Guia do usuário

AWS Configuração

AWS Configuração: Guia do usuário

Table of Contents

Visão geral

Este guia fornece instruções para criar um novo Conta da AWS e configurar seu primeiro usuário administrativo Centro de Identidade do AWS IAM seguindo as práticas recomendadas de segurança mais recentes.

Conta da AWS É necessário um para acessar Serviços da AWS e serve como duas funções básicas:

- Contêiner — Um Conta da AWS é um contêiner para todos os AWS recursos que você pode criar como AWS cliente. Quando você cria um bucket do Amazon Simple Storage Service (Amazon S3) ou um banco de dados do Amazon Relational Database Service (Amazon RDS) para armazenar seus dados, ou uma instância do Amazon Elastic Compute Cloud EC2 (Amazon) para processar seus dados, você está criando um recurso em sua conta. Cada recurso é identificado exclusivamente por um nome do recurso da Amazon (ARN) que inclui o ID da conta que contém ou possui o recurso.
- Limite de segurança — An Conta da AWS é o limite básico de segurança para seus AWS recursos. Os recursos que você cria em sua conta estão disponíveis somente para usuários que tenham credenciais para essa mesma conta.

  Entre os principais recursos que você pode criar em sua conta estão identidades, como usuários e funções do IAM, e identidades federadas, como usuários do diretório de usuários corporativo, um provedor de identidade da web, o diretório do IAM Identity Center ou qualquer outro usuário que acesse usando credenciais fornecidas Serviços da AWS por meio de uma fonte de identidade. Essas identidades têm credenciais que alguém pode usar para fazer login ou se autenticar na AWS. As identidades também têm políticas de permissão que especificam o que a pessoa que fez login está autorizada a fazer com os recursos da conta.

Terminologia

A Amazon Web Services (AWS) usa terminologia comum para descrever o processo de login. Recomendamos que você leia e compreenda esses termos.

Administrador

Também conhecido como Conta da AWS administrador ou administrador do IAM. O administrador, normalmente o pessoal de Tecnologia da Informação (TI), é um indivíduo que supervisiona uma Conta da AWS. Os administradores têm um nível mais alto de permissões na Conta da AWS do que outros membros de sua organização. Os administradores estabelecem e implementam configurações para o. Conta da AWS Eles também criam usuários do IAM ou do IAM Identity Center. O administrador fornece a esses usuários suas credenciais de acesso e uma URL de login para acessar a AWS.

Conta

Um padrão Conta da AWS contém seus AWS recursos e as identidades que podem acessar esses recursos. As contas são associadas ao endereço de e-mail e à senha do proprietário da conta.

Credenciais

Também chamado de credenciais de acesso ou credenciais de segurança. As credenciais são as informações que os usuários fornecem AWS para entrar e obter acesso aos AWS recursos. As credenciais podem incluir um endereço de e-mail, um nome de usuário, uma senha definida pelo usuário, um ID de conta ou alias, um código de verificação e um código de autenticação multifator (MFA) de uso único. Em autenticação e autorização, um sistema usa credenciais para identificar quem está fazendo uma chamada e se irá permitir o acesso solicitado. Em AWS, essas credenciais geralmente são o ID da chave de acesso e a chave de acesso secreta.

Para obter mais informações sobre credenciais, consulte Compreender e obter as credenciais da AWS.

> **Note**
>
> O tipo de credenciais que um usuário deve enviar depende do seu tipo de usuário.

Credenciais corporativas

As credenciais que os usuários fornecem ao acessar a rede e seus recursos corporativos. Seu administrador corporativo pode configurar seu Conta da AWS acesso com as mesmas credenciais que você usa para acessar sua rede e seus recursos corporativos. Essas credenciais são fornecidas a você pelo administrador ou funcionário do suporte técnico.

Perfil

Ao se inscrever para obter um AWS Builder ID, você cria um perfil. O perfil inclui as informações de contato fornecidas, a capacidade de gerenciar dispositivos de autenticação multifator (MFA), e sessões ativas. Você também pode aprender mais sobre privacidade e como lidamos com seus dados em seu perfil. Para obter mais informações sobre seu perfil e como ele se relaciona com um Conta da AWS, consulte AWS Builder ID e outras AWS credenciais.

Usuário

Um usuário é uma pessoa ou aplicação em uma conta que precisa fazer chamadas de API para produtos da AWS . Cada usuário tem um nome exclusivo Conta da AWS e um conjunto de credenciais de segurança que não são compartilhadas com outras pessoas. Essas credenciais são separadas de credenciais de segurança da conta da Conta da AWS. Cada usuário está associado a uma única Conta da AWS.

Credenciais do usuário raiz.

As credenciais do usuário raiz são as mesmas usadas para entrar no Console de gerenciamento da AWS como usuário raiz. Para obter mais informações sobre o usuário raiz, consulte Usuário raiz.

Código de verificação

Um código de verificação verifica sua identidade durante o processo de login usando autenticação multifator (MFA). Os métodos de entrega dos códigos de verificação variam. Eles podem ser enviados por mensagem de texto ou e-mail. Para obter mais informações, consulte o administrador.

AWS usuários e credenciais

Ao interagir com AWS, você especifica suas credenciais de AWS segurança para verificar quem você é e se tem permissão para acessar os recursos que está solicitando. AWS usa credenciais de segurança para autenticar e autorizar solicitações.

Por exemplo, se você quiser baixar um arquivo protegido de um bucket do Amazon Simple Storage Service (Amazon S3), suas credenciais devem permitir esse acesso. Se suas credenciais mostrarem que você não está autorizado a baixar o arquivo, AWS nega sua solicitação. Porém, as credenciais de segurança não são obrigatórias para baixar um arquivo em buckets do Amazon S3 compartilhados publicamente.

Usuário raiz

Também conhecido como proprietário da conta ou usuário raiz da conta. Como usuário root, você tem acesso completo a todos os AWS serviços e recursos do seu Conta da AWS. Ao criar um Conta da AWS, você começa com uma identidade de login único que tem acesso completo a todos os AWS serviços e recursos da conta. Essa identidade é o usuário raiz da AWS conta. Você pode fazer login no Console de gerenciamento da AWS como usuário raiz usando o endereço de e-mail e a senha que usou para criar a conta. Para obter instruções passo a passo sobre como fazer login, consulte Fazer login no Console de gerenciamento da AWS como usuário root.

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

Para obter mais informações sobre as identidades do IAM incluindo o usuário raiz, consulte Identidades do IAM (usuários, grupos de usuários e perfis).

Usuários do IAM Identity Center

Um usuário do IAM Identity Center faz login por meio do portal de AWS acesso. O portal de AWS acesso ou URL de login específico é fornecido pelo administrador ou funcionário do suporte técnico. Se você criou um usuário do Centro de Identidade do IAM para a sua Conta da AWS, um convite para ingressar no usuário do Centro de Identidade do IAM foi enviado para o endereço de e-mail da Conta da AWS. O URL de login específico está incluído no convite por e-mail. Os usuários do IAM Identity Center não podem fazer login por meio do Console de gerenciamento da AWS. Para obter instruções passo a passo sobre como fazer login, consulte Entrar no portal de AWS acesso.

> **Note**
>
> Recomendamos que você adicione aos favoritos a URL de login específica do portal de AWS acesso para que você possa acessá-la rapidamente mais tarde.

Para obter mais informações sobre o Centro de Identidade do IAM, consulte O que é o Centro de Identidade do IAM?.

Identidade federada

Uma identidade federada é um usuário que pode fazer login usando um provedor de identidades (IdP) externo como Login with Amazon, Facebook, Google ou qualquer outro IdP compatível com OpenID Connect (OIDC). Com a federação de identidade da web, você pode receber um token de autenticação e depois trocar esse token por credenciais de segurança temporárias AWS nesse mapa para uma função do IAM com permissões para usar os recursos em seu Conta da AWS. Você não entra com o portal Console de gerenciamento da AWS ou AWS acessa. Em vez disso, a identidade externa em uso determina como você faz login.

Para obter mais informações, consulte Fazer login como uma identidade federada.

IAM user (Usuário do IAM)

Um usuário do IAM é uma entidade que você cria em AWS. Esse usuário é uma identidade dentro da sua Conta da AWS que recebe permissões personalizadas específicas. Suas credenciais de usuário do IAM consistem em um nome e senha usados para fazer login no Console de gerenciamento da AWS. Para obter instruções passo a passo sobre como fazer login, consulte Fazer login no Console de gerenciamento da AWS como usuário do IAM.

Para obter mais informações sobre as identidades do IAM incluindo o usuário do IAM, consulte Identidades do IAM (usuários, grupos de usuários e perfis).

AWS Usuário Builder ID

Como usuário do AWS Builder ID, você entra especificamente no AWS serviço ou na ferramenta que deseja acessar. Um usuário do AWS Builder ID complementa qualquer um Conta da AWS que você já tenha ou queira criar. Um AWS Builder ID representa você como pessoa, e você pode usá-lo para acessar AWS serviços e ferramentas sem um Conta da AWS. Você também tem um perfil onde pode ver e atualizar suas informações. Para obter mais informações, consulte Para fazer login com o AWS Builder ID.

Pré-requisitos e considerações

Antes de começar o processo de configuração, analise os requisitos da conta, considere se você precisará de mais de uma Conta da AWS e entenda os requisitos para configurar sua conta para acesso administrativo no IAM Identity Center.

Conta da AWS requisitos

Para se inscrever em um Conta da AWS, você precisa fornecer as seguintes informações:

- Um nome de conta — O nome da conta aparece em vários lugares, como na sua fatura, e em consoles, como o painel Billing and Cost Management e o console. AWS Organizations

  Recomendamos que você use um padrão de nomenclatura de conta para que o nome da conta possa ser facilmente reconhecido e diferenciado de outras contas que você possa ter. Se for uma conta corporativa, considere usar um padrão de nomenclatura, como organização - propósito - ambiente (por exemplo, AnyCompany- auditoria - produção). Se for uma conta pessoal, considere usar um padrão de nomenclatura, como nome - sobrenome - finalidade (por exemplo, paulo-santos-testaccount).
- Endereço de e-mail — Este endereço de e-mail é usado como nome de login do usuário raiz da conta e é necessário para a recuperação da conta, como esquecer a senha. É preciso poder receber mensagens enviadas para esse endereço de e-mail. Antes de realizar determinadas tarefas, você precisará verificar se você tem acesso à conta de e-mail.

  > **Important**
  >
  > Se essa conta for empresarial, recomendamos que você use uma lista de distribuição corporativa (por exemplo, `it.admins@example.com`). Evite usar o endereço de e-mail corporativo de um indivíduo (por exemplo, `paulo.santos@example.com`). Isso ajuda a garantir que sua empresa possa acessar o Conta da AWS caso um funcionário mude de posição ou saia da empresa. O endereço de e-mail pode ser usado para redefinir as credenciais do usuário raiz da conta. Proteja o acesso a essa lista de distribuição ou endereço.
- Um número de telefone — Este número pode ser usado quando a confirmação da titularidade da conta é necessária. Este número precisa estar disponível para receber chamadas.

> **Important**
>
> Se essa conta for empresarial, recomendamos usar um número de telefone corporativo em vez de um número de telefone pessoal. Isso ajuda a garantir que sua empresa possa acessar o Conta da AWS caso um funcionário mude de posição ou saia da empresa.

- Um dispositivo de autenticação multifator — Para proteger seus AWS recursos, habilite a autenticação multifator (MFA) na conta do usuário raiz. Além de suas credenciais de login regulares, uma autenticação secundária é necessária quando a MFA é ativada, fornecendo uma camada extra de segurança. Para obter mais informações sobre o MFA, consulte O que é a MFA? no Manual do usuário do IAM.
- Suporte plano — Você deverá escolher um dos planos disponíveis durante o processo de criação da conta. Para obter uma descrição dos planos disponíveis, consulte Comparar planos do Suporte.

Considerações do Centro de Identidade do IAM

Os tópicos a seguir fornecem diretrizes para a configuração do Centro de Identidade do IAM para ambientes específicos. Entenda a orientação que se aplica ao seu ambiente antes de continuar para Parte 2: criar um usuário administrativo no Centro de Identidade do IAM.

Tópicos

- Active Directory ou IdP externo
- AWS Organizations
- Perfis do IAM
- Firewalls de próxima geração e gateways web seguros

Active Directory ou IdP externo

Se você já estiver gerenciando usuários e grupos no Active Directory ou em um IdP externo, recomendamos que considere conectar essa fonte de identidade ao habilitar o Centro de Identidade do IAM e escolher sua fonte de identidade. Fazer isso antes de criar qualquer usuário e grupo no diretório padrão do Centro de Identidade ajudará a evitar a configuração adicional necessária se você alterar sua fonte de identidade posteriormente.

Se você quiser usar o Active Directory como sua fonte de identidade, a configuração deve atender aos seguintes pré-requisitos:

- Se você estiver usando AWS Managed Microsoft AD, você deve habilitar o IAM Identity Center no mesmo Região da AWS local em que seu AWS Managed Microsoft AD diretório está configurado. O IAM Identity Center armazena os dados de atribuição na mesma região do diretório. Para administrar o IAM Identity Center, talvez seja necessário mudar para a região em que o IAM Identity Center está configurado. Além disso, observe que o portal de AWS acesso usa a mesma URL de acesso do seu diretório.
- Use um Active Directory residente em sua conta de gerenciamento:

  Você deve ter um AD Connector ou AWS Managed Microsoft AD diretório existente configurado e ele deve residir em sua conta AWS Organizations de gerenciamento. AWS Directory Service Você pode conectar somente um AD Connector ou um por AWS Managed Microsoft AD vez. Se você precisar oferecer suporte a vários domínios ou florestas, use AWS Managed Microsoft AD. Para obter mais informações, consulte:

  - Conecte um diretório AWS Managed Microsoft AD ao IAM Identity Center no Guia Centro de Identidade do AWS IAM do usuário.
  - Conectar um diretório autogerenciado no Active Directory ao Centro de Identidade do IAM no Guia do usuário do Centro de Identidade do AWS IAM .
- Use um Active Directory residente na conta de administrador delegado:

  Se você planeja habilitar o administrador delegado do IAM Identity Center e usar o Active Directory como sua fonte de identidade do IAM, você pode usar um AD Connector ou AWS Managed Microsoft AD diretório existente configurado no AWS diretório que reside na conta de administrador delegado.

  Se você decidir alterar a fonte do Centro de Identidade do IAM de qualquer outra fonte para o Active Directory ou alterá-la do Active Directory para qualquer outra fonte, o diretório deverá pertencer à (ou seja, residir na) conta de membro do administrador delegado do Centro de Identidade do IAM, se houver uma; caso contrário, deverá estar na conta de gerenciamento.

AWS Organizations

Você Conta da AWS deve ser gerenciado por AWS Organizations. Se você não configurou uma organização, não é necessário fazer isso. Ao ativar o IAM Identity Center, você escolherá se deseja AWS criar uma organização para você.

Se você já configurou AWS Organizations, verifique se todos os recursos estão ativados. Para obter mais informações, consulte Habilitar todos os recursos em sua organização no Manual do usuário do AWS Organizations .

Para habilitar o IAM Identity Center, você deve entrar no Console de gerenciamento da AWS usando as credenciais da sua conta de AWS Organizations gerenciamento. Você não pode ativar o IAM Identity Center enquanto estiver conectado com as credenciais de uma conta de AWS Organizations membro. Para obter mais informações, consulte Criação e gerenciamento de uma AWS organização no Guia AWS Organizations do usuário.

Perfis do IAM

Se você já configurou funções do IAM no seu Conta da AWS, recomendamos que verifique se sua conta está se aproximando da cota para funções do IAM. Para obter mais informações, consulte Cotas de objetos do IAM.

Se você estiver se aproximando da cota, considere solicitar um aumento de cota. Caso contrário, você poderá ter problemas com o IAM Identity Center ao provisionar conjuntos de permissões para contas que excederam a cota de perfis do IAM. Para obter informações sobre como solicitar o aumento da cota, consulte Solicitar um aumento de cota no Guia do usuário do Service Quotas.

Firewalls de próxima geração e gateways web seguros

Se você filtrar o acesso a AWS domínios ou endpoints de URL específicos usando uma solução de filtragem de conteúdo da web, como NGFWs ou SWGs, deverá adicionar os seguintes domínios ou endpoints de URL às suas listas de permissões da solução de filtragem de conteúdo da web.

Domínios DNS específicos

- *.awsapps.com (http://awsapps.com/)
- *.signin.aws

Endpoints de URL específicos

- *[yourdirectory]*https://.awsapps.com/start
- *[yourdirectory]*https://.awsapps.com/login
- *[yourregion]*https://.signin. aws/platform/login

Usando vários Contas da AWS

Contas da AWS servem como limite fundamental de segurança em AWS. Elas servem como um contêiner de recursos que fornece um nível útil de isolamento. A capacidade de isolar recursos e usuários é um requisito fundamental para estabelecer um ambiente seguro e bem governado.

Separar seus recursos em partes Contas da AWS ajuda você a apoiar os seguintes princípios em seu ambiente de nuvem:

- Controle de segurança — Aplicações diferentes podem ter perfis de segurança diversos que exigem políticas e mecanismos de controle diferentes. Por exemplo, é mais fácil falar com um auditor e ser capaz de apontar para um único Conta da AWS que hospeda todos os elementos de sua carga de trabalho que estão sujeitos aos padrões de segurança do setor de cartões de pagamento (PCI).
- Isolamento — An Conta da AWS é uma unidade de proteção de segurança. Os riscos potenciais e as ameaças à segurança devem estar contidos dentro e Conta da AWS sem afetar os outros. Pode haver necessidades de segurança diferentes devido a equipes ou perfis de segurança diferentes.
- Muitas equipes — Equipes diferentes têm responsabilidades e necessidades de recursos diversas. Você pode evitar que as equipes interfiram umas nas outras movendo-as para uma posição separada Contas da AWS.
- Isolamento de dados — Além de isolar as equipes, é importante isolar os armazenamentos de dados em uma conta. Isso pode ajudar a limitar o número de pessoas que podem acessar e gerenciar esse armazenamento de dados. Isso ajuda a conter a exposição a dados altamente privados e, portanto, pode ajudar na conformidade com o Regulamento Geral de Proteção de Dados (GDPR) da União Europeia.
- Processo de negócios — Diferentes unidades de negócios ou produtos podem ter finalidades e processos completamente diferentes. Com vários Contas da AWS, você pode atender às necessidades específicas de uma unidade de negócios.
- Faturamento — Uma conta é a única maneira verdadeira de separar itens em um nível de faturamento. Várias contas ajudam a separar itens em um nível de cobrança entre unidades de negócios, equipes funcionais ou usuários individuais. Você ainda pode consolidar todas as suas contas em um único pagador (usando AWS Organizations e consolidando o faturamento) enquanto separa os itens de linha por. Conta da AWS

- Alocação de cotas — as cotas AWS de serviço são aplicadas separadamente para cada uma. Conta da AWS Separar as workloads em diferentes Contas da AWS impede que elas consumam cotas umas das outras.

Todas as recomendações e procedimentos descritos neste guia estão em conformidade com o AWS Well-Architected Framework. Essa estrutura tem como objetivo ajudar você a projetar uma infraestrutura de nuvem flexível, resiliente e escalável. Mesmo quando você está começando aos poucos, recomendamos que prossiga de acordo com as orientações da estrutura. Isso pode ajudar a escalar seu ambiente com segurança e sem afetar suas operações contínuas à medida que a empresa cresce.

Antes de começar a adicionar várias contas, você deve desenvolver um plano para gerenciá-las. Para isso, recomendamos que você use AWS Organizations, que é um AWS serviço gratuito, para gerenciar tudo Contas da AWS em sua organização.

AWS também oferece AWS Control Tower, que adiciona camadas de automação AWS gerenciada ao Organizations e a integra automaticamente a outros AWS serviços AWS CloudTrail AWS Config, como Amazon CloudWatch e outros. AWS Service Catalog Esses serviços podem incorrer em custos adicionais. Para obter mais informações, consulte Definição de preço do AWS Control Tower.

Parte 1: Configurar um novo Conta da AWS

Essas instruções ajudarão você a criar Conta da AWS e proteger as credenciais do usuário root. Conclua todas as etapas antes de continuar para Parte 2: criar um usuário administrativo no Centro de Identidade do IAM.

Tópicos

Etapa 1: inscrever-se em uma AWS conta

1. Abra a https://portal.aws.amazon.com/billing/inscrição.
2. Escolha Criar um Conta da AWS.

   > **Note**
   >
   > Se você se conectou AWS recentemente, escolha Entrar no console. Se a opção Criar uma nova Conta da AWS não estiver visível, primeiro escolha Fazer login com uma conta diferente e, em seguida, escolha Criar uma nova Conta da AWS.

3. Insira as informações da conta e, em seguida, escolha Continuar.

   Insira as informações corretas da sua conta, especialmente seu endereço de e-mail. Se você digitar seu endereço de e-mail incorretamente, não poderá acessar sua conta.

4. Escolha Pessoal ou Profissional.

   A diferença entre essas opções está apenas nas informações que solicitamos. Ambos os tipos de conta têm os mesmos atributos e funções.

5. Insira suas informações pessoais ou da empresa com base nas orientações fornecidas em Conta da AWS requisitos.
6. Leia e aceite o Contrato do cliente da AWS.
7. Escolha Criar conta e continuar.

Nesse momento, você receberá uma mensagem de e-mail confirmando que a Conta da AWS está pronta para uso. Você pode fazer login na sua nova conta usando o endereço de e-mail e a senha que forneceu durante o cadastro. No entanto, você não pode usar nenhum AWS serviço até terminar de ativar sua conta.

8. Na página Informações de pagamento, insira as informações sobre sua forma de pagamento. Se quiser usar um endereço diferente daquele usado para criar a conta, escolha Usar um novo endereço e insira o endereço que você deseja usar para fins de cobrança.
9. Escolha Verificar e pagar.

> **Note**
>
> Se seu endereço de contato for na Índia, seu contrato de usuário para sua conta é com a AISPL, um vendedor AWS local na Índia. É necessário fornecer o CVV como parte do processo de verificação. Talvez você também precise inserir uma senha de uso único, dependendo do seu banco. A AISPL faz uma cobrança de INR 2 no seu método de pagamento como parte do processo de verificação. A AISPL reembolsa esse valor após a conclusão da verificação.

10. Para verificar seu número de telefone, escolha o código do seu país ou região na lista e insira um número de telefone no qual você possa receber ligações nos próximos minutos. Insira o código CAPTCHA e envie.
11. O sistema de verificação AWS automática liga para você e fornece um PIN. Insira o PIN usando seu telefone e escolha Continuar.
12. Selecione um Suporte plano.

    Para obter uma descrição dos planos disponíveis, consulte Comparar planos do Suporte.

    É exibida uma página de confirmação indicando que sua conta está sendo ativada. Isso geralmente leva apenas alguns minutos, mas às vezes pode demorar até 24 horas. Durante a ativação, você pode entrar no seu novo Conta da AWS. Até que a ativação seja concluída, você poderá ver o botão Concluir cadastro. Você pode ignorá-lo.

    AWS envia uma mensagem de e-mail de confirmação quando a ativação da conta é concluída. Verifique sua pasta de e-mail e spam para ver a mensagem de e-mail de confirmação. Depois de receber essa mensagem, você terá acesso total a todas as ofertas da AWS .

Etapa 2: fazer login como usuário raiz

Ao criar um 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.

> **Important**
>
> É altamente recomendável não usar o usuário-raiz para tarefas diárias. Proteja as credenciais do usuário-raiz e use-as para executar as tarefas que somente ele puder executar. Para obter a lista completa das tarefas que exigem login como usuário-raiz, consulte Tarefas que exigem credenciais de usuário-raiz no Guia do Usuário do IAM.

Como fazer login como usuário raiz

1. Abra o Console de gerenciamento da AWS em https://console.aws.amazon.com/.

   > **Note**
   >
   > Se você fez login anteriormente como usuário raiz usando esse navegador, talvez ele se lembre do endereço de e-mail da Conta da AWS.
   > Se você fez login anteriormente como usuário do IAM usando este navegador, ele poderá exibir a página de login do usuário do IAM. Para retornar à página de login principal, escolha Sign in using root user email (Fazer login usando o e-mail do usuário raiz).

2. Se você não fez login anteriormente usando esse navegador, a página principal de login será exibida. Se você for o proprietário da conta, escolha Usuário raiz. Digite o endereço de e-mail associado à sua conta da Conta da AWS e escolha Próximo.
3. Talvez você precise fazer uma verificação de segurança completa. Conclua a verificação para seguir para a próxima etapa. Se você não conseguir concluir a verificação de segurança, tente ouvir o áudio ou atualizar a verificação de segurança para um novo conjunto de caracteres.
4. Insira a senha e selecione Fazer login.

Etapa 3: ativar o MFA para seu usuário root Conta da AWS

Para aprimorar a segurança das credenciais do seu usuário raiz, recomendamos seguir a prática de segurança recomendada para ativar a autenticação multifator (MFA) da sua Conta da AWS. Como o usuário raiz pode executar operações confidenciais em sua conta, adicionar uma camada extra de autenticação ajuda a proteger melhor sua conta. Vários tipos de MFA estão disponíveis.

Para obter instruções sobre como ativar a MFA para o usuário raiz, consulte Habilitar dispositivos de MFA para usuários na AWS no Guia do usuário do IAM.

Parte 2: criar um usuário administrativo no Centro de Identidade do IAM

Depois de concluirParte 1: Configurar um novo Conta da AWS, as etapas a seguir ajudarão você a configurar o Conta da AWS acesso de um usuário administrativo, que será usado para realizar tarefas diárias.

> **Note**
>
> Este tópico fornece as etapas mínimas necessárias para configurar com êxito o acesso de administrador para um Conta da AWS e criar um usuário administrativo no IAM Identity Center. Para obter mais informações, consulte Conceitos básicos no Guia do usuário do Centro de Identidade do AWS IAM .

Tópicos

Etapa 1: habilitar o Centro de identidade do IAM

> **Note**
>
> Se você não ativou a autenticação multifator (MFA) para o usuário raiz, conclua a Etapa 3: ativar o MFA para seu usuário root Conta da AWS antes de continuar.

Para habilitar o Centro de Identidade do IAM

1. Faça login Console de gerenciamento da AWScomo proprietário da conta escolhendo Usuário raiz e inserindo seu endereço de Conta da AWS e-mail. Na próxima página, insira a senha.

2. Abra o console do Centro de Identidade do IAM.
3. Em Habilitar o IAM Identity Center, escolha Habilitar.
4. O IAM Identity Center exige AWS Organizations. Se você não configurou uma organização, deve escolher se deseja AWS criar uma para você. Escolha Criar AWS organização para concluir esse processo.

   AWS Organizations envia automaticamente um e-mail de verificação para o endereço associado à sua conta de gerenciamento. Talvez haja um atraso até você receber o e-mail de verificação. Verifique o endereço de e-mail em 24 horas.

> **Note**
>
> Se você estiver usando um ambiente com várias contas, recomendamos que você configure a administração delegada. Com a administração delegada, você pode limitar o número de pessoas que precisam de acesso à conta de gerenciamento no AWS Organizations. Para obter mais informações, consulte Administração delegada, no Guia de usuário do Centro de Identidade do AWS IAM .

Etapa 2: escolher fonte de identidade

Sua fonte de identidade no Centro de Identidade do IAM define onde seus usuários e grupos são gerenciados. Você pode escolher uma das seguintes opções como fonte de identidade:

- Diretório do Centro de Identidade do IAM — Quando você habilita o Centro de Identidade do IAM pela primeira vez, ele é configurado automaticamente com um diretório do Centro de Identidade do IAM como sua fonte de identidade padrão. É aqui que você cria seus usuários e grupos e atribui seu nível de acesso a aplicações e contas da AWS.
- Active Directory — Escolha esta opção se quiser continuar gerenciando usuários em seu diretório do AWS Managed Microsoft AD usando o AWS Directory Service ou em seu diretório autogerenciado no Active Directory (AD).
- Provedor de identidades (IdP) externo — Escolha esta opção se quiser gerenciar usuários em um provedor de identidades (IdP) externo, como o Okta ou o Azure Active Directory.

Depois de habilitar o Centro de Identidade do IAM, você deve escolher sua fonte de identidade. A fonte de identidade que você escolhe determina onde o IAM Identity Center pesquisa usuários e

grupos que precisam de acesso de login único. Depois de escolher a fonte de identidade, você criará ou especificará um usuário e atribuirá a ele permissões administrativas para sua Conta da AWS.

> **Important**
>
> Se já estiver gerenciando usuários e grupos no Active Directory ou em um provedor de identidades externo (IdP), recomendamos que considere conectar essa fonte de identidade ao habilitar o Centro de Identidade do IAM e escolher sua fonte de identidade. Isso deve ser feito antes de você criar qualquer usuário e grupo no diretório padrão do Centro de Identidade e fazer qualquer atribuição. Se você já estiver gerenciando usuários e grupos em uma fonte de identidade, mudar para outra fonte de identidade pode remover todas as atribuições de usuários e grupos que você configurou no Centro de Identidade do IAM. Se isso ocorrer, todos os usuários, incluindo o usuário administrativo no IAM Identity Center, perderão o acesso de login único a seus aplicativos Contas da AWS e aplicativos.

Tópicos

Conectar o Active Directory ou outro IdP e especificar um usuário

Se você já estiver usando o Active Directory ou um provedor de identidades (IdP) externo, os tópicos a seguir ajudarão você a conectar seu diretório ao IAM Identity Center.

Você pode conectar um AWS Managed Microsoft AD diretório, um diretório autogerenciado no Active Directory ou um IdP externo ao IAM Identity Center. Se você planeja conectar um AWS Managed Microsoft AD diretório ou um diretório autogerenciado no Active Directory, verifique se a configuração do Active Directory atende aos pré-requisitos do. Active Directory ou IdP externo

> **Note**
>
> Como uma prática recomendada de segurança, recomendamos habilitar a autenticação multifator. Se você planeja conectar um AWS Managed Microsoft AD diretório ou um diretório autogerenciado no Active Directory e não está usando o RADIUS MFA com, AWS Directory Service habilite o MFA no IAM Identity Center. Se você planeja usar um provedor de identidades externo, observe que o IdP externo, e não o IAM Identity Center, gerencia

as configurações de MFA. O MFA no IAM Identity Center não é suportado para uso externo. IdPs Para obter mais informações, consulte Habilitar a MFA no Guia do usuário do Centro de Identidade do AWS IAM .

AWS Managed Microsoft AD

1. Consulte a orientação em Conectar a um Microsoft Active Directory.
2. Siga as etapas em Conectar um diretório AWS Managed Microsoft AD ao IAM Identity Center.
3. Configure o Active Directory para sincronizar o usuário ao qual você deseja conceder permissões administrativas no IAM Identity Center. Para obter mais informações, consulte Sincronizar um usuário administrativo no Centro de Identidade do IAM.

Diretório autogerenciado no Active Directory

1. Consulte a orientação em Conectar a um Microsoft Active Directory.
2. Siga as etapas em Conectar um diretório autogerenciado no Active Directory ao Centro de Identidade do IAM.
3. Configure o Active Directory para sincronizar o usuário ao qual você deseja conceder permissões administrativas no Centro de Identidade do IAM. Para obter mais informações, consulte Sincronizar um usuário administrativo no Centro de Identidade do IAM.

IdP externo

1. Leia as orientações em Conectar-se a um provedor de identidades externo.
2. Siga as instruções em Conectar-se a um provedor de identidades externo.
3. Configure seu IdP para provisionar usuários no Centro de Identidade do IAM.

> **Note**
>
> Antes de configurar o provisionamento automático baseado em grupos de todas as identidades da sua força de trabalho do seu IdP no Centro de Identidade do IAM, recomendamos que você sincronize o usuário ao qual deseja conceder permissões administrativas no Centro de Identidade do IAM.

Sincronizar um usuário administrativo para o Centro de Identidade do IAM

Após conectar seu diretório ao IAM Identity Center, você pode especificar um usuário ao qual deseja conceder permissões administrativas e, em seguida, sincronizar esse usuário do seu diretório com o IAM Identity Center.

1. Abra o console do IAM Identity Center.
2. Escolha Settings.
3. Na página Configurações, escolha a guia Identity source, escolha Actions e, em seguida, escolha Manage Sync.
4. Na página Manage Sync, escolha a guia Usuários e Adicionar usuários e grupos.
5. Na guia User, em User, insira o nome de usuário exato e escolha Adicionar.
6. Em Usuários e grupos adicionados, faça o seguinte:
    a. Confirme se o usuário para o qual você deseja conceder permissões administrativas foi especificado.
    b. Marque a caixa de seleção à esquerda do nome do usuário.
    c. Selecione Enviar.
7. Na página Gerenciar sincronização, o usuário que você especificou aparece na lista Usuários no escopo de sincronização.
8. No painel de navegação, escolha Users.
9. Na página Usuários, pode levar algum tempo para que o usuário que você especificou apareça na lista. Escolha o ícone de atualização para atualizar a lista de usuários.

Neste momento, seu usuário não tem acesso à conta de gerenciamento. Você configurará o acesso administrativo dessa conta criando um conjunto de permissões administrativas e atribuindo o usuário a esse conjunto de permissões.

Próxima etapa: Etapa 3: criar um conjunto de permissões administrativas

Use o diretório padrão e crie um usuário no Centro de Identidade do IAM

Quando você habilita o Centro de Identidade do IAM pela primeira vez, ele é configurado automaticamente com um diretório do Centro de Identidade do IAM como sua fonte de identidade padrão. Para criar um usuário no Centro de Identidade do IAM, conclua as seguintes etapas.

1. Faça login Console de gerenciamento da AWScomo proprietário da conta escolhendo Usuário raiz e inserindo seu endereço de Conta da AWS e-mail. Na próxima página, insira a senha.
2. Abra o console do Centro de Identidade do IAM.
3. Siga as etapas em Adicionar usuários para criar um usuário.

   Ao especificar os detalhes do usuário, você pode enviar um e-mail com as instruções de configuração da senha (essa é a opção padrão) ou gerar uma senha de uso único. Se você enviar um e-mail, certifique-se de especificar um endereço de e-mail que você possa acessar.
4. Após adicionar o usuário, retorne para esse procedimento. Se você manteve a opção padrão de enviar um e-mail com as instruções de configuração da senha, faça o seguinte:

   a. Você receberá um e-mail com o assunto Convite para participar do AWS Single Sign-On. Abra o e-mail e escolha Aceitar convite.
   b. Na página de Registro de novo usuário, insira e confirme uma senha e escolha Definir nova senha.

   > **Note**
   >
   > Salve a senha. Você precisará dela mais tarde para Etapa 5: Entre no portal de AWS acesso com suas credenciais administrativas.

Neste momento, seu usuário não tem acesso à conta de gerenciamento. Você configurará o acesso administrativo dessa conta criando um conjunto de permissões administrativas e atribuindo o usuário a esse conjunto de permissões.

Próxima etapa: Etapa 3: criar um conjunto de permissões administrativas

Etapa 3: criar um conjunto de permissões administrativas

Os conjuntos de permissões são armazenados no Centro de Identidade do IAM e definem o nível de acesso que os usuários e grupos têm a uma conta da Conta da AWS. Execute as etapas a seguir para criar um conjunto de permissões que conceda permissões administrativas.

1. Faça login Console de gerenciamento da AWScomo proprietário da conta escolhendo Usuário raiz e inserindo seu endereço de Conta da AWS e-mail. Na próxima página, insira a senha.
2. Abra o console do Centro de Identidade do IAM.

3. No painel de navegação do IAM Identity Center, em Permissões de várias contas, escolha Conjuntos de permissões.
4. Escolha Create permission set (Criar conjunto de permissões).
5. Para a Etapa 1: selecionar o tipo de conjunto de permissões, na página Selecionar tipo de conjunto de permissões, mantenha as configurações padrão e escolha Próximo. As configurações padrão concedem acesso total aos AWS serviços e recursos usando o conjunto de permissões AdministratorAccesspredefinido.

   > **Note**
   >
   > O conjunto de AdministratorAccesspermissões predefinido usa a política AdministratorAccess AWS gerenciada.

6. Para a Etapa 2: especificar detalhes do conjunto de permissões, na página Especificar detalhes do conjunto de permissões, mantenha as configurações padrão e escolha Próximo. A configuração padrão limita sua sessão a uma hora.
7. Para a Etapa 3: revisar e criar, na página Revisar e criar, faça o seguinte:
   1. Revise o tipo de conjunto de permissões e confirme se é AdministratorAccess.
   2. Revise a política AWS gerenciada e confirme se está AdministratorAccess.
   3. Escolha Criar.

Etapa 4: configurar o Conta da AWS acesso para um usuário administrativo

Para configurar o Conta da AWS acesso de um usuário administrativo no IAM Identity Center, você deve atribuir o usuário ao conjunto de AdministratorAccesspermissões.

1. Faça login Console de gerenciamento da AWScomo proprietário da conta escolhendo Usuário raiz e inserindo seu endereço de Conta da AWS e-mail. Na próxima página, insira a senha.
2. Abra o console do Centro de Identidade do IAM.
3. No painel de navegação, em Permissões de várias contas, escolha Contas da AWS.
4. Na página Contas da AWS, aparece uma lista de visualização em árvore da sua organização. Marque a caixa de seleção ao lado da Conta da AWS qual você deseja atribuir acesso

administrativo. Se você tiver várias contas em sua organização, marque a caixa de seleção ao lado da conta de gerenciamento.

5. Escolha Atribuir usuários ou grupos.
6. Para a Etapa 1: Selecionar usuários e grupos, na página Atribuir usuários e grupos a ***AWS-account-name*** "", faça o seguinte:

    1. Na guia Usuários, selecione o usuário para o qual você deseja conceder permissões administrativas.

        Para filtrar os resultados, comece a digitar o nome do usuário desejado na caixa de pesquisa.

    2. Após confirmar que o usuário correto foi selecionado, escolha Próximo.
7. Para a Etapa 2: Selecionar conjuntos de permissões, na página Atribuir conjuntos de permissões a ***AWS-account-name*** "", em Conjuntos de permissões, selecione o conjunto de AdministratorAccesspermissões.
8. Escolha Próximo.
9. Para a Etapa 3: Revisar e enviar, na página Revisar e enviar exercícios para ***AWS-account-name*** "", faça o seguinte:

    1. Revise o usuário selecionado e o conjunto de permissões.
    2. Após confirmar que o usuário correto foi atribuído ao conjunto de permissões de AdministratorAccess, escolha Enviar.

    > **Important**
    >
    > O processo de atribuição de usuário pode demorar alguns minutos para ser concluído. Mantenha a página aberta até que o processo seja concluído com êxito.

10. Se alguma das opções a seguir se aplicar, siga as etapas em Habilitar a MFA para habilitar a MFA para o Centro de Identidade do IAM:

    - Você está usando o diretório padrão do Centro de Identidade como sua fonte de identidade.
    - Você está usando um AWS Managed Microsoft AD diretório ou um diretório autogerenciado no Active Directory como sua fonte de identidade e não está usando o RADIUS MFA com. AWS Directory Service

> **Note**
>
> Se você estiver usando um provedor de identidades externo, observe que o IdP externo, e não o IAM Identity Center, gerencia as configurações de MFA. O MFA no IAM Identity Center não é suportado para uso externo. IdPs

Quando você configura o acesso à conta para o usuário administrativo, o IAM Identity Center cria um perfil do IAM correspondente. Essa função, que é controlada pelo IAM Identity Center, é criada no local relevante Conta da AWS e as políticas especificadas no conjunto de permissões são anexadas à função.

Etapa 5: Entre no portal de AWS acesso com suas credenciais administrativas

Conclua as etapas a seguir para confirmar que você pode entrar no portal de AWS acesso usando as credenciais do usuário administrativo e se você pode acessar o. Conta da AWS

1. Faça login Console de gerenciamento da AWScomo proprietário da conta escolhendo Usuário raiz e inserindo seu endereço de Conta da AWS e-mail. Na próxima página, insira a senha.
2. Abra o Centro de Identidade do AWS IAM console em https://console.aws.amazon.com/singlesignon/.
3. No painel de navegação, escolha Painel.
4. Na página Painel, em Resumo das configurações, copie a URL do portal de AWS acesso.
5. Abra um navegador separado, cole a URL do portal de AWS acesso que você copiou e pressione Enter.
6. Faça login com uma destas opções:
   - Se você estiver usando o Active Directory ou um provedor de identidades (IdP) externo como fonte de identidade, faça login usando as credenciais do usuário do Active Directory ou do IdP que você atribuiu ao conjunto de permissões de AdministratorAccess no IAM Identity Center.
   - Se você estiver usando o diretório padrão do Centro de Identidade do IAM como sua fonte de identidade, faça login usando o nome de usuário que você especificou ao criar o usuário e a nova senha que você especificou para o usuário.

7. Depois de fazer login, verá um ícone Conta da AWS no portal.
8. Quando você seleciona o ícone Conta da AWS, o nome da conta, o ID da conta e o endereço de e-mail associados à conta aparecem.
9. Escolha o nome da conta para exibir o conjunto de permissões de AdministratorAccess e selecione o link do Console de Gerenciamento à direita do AdministratorAccess.

   Quando você entra, o nome do conjunto de permissões ao qual o usuário está atribuído aparece como uma função disponível no portal de AWS acesso. Como você atribuiu esse usuário ao conjunto de `AdministratorAccess` permissões, a função aparecerá no portal de AWS acesso como:`AdministratorAccess/`*`username`*
10. Se você for redirecionado para o AWS Management Console, você concluiu com êxito a configuração do acesso administrativo ao Conta da AWS. Prossiga para a etapa 10.
11. Mude para o navegador que você usou para entrar Console de gerenciamento da AWS e configurar o IAM Identity Center e saia do seu usuário Conta da AWS raiz.

> **Important**
>
> É altamente recomendável que você adote a melhor prática de usar as credenciais do usuário administrativo ao entrar no portal de AWS acesso e que não use as credenciais do usuário raiz para suas tarefas diárias.

Para permitir que outros usuários acessem suas contas e aplicações e administrem o Centro de Identidade do IAM, crie e atribua conjuntos de permissões somente por meio do Centro de Identidade do IAM.

Solução para problemas de criação da Conta da AWS

Use as informações aqui contidas para obter ajuda para solucionar problemas relacionados à criação de uma Conta da AWS.

Problemas

- Não recebi a ligação de AWS para verificar minha nova conta
- Recebo um erro sobre “número máximo de tentativas malsucedidas” quando tento verificar minhas Conta da AWS por telefone
- Já se passaram mais de 24 horas e minha conta não está ativada

Não recebi a ligação de AWS para verificar minha nova conta

Ao criar um Conta da AWS, você deve fornecer um número de telefone no qual possa receber uma mensagem de texto SMS ou uma chamada de voz. Você especifica qual método será usado para verificar o número.

Se você não receber a mensagem ou a chamada, verifique o seguinte:

- Você inseriu o número de telefone correto e selecionou o código do país correto durante o processo de inscrição.
- Se você estiver usando um telefone celular, verifique se você tem um sinal de celular para receber mensagens de SMS ou ligações.
- As informações que você inseriu para sua forma de pagamento estão corretas.

Se você não recebeu uma mensagem de texto SMS ou uma ligação para concluir o processo de verificação de identidade, Suporte pode ajudá-lo a ativá-la Conta da AWS manualmente. Use as seguintes etapas:

1. Certifique-se de que você possa ser contatado pelo número de telefone fornecido para a sua Conta da AWS.
2. Abra o console do AWS Support e escolha Criar caso.
   a. Escolha Suporte à conta e faturamento.
   b. Em Tipo, selecione Conta.

c. Em Categoria, selecione Ativação.
d. Na seção Descrição do caso, forneça uma data e hora em que você possa ser contatado.
e. Na seção Opções de contato, selecione Chat para Métodos de contato.
f. Selecione Enviar.

> **Note**
>
> Você pode criar um caso Suporte mesmo que o seu Conta da AWS não esteja ativado.

Recebo um erro sobre “número máximo de tentativas malsucedidas” quando tento verificar minhas Conta da AWS por telefone

Suporte pode ajudá-lo a ativar manualmente sua conta. Siga estas etapas:

1. Faça login na sua Conta da AWS usando o endereço de e-mail e a senha especificados ao criá-la.
2. Abra o console do Suporte e escolha Criar caso.
3. Escolha Suporte à conta e faturamento.
4. Em Tipo, selecione Conta.
5. Em Categoria, selecione Ativação.
6. Na seção Descrição do caso, forneça uma data e hora em que você possa ser contatado.
7. Na seção Opções de contato, selecione Chat para Métodos de contato.
8. Selecione Enviar.

Suporte entrará em contato com você e tentará ativar manualmente seu Conta da AWS.

Já se passaram mais de 24 horas e minha conta não está ativada

Às vezes, a ativação da conta pode atrasar. Se o processo levar mais de 24 horas, verifique o seguinte:

- Você concluiu o processo de ativação da conta.

Se você fechou a janela do processo de inscrição antes de adicionar todas as informações necessárias, abra a página de registro. Escolha Fazer login em uma Conta da AWS existente e entre usando o endereço de e-mail e a senha que você escolheu para a conta.

- Verifique as informações associadas à sua forma de pagamento.

  No Gerenciamento de Faturamento e Custos da AWS console, verifique se há erros em Formas de pagamento.
- Entre em contato com sua instituição financeira.

  Às vezes, as instituições financeiras rejeitam solicitações de autorização de AWS. Entre em contato com a instituição associada à sua forma de pagamento e peça que ela aprove as solicitações de autorização da AWS. AWS cancela a solicitação de autorização assim que ela é aprovada pela sua instituição financeira, para que você não seja cobrado pela solicitação de autorização. As solicitações de autorização ainda podem aparecer como uma pequena taxa (geralmente USD 1) nos extratos da sua instituição financeira.
- Verifique sua pasta de e-mail e spam para obter solicitações de informações adicionais.
- Tente um navegador diferente.
- Entre em contato AWS Support.

  Entre em contato com a AWS Support para obter ajuda. Mencione todas as etapas de solução de problemas que você já tentou.

> **Note**
>
> Não forneça informações confidenciais, como números de cartão de crédito, em nenhum contato com a 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.