em AWS criando políticas e anexando-as a AWS identidades ou recursos. Uma política é um objeto em AWS que, quando associados a uma identidade ou recurso, definem 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 em AWS como JSON documentos. Para obter mais informações sobre a estrutura e o conteúdo dos documentos de JSON política, consulte Visão geral das JSON políticas no Guia IAM do usuário.

Os administradores podem usar AWS JSONpolíticas 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 permissão aos usuários para realizar ações nos recursos de que precisam, um IAM administrador pode criar IAM políticas. O administrador pode então adicionar as IAM políticas às funções e os usuários podem assumir as funções.

IAMas políticas definem permissões para uma ação, independentemente do método usado para realizar 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 do AWS Management Console, o AWS CLI, ou o AWS API.

Políticas baseadas em identidade

Políticas baseadas em identidade são documentos de políticas de JSON permissões que você pode anexar a uma identidade, como um IAM usuário, grupo de usuários ou função. 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 IAM políticas no Guia do IAMusuário.

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

Políticas baseadas no recurso

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

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

Listas de controle de acesso (ACLs)

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

Amazon S3, AWS WAF, e a Amazon VPC são exemplos de serviços que oferecem suporteACLs. Para saber maisACLs, consulte a 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 recurso avançado no qual você define as permissões máximas que uma política baseada em identidade pode conceder a uma IAM entidade (IAMusuário ou função). É possível definir um limite de permissões para uma entidade. As permissões resultantes são a interseção das políticas baseadas em identidade de uma entidade com seus limites de permissões. As políticas baseadas em recurso que especificam o usuário ou o perfil no campo `Principal` não são limitadas pelo limite de permissões. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações sobre limites de permissões, consulte Limites de permissões para IAM entidades no Guia IAM do usuário.
- Políticas de controle de serviço (SCPs) — SCPs são JSON políticas 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 recursos em uma organização, poderá aplicar políticas de controle de serviço (SCPs) a qualquer uma ou a todas as suas contas. Os SCP limites de permissões para entidades em contas de membros, incluindo cada Usuário raiz da conta da AWS. Para obter mais informações sobre Organizations eSCPs, consulte Políticas de controle de serviços no AWS Organizations Guia do usuário.
- Políticas de sessão: são políticas avançadas que você transmite como um parâmetro quando cria de forma programática uma sessão temporária para um perfil ou um usuário federado. As permissões da sessão resultante são a interseção das políticas baseadas em identidade do usuário ou do perfil e das políticas de sessão. As permissões também podem ser provenientes de uma política baseada em atributo. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações, consulte Políticas de sessão no Guia IAM do usuário.

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 determina se uma solicitação deve ser permitida quando vários tipos de política estão envolvidos, consulte Lógica de avaliação de políticas no Guia IAM do usuário.

Como o AWS Control Catalog funciona com IAM

Antes de usar IAM para gerenciar o acesso ao AWS Control Catalog, saiba quais IAM recursos estão disponíveis para uso com o AWS Control Catalog.

IAMrecursos que você pode usar com o AWS Control Catalog

IAMrecurso	AWSSuporte ao Control Catalog
Políticas baseadas em identidade	Sim
Políticas baseadas em recursos	Não
Ações das políticas	Sim
Atributos de políticas	Sim
Chaves de condição de políticas	Sim
ACLs	Não
ABAC(tags nas políticas)	Não
Credenciais temporárias	Sim
Permissões de entidade principal	Não
Perfis de serviço	Não
Funções vinculadas ao serviço	Não

Para obter uma visão de alto nível de como AWS Controlar o Catálogo e outros AWS os serviços funcionam com a maioria dos IAM recursos, consulte AWS serviços que funcionam com IAM o Guia IAM do Usuário.

Políticas baseadas em identidade para AWS o Control Catalog

Compatível com políticas baseadas em identidade: Sim

Políticas baseadas em identidade são documentos de políticas de JSON permissões que você pode anexar a uma identidade, como um IAM usuário, grupo de usuários ou função. 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 IAM políticas no Guia do IAMusuário.

Com políticas IAM baseadas em identidade, você pode especificar ações e 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 perfil ao qual ela está anexada. Para saber mais sobre todos os elementos que você pode usar em uma JSON política, consulte a referência IAM JSON de elementos de política no Guia IAM do usuário.

Exemplos de políticas baseadas em identidade para AWS o Control Catalog

Para ver exemplos de políticas baseadas em identidade do AWS Control Catalog, consulte. Exemplos de políticas baseadas em identidade para AWS o Control Catalog

Políticas baseadas em recursos no Control Catalog AWS

Suporte a políticas baseadas em recursos: não

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

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

Ações de política para o AWS Control Catalog

Compatível com ações de políticas: Sim

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

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

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

Para ver uma lista de ações do AWS Control Catalog, consulte Ações definidas pelo AWS Control Catalog na Referência de Autorização de Serviço.

As ações de política no Catálogo de AWS Controle usam o seguinte prefixo antes da ação:

```
controlcatalog
```

Para especificar várias ações em uma única instrução, separe-as com vírgulas.

```
"Action": [
      "controlcatalog:ListCommonControls",
      "controlcatalog:ListDomains"
         ]
```

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

```
"Action": "controlcatalog:List*"
```

Para ver exemplos de políticas baseadas em identidade do AWS Control Catalog, consulte. Exemplos de políticas baseadas em identidade para AWS o Control Catalog

Recursos de políticas para o AWS Control Catalog

Compatível com recursos de políticas: Sim

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

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

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

Para ver uma lista dos tipos de recursos do AWS Control Catalog e seusARNs, consulte Recursos definidos pelo AWS Control Catalog na Referência de Autorização de Serviço. Para saber com quais ações você pode especificar cada recurso, consulte Ações definidas pelo Catálogo AWS de Controle. ARN

Um domínio do AWS Control Catalog tem o seguinte formato Amazon Resource Name (ARN):

```
arn:${Partition}:controlcatalog:::domain/${domainId}
```

Um objetivo do Catálogo de AWS Controle tem o seguinte ARN formato:

```
arn:${Partition}:controlcatalog:::objective/${objectiveId}
```

Um AWS controle comum do Catálogo de Controle tem o seguinte ARN formato:

```
arn:${Partition}:controlcatalog:::commonControl/${commonControlId}
```

Para obter mais informações sobre o formato deARNs, consulte Amazon Resource Names (ARNs).

Por exemplo, para especificar o `i-1234567890abcdef0` domínio em sua declaração, use o seguinteARN.

```
"Resource": "arn:aws:controlcatalog:::domain/i-1234567890abcdef0"
```

Para especificar todas as instâncias que pertencem a uma conta específica, use o caractere curinga (*).

```
"Resource": "arn:aws:controlcatalog:::domain/*"
```

Algumas ações do Catálogo de AWS Controle, como aquelas para criar recursos, não podem ser executadas em um recurso específico. Nesses casos, você deve utilizar o caractere curinga (*).

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

Algumas API ações AWS do Control Catalog oferecem suporte a vários recursos. Por exemplo, `ListCommonControls` acessa um controle comum, um objetivo e um domínio, portanto, o diretor deve ter permissões para acessar cada um desses recursos. Para especificar vários recursos em uma única instrução, separe-os ARNs com vírgulas.

```
"Resource": [
      "commonControl",
      "objective",
      "domain"
```

Para ver exemplos de políticas baseadas em identidade do AWS Control Catalog, consulte. Exemplos de políticas baseadas em identidade para AWS o Control Catalog

Chaves de condição de política para o AWS Control Catalog

Compatível com chaves de condição de política específicas de serviço: Sim

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

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

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

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

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

Para ver uma lista das chaves de condição do AWS Control Catalog, consulte Chaves de condição do AWS Control Catalog na Referência de Autorização de Serviço. Para saber com quais ações e recursos você pode usar uma chave de condição, consulte Ações definidas pelo Catálogo AWS de Controle.

Para ver exemplos de políticas baseadas em identidade do AWS Control Catalog, consulte. Exemplos de políticas baseadas em identidade para AWS o Control Catalog

ACLsno Catálogo AWS de Controle

SuportesACLs: Não

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

ABACcom o AWS Control Catalog

Suportes ABAC (tags nas políticas): Não

O controle de acesso baseado em atributos (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 IAM entidades (usuários ou funções) e a muitas AWS recursos. Marcar entidades e recursos é a primeira etapa doABAC. Em seguida, você cria ABAC políticas para permitir operações quando a tag do diretor corresponde à tag do recurso que ele está tentando acessar.

ABACé útil em ambientes que estão crescendo rapidamente e ajuda em situações em que o gerenciamento de políticas se torna complicado.

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

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

Para obter mais informações sobreABAC, consulte O que éABAC? no Guia do IAM usuário. Para ver um tutorial com etapas de configuraçãoABAC, consulte Usar controle de acesso baseado em atributos (ABAC) no Guia do IAMusuário.

Usando credenciais temporárias com o AWS Control Catalog

Compatível com credenciais temporárias: Sim

Alguns Serviços da AWS não funcionam quando você faz login usando credenciais temporárias. Para obter informações adicionais, incluindo quais Serviços da AWS trabalhar com credenciais temporárias, consulte Serviços da AWS que funcionam com IAM o Guia IAM do Usuário.

Você está usando credenciais temporárias se fizer login no 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 a troca de funções, consulte Alternando para uma função (console) no Guia IAM do usuário.

Você pode criar manualmente credenciais temporárias usando o AWS CLI ou AWS API. Você pode então 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 emIAM.

Permissões principais entre serviços para o AWS Control Catalog

Suporta sessões de acesso direto (FAS): Não

Quando você usa um IAM usuário ou uma função para realizar ações no AWS, você é considerado um diretor. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. FASusa as permissões do diretor chamando um AWS service (Serviço da AWS), combinado com a solicitação AWS service (Serviço da AWS) para fazer solicitações para serviços posteriores. FASas solicitações são feitas somente quando um serviço recebe uma solicitação que requer interações com outros Serviços da AWS ou recursos para concluir. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer FAS solicitações, consulte Encaminhar sessões de acesso.

Funções de serviço para o AWS Control Catalog

Compatível com perfis de serviço: não

Uma função de serviço é uma IAMfunção que um serviço assume para realizar ações em seu nome. Um IAM administrador pode criar, modificar e excluir uma função de serviço internamenteIAM. Para obter mais informações, consulte Criação de uma função para delegar permissões a um AWS service (Serviço da AWS) no IAM Guia do usuário.

> **Warning**
>
> Alterar as permissões de uma função de serviço pode interromper a funcionalidade do Catálogo de AWS Controle. Edite as funções de serviço somente quando AWS o Control Catalog fornecer orientação para fazer isso.

Funções vinculadas a serviços para AWS o Control Catalog

Compatível com perfis vinculados ao serviço: Não

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 realizar uma ação em seu nome. As funções vinculadas ao serviço aparecem em seu Conta da AWS e são de propriedade do serviço. Um IAM administrador pode visualizar, mas não editar, as permissões das funções vinculadas ao serviço.

Para obter detalhes sobre a criação ou o gerenciamento de funções vinculadas ao serviço, consulte AWS serviços que funcionam com IAM. Encontre um serviço na tabela que inclua um `Yes` na coluna

Função vinculada ao serviço. Escolha o link Sim para visualizar a documentação do perfil vinculado a serviço desse serviço.

Exemplos de políticas baseadas em identidade para AWS o Control Catalog

Por padrão, usuários e funções não têm permissão para criar ou modificar recursos do Catálogo de AWS Controle. Eles também não podem realizar tarefas usando o AWS Management Console, AWS Command Line Interface (AWS CLI), ou AWS API. Para conceder permissão aos usuários para realizar ações nos recursos de que precisam, um IAM administrador pode criar IAM políticas. O administrador pode então adicionar as IAM políticas às funções e os usuários podem assumir as funções.

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

Para obter detalhes sobre ações e tipos de recursos definidos pelo Catálogo de AWS Controle, incluindo o formato do ARNs para cada um dos tipos de recursos, consulte Ações, recursos e chaves de condição para o Catálogo de AWS Controle na Referência de Autorização de Serviço.

Tópicos

- Melhores práticas de política
- Permitir que usuários visualizem suas próprias permissões
- Permitir que os usuários visualizem recursos do Catálogo AWS de Controle

Melhores práticas de política

As políticas baseadas em identidade determinam se alguém pode criar, acessar ou excluir recursos do Catálogo AWS de Controle em sua conta. Essas ações podem incorrer em custos para o seu Conta da AWS. Ao criar ou editar políticas baseadas em identidade, siga estas diretrizes e recomendações:

- Comece com AWS políticas gerenciadas e migrar para permissões com privilégios mínimos — Para começar a conceder permissões para seus usuários e cargas de trabalho, use o AWS políticas gerenciadas que concedem permissões para muitos casos de uso comuns. Eles estão disponíveis em seu Conta da AWS. Recomendamos que você reduza ainda mais as permissões definindo AWS políticas gerenciadas pelo cliente que são específicas para seus casos de uso.

Para ter mais informações, consulte AWS políticas gerenciadas ou AWS políticas gerenciadas para funções de trabalho no Guia IAM do usuário.

- Aplique permissões com privilégios mínimos — Ao definir permissões com IAM políticas, conceda somente as permissões necessárias para realizar uma tarefa. Você faz isso definindo as ações que podem ser executadas em atributos específicos sob condições específicas, também conhecidas como permissões de privilégio mínimo. Para obter mais informações sobre IAM como usar para aplicar permissões, consulte Políticas e permissões IAM no Guia IAM do usuário.
- Use condições nas IAM políticas para restringir ainda mais o acesso — Você pode adicionar uma condição às suas 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 usandoSSL. Você também pode usar condições para conceder acesso às ações de serviço se elas forem usadas por meio de um determinado AWS service (Serviço da AWS), por exemplo, AWS CloudFormation. Para obter mais informações, consulte elementos IAM JSON da política: Condição no Guia IAM do usuário.
- Use o IAM Access Analyzer para validar suas IAM políticas e garantir permissões seguras e funcionais — o IAM Access Analyzer valida políticas novas e existentes para que as políticas sigam a linguagem da IAM política (JSON) e as melhores práticas. IAM IAMO Access Analyzer fornece mais de 100 verificações de políticas e recomendações práticas para ajudá-lo a criar políticas seguras e funcionais. Para obter mais informações, consulte Validação da política do IAM Access Analyzer no Guia do IAM Usuário.
- Exigir autenticação multifatorial (MFA) — Se você tiver um cenário que exija IAM usuários ou um usuário root em seu Conta da AWS, ative MFA para obter segurança adicional. Para exigir MFA quando API as operações são chamadas, adicione MFA condições às suas políticas. Para obter mais informações, consulte Configurando o API acesso MFA protegido no Guia do IAMusuário.

Para obter mais informações sobre as melhores práticas emIAM, consulte as melhores práticas de segurança IAM no Guia IAM do usuário.

Permitir que usuários visualizem suas próprias permissões

Este exemplo mostra como você pode criar uma política que permita IAM aos usuários visualizar as políticas embutidas e gerenciadas que estão anexadas à identidade do usuário. Essa política inclui permissões para concluir essa ação no console ou programaticamente usando o AWS CLI ou AWS API.

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

Permitir que os usuários visualizem recursos do Catálogo AWS de Controle

A política a seguir concede permissões para listar domínios, objetivos e controles comuns do Catálogo de AWS Controle.

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

```
                "controlcatalog:ListDomains",
                "controlcatalog:ListObjectives",
                "controlcatalog:ListCommonControls"
            ],
            "Resource": "*"
        }
    ]
}
```

Solução de problemas AWS de identidade e acesso ao Control Catalog

Use as informações a seguir para ajudá-lo a diagnosticar e corrigir problemas comuns que você pode encontrar ao trabalhar com o AWS Control Catalog e. IAM

Tópicos

- Não estou autorizado a realizar uma ação no Catálogo AWS de Controle
- Não estou autorizado a realizar iam: PassRole
- Quero permitir que pessoas fora da minha Conta da AWS para acessar meus recursos do AWS Control Catalog

Não estou autorizado a realizar uma ação no Catálogo AWS de Controle

Se você receber uma mensagem de erro informando que não tem autorização para executar uma ação, é preciso atualizar suas políticas para permitir que você realize a ação.

O exemplo de erro a seguir ocorre quando o `mateojackson` IAM usuário tenta usar o console para ver detalhes sobre um *`my-example-widget`* recurso fictício, mas não tem as permissões fictícias`controlcatalog:`*`GetWidget`*.

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

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

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

Não estou autorizado a realizar iam: PassRole

Se você receber um erro informando que não está autorizado a realizar a `iam:PassRole` ação, suas políticas devem ser atualizadas para permitir que você passe uma função para o Catálogo AWS de Controle.

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

O exemplo de erro a seguir ocorre quando um IAM usuário chamado `marymajor` tenta usar o console para realizar uma ação no Catálogo AWS de Controle. No entanto, a ação exige que o serviço tenha permissões concedidas por um perfil de serviço. Mary não tem permissões para passar o perfil para o serviço.

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

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

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

Quero permitir que pessoas fora da minha Conta da AWS para acessar meus recursos do AWS Control Catalog

Você pode criar um perfil 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 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 AWS Control Catalog oferece suporte a esses recursos, consulteComo o AWS Control Catalog funciona com IAM.
- Para saber como fornecer acesso aos seus recursos em Contas da AWS que você possui, consulte Fornecendo acesso a um IAM usuário em outro Conta da AWS que você possui no Guia do IAM Usuário.

- Para saber como fornecer acesso aos seus recursos a terceiros Contas da AWS, consulte Fornecendo acesso a Contas da AWS propriedade de terceiros no Guia do IAM Usuário.
- Para saber como fornecer acesso por meio da federação de identidades, consulte Fornecendo acesso a usuários autenticados externamente (federação de identidades) no Guia do IAMusuário.
- Para saber a diferença entre usar funções e políticas baseadas em recursos para acesso entre contas, consulte Acesso a recursos entre contas IAM no Guia do IAM usuário.

Validação de conformidade para o AWS Control Catalog

Para saber se um AWS service (Serviço da AWS) está dentro do escopo de programas de conformidade específicos, consulte Serviços da AWS no escopo do Programa de Conformidade e escolha o programa de conformidade no qual você está interessado. Para obter informações gerais, consulte AWS Programas de conformidade .

Você pode baixar relatórios de auditoria de terceiros usando AWS Artifact. Para obter mais informações, consulte Baixando relatórios em AWS Artifact.

Sua responsabilidade de conformidade ao usar Serviços da AWS é determinado pela confidencialidade de seus dados, pelos objetivos de conformidade da sua empresa e pelas leis e regulamentações aplicáveis. AWS fornece os seguintes recursos para ajudar na conformidade:

- Guias de início rápido sobre segurança e conformidade — Esses guias de implantação discutem considerações arquitetônicas e fornecem etapas para a implantação de ambientes básicos em AWS que se concentram na segurança e na conformidade.
- Arquitetura para HIPAA segurança e conformidade na Amazon Web Services — Este whitepaper descreve como as empresas podem usar AWS para criar HIPAA aplicativos elegíveis.

> **Note**
>
> Nem todos Serviços da AWS são HIPAA elegíveis. Para obter mais informações, consulte a Referência de serviços HIPAA elegíveis.

- AWS Recursos 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 mapeie a orientação para controles de segurança em várias estruturas (incluindo Instituto

Nacional de Padrões e Tecnologia (NIST), Conselho de Padrões de Segurança do Setor de Cartões de Pagamento (PCI) e Organização Internacional de Padronização (ISO)).

- Avaliando recursos com regras no AWS Config Guia do desenvolvedor — O AWS Config O serviço avalia o quão bem suas configurações de recursos estão em conformidade com as práticas internas, as diretrizes do setor e os regulamentos.
- AWS Security Hub— Isso AWS service (Serviço da AWS) fornece uma visão abrangente do seu estado de segurança em AWS. O Security Hub usa controles de segurança para avaliar sua AWS recursos e para verificar sua conformidade com os padrões e as melhores práticas do setor de segurança. Para obter uma lista dos serviços e controles aceitos, consulte a Referência de controles do Security Hub.
- Amazon GuardDuty — Isso AWS service (Serviço da AWS) detecta possíveis ameaças ao seu Contas da AWS, cargas de trabalho, contêineres e dados monitorando seu ambiente em busca de atividades suspeitas e maliciosas. GuardDuty pode ajudá-lo a atender a vários requisitos de conformidade, por exemplo PCIDSS, atendendo aos requisitos de detecção de intrusões exigidos por determinadas estruturas de conformidade.
- AWS Audit Manager— Isso AWS service (Serviço da AWS) ajuda você a auditar continuamente seu AWS uso para simplificar a forma como você gerencia o risco e a conformidade com as regulamentações e os padrões do setor.

Resiliência em AWS Catálogo de controle

A ferramenta AWS a infraestrutura global é construída em torno de Regiões da AWS e zonas de disponibilidade. Regiões da AWS fornecem várias zonas de disponibilidade fisicamente separadas e isoladas, conectadas a redes de baixa latência, alta taxa de transferência e alta redundância. Com as zonas de disponibilidade, é possível projetar e operar aplicativos e bancos de dados que automaticamente executam o failover entre as zonas sem interrupção. As zonas de disponibilidade são mais altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de data center tradicionais.

Para obter mais informações sobre Regiões da AWS e zonas de disponibilidade, consulte AWS Infraestrutura global.

Segurança de infraestrutura no catálogo AWS de controle

Como um serviço gerenciado, AWS o Control Catalog é protegido pelo AWS procedimentos globais de segurança de rede descritos no whitepaper Amazon Web Services: Visão geral dos processos de segurança.

Você usa AWS APIchamadas publicadas para acessar AWS o Catálogo de Controle pela rede. Os clientes devem oferecer suporte ao Transport Layer Security (TLS) 1.0 ou posterior. Recomendamos TLS 1.2 ou posterior. Os clientes também devem oferecer suporte a pacotes de criptografia com sigilo direto perfeito (), como (Ephemeral Diffie-HellmanPFS) ou DHE (Elliptic Curve Ephemeral Diffie-Hellman). ECDHE A maioria dos sistemas modernos, como Java 7 e versões posteriores, comporta esses modos.

Além disso, as solicitações devem ser assinadas usando uma ID de chave de acesso e uma chave de acesso secreta associada a um IAM principal. Ou você pode usar o AWS Security Token Service (AWS STS) para gerar credenciais de segurança temporárias para assinar solicitações.

Análise de configuração e vulnerabilidade em AWS Catálogo de controle

A configuração e os controles de TI são uma responsabilidade compartilhada entre AWS e você, nosso cliente. Para obter mais informações, consulte o AWS modelo de responsabilidade compartilhada.

Monitorando o AWS Control Catalog

O monitoramento é uma parte importante da manutenção da confiabilidade, disponibilidade e desempenho do AWS Control Catalog e de suas outras AWS soluções. AWS fornece as seguintes ferramentas de monitoramento para monitorar o AWS Control Catalog, relatar quando algo está errado e realizar ações automáticas quando apropriado:

- AWS CloudTrailcaptura chamadas de API e eventos relacionados feitos por ou em nome de sua AWS conta e entrega os arquivos de log para um bucket do Amazon S3 que você especificar. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem a partir do qual as chamadas foram feitas e quando elas ocorreram. Para obter mais informações, consulte o Guia do usuário da AWS CloudTrail.

Registro de chamadas de API do AWS Control Catalog usando AWS CloudTrail

O AWS Control Catalog é integrado com AWS CloudTrail um serviço que fornece um registro das ações realizadas por um usuário, função ou AWS serviço no AWS Control Catalog. CloudTrail captura todas as chamadas de API para o AWS Control Catalog como eventos. As chamadas capturadas incluem chamadas do console do AWS Control Catalog e chamadas de código para as operações da API do AWS Control Catalog. Se você criar uma trilha, poderá habilitar a entrega contínua de CloudTrail eventos para um bucket do Amazon S3, incluindo eventos para o AWS Control Catalog. 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 AWS Control Catalog, o endereço IP a partir do qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita e detalhes adicionais.

Para saber mais CloudTrail, consulte o Guia AWS CloudTrail do usuário.

Informações do AWS Control Catalog em CloudTrail

CloudTrail é ativado no seu Conta da AWS quando você cria a conta. Quando a atividade ocorre no AWS Control Catalog, essa atividade é registrada em um CloudTrail evento junto com outros eventos AWS de serviço no histórico de eventos. Você pode visualizar, pesquisar e baixar eventos recentes no seu Conta da AWS. Para obter mais informações, consulte Visualização de eventos com histórico de CloudTrail eventos.

Para obter um registro contínuo dos eventos em seu Conta da AWS, incluindo eventos do AWS Control Catalog, 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 AWS serviços para analisar e agir com base nos dados de eventos coletados nos CloudTrail registros. Para mais informações, consulte:

- Visão geral da criação de uma trilha
- CloudTrail serviços e integrações suportados
- 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 AWS Control Catalog são registradas CloudTrail e documentadas na AWS Control Catalog API Reference. . Por exemplo, chamadas para as `ListDomains` ações `ListCommonControlsListObjectives`, e 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 root ou AWS Identity and Access Management (IAM).
- Se a solicitação foi feita com credenciais de segurança temporárias de um perfil ou de um usuário federado.
- Se a solicitação foi feita por outro AWS serviço.

Para obter mais informações, consulte o elemento CloudTrail userIdentity.

Compreendendo as entradas do arquivo de log do AWS Control Catalog

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 `ListDomains` 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:"controlcatalog.amazonaws.com",
      eventName:"ListDomains",
      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: null,
      responseElements: null,
      requestID:"0d950f8c-5211-40db-8c37-2ed38ffcc894",
      eventID:"a782029a-959e-4549-81df-9f6596775cb0",
      readOnly:false,
      eventType:"AwsApiCall",
      recipientAccountId:"recipientAccountId"
}
```

Catálogo AWS de controle de acesso usando um endpoint de interface ()AWS PrivateLink

Você pode usar AWS PrivateLink para criar uma conexão privada entre você VPC e o AWS Control Catalog. Você pode acessar o Catálogo de AWS Controle como se estivesse no seuVPC, sem o uso de um gateway de internet, NAT dispositivo, VPN conexão ou AWS Direct Connect conexão. As instâncias em seu VPC não precisam de endereços IP públicos para acessar o Catálogo AWS de Controle.

Você estabelece essa conectividade privada criando um endpoint de interface, desenvolvido pelo AWS PrivateLink. Criaremos um endpoint de interface de rede em cada sub-rede que você habilitar para o endpoint de interface. Essas são interfaces de rede gerenciadas pelo solicitante que servem como ponto de entrada para o tráfego destinado ao Control Catalog. AWS

Para obter mais informações, consulte Acesso Serviços da AWS por meio AWS PrivateLink do AWS PrivateLink Guia.

Considerações sobre o AWS Control Catalog

Antes de configurar um endpoint de interface para o AWS Control Catalog, revise Considerações no AWS PrivateLink Guia.

AWS O Control Catalog suporta a realização de chamadas para todas as suas API ações por meio do endpoint da interface.

Crie um endpoint de interface para o AWS Control Catalog

Você pode criar um endpoint de interface para o AWS Control Catalog usando o VPC console da Amazon ou o AWS Command Line Interface (AWS CLI). Para obter mais informações, consulte Criar um endpoint de interface no Guia do usuário do AWS PrivateLink .

Crie um endpoint de interface para o AWS Control Catalog usando o seguinte nome de serviço:

```
com.amazonaws.region.controlcatalog
```

Se você habilitar privado DNS para o endpoint da interface, poderá fazer API solicitações ao AWS Control Catalog usando seu DNS nome regional padrão. Por exemplo, `service-name.us-east-1.amazonaws.com`.

Crie uma política de endpoint para seu endpoint de interface.

Uma política de endpoint é um IAM recurso que você pode anexar a um endpoint de interface. A política de endpoint padrão permite acesso total ao AWS Control Catalog por meio do endpoint da interface. Para controlar o acesso permitido ao Catálogo de AWS Controle a partir do seuVPC, anexe uma política de endpoint personalizada ao endpoint da interface.

Uma política de endpoint especifica as seguintes informações:

- Os diretores que podem realizar ações (Contas da AWS, IAM usuários e IAM funções).
- As ações que podem ser executadas.
- Os recursos nos quais as ações podem ser executadas.

Para obter mais informações, consulte Controlar o Acesso a Serviços Usando Políticas de Endpoint no AWS PrivateLink Guia.

Exemplo: política de VPC endpoint para ações do AWS Control Catalog

O exemplo a seguir refere-se a uma política de endpoint personalizada. Quando você anexa essa política ao seu endpoint de interface, ela concede acesso às ações listadas do Catálogo AWS de Controle para todos os diretores em todos os recursos.

```
{
   "Statement": [
      {
         "Principal": "*",
         "Effect": "Allow",
         "Action": [
            "controlcatalog:ListDomains",
            "controlcatalog:ListObjectives",
            "controlcatalog:ListCommonControls"
         ],
         "Resource":"*"
      }
   ]
}
```

> **Note**
>
> As `ListControls` API operações `GetControl` e exigem uma permissão diferente, a permissão total padrão. Para ver um exemplo, consulte a política de endpoint padrão. Não há suporte para outras AWS Control Tower API operações AWS PrivateLink.

Histórico de documentos do guia de informações de segurança do AWS Control Catalog

A tabela a seguir descreve as versões da documentação do AWS Control Catalog.

Alteração	Descrição	Data
Lançamento inicial	Versão inicial das APIs do AWS Control Catalog e do guia de informações de segurança.	8 de abril de 2024

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.