Guia do administrador

# Amazon Nimble Studio

Copyright © 2020 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

# Amazon Nimble Studio: Guia do administrador

Copyright © 2020 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

As marcas comerciais e imagens de marcas da Amazon não podem ser usadas no contexto de nenhum produto ou serviço que não seja da Amazon, nem de qualquer maneira que possa gerar confusão entre os clientes ou que deprecie ou desprestigie a Amazon. Todas as outras marcas comerciais que não pertencem à Amazon pertencem a seus respectivos proprietários, que podem ou não ser afiliados, conectados ou patrocinados pela Amazon.

# Table of Contents

# O que é o Amazon Nimble Studio?

O Nimble Studio fornece infraestrutura e gerenciamento centralizado para um conjunto de aplicações e serviços que os artistas podem usar para produzir efeitos visuais, animação e conteúdo de jogos na nuvem.

Com o Nimble Studio, você obtém ferramentas essenciais para gerenciamento de usuários e grupos. Você também pode adicionar e gerenciar aplicações, incluindo AWS, Thinkbox e o Nimble Studio File Transfer.

O Nimble Studio apresenta uma interface unificada que coloca todos os atributos do seu estúdio em um só lugar. Você pode integrar usuários, atribuir aplicações e anexar permissões específicas para suas funções de trabalho. O Nimble Studio não requer experiência AWS e você pode configurá-lo em cerca de cinco minutos.

Índice



## Atributos e benefícios

Aqui estão alguns dos atributos e benefícios que você obtém com o Nimble Studio:

- Use o Nimble Studio gratuitamente; pague somente pelos recursos de estúdio que suas aplicações usam.
- Gerencie centralmente seu estúdio, verifique seu status e obtenha informações de alto nível sobre sua operação.
- Adicione e gerencie aplicações, usuários e grupos do Nimble Studio e anexe permissões.
- Gerencie com segurança o acesso aos recursos do estúdio com políticas e perfis AWS Identity and Access Management (IAM).
- Gerencie a segurança de login para usuários do estúdio e provedores de identidade externos com AWS IAM Identity Center (IAM Identity Center).
- Organize e encontre facilmente os recursos do estúdio com tags nos recursos do seu estúdio.

# Aplicações relacionadas

O Nimble Studio fornece aplicações para criadores de conteúdo digital operarem um estúdio baseado em nuvem para produzir efeitos visuais (VFX), animação e conteúdo interativo.

Você pode instalar esses aplicações no seu computador local ou na nuvem com uma instância do Amazon Elastic Compute Cloud (Amazon EC2). Você pode também usar o Amazon Simple Storage Service (Amazon S3) para transferir e armazenar ativos de mídia digital de forma segura. Isso significa que você pode usar o Nimble Studio para reduzir os custos de infraestrutura física, equipamentos e equipe técnica.

Atualmente, o Nimble Studio fornece os seguintes aplicações:

- AWS Thinkbox: o Thinkbox software inclui o gerente do parque de renderização Deadline Thinkbox e o plugin 3D, Krakatoa Thinkbox. Você pode usar o software Thinkbox para ajudá-lo a aumentar a produção criativa do seu estúdio on-premises, na nuvem com o Amazon EC2 ou uma combinação de ambos. Para obter mais informações, consulte ProdutosAWS Thinkbox.
- Nimble Studio File Transfer: File Transfer acelera as transferências de ativos de mídia digital de e para o Amazon S3. File Transfer fornece uma interface gráfica de usuário, que você pode usar para mover rapidamente milhares de arquivos de mídia grandes. Para obter mais informações, consulte a página O que éNimble Studio File Transfer.

# Preços do Nimble Studio

Não há cobrança para configurar o Nimble Studio e usá-lo para gerenciar a infraestrutura, os usuários, a segurança e os serviços do seu estúdio.

No entanto, se você configurar serviços e aplicações em seu estúdio, poderá ser cobrado pelo armazenamento e outros recursos do estúdio. Para obter mais informações sobre a definição de preço da aplicação Nimble Studio, consulte a página de preço da aplicação individual.

Para obter informações sobre como gerenciar seus custos AWS, consulte AWS Cost Explorer Service e AWS Budgets.

# Comece a usar o Nimble Studio

A configuração e implantação do Nimble Studio levam cerca de cinco minutos.

Depois de se familiarizar com os conceitos e a terminologia do Nimble Studio, consulte Introdução ao Amazon Nimble Studio. Nele, você encontrará instruções passo a passo para implantar o estúdio.

# Conceitos e terminologia do Amazon Nimble Studio

Para ajudar você a começar a usar o Amazon Nimble Studio e entender como ele funciona, consulte os principais conceitos e terminologia deste guia.

## Recursos principais

Amazon Nimble Studio

O Amazon Nimble Studio é um AWS service (Serviço da AWS) que permite que estúdios criativos produzam efeitos visuais, animação e conteúdo interativo inteiramente na nuvem, desde o esboço do storyboard até a entrega final.

Amazon Nimble Studio

O console do Nimble Studio é uma parte do AWS Management Console que é dedicado aos nossos clientes administrativos de TI. Esse console é onde os administradores criam seu estúdio na nuvem e gerenciam várias configurações. Por exemplo, a página do gerenciador do Studio permite que você adicione ou remova recursos, adicione aplicações e conceda permissões a usuários e grupos.

Amazon Nimble Studio

O portal do Nimble Studio fornece uma interface de usuário para interações diárias com as aplicações e serviços do Nimble Studio. Os usuários entram diretamente no portal com seu nome de usuário e senha sem precisar interagir com AWS Management Console.

Nimble Studio File Transfer

File Transfer acelera as transferências de ativos de mídia de ativos de mídia digital de e para o Amazon Simple Storage Service (Amazon S3). File Transfer fornece uma interface gráfica de usuário, que você pode usar para mover rapidamente milhares de arquivos de mídia grandes. Para obter mais informações, consulte a página O que é?.

AWS Thinkbox

O software Thinkbox inclui o parque de renderização, o Deadline Thinkbox e o plugin 3D, Krakatoa Thinkbox. Você pode usar o software Thinkbox para ajudá-lo a aumentar a produção criativa do seu estúdio on-premises, na nuvem com o Amazon EC2 ou uma combinação de ambos. Para obter mais informações, consulte Produtos AWS Thinkbox.

# Conceitos principais e terminologia

Políticas gerenciadas por AWS

Uma AWS política gerenciada pela é uma política independente que é criada e administrada pela AWS. Política independente significa que a política tem seu próprio nome de recurso da Amazon (ARN) que inclui o nome da política. Por exemplo, arn:aws:iam::aws:policy/IAMReadOnlyAccess é uma política gerenciada por AWS. Para obter mais informações sobre ARNs, consulte ARNs do IAM.

Políticas gerenciadas por AWS são usadas para conceder permissões para funções de trabalho comuns. As políticas de função de trabalho são mantidas e atualizadas quando AWS novos serviços e operações de API são introduzidos. Por exemplo, a função de trabalho AdministratorAccess fornece acesso total e delegação de permissões para cada serviço e recurso na AWS. Por outro lado, políticas gerenciadas por AWS de acesso parcial, como AmazonMobileAnalyticsWriteOnlyAccess e AmazonEC2ReadOnlyAccess, podem fornecer níveis específicos de acesso a Serviços da AWS sem permitir o acesso total. Para obter mais informações sobre políticas de acesso, consulte Noções básicas sobre resumos de nível de acesso em resumos de política.

AWS Management Console

O AWS Management Console é uma aplicação da web que fornece acesso a uma ampla coleção de consoles de serviço para gerenciamento de aplicações Serviços da AWS.

Cada serviço também inclui seu próprio console. Esses consoles oferecem uma ampla variedade de ferramentas para computação em nuvem. Existe até um serviço que ajuda no faturamento e no gerenciamento de custos.

IAM Identity Center AWS IAM Identity Center

O IAM Identity Center é um serviço AWS que facilita o gerenciamento centralizado do acesso a várias aplicações Contas da AWS comerciais. Com o IAM Identity Center, você poderá fornecer aos usuários acesso de logon único a todas as contas e aplicações atribuídas em um só lugar. Você também pode gerenciar centralmente o acesso a várias contas e as permissões de usuário para todas as suas contas no AWS Organizations. Para obter mais informações, visite Perguntas frequentes AWS IAM Identity Center.

AWSPrivateLink

O PrivateLink AWS fornece conectividade privada entre VPCs, Serviços da AWS e suas redes on-premises, sem expor seu tráfego à Internet pública. AWS PrivateLink facilita a conexão de serviços

em diferentes contas e VPCs. AWS PrivateLink está disponível por uma taxa mensal que é cobrada de você Conta da AWS.

Criação de conteúdo digital (DCC)

Criação de conteúdo digital (DCC) se refere à categoria de aplicações usadas para produzir conteúdo criativo, incluindo Blender, Nuke, Maya e Houdini.

Regiões

O Nimble Studio oferece onze opções Regiões da AWS para você escolher e implantar seu estúdio. As regiões são onde existe a infraestrutura essencial do estúdio, como seus dados e aplicações.

A região deve estar localizada mais próxima dos usuários do seu estúdio. Isso reduz o atraso e melhora as velocidades de transferência de dados.

Studio

Um estúdio é o contêiner de nível superior para outros recursos relacionados ao Nimble Studio. Seu estúdio em nuvem gerencia o portal web do Nimble Studio e as conexões com recursos essenciais em seu Conta da AWS, como sua VPC, diretório de usuários e chaves de criptografia de armazenamento.

Aplicações do Studio

Os componentes do Studio são configurações no Nimble Studio de um cliente que informam ao serviço como acessar recursos como sistemas de arquivos, servidores de licenças e parques de renderização em seu Conta da AWS.

O Nimble Studio contém vários subtipos de componentes de estúdio, incluindo um sistema de arquivos compartilhado, fazenda de computação, Active Directory e componente de licença. Esses subtipos descrevem os recursos que você gostaria que seu estúdio usasse.

Recursos do Studio

Recursos do Studio é um termo que encapsula as coisas que um estúdio precisa em suas operações diárias. Ao descrever como os recursos se encaixam na infraestrutura de um estúdio em nuvem, eles também podem ser chamados de componentes de estúdio.

Tags

Uma tag é um rótulo atribuído a um recurso da AWS. Cada tag consiste em uma chave e um valor opcional que você define.

As etiquetas permitem categorizar seus recursos da AWS de maneiras diferentes. Por exemplo, você pode definir um conjunto de tags para as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) da sua conta que ajudam a rastrear o proprietário e o nível de pilha de cada instância. As tags também permitem que você integre os sistemas de arquivos compartilhados e os parques de renderização de sua organização com o Nimble Studio, para manter seus fluxos de trabalho ininterruptos enquanto você move sua força de trabalho para a nuvem.

Com tags, você pode categorizar seus recursos AWS por finalidade, proprietário ou ambiente. Isso é útil quando você tem muitos recursos do mesmo tipo — é possível identificar rapidamente um recurso específico baseado nas tags que você atribuiu a ele.

# Configurar o Nimble Studio

Este tutorial é para usuários administradores que desejam configurar um Amazon Nimble Studio.

As seções a seguir guiarão você pelas etapas que você precisa concluir antes de implantar um estúdio no Nimble Studio.

Conteúdos



# Configurar o IAM

Revise a documentação a seguir AWS Identity and Access Management (IAM) antes de começar.

- Práticas recomendadas de segurança no IAM
- Faça login em Conta da AWS como usuário administrador para concluir a configuração restante.

## Cadastrar-se em uma Conta da AWS

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

Para se cadastrar em uma Conta da AWS

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

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

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

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

## Crie um usuário administrador

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

Proteger seu Usuário raiz da conta da AWS

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

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

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

Criar um usuário administrativo

1. Habilitar o IAM Identity Center.

   Consulte instruções em Enabling AWS IAM Identity Center no Guia do usuário do AWS IAM Identity Center.
2. No Centro de Identidade do IAM, conceda acesso administrativo a um usuário administrativo.

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

Login como usuário administrativo

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

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

# Recursos relacionados

- Práticas recomendadas de segurança no IAM
- Cotas do AWS service (Serviço da AWS) – Referência geral da AWS

# Conceitos básicos do Amazon Nimble Studio

Este capítulo mostra como usar o console do Nimble Studio para criar a infraestrutura do seu estúdio, confirmar Região da AWS, revisar as configurações e criar seu estúdio. Você também pode personalizar sua configuração com configurações adicionais.

Para clientes iniciantes AWS, consulte os tutoriais Configurar o Nimble Studio.

Tópicos



# Configurar o Nimble Studio

Este guia mostra como configurar sua infraestrutura, revisar suas configurações e criar seu estúdio. Você também pode personalizar seu estúdio com Configurações adicionais do Studio.

## Etapa 1: configurar o Studio Infrastructure

A infraestrutura do seu estúdio consiste nos componentes a seguir:

- Nome de exibição do estúdio: O nome de exibição do Studio é como você pode identificar seu estúdio — por exemplo, AnyCompanyStudio. O nome do seu estúdio também determina a URL do portal do Studio. Você pode alterar o nome de exibição do Studio depois de concluir a configuração, a qualquer momento.
- URL do portal do Studio: você pode acessar seu estúdio usando a URL do portal do Studio. O URL é baseado no nome de exibição do Studio — por exemplo, https://anycompanystudio.awsapps.com. Você pode alterar a URL do portal do Studio depois de concluir a configuração, a qualquer momento.
- Região da AWS: Região da AWS é o local físico de uma coleção de data centers AWS. Quando você configura seu estúdio, o padrão da Região é o local mais próximo de você Você deve alterar a região para que ela fique mais próxima de seus usuários. Isso reduz o atraso e melhora as velocidades de transferência de dados.

> **Important**
>
> Você não pode mudar sua região depois de terminar de configurar o Nimble Studio.

Conclua as tarefas nesta seção para configurar a infraestrutura do seu estúdio.

Para configurar a infraestrutura do seu estúdio

1. Faça login em AWS Management Console e abra o console do Nimble Studio.
2. Escolha Configurar o Nimble Studio e, em seguida, escolha Avançar.
3. Insira o nome de exibição do Studio — por exemplo **`AnyCompany Studio`**.
4. (Opcional) Para alterar o nome do portal do Studio, escolha Editar URL.
5. (Opcional) Para alterar para Região da AWSque fique mais próximo dos usuários do seu estúdio, escolha Alterar região.
   a. Escolha a região mais próxima para a maioria dos seus usuários.
   b. Escolha Aplicar região.
6. (Opcional) Para personalizar ainda mais a configuração do seu estúdio, selecione Configurações adicionais do Studio.
7. Para revisar suas configurações antes de criar seu estúdio, escolha Avançar.

## Etapa 2: revisar e criar o seu estúdio

Depois de configurar a infraestrutura do seu estúdio, você pode revisar, fazer alterações e criar seu estúdio.

Para revisar e criar seu estúdio

1. Na página Revisar e criar, revise sua infraestrutura do Studio.
2. Confirme se o Região da AWS é o mais próximo dos usuários do seu estúdio.
3. (Opcional) Escolha Editar para fazer alterações na configuração do seu estúdio.
4. Quando quiser, escolha Criar estúdio.

# Configurações adicionais do Studio

A configuração do Nimble Studio inclui configurações adicionais de estúdio. Com essas configurações, você pode visualizar todas as alterações que a configuração do Nimble Studio faz em seu Conta da AWS, configurar sua função de usuário do estúdio e alterar o tipo de chave de criptografia. Você também pode adicionar tags opcionais aos recursos do estúdio.

## Configurar a função de usuário do estúdio

Um serviço AWS pode assumir uma função de serviço para executar ações em seu nome. O Nimble Studio requer um perfil de usuário de estúdio para dar aos usuários acesso aos recursos em seu estúdio.

Você pode anexar políticas gerenciadas AWS Identity and Access Management (IAM) ao perfil de usuário do estúdio. As políticas permitem que os usuários realizem determinadas ações, como criar trabalhos em uma aplicação específica do Nimble Studio. Como as aplicações dependem de condições específicas na política gerenciada, se você não usar as políticas gerenciadas, a aplicação pode não funcionar conforme o esperado.

Você pode alterar o perfil do usuário do Studio depois de concluir a configuração, a qualquer momento. Para obter mais informações sobre perfis de usuário, consulte Perfis do IAM.

As guias a seguir contêm instruções para dois casos de uso diferentes. Para criar e usar um novo perfil de serviço, escolha a guia Novo perfil de serviço. Para usar um perfil de serviço existente, escolha a guia Perfil de serviço existente.

New service role

Para criar e usar um novo perfil de serviço

1. Selecione Criar e usar um novo perfil de serviço.
2. (Opcional) Insira um nome de perfil de usuário do serviço.
3. Escolha Exibir detalhes da permissão para obter mais informações sobre a função.

Existing service role

Para usar um perfil de serviço existente

1. Selecione Usar um perfil de serviço existente.

2. Abra a lista suspensa para escolher um perfil de serviço existente.
3. (Opcional) Escolha Exibir no console do IAM para obter mais informações sobre o perfil.

## AWS IAM Identity Center

AWS IAM Identity Center é um serviço de login único baseado em nuvem para gerenciar usuários e grupos. O IAM Identity Center também pode ser integrado ao seu provedor corporativo de autenticação única (SSO) para que os usuários possam fazer login com a conta da empresa.

O Nimble Studio habilita o IAM Identity Center por padrão e é necessário configurar e usar o Nimble Studio. Para obter mais informações, consulte O que é o AWS IAM Identity Center.

## Configurar chave de criptografia AWS KMS

As chaves AWS Key Management Service (AWS KMS) são o principal tipo de chave do KMS que você pode usar para criptografar, descriptografar e recriptografar dados.

O Nimble Studio inclui os seguintes tipos de chave AWS KMS de criptografia:

- Chave de propriedade AWS – AWS chaves de propriedade são chaves KMS que AWS service (Serviço da AWS) ela possui e gerencia para uso em vários arquivos Contas da AWS. As chaves próprias AWS não residem em sua conta Conta da AWS, mas o Nimble Studio pode usar uma chave própria AWS para proteger os recursos em sua conta.

  Para usar AWS KMS, você não precisa criar ou manter a chave ou sua política de chaves. Não há cobrança pelo uso de chaves próprias AWS e elas não contam nas cotas AWS KMS de sua propriedade Conta da AWS.
- Chave gerenciada pelo cliente AWS KMS – Uma chave gerenciada pelo cliente é uma chave do KMS na sua Conta da AWS criada e gerenciada por você.

  Você tem controle total sobre essas chaves KMS. As chaves gerenciadas pelo cliente incorrem em uma taxa mensal. Eles também cobram uma taxa para cada solicitação de API AWS KMS além do nível gratuito. Para obter mais informações sobre definição de preço do AWS KMS, consulte Definição de preço do AWS Key Management Service.

O tipo de chave de criptografia não pode ser alterado após a conclusão da configuração. Para obter mais informações AWS KMS e tipos de chaves de criptografia, consulte a documentação AWS KMS.

Para escolher um tipo de chave de criptografia diferente

1. Selecione Escolher uma tecla diferente AWS KMS (avançada).
2. Selecione uma chave AWS KMS ou insira um número de recurso da Amazon (ARN).
3. Escolha Criar chave AWS KMS.

## Configurar tags

As tags funcionam como etiquetas para organizar seus recursos do Nimble Studio. Você pode adicionar até 50 tags para identificar, organizar, filtrar e pesquisar recursos.

Cada tag consiste em duas partes, que você define: uma chave de tag e um valor de tag opcional – por exemplo, chave: `domain` e valor: `anycompanystudio.com`.

Você pode adicionar ou remover tags após concluir a configuração a qualquer momento. Para obter mais informações sobre tags, consulte Marcando seus recursos AWS.

Para adicionar tags aos recursos do seu estúdio

1. Selecione Add new tag (Adicionar nova tag).
2. Insira a tag Key (Chave).
3. (Opcional) Insira o Valor da tag.

# Excluir um estúdio

Se você não precisa mais do estúdio, você pode excluí-lo. Quando você exclui seu estúdio, somente a infraestrutura do estúdio é excluída. Seus outros recursos AWS, como perfis de usuário, políticas e dados de aplicações, permanecem intactos.

> **Important**
>
> Não é possível recuperar um estúdio após sua exclusão.

Para excluir seu estúdio

1. Faça login em AWS Management Console e abra o console do Nimble Studio.
2. Selecione Visão geral do Studio.
3. Selecione Ações e escolha Excluir estúdio.
4. Insira **`delete`** e escolha Excluir.

# Segurança em Amazon Nimble Studio

A segurança para com a nuvem na AWS é a nossa maior prioridade. Como cliente da AWS, você se beneficiará de data centers e arquiteturas de rede criados para atender aos requisitos das empresas com as maiores exigências de segurança.

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

- Segurança da nuvem: AWS é responsável pela proteção da infraestrutura que executaAWS produtos da Nuvem AWS na AWS. A também fornece serviços que podem ser usados com segurança. Auditores de terceiros testam e verificam regularmente a eficácia da nossa segurança como parte dos AWSProgramas de conformidade. Para saber mais sobre os programas de conformidade que se aplicam ao Amazon Nimble Studio, consulte AWSServiços da em escopo por programa de conformidade.
- Segurança na nuvem: sua responsabilidade é determinada pelo 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.

> **Important**
>
> É altamente recomendável que você leia e se familiarize com o Security Pillar - Well-Architected Framework AWS. Este artigo contém os principais princípios para proteger sua infraestrutura AWS.

Esta documentação ajuda a entender como aplicar o modelo de responsabilidade compartilhada ao usar o .Nimble Studio Os tópicos a seguir mostram como configurar o Nimble Studio para atender aos seus objetivos de segurança e conformidade. Saiba também como usar outros produtos da AWS que ajudam a monitorar e proteger os recursos do Nimble Studio.

## Mais informações

- Security Pillar - Well-Architected Framework AWS
- Segurança para o AWS Cloud Development Kit (AWS CDK) (AWS CDK)

- Segurança na Amazon Virtual Private Cloud (VPC)
- Credenciais de segurança de AWS
- Segurança no Amazon EC2
  - Linux
  - Windows

# Configurar a segurança Conta da AWS

Este guia mostra como configurar Conta da AWS para receber notificações quando seus recursos forem comprometidos e permitir que usuários Conta da AWS específicos os acessem. Para proteger seus recursos Conta da AWS e monitorar seus, conclua as etapas a seguir.

Conteúdos

- Exclua as chaves de acesso da sua conta
- Habilitar a autenticação multifator
- Ative o CloudTrail em todas as Regiões da AWS.
- Configurar notificações e configurar Amazon GuardDuty e notificações

## Exclua as chaves de acesso da sua conta

Você pode permitir o acesso programático aos seus recursos AWS a partir de AWS Command Line Interface (AWS CLI) ou com APIs AWS. No entanto, AWS recomenda que você não crie nem use as chaves de acesso associadas à sua conta raiz para acesso programático.

Se você ainda tiver chaves de acesso, recomendamos excluí-las e criar um usuário. Em seguida, conceda ao usuário somente as permissões necessárias para as APIs que você planeja chamar. Você pode usar esse usuário para emitir chaves de acesso.

Para obter mais informações, consulte Gerenciando chaves de acesso ao seu Conta da AWS no guia Referência geral da AWS.

## Habilitar a autenticação multifator

A autenticação multifator (MFA) é um recurso de segurança que fornece uma camada de autenticação além do seu nome de usuário e senha.

O MFA funciona assim: depois de fazer login com seu nome de usuário e senha, você também deve fornecer uma informação adicional à qual somente você tem acesso físico. Essas informações podem vir de um dispositivo de hardware de MFA dedicado ou de um aplicativo em um telefone.

Você deve selecionar o tipo de dispositivo de MFA que deseja usar na lista de dispositivos de MFA compatíveis. Para um dispositivo de hardware, mantenha o dispositivo de MFA em um local seguro.

Se você usa um dispositivo de MFA virtual (como um aplicativo de telefone), pense no que pode acontecer se seu telefone for perdido ou danificado. Uma abordagem é manter o dispositivo de MFA virtual que você usa em um local seguro. Outra opção é ativar mais de um dispositivo ao mesmo tempo ou usar uma opção de MFA virtual para recuperar a chave do dispositivo.

Para saber mais sobre MFA, consulte Habilitar um dispositivo de autenticação multifator virtual (MFA).

### Recursos relacionados

- Começando com a autenticação multifatorial
- Protegendo o acesso ao uso AWS da MFA

## Ative o CloudTrail em todas as Regiões da AWS.

Você pode acompanhar todas as atividades em seus recursos AWS usando AWS CloudTrail. Recomendamos que você ative o CloudTrail agora. Isso pode ajudar seu arquiteto AWS Support de soluções AWS a solucionar um problema de segurança ou configuração posteriormente.

Para ativar o login do CloudTrail em todos os Regiões da AWS, consulte Atualizar AWS CloudTrail — ativar em todas as regiões e usar várias trilhas.

Para saber mais sobre o CloudTrail, consulte Ativar o CloudTrail: registrar a atividade da API em seu Conta da AWS. Para saber como o CloudTrail monitora o Nimble Studio, consulte Registrando chamadas do Nimble Studio usando AWS CloudTrail.

## Configurar notificações e configurar Amazon GuardDuty e notificações

O Amazon GuardDuty é um serviço de monitoramento contínuo de segurança que analisa e processa o seguinte:

- Fontes de dados

- Logs de fluxo do Amazon VPC
- Logs de eventos de gerenciamento AWS CloudTrail
- Logs de eventos de dados do CloudTrail S3
- Logs de DNS

O Amazon GuardDuty identifica atividades inesperadas, potencialmente não autorizadas e maliciosas em seu ambiente AWS. A atividade maliciosa pode incluir problemas como escalonamento de privilégios, uso de credenciais expostas ou comunicação com endereços IP ou domínios maliciosos. Para identificar essas atividades, o GuardDuty usa feeds de inteligência de ameaças, como listas de endereços IP e domínios maliciosos e machine learning. Por exemplo, o GuardDuty pode detectar instâncias comprometidas do Amazon EC2 que veiculam malware ou mineram bitcoin.

O GuardDuty também monitora o comportamento de acesso Conta da AWS em busca de sinais de comprometimento. Isso inclui implantações de infraestrutura não autorizadas, como instâncias implantadas em uma Região da AWS que nunca foi usada. Também inclui chamadas de API incomuns, como uma alteração na política de senha para reduzir a força da senha.

O GuardDuty informa você sobre o status do seu ambiente AWS produzindo descobertas de segurança. Você pode ver essas descobertas no console do GuardDuty ou por meio do Amazon CloudWatch Events.

### Configurar um tópico e endpoint do Amazon SNS

Siga as instruções no tutorial Configurar um tópico e endpoint do Amazon SNS.

### Configure um evento do EventBridge para as descobertas do GuardDuty

Crie uma regra para que o EventBridge envie eventos para todas as descobertas geradas pelo GuardDuty.

Para criar um evento do EventBridge para descobertas do GuardDuty

1. Faça login no console do Amazon EventBridge: https://console.aws.amazon.com/events/
2. No painel de navegação, escolha Regras. Em seguida, escolha Create rule (Criar regra).
3. Insira um Nome e uma Descrição para a nova regra. Em seguida, escolha Próximo.
4. Deixe eventos AWS ou eventos de parceiros do EventBridge selecionados para Origem do evento.

5. Em Padrão do evento, escolha Serviços AWS para Fonte do evento. Em seguida, GuardDuty para Serviços AWS e GuardDuty Finding para Tipo de evento. Este é o tópico que você criou em Configurar um tópico e endpoint do Amazon SNS.
6. Escolha Next (Próximo).
7. Para Destino 1, selecione Serviço AWS. Escolha o Tópico SNS na lista suspensa Selecionar um destino. Em seguida, escolha seu tópico GuardDuty_to_Email.
8. Na seção Configurações adicionais: Use o menu suspenso Configurar entrada de destino para escolher Transformador de entrada. Selecione Configurar transformador de entrada.
9. Insira o código a seguir no campo Caminho de entrada na seção Transformador de entrada de destino.

```
{
    "severity": "$.detail.severity",
    "Account_ID": "$.detail.accountId",
    "Finding_ID": "$.detail.id",
    "Finding_Type": "$.detail.type",
    "region": "$.region",
    "Finding_description": "$.detail.description"
}
```

10. Para formatar o e-mail, insira o código a seguir no campo Modelo.

```
"AWS <Account_ID> has a severity <severity> GuardDuty finding type <Finding_Type>
 in the <region> region."
"Finding Description:"
"<Finding_description>. "
"For more details open the GuardDuty console at https://console.aws.amazon.com/
guardduty/home?region=<region>#/findings?search=id=<Finding_ID>"
```

11. Escolha Create (Criar). Em seguida, escolha Próximo.
12. (Opcional) Adicione tags se você estiver usando tags para monitorar seus recursos AWS.
13. Escolha Next (Próximo).
14. Revise sua regra. Em seguida, escolha Create rule (Criar regra).

Agora que você configurou sua segurança Conta da AWS, pode conceder acesso a usuários específicos e receber notificações quando seus recursos forem comprometidos.

# Proteção de dados no Amazon Nimble Studio

O modelo de responsabilidade compartilhada da AWS se aplica à proteção de dados no Amazon Nimble Studio. Conforme descrito nesse modelo, a AWS é responsável por proteger a infraestrutura global que executa toda a Nuvem AWS. Você é responsável por manter o controle sobre seu conteúdo hospedado nessa infraestrutura. Você também é responsável pelas tarefas de configuração e gerenciamento de segurança dos Serviços da AWS que usa. Para obter mais informações sobre a privacidade de dados, consulte as Perguntas frequentes sobre privacidade de dados. Para mais informações sobre a proteção de dados na Europa, consulte o artigo AWS Shared Responsibility Model and GDPR no Blog de segurança da AWS.

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

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

É altamente recomendável que nunca sejam colocadas informações de identificação confidenciais, como endereços de e-mail dos seus clientes, em marcações ou campos de formato livre, como um campo Nome. Isso inclui trabalhar com a Nimble Studio ou outros Serviços da AWS usando o console, a API, a AWS CLI ou os 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, recomendemos fortemente que não sejam incluídas informações de credenciais no URL para validar a solicitação a esse servidor.

O modelo de responsabilidade compartilhada AWS se aplica à proteção de dados no Amazon Nimble Studio. Conforme descrito nesse modelo, a AWS é responsável por proteger a infraestrutura global que executa toda a Nuvem AWS. Você é responsável por manter o controle sobre o conteúdo hospedado nesta infraestrutura. Esse conteúdo inclui as tarefas de configuração e gerenciamento de segurança dos Serviços da AWS que você usa.

Para obter mais informações sobre a privacidade de dados, consulte as Perguntas frequentes sobre privacidade de dados. Para obter informações sobre proteção de dados na União Europeia, visite o Centro do GDPR.

## Criptografia inativa

O Nimble Studio protege dados confidenciais do estúdio criptografando-os em repouso usando chaves de criptografia armazenadas em AWS Key Management Service (AWS KMS). A criptografia em repouso está disponível em todos os lugares Regiões da AWS onde o Nimble Studio está disponível. Os dados de estúdio que criptografamos incluem o nome e as descrições de todos os tipos de recursos, bem como scripts de componentes de estúdio, parâmetros de script, pontos de montagem, nomes de compartilhamento e outros dados.

Criptografar dados significa que dados confidenciais salvos em discos não podem ser lidos por nenhum usuário ou aplicativo sem uma chave válida. Os dados criptografados podem ser armazenados com segurança em repouso e podem ser descriptografados somente por uma parte com acesso autorizado à chave gerenciada.

Para obter informações sobre como o Nimble Studio usa AWS KMS para criptografar dados em repouso, consulte Gerenciamento de chaves do Amazon Nimble Studio.

### Usando subsídios com chaves AWS KMS

Uma concessão é um instrumento de política que permite que as entidades principais AWS usem chaves em operações criptográficas. Ele também pode permitir que eles visualizem uma chave KMS com o comando `DescribeKey` e criem e gerenciem concessões.

As concessões são comumente usadas por Serviços da AWS que se integram a AWS KMS para criptografar seus dados em repouso. O serviço cria uma concessão em nome de um usuário na conta, usa suas permissões e desativa a concessão assim que sua tarefa é concluída.

Quando o Nimble Studio cria seu estúdio, fornecemos duas funções para os usuários do portal do Nimble Studio: funções de usuário e administrador. O Nimble Studio cria concessões em chaves gerenciadas pelo cliente para essas funções, a fim de fornecer acesso aos dados criptografados do estúdio.

> **Important**
>
> Se você excluir uma concessão, o portal do Nimble Studio ficará inutilizável para os usuários até que o administrador crie uma nova concessão.

Para obter detalhes sobre como Serviços da AWS usa concessões, consulte Como Serviços da AWS usa AWS KMS ou o tópico Criptografia em repouso no Guia do usuário ou no Guia do desenvolvedor do serviço.

## Criptografia em trânsito

A tabela a seguir fornece informações sobre como os dados são criptografados em trânsito. Quando aplicável, outros métodos de proteção de dados do Nimble Studio também são listados.

| Dados | Caminho de rede | Proteção |
| --- | --- | --- |
| Ativos da Web, como imagens e arquivos JavaScript | O caminho da rede é entre os usuários do Nimble Studio e o Nimble Studio. | A criptografia de dados usa TLS 1.2 ou posterior. |
| Tráfego de pixel e streaming relacionado | O caminho da rede é entre os usuários do Nimble Studio e o Nimble Studio. | Criptografado usando Advanced Encryption Standard (AES-256) de 256 bits e transportado usando TLS 1.2 ou posterior. |
| Tráfego de API | O caminho é entre os usuários do Nimble Studio e o Nimble Studio. | Criptografado usando TLS 1.2 ou posterior. As solicitações para criar uma conexão são assinadas usando SigV4. |

# Gerenciamento de chaves do Amazon Nimble Studio

Ao criar um novo estúdio, você pode escolher uma das seguintes chaves para criptografar os dados do seu estúdio:

- Chave KMS de propriedade de AWS – Tipo de criptografia padrão. A chave é propriedade do Nimble Studio (sem custo adicional).
- Chave KMS gerenciada pelo cliente – A chave é armazenada em sua conta e é criada, de propriedade e gerenciada por você. Você tem controle total sobre a chave. Aplicam-se taxas AWS KMS.

Excluir uma chave KMS gerenciada pelo cliente em AWS Key Management Service (AWS KMS) é destrutivo e potencialmente perigoso. Exclui irreversivelmente o material da chave e todos os metadados associados à chave. Depois que uma chave do KMS gerenciada pelo cliente é excluída, não é mais possível descriptografar os dados que foram criptografados com ela. Isso significa que os dados se tornam irrecuperáveis.

É por isso que AWS KMS oferece aos clientes um período de espera de até 30 dias antes de excluir a chave. O período de espera padrão é de 30 dias.

## Sobre o período de espera

Como é destrutivo e potencialmente perigoso excluir uma chave KMS gerenciada pelo cliente, solicitamos que você defina um período de espera de 7 a 30 dias. O período de espera padrão é de 30 dias.

No entanto, o período de espera real pode ser até 24 horas mais longo do que o programado. Para obter a data e hora reais em que a chave será excluída, use a operação DescribeKey. Você também pode ver a data de exclusão agendada de uma chave no console AWS KMS, na página de detalhes da chave, na seção Configuração geral. Observe o fuso horário.

Durante o período de espera, o status e o estado da chave gerenciada pelo cliente são Exclusão pendente.

- Uma chave KMS gerenciada pelo cliente que está com exclusão pendente não pode ser usada em nenhuma operação criptográfica.
- AWS KMS não rotaciona as chaves de reserva gerenciadas pelo cliente AWS KMS que estão pendentes de exclusão.

Para obter mais informações sobre como excluir uma chave gerenciada pelo cliente AWS KMS, consulte Excluindo chaves mestras do cliente.

## Medidas de segurança dos dados

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

- Use uma autenticação multifator (MFA [multi-factor authentication]) com cada conta.
- Use SSL/TLS para se comunicar com os recursos da AWS. Recomendamos TLS 1.2 ou posterior.
- Configure o registro em log das atividades da API e do usuário com o .AWS CloudTrail
- Use AWS as soluções de criptografia da , juntamente com todos os controles de segurança padrão dos Serviços da AWS.
- Se você precisar de módulos criptográficos validados pelo FIPS 140-2 ao acessar a AWS por meio de uma interface de linha de comandos ou uma API, use um endpoint do FIPS. Para ter mais informações sobre endpoints do FIPS, consulte Federal Information Processing Standard (FIPS) 140-2.

É altamente recomendável que você nunca coloque informações de identificação confidenciais, como números de contas de clientes, em campos de formato livre, como o campo Nome. Isso inclui quando você trabalha com o Amazon Nimble Studio ou outro Serviços da AWS usando o console, API, AWS CLI ou SDKs AWS. Todos os dados inseridos no Amazon Nimble Studio ou em outros serviços podem ser coletados para inclusão em logs de diagnóstico. Ao fornecer um URL para um servidor externo, não inclua informações de credenciais no URL para validar a solicitação a esse servidor.

## Dados e métricas de diagnóstico

Durante a implantação e exclusão do StudioBuilder, o Amazon Nimble Studio coleta determinadas métricas que usamos para diagnosticar problemas e melhorar os atributos e a experiência do usuário do Nimble Studio.

### Tipos de métricas coletadas

- Informações de uso — Os comandos e subcomandos genéricos que são executados.

- Erros e informações de diagnóstico — O status e a duração dos comandos que são executados, incluindo códigos de saída, nomes de exceções internas e falhas.
- Informações do sistema e do ambiente — A versão do Python, o sistema operacional (Windows, Linux ou macOS) e o ambiente no qual o StudioBuilder é executado.

# Gerenciamento de identidade e acesso para Amazon Nimble Studio

O AWS Identity and Access Management (IAM) é um AWS service (Serviço da AWS) que ajuda o administrador a controlar o acesso aos recursos da AWS de forma segura. Os administradores controlam quem pode ser autenticado (conectado) e autorizado (ter permissões) para usar os recursos do Amazon Nimble Studio. O IAM é um AWS service (Serviço da AWS) que pode ser usado sem custo adicional.

Tópicos



## Público

A forma como você usa (IAM) AWS Identity and Access Management difere, dependendo do trabalho que você realiza no Nimble Studio.

Usuário do serviço: se você usar o serviço Nimble Studio para fazer o trabalho, é um usuário do serviço. Nesse caso, o administrador fornecerá as credenciais e as permissões necessárias para acessar os recursos atribuídos. À medida que você usa mais atributos do Nimble Studio para fazer seu trabalho, você pode precisar de permissões adicionais. Entender como o acesso é gerenciado pode ajudá-lo a solicitar as permissões corretas ao seu administrador. Se você não conseguir

acessar um atributo no Nimble Studio, consulte Solução de problemas de identidade e acesso do Amazon Nimble Studio.

Administrador de serviço – Se você é responsável pelos recursos do Nimble Studio em sua empresa, provavelmente tem acesso total ao Nimble Studio. É sua função determinar quais recursos e recursos do Nimble Studio seus funcionários devem acessar. Em seguida, envie solicitações ao administrador para alterar as permissões dos usuários do serviço. Revise as informações nesta página para entender os Introdução ao IAM. Para saber mais sobre como sua empresa pode usar o IAM com o Nimble Studio, consulte Como o Amazon Nimble Studio funciona com o IAM.

## Autenticando com identidades

A autenticação é a forma como você faz login na AWS usando suas credenciais de identidade. Para obter mais informações sobre como fazer login usando o AWS Management Console, consulte Login no AWS Management Console como usuário do IAM ou usuário root no Guia do usuário do IAM.

Você precisa estar autenticado (conectado a AWS) como usuário raiz Conta da AWS, um usuário ou assumindo um perfil do IAM. Você também pode usar a autenticação de logon único da sua empresa ou até mesmo fazer login usando o Google ou Facebook. Nesses casos, o administrador configurou anteriormente federação de identidades usando perfis do IAM. Ao acessar AWS usando credenciais de outra empresa, você assume uma função indiretamente.

Para entrar diretamente no AWS Management Console, use sua senha com seu endereço de e-mail de usuário raiz ou seu nome de usuário. Você pode acessar programaticamente AWS usando seu usuário raiz ou chaves de acesso de usuário.

AWS fornece SDK e ferramentas de linha de comando para assinar criptograficamente sua solicitação usando suas credenciais. Se você não usa ferramentas AWS, assine você mesmo a solicitação. Faça isso usando o Signature versão 4, um protocolo para autenticação de solicitações de API de entrada. Para obter mais informações sobre a autenticação de solicitações, consulte Processo de cadastramento do Signature versão 4 na Referência geral da AWS.

Independentemente do método de autenticação usado, também pode ser exigido que você forneça informações adicionais de segurança. Por exemplo, a AWS recomenda o uso da autenticação multifator (MFA) para aumentar a segurança de sua conta. Para saber mais, consulte Usando a autenticação multifator (MFA) no Guia do usuário do IAM.

## Usuário raiz da Conta da AWS

Ao criar uma Conta da AWS, você começa com uma única identidade de login que tenha acesso total a todos os recursos e Serviços da AWS na conta. Essa identidade, denominada usuário raiz da Conta da AWS, e é acessada por login com o endereço de e-mail e a senha que você usou para criar a conta. Recomendamos fortemente que você não utilize o usuário raiz para suas tarefas diárias, mesmo as administrativas. Em vez disso, siga as práticas recomendadas sobre utilização de usuário raiz somente para criar seu primeiro usuário do IAM. Depois, guarde as credenciais do usuário raiz em um lugar seguro e utilize-as para executar somente algumas tarefas de gerenciamento de contas e serviços.

## Usuários e grupos

Um usuário é uma identidade dentro do seu Conta da AWS que possui permissões específicas para uma única pessoa ou aplicativo. Um usuário pode ter credenciais de longo prazo ou um conjunto de chaves de acesso. Para saber como gerar chaves de acesso, consulte Gerenciar chaves de acesso para usuários do IAM no Guia do usuário do IAM. Ao gerar chaves de acesso para um usuário, visualize e salve com segurança o par de chaves. Você não poderá recuperar a chave de acesso secreta no futuro. Em vez disso, gere um novo par de chaves de acesso.

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

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

## Perfis do IAM

Um perfil do IAM é uma identidade dentro do seu Conta da AWS que possui permissões específicas. É semelhante a um usuário, mas não está associado a uma pessoa específica. É possível assumir temporariamente um perfil do IAM no AWS Management Console alternando perfis. É possível assumir um perfil chamando uma operação de API da AWS CLI ou da AWS, ou usando um URL personalizado. Para obter mais informações sobre métodos para o uso de perfis, consulte Usar perfis do IAM no Guia do usuário do IAM.

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

- Permissões temporárias para usuários: um usuário pode assumir um perfil do IAM para obter temporariamente permissões diferentes para uma tarefa específica.
- Acesso de usuário federado – em vez de criar um usuário, você pode usar identidades existentes do diretório de usuários corporativos ou de um provedor de identidade da web. Eles são conhecidos como usuários federados. A AWS atribui uma função a um usuário federado quando o acesso é solicitado por meio de um provedor de identidades. Para obter mais informações sobre usuários federados, consulte Usuários e perfis federados no Guia do usuário do IAM.
  - Associação — O Nimble Studio usa um conceito chamado “associação” para fornecer ao usuário acesso a um perfil de inicialização específico. A associação permite que os administradores do estúdio deleguem acesso aos recursos aos usuários, sem precisar escrever ou entender as políticas do IAM. Quando um administrador do Nimble Studio cria uma associação para um usuário em um perfil de inicialização, o usuário está autorizado a realizar ações do IAM necessárias para usar um perfil de inicialização, como visualizar suas propriedades e iniciar uma sessão de streaming usando esse perfil de lançamento.
  - Perfil de serviço: um perfil de serviço é um perfil do IAM que um serviço assume para realizar ações em seu nome. Os perfis de serviço fornecem acesso somente na sua conta e não podem ser usadas para conceder acesso a serviços em outras contas. Um administrador pode criar, modificar e excluir um perfil de serviço no IAM. Para obter mais informações, consulte Criando uma função para delegar permissões a um AWS service (Serviço da AWS) no Guia do usuário do IAM.
  - Perfil vinculado ao serviço: um perfil vinculado ao serviço é um tipo de perfil de serviço vinculado a uma AWS service (Serviço da AWS). O serviço pode assumir o perfil para executar uma ação em seu nome. O Nimble Studio não oferece suporte às funções vinculadas ao serviço.
- Aplicações em execução no Amazon EC2: é possível usar um perfil do IAM para gerenciar credenciais temporárias para aplicações em execução em uma instância do EC2 e fazer solicitações da AWS CLI ou da AWS API. É preferível fazer isso a armazenar chaves de acesso na instância do EC2. Para atribuir um perfil da AWS a uma instância do EC2 e disponibilizá-la para todas as suas aplicações, crie um perfil de instância que esteja anexado a ela. Um perfil de instância contém a perfil e permite que os programas em execução na instância do EC2 obtenham credenciais temporárias. Para obter mais informações, consulte Uso de um perfil do IAM para conceder permissões a aplicações em execução nas instâncias do Amazon EC2 no Guia do usuário do IAM.

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

## Gerenciamento do acesso usando políticas

Você controla o acesso na AWS criando e anexando políticas às identidades do IAM ou aos recursos da AWS. Uma política é um objeto na AWS que, quando associado a uma identidade ou recurso, define suas permissões. Você pode fazer login como usuário root ou como usuário, ou pode assumir uma função do IAM. Quando você faz uma solicitação, a AWS avalia as políticas relacionadas baseadas em identidade ou baseadas em recursos. As permissões nas políticas determinam se a solicitação será permitida ou negada. A maioria das políticas são armazenadas na AWS como documentos JSON. Para obter mais informações sobre a estrutura e o conteúdo de documentos de políticas JSON, consulte Visão geral das políticas JSON no Guia do usuário do IAM.

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

Cada entidade do IAM (usuário ou função) começa sem permissões. Em outras palavras, por padrão, os usuários não podem fazer nada, nem mesmo alterar sua própria senha. Para dar permissão a um usuário para fazer algo, um administrador deve anexar uma política de permissões ao usuário. Ou o administrador pode adicionar o usuário a um grupo que tenha as permissões pretendidas. Quando um administrador concede permissões a um grupo, todos os usuários desse grupo recebem essas permissões.

As políticas do IAM definem permissões para uma ação, independentemente do método usado para executar a operação. Por exemplo, suponha que você tenha uma política que permite a ação `iam:GetRole`. Um usuário com essa política pode obter informações de perfil do AWS Management Console, da AWS CLI ou da AWS API.

### Políticas baseadas em identidade

Políticas baseadas em identidade são documentos de política de permissões JSON que você pode anexar a uma identidade, como um usuário, grupo de usuários ou função. Estas políticas controlam quais ações os usuários e funções podem executar, em quais recursos e em quais condições. Para saber como criar uma política baseada em identidade, consulte Criar políticas do IAM no Guia do usuário do IAM.

As políticas baseadas em identidade podem ser categorizadas ainda mais como políticas embutidas ou políticas gerenciadas. As políticas embutidas são anexadas diretamente a um único usuário, grupo ou função. As políticas gerenciadas são políticas independentes que podem ser anexadas

a vários usuários, grupos e perfis na Conta da AWS. As políticas gerenciadas incluem políticas gerenciadas pela AWS e políticas gerenciadas pelo cliente. Para saber como escolher entre uma política gerenciada ou uma política em linha, consulte Escolher entre políticas gerenciadas e políticas embutidas no Guia do usuário do IAM.

### Políticas baseadas em recurso

Políticas baseadas em atributos são documentos de políticas JSON que você anexa a um atributo. São exemplos de políticas baseadas em recurso as políticas de confiança de função do IAM e as políticas de bucket do Amazon S3. Em serviços compatíveis com políticas baseadas em recurso, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o recurso ao qual a política está anexada, a política define quais ações uma entidade principal especificada pode executar nesse recurso e em quais condições. Especifique uma entidade principal em uma política baseada em recursos. As entidades principais podem incluir contas, usuários, perfis, usuários federados ou Serviços da AWS.

Políticas baseadas em recursos são políticas embutidas que estão localizadas nesse serviço. Não é possível usar as políticas do IAM gerenciadas por AWS em uma política baseada em recursos.

### Listas de controle de acesso (ACLs) no Nimble Studio

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

Amazon S3, AWS WAF e Amazon VPC são exemplos de serviços compatíveis com ACLs. Para saber mais sobre ACLs, consulte Visão geral da lista de controle de acesso (ACL) no Guia do desenvolvedor do Amazon Simple Storage Service.

### Outros tipos de política

A AWS aceita tipos de política 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 o máximo de permissões que uma política baseada em identidade pode conceder a uma entidade do IAM (usuário ou função). É possível definir um limite de permissões para uma entidade. As permissões resultantes são a intersecção das políticas baseadas em identidade da entidade e dos seus limites de permissões. As políticas baseadas em recursos que especificam o usuário ou a função no campo `Principal` não são limitadas pelo limite de permissões. Uma negação

explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações sobre limites de permissões, consulte Limites de permissões para identidades do IAM no Guia do usuário do IAM.

- Políticas de controle de serviço (SCPs) – SCPs são políticas JSON que especificam as permissões máximas para uma organização ou unidade organizacional (OU) em Organizações. Organizações 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 contas. Uma SCP limita as permissões para entidades em contas-membro, inclusive para cada usuário raiz da Conta da AWS. Para obter mais informações sobre o Organizations e SCPs, consulte Como os SCPs funcionam no Guia do usuário do AWS Organizations.
- Políticas de sessão: são políticas avançadas que você transmite como um parâmetro quando cria de forma programática uma sessão temporária para um perfil ou um usuário federado. As permissões da sessão resultante são a interseção das políticas baseadas em identidade do usuário ou da função e as políticas da sessão. As permissões também podem ser provenientes de uma política baseada em atributo. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações, consulte Políticas de sessão no Guia do usuário do IAM.

### Vários tipos de política

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

## Como o Amazon Nimble Studio funciona com o IAM

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

Recursos do IAM que você pode usar com o Amazon Nimble Studio

| atributo do IAM | Suporte do Nimble Studio |
| --- | --- |
| Ações de políticas do Nimble Studio | Sim |
| Recursos de políticas para o Nimble Studio | Sim |

| atributo do IAM | Suporte do Nimble Studio |
| --- | --- |
| Chaves de condição de política para Nimble Studio | Sim |
| Listas de controle de acesso (ACLs) no Nimble Studio | Não |
| Controle de acesso baseado em atributos (ABAC) com Nimble Studio | Sim |
| Usando credenciais temporárias com Nimble Studio | Sim |
| Permissões de entidades principais entre serviços para o Nimble Studio | Sim |
| Perfis de serviço para o Nimble Studio | Sim |
| Funções vinculadas ao serviço para o Nimble Studio | Não |

Para obter uma visão de alto nível de como o Nimble Studio e outros Serviços da AWS funcionam com a maioria dos recursos do IAM, consulte Serviços da AWS que funcionam com o IAM no Guia do usuário do IAM.

## Políticas baseadas em identidade para o Nimble Studio

| | |
| --- | --- |
| Suporta políticas baseadas em identidade | Sim |

Políticas baseadas em identidade são documentos de política de permissões JSON que você pode anexar a uma identidade, como um usuário, grupo de usuários ou função. Estas políticas controlam quais ações os usuários e funções podem executar, em quais recursos e em quais condições. Para saber como criar uma política baseada em identidade, consulte Criar políticas do IAM no Guia do usuário do IAM.

Com as políticas baseadas em identidade do IAM, você pode especificar ações e recursos permitidos ou negados, bem como as condições para as quais as ações são permitidas ou negadas. Não é

possível especificar a entidade principal de segurança em uma política baseada em identidade porque ela se aplica ao usuário ou à função à qual está anexada. Para saber mais sobre todos os elementos que podem ser usados em uma política JSON, consulte Referência de elementos de política JSON do IAM no Guia do usuário do IAM.

Exemplos de políticas baseadas em identidade para Amazon Nimble Studio

Para visualizar exemplos de políticas baseadas em identidade do Nimble Studio, consulte Exemplos de políticas baseadas em identidade para Amazon Nimble Studio.

## Políticas baseadas em recursos no Nimble Studio

| | |
|---|---|
| Oferece suporte a políticas baseadas em recurso | Não |

O Nimble Studio não oferece suporte a políticas baseadas em recurso ou acesso entre contas. Políticas baseadas em atributos são documentos de políticas JSON que você anexa a um atributo. São exemplos de políticas baseadas em recurso as políticas de confiança de função do IAM e as políticas de bucket do Amazon S3. Em serviços compatíveis com políticas baseadas em recurso, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o recurso ao qual a política está anexada, a política define quais ações uma entidade principal especificada pode executar nesse recurso e em quais condições. Especifique uma entidade principal em uma política baseada em recursos. As entidades principais podem incluir contas, usuários, perfis, usuários federados ou Serviços da AWS.

## Ações de políticas do Nimble Studio

| | |
|---|---|
| Oferece suporte a ações de políticas | Sim |

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

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

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

Para ver uma lista de ações do Nimble Studio, consulte Ações definidas pelo Amazon Nimble Studio na Referência de autorização de serviço.

As ações de política no Nimble Studio usam o seguinte prefixo antes da ação:

```
nimble
```

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

```
"Action": [
      "nimble:action1",
      "nimble:action2"
         ]
```

Para visualizar exemplos de políticas baseadas em identidade do Nimble Studio, consulte Exemplos de políticas baseadas em identidade para Amazon Nimble Studio.

## Recursos de políticas para o Nimble Studio

| | |
|---|---|
| Oferece suporte a atributos de políticas | Sim |

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

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

Para ações que não oferecem suporte a 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 visualizar exemplos de políticas baseadas em identidade do Nimble Studio, consulte Exemplos de políticas baseadas em identidade para Amazon Nimble Studio.

## Chaves de condição de política para Nimble Studio

| | |
|---|---|
| Oferece suporte a chaves de condição de políticas | Sim |

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

O elemento `Condition` (ou elemento `Condition`**`block`**`) lets you specify conditions in which a statement is in effect. The `Condition`) é opcional. É possível criar expressões condicionais que usam agentes de condição, como “igual a” ou “menor que”, para fazer a condição da política corresponder aos valores na solicitação.

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

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

A AWS oferece suporte a chaves de condição globais e chaves de condição específicas do serviço. Para ver todas as AWS chaves de condição globais da , consulte AWSChaves de contexto de condição globais da no Guia do usuário do IAM.

Para visualizar exemplos de políticas baseadas em identidade do Nimble Studio, consulte Exemplos de políticas baseadas em identidade para Amazon Nimble Studio.

## Listas de controle de acesso (ACLs) no Nimble Studio

| | |
|---|---|
| Oferece suporte a ACLs | Não |

O Nimble Studio não oferece suporte às listas de controle de acesso (ACLs). As ACLs controlam quais entidades principais (membros da conta, usuários ou funções) têm permissões para acessar

um recurso. As ACLs são semelhantes às políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

## Controle de acesso baseado em atributos (ABAC) com Nimble Studio

| | |
|---|---|
| Oferece suporte a ABAC (tags em políticas) | Sim |

O controle de acesso por atributo (ABAC) é uma estratégia de autorização que define permissões com base em atributos. Na AWS, esses atributos são chamados de tags. É possível anexar tags a entidades do IAM (usuários ou perfis) e a muitos atributos da AWS. A marcação de entidades e atributos é a primeira etapa do ABAC. Em seguida, você cria políticas ABAC para permitir operações quando a tag do principal corresponde à tag no recurso que eles estão tentando acessar.

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

Para obter mais informações sobre o ABAC, consulte O que é ABAC? no Guia do usuário do IAM. Para visualizar um tutorial com etapas para configurar o ABAC, consulte Usar controle de acesso baseado em atributos (ABAC) (Use attribute-based access control [ABAC]) no Guia do usuário do IAM.

## Usando credenciais temporárias com Nimble Studio

| | |
|---|---|
| Oferece suporte a credenciais temporárias | Sim |

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

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

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

## Permissões de entidades principais entre serviços para o Nimble Studio

| | |
|---|---|
| Oferece suporte a permissões de entidade principal | Sim |

## Perfis de serviço para o Nimble Studio

| | |
|---|---|
| Oferece suporte a perfis de serviço | Sim |

O perfil de serviço é um perfil do IAM que um serviço assume para realizar ações em seu nome. Os perfis de serviço fornecem acesso somente na sua conta e não podem ser usadas para conceder acesso a serviços em outras contas. Um administrador pode criar, modificar e excluir um perfil de serviço no IAM. Para obter mais informações, consulte Criando uma função para delegar permissões a um AWS service (Serviço da AWS) no Guia do usuário do IAM.

> **Warning**
>
> Alterar as permissões de um perfil de serviço pode interromper a funcionalidade do Nimble Studio. Edite perfis de serviço somente quando o Nimble Studio fornecer orientação para isso.

## Funções vinculadas ao serviço para o Nimble Studio

| | |
|---|---|
| Oferece suporte a perfis vinculados ao serviço | Não |

O Nimble Studio não oferece suporte às funções vinculadas ao serviço. Uma função vinculada ao serviço é um tipo de perfil de serviço vinculada a um AWS service (Serviço da AWS). O serviço pode presumir a função de executar uma ação em seu nome. As funções vinculadas ao serviço aparecem

em sua conta do IAM e são de propriedade do serviço. Um administrador do pode visualizar, mas não pode editar as permissões para funções vinculadas ao serviço.

Para obter detalhes sobre como criar ou gerenciar funções vinculadas ao serviço, consulte Serviços da AWS que trabalham com o IAM. Encontre um serviço na tabela que inclua um `Yes` na coluna Perfil vinculado ao serviço. Escolha o link Sim para visualizar a documentação do perfil vinculado a esse serviço .

## Exemplos de políticas baseadas em identidade para Amazon Nimble Studio

Por padrão, usuários e funções não têm permissão para criar ou modificar recursos do Nimble Studio. Eles também não podem executar tarefas usando AWS Management Console, AWS CLI ou uma API AWS. Um administrador deve criar políticas do IAM que concedam permissão aos usuários e funções para executar ações nos recursos de que precisam. O administrador deve anexar essas políticas aos usuários ou grupos que exigem essas permissões.

Para saber como criar uma política baseada em identidade do IAM usando esses exemplos de documentos de política JSON, consulte Criar políticas na guia JSON no Guia do usuário do IAM.

Tópicos

- Práticas recomendadas de políticas

### Práticas recomendadas de políticas

As políticas baseadas em identidade são muito eficientes. Eles determinam se alguém pode criar, acessar ou excluir recursos do Nimble Studio em sua conta. Essas ações podem incorrer em custos para a Conta da AWS. Ao criar ou editar políticas baseadas em identidade, siga estas diretrizes e recomendações:

- Comece a usar políticas gerenciadas por AWS – para começar a usar o Nimble Studio rapidamente, use políticas gerenciadas para conceder aos seus funcionários as permissões necessárias. Essas políticas já estão disponíveis em sua conta e são mantidas e atualizadas pela AWS. Para obter mais informações, consulte Introdução ao uso de permissões com políticas gerenciadas por AWS no Guia do usuário do IAM.
- Conceder privilégio mínimo: ao criar políticas personalizadas, conceda apenas as permissões necessárias para executar uma tarefa. Comece com um conjunto mínimo de permissões e conceda permissões adicionais conforme necessário. Fazer isso é mais seguro do que começar

com permissões que são muito lenientes e tentar restringi-las superiormente. Para obter mais informações, consulte Conceder privilégio mínimo no Guia do usuário do IAM.

- Habilitar MFA para operações confidenciais – para segurança extra, exija que os usuários usem autenticação multifator (MFA) para acessar recursos confidenciais ou operações de API. Para obter mais informações, consulte Usando autenticação multifator (MFA) no AWS no Guia do usuário do IAM.
- Utilize condições de política para segurança extra – Na medida em que for prático, defina as condições em que as suas políticas baseadas em identidade permitem o acesso a um recurso. Por exemplo, você pode gravar condições para especificar um intervalo de endereços IP permitidos do qual a solicitação deve partir. Você também pode escrever condições para permitir somente solicitações em uma data especificada ou período ou para exigir o uso de SSL ou MFA. Para obter mais informações, consulte Elementos de política JSON do IAM: condição no Guia do usuário do IAM.

## Políticas gerenciadas por AWS para o Amazon Nimble Studio

Para adicionar permissões a usuários, grupos e funções, é mais fácil usar políticas gerenciadas pela AWS do que elaborar políticas por conta própria. É necessário tempo e experiência para criar políticas gerenciadas pelo cliente do IAM que fornecem à sua equipe apenas as permissões de que precisam. Para começar rapidamente, você pode usar nossas políticas gerenciadas pela AWS. Essas políticas abrangem casos de uso comuns e estão disponíveis na sua Conta da AWS. Para obter mais informações sobre as políticas gerenciadas da AWS, consulte Políticas gerenciadas da AWS no IAM User Guide.

Os serviços da AWS mantêm e atualizam políticas gerenciadas pela AWS. Não é possível alterar as permissões em políticas gerenciadas pela AWS. Os serviços ocasionalmente acrescentam permissões adicionais a uma política gerenciada pela AWS para oferecer suporte a novos atributos. Esse tipo de atualização afeta todas as identidades (usuários, grupos e perfis) em que a política está anexada. É mais provável que os serviços atualizem uma política gerenciada pela AWS quando um novo atributo for iniciado ou novas operações se tornarem disponíveis. Os serviços não removem permissões de uma política gerenciada por AWS, portanto, as atualizações de políticas não quebrarão suas permissões existentes.

Além disso, a AWS oferece suporte a políticas gerenciadas para perfis de trabalho que abrangem vários serviços. Por exemplo, a política gerenciada pela denominada ReadOnlyAccess AWS fornece acesso somente leitura a todos os serviços e recursos da AWS. Quando um serviço executa um novo atributo, a AWS adiciona permissões somente leitura para novas operações e recursos. Para

obter uma lista e descrições das políticas de perfis de trabalho, consulte Políticas gerenciadas pela AWS para perfis de trabalho no Guia do usuário do IAM.

Seus usuários finais acessarão o Amazon Nimble Studio principalmente usando o portal do Nimble Studio. Ao criar seu estúdio usando o StudioBuilder ou o console do Nimble Studio, um perfil do IAM é criada para cada pessoa do estúdio: o administrador do estúdio e o usuário do estúdio. Cada um tem a respectiva política gerenciada do IAM anexada. O portal do Nimble Studio fornece uma experiência em que os usuários só podem listar e usar os recursos que eles têm permissão para acessar.

O portal do Nimble Studio fornece uma experiência em que os usuários só podem listar e usar os recursos aos quais têm acesso, e o portal depende do conteúdo dessas políticas para operar corretamente. Os usuários finais do Nimble Studio usarão o portal para acessar seu estúdio na nuvem. Portanto, quando os administradores criam seu estúdio usando o StudioBuilder, um perfil do IAM é criada para cada pessoa que precisa acessar o estúdio. Isso inclui o administrador do estúdio e o usuário do Studio, cada um com sua respectiva política gerenciada do IAM anexada.

Para obter uma lista e descrições de políticas de funções de trabalho, consulte Políticas gerenciadas por AWS para funções de trabalho no Guia do usuário do IAM.

## Política gerenciada da AWS: **`AmazonNimbleStudio-LaunchProfileWorker`**

É possível anexar a política `AmazonNimbleStudio-LaunchProfileWorker` a suas identidades do IAM.

Anexe essa política às instâncias do EC2 criadas pelo Nimble Studio Builder para conceder acesso aos recursos necessários aos trabalhadores do perfil de inicialização do Nimble Studio.

Detalhes das permissões

Esta política inclui as seguintes permissões.

- ds - Permite que os trabalhadores do LaunchProfile descubram informações de conexão AWS Managed Microsoft AD associadas a um LaunchProfile.
- ec2 - Permite que os trabalhadores do LaunchProfile descubram informações do grupo de segurança e da sub-red e para se conectar a um LaunchProfile.
- fsx - Permite que os trabalhadores do LaunchProfile descubram informações de conexão com os volumes do Amazon FSx associados a um LaunchProfile.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "fsx:DescribeFileSystems",
        "ds:DescribeDirectories"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:CalledViaLast": "nimble.amazonaws.com"
        }
      },
      "Sid": "GetLaunchProfileInitializationDependencies"
    }
  ],
  "Version": "2012-10-17"
}
```

## AWSPolítica gerenciada da : **AmazonNimbleStudio-StudioAdmin**

É possível anexar a política AmazonNimbleStudio-StudioAdmin a suas identidades do IAM.

Anexe essa política à função de administrador associada ao seu estúdio para conceder acesso aos recursos do Amazon Nimble Studio associados ao administrador do estúdio e aos recursos relacionados do estúdio em outros serviços.

Detalhes das permissões

Esta política inclui as seguintes permissões.

- nimble - Permite que os usuários do Studio acessem os recursos do Nimble que foram delegados a eles pelos StudioAdmins.
- sso - Permite que os usuários do Studio visualizem os nomes de outros usuários no estúdio.
- identitystore - Permite que os usuários do Studio visualizem os nomes de outros usuários no estúdio.

- ds - Permite que o Nimble Studio adicione estações de trabalho virtuais às AWS Managed Microsoft AD associadas ao estúdio.
- ec2 - Permite que o Nimble Studio conecte estações de trabalho virtuais à sua VPC configurada.
- fsx - Permite que o Nimble Studio conecte estações de trabalho virtuais aos seus volumes Amazon FSx configurados.
- cloudwatch - Permite que o Nimble Studio recupere métricas do CloudWatch.

```
{
  "Statement": [
    {
      "Sid": "StudioAdminFullAccess",
      "Effect": "Allow",
      "Action": [
        "nimble:CreateStreamingSession",
        "nimble:GetStreamingSession",
        "nimble:StartStreamingSession",
        "nimble:StopStreamingSession",
        "nimble:CreateStreamingSessionStream",
        "nimble:GetStreamingSessionStream",
        "nimble:DeleteStreamingSession",
        "nimble:ListStreamingSessionBackups",
        "nimble:GetStreamingSessionBackup",
        "nimble:ListEulas",
        "nimble:ListEulaAcceptances",
        "nimble:GetEula",
        "nimble:AcceptEulas",
        "nimble:ListStudioMembers",
        "nimble:GetStudioMember",
        "nimble:ListStreamingSessions",
        "nimble:GetStreamingImage",
        "nimble:ListStreamingImages",
        "nimble:GetLaunchProfileInitialization",
        "nimble:GetLaunchProfileDetails",
        "nimble:GetFeatureMap",
        "nimble:PutStudioLogEvents",
        "nimble:ListLaunchProfiles",
        "nimble:GetLaunchProfile",
        "nimble:GetLaunchProfileMember",
        "nimble:ListLaunchProfileMembers",
        "nimble:PutLaunchProfileMembers",
        "nimble:UpdateLaunchProfileMember",
```

```
        "nimble:DeleteLaunchProfileMember"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "sso-directory:DescribeUsers",
        "sso-directory:SearchUsers",
        "identitystore:DescribeUser",
        "identitystore:ListUsers"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "ds:CreateComputer",
        "ds:DescribeDirectories",
        "ec2:DescribeSubnets",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DeleteNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DescribeSecurityGroups",
        "fsx:DescribeFileSystems"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:CalledViaLast": "nimble.amazonaws.com"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": "cloudwatch:GetMetricData",
      "Resource": "*",
      "Condition": {
```

```
        "StringEquals": {
          "cloudwatch:namespace": "AWS/NimbleStudio"
        }
      }
    }
  ],
  "Version": "2012-10-17"
}
```

## AWSPolítica gerenciada da : **AmazonNimbleStudio-StudioUser**

É possível anexar a política AmazonNimbleStudio-StudioUser a suas identidades do IAM.

Anexe esta política à função de usuário associada ao seu estúdio para conceder acesso aos recursos do Amazon Nimble Studio associados ao usuário do estúdio e aos recursos de estúdio relacionados em outros serviços.

Detalhes das permissões

Esta política inclui as seguintes permissões.

- nimble - Permite que os usuários do Studio acessem os recursos do Nimble que foram delegados a eles pelos StudioAdmins.
- sso - Permite que os usuários do Studio visualizem os nomes de outros usuários no estúdio.
- identitystore - Permite que os usuários do Studio visualizem os nomes de outros usuários no estúdio.
- ds - Permite que o Nimble Studio adicione estações de trabalho virtuais às AWS Managed Microsoft AD associadas ao estúdio.
- ec2 - Permite que o Nimble Studio conecte estações de trabalho virtuais à sua VPC configurada.
- fsx - Permite que o Nimble Studio conecte estações de trabalho virtuais aos seus volumes Amazon FSx configurados.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ds:CreateComputer",
        "ec2:DescribeSubnets",
```

```
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeSecurityGroups",
        "fsx:DescribeFileSystems",
        "ds:DescribeDirectories"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:CalledViaLast": "nimble.amazonaws.com"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "sso-directory:DescribeUsers",
        "sso-directory:SearchUsers",
        "identitystore:DescribeUser",
        "identitystore:ListUsers"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "nimble:ListLaunchProfiles"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "nimble:requesterPrincipalId": "${nimble:principalId}"
        }
      }
    },
    {
      "Effect": "Allow",
```

```
      "Action": [
        "nimble:ListStudioMembers",
        "nimble:GetStudioMember",
        "nimble:ListEulas",
        "nimble:ListEulaAcceptances",
        "nimble:GetFeatureMap",
        "nimble:PutStudioLogEvents"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "nimble:StartStreamingSession",
        "nimble:StopStreamingSession",
        "nimble:DeleteStreamingSession",
        "nimble:GetStreamingSession",
        "nimble:CreateStreamingSessionStream",
        "nimble:GetStreamingSessionStream",
        "nimble:ListStreamingSessions"
        "nimble:ListStreamingSessionBackups",
        "nimble:GetStreamingSessionBackup"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "nimble:ownedBy": "${nimble:requesterPrincipalId}"
        }
      }
    }
  ],
  "Version": "2012-10-17"
}
```

## Atualizações do Nimble Studio para políticas AWS gerenciadas

Veja detalhes sobre atualizações nas políticas gerenciadas por AWS do Amazon Nimble Studio desde que esse serviço começou a monitorar essas alterações.

| Alteração | Descrição | Data |
| --- | --- | --- |
| AWSPolítica gerenciada da : AmazonNimbleStudio -StudioUser - Atualizar política | O Amazon Nimble Studio atualizou uma política para usar a versão mais recente do serviço Identity Store. | 22 de setembro de 2023 |
| AWSPolítica gerenciada da : AmazonNimbleStudio- StudioAdmin - Atualizar política | O Amazon Nimble Studio atualizou uma política para usar a versão mais recente do serviço Identity Store. | 22 de setembro de 2023 |
| AWSPolítica gerenciada da : AmazonNimbleStudio -StudioUser - Atualizar política | O Amazon Nimble Studio atualizou uma política para permitir que os usuários do estúdio visualizem seus backups de estações de trabalho. | 20 de dezembro de 2022 |
| AWSPolítica gerenciada da : AmazonNimbleStudio- StudioAdmin - Atualizar política | O Amazon Nimble Studio atualizou a política para permitir que os administr adores do estúdio visualizem seus backups de estações de trabalho. | 20 de dezembro de 2022 |
| AWSPolítica gerenciada da : AmazonNimbleStudio -StudioUser - Atualizar política | O Amazon Nimble Studio atualizou uma política para permitir que os administr adores do estúdio recuperem as métricas do CloudWatch. | 11 de novembro de 2021 |
| AWSPolítica gerenciada da : AmazonNimbleStudio -StudioUser - Atualizar política | O Amazon Nimble Studio atualizou a política para permitir que os usuários do estúdio iniciem e parem suas estações de trabalho. | 1º de novembro de 2023 |

| Alteração | Descrição | Data |
| --- | --- | --- |
| AWSPolítica gerenciada da : AmazonNimbleStudio-StudioAdmin - Atualizar política | O Amazon Nimble Studio atualizou a política para permitir que os administradores do estúdio iniciem e parem suas estações de trabalho. | 1º de novembro de 2023 |
| AWSPolítica gerenciada da : AmazonNimbleStudio-StudioUser - Atualizar política | O Amazon Nimble Studio atualizou a política para permitir condicionalmente o acesso aos recursos da sessão de streaming com base em `nimble:ownedBy` em vez de `nimble:createdBy` . | 16 de agosto de 2021 |
| AWSPolítica gerenciada da : AmazonNimbleStudio-StudioUser – Nova política | O Amazon Nimble Studio adicionou uma nova política que permite o acesso aos recursos associados ao usuário do estúdio e aos recursos relacionados do estúdio em outros serviços. | 28 de abril de 2021 |
| AWSPolítica gerenciada da : AmazonNimbleStudio-StudioAdmin - nova política | O Amazon Nimble Studio adicionou uma nova política que permite o acesso aos recursos associados ao administrador do estúdio e aos recursos relacionados do estúdio em outros serviços. | 28 de abril de 2021 |

| Alteração | Descrição | Data |
| --- | --- | --- |
| Política gerenciada da AWS: `AmazonNimbleStudio-LaunchProfileWorker` – Nova política | O Amazon Nimble Studio adicionou uma nova política que permite o acesso aos recursos necessários aos funcionários do perfil de inicialização do Nimble Studio. | 28 de abril de 2021 |
| O Amazon Nimble Studio passou a monitorar alterações | O Amazon Nimble Studio começou a monitorar alterações em suas políticas gerenciadas por AWS. | 28 de abril de 2021 |

## Prevenção contra o ataque do “substituto confuso” em todos os serviços

O problema do substituto confuso é um problema de segurança em que uma entidade que não tem permissão para executar uma ação pode coagir uma entidade mais privilegiada a executar a ação. Em AWS, a personificação entre serviços pode resultar no problema do "substituto confuso". A imitação entre serviços pode ocorrer quando um serviço (o serviço de chamada) chama outro serviço (o serviço chamado). O serviço de chamada pode ser manipulado para que ele use as respectivas permissões com o objetivo de acessar os recursos de outro cliente de uma forma que, normalmente, ele não deveria ter permissão. Para evitar isso, o AWS fornece ferramentas que ajudam você a proteger seus dados para todos os serviços com entidades principais de serviço que receberam acesso aos recursos em sua conta.

Recomendamos o uso das chaves de contexto de condição `aws:SourceAccount` global `aws:SourceArn` e de contexto em políticas de recursos para limitar as permissões que o Identity and Access Management (IAM) concede ao Amazon Nimble Studio para acessar seus recursos. Se você utilizar ambas as chaves de contexto de condição global, o valor `aws:SourceAccount` e a conta `aws:SourceArn` no valor deverão utilizar o mesmo ID de conta quando utilizados na mesma instrução de política.

O valor de `aws:SourceArn` deve ser o ARN do Studio e `aws:SourceAccount` deve ser o ID da sua conta. Você não saberá qual é o ID do estúdio até que o estúdio seja criado, pois ele é gerado pelo Nimble Studio. Depois que seu estúdio for criado, você poderá atualizar a política de confiança com o ID final do estúdio definido como `aws:SourceArn`.

A maneira mais eficaz de se proteger contra o problema do substituto confuso é usar a chave de contexto de condição global `aws:SourceArn` com o ARN completo do recurso. Se você não souber o ARN completo do recurso ou se estiver especificando vários recursos, use a chave de condição de contexto global `aws:SourceArn` com curingas (*) para as partes desconhecidas do ARN. Por exemplo, `arn:aws:nimble::123456789012:*`.

Seus usuários finais assumem sua função de estúdio quando entram no portal do Nimble Studio. Ao criar seu estúdio, AWS configura a função e avalia a política. AWS avalia a política toda vez que um de seus usuários fizer login no portal do Nimble Studio. Quando você cria um estúdio, não é possível modificar o `aws:SourceArn`. Depois de terminar de criar seu estúdio, você pode usar seu StudioARN para o `aws:SourceArn`.

O exemplo a seguir é uma política de assumir função que mostra como você pode usar as chaves de contexto de condição global `aws:SourceArn` e `aws:SourceAccount` no Nimble Studio para evitar o problema confused deputy.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "identity.nimble.amazonaws.com"
      },
      "Action": [
        "sts:AssumeRole",
        "sts:TagSession"
      ],
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "123456789012"
        },
        "StringLike": {
          "aws:SourceArn": "arn:aws:nimble:us-west-2:123456789012:studio/*"
        }
      }
    }
  ]
}
```

# Solução de problemas de identidade e acesso do Amazon Nimble Studio

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

Tópicos



## Não estou autorizado a realizar uma ação no Nimble Studio.

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

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

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

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

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

## Não estou autorizado a executar iam:PassRole.

Se você receber um erro informando que não está autorizado a executar a ação `iam:PassRole`, entre em contato com seu administrador para obter assistência. Peça que atualizem suas políticas para permitir que você passe uma função para o Nimble Studio.

Alguns Serviços da AWS permitem que você transmita uma função existente para o serviço, em vez de criar uma função de serviço ou uma função vinculada ao serviço. Para fazer isso, você precisa de permissões para passar a função ao serviço.

O erro de exemplo a seguir ocorre quando um usuário chamado `johndoe` tenta usar o console para executar uma ação no Nimble Studio. No entanto, a ação exige que o serviço tenha permissões concedidas por um perfil de serviço. John não tem permissões para passar a função para o serviço.

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

Nesse caso, John pede ao administrador para atualizar suas políticas para conceder permissão para executar a ação `iam:PassRole`.

## Quero visualizar minhas chaves de acesso

O Amazon Nimble Studio não fornece chaves de acesso. Para saber mais sobre chaves de acesso secretas, consulte Gerenciar chaves de acesso no Guia do usuário do IAM.

> **Important**
>
> Não forneça suas chaves de acesso a terceiros, mesmo para ajudar a encontrar seu ID de usuário canônico. Ao fazer isso, você pode dar a alguém acesso permanente à sua conta.

Ao criar um par de chaves de acesso, você será solicitado a salvar o ID da chave de acesso e a chave de acesso secreta em um local seguro. A chave de acesso secreta só está disponível no momento em que é criada. Se você perder sua chave de acesso secreta, adicione novas chaves de acesso ao seu usuário. Você pode ter no máximo duas chaves de acesso. Se você já possui dois, exclua um par de chaves antes de criar um novo. Para visualizar as instruções, consulte Gerenciar chaves de acesso no Guia do usuário do IAM.

## Sou administrador e quero permitir que outras pessoas acessem o Nimble Studio.

Para permitir que outras pessoas acessem o Nimble Studio, crie uma entidade IAM (usuário ou função) para a pessoa ou aplicativo que precisa de acesso. Elas usarão as credenciais dessa entidade para acessar a AWS. Em seguida, anexe uma política à entidade que conceda as permissões corretas.

O Nimble Studio fornece a a você `AmazonNimbleStudio-StudioUser` em AWS Management Console. O administrador de TI que gerencia o console usa essa política para conceder acesso ao estúdio a outras pessoas.

Para ver um tutorial sobre como usar a política administrativa, consulte o guia Configurar o Nimble Studio. Para saber como vincular políticas existentes aos usuários, como políticas de perfil de usuário e de lançamento, consulte Criação de usuários do IAM (console).

Para obter informações sobre como importar políticas, consulte Criar o primeiro usuário e grupo delegados do IAM no Guia do usuário do IAM.

## Quero permitir que pessoas fora da minha Conta da AWS acessem meus recursos do Nimble Studio.

Você pode criar um perfil que os usuários de outras contas ou pessoas fora da sua organização possam usar para acessar seus recursos. Você pode especificar quem é confiável para assumir o perfil. Para serviços que oferecem suporte a políticas baseadas em recurso 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 Nimble Studio oferece suporte a esses recursos, consulte Como o Amazon Nimble Studio funciona com o IAM.
- Para saber como fornecer acesso aos recursos Contas da AWS de sua propriedade, consulte Fornecendo acesso a um usuário do IAM em outro Conta da AWS de sua propriedade no Guia do usuário do IAM.
- Para saber como fornecer acesso aos seus recursos a terceiros Contas da AWS, consulte Fornecer acesso a recursos de propriedade de terceiros Contas da AWS no Guia do usuário do IAM.
- Para saber como conceder acesso por meio da federação de identidades, consulte Conceder acesso a usuários autenticados externamente (federação de identidades) no Guia do usuário do IAM.
- Para saber a diferença entre usar perfis e políticas baseadas em recursos para acesso entre contas, consulte Como os perfis do IAM diferem de políticas baseadas em recursos no Guia do usuário do IAM.

# Registro e monitoramento de eventos de segurança com o Nimble Studio

O monitoramento é uma parte importante para manter a confiabilidade, a disponibilidade e o desempenho do Amazon Nimble Studio e de suas soluções AWS. Colete dados de monitoramento de todas as partes da sua solução AWS para que você possa depurar mais facilmente uma falha multiponto, caso ela ocorra.

AWS e o Nimble Studio fornecem ferramentas para monitorar seus recursos e responder a incidentes potenciais, incluindo Registrando chamadas do Nimble Studio usando AWS CloudTrail e Guia do usuário AWS CloudFormation.

Para obter mais informações sobre como o Amazon Nimble Studio funcionaAWS CloudFormation, incluindo exemplos de modelos JSON e YAML, consulte a referência de recursos e propriedades do Amazon Nimble Studio no Guia do usuário AWS CloudFormation. Para entender como usar os modelos do CloudFormation, consulte conceitos AWS CloudFormation.

Tópicos



## Registrando chamadas do Nimble Studio usando AWS CloudTrail

O Amazon Nimble Studio está integrado ao AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, uma função ou um usuário AWS service (Serviço da AWS) no Nimble Studio. O CloudTrail captura todas as chamadas de API do Nimble Studio como eventos. As chamadas capturadas incluem chamadas do console do Nimble Studio e chamadas de código para as operações do Amazon Nimble Studio.

Se você criar uma trilha, poderá habilitar a entrega contínua de eventos do CloudTrail para um bucket do Amazon S3, incluindo eventos para o Nimble Studio. Se você não configurar uma trilha, ainda poderá visualizar os eventos mais recentes no console do CloudTrail em Histórico de eventos. Usando as informações coletadas pelo CloudTrail, você pode determinar a solicitação feita ao Nimble Studio, o endereço IP do qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita e detalhes adicionais.

## Informações sobre o Nimble Studio no CloudTrail

O CloudTrail é habilitado em sua Conta da AWS quando ela é criada. Quando ocorre uma atividade no Nimble Studio, essa atividade é registrada em um evento AWS service (Serviço da AWS) do CloudTrail junto com outros eventos no Histórico de eventos. Você pode exibir, pesquisar e baixar eventos recentes em sua Conta da AWS. Para obter mais informações, consulte Visualizar eventos com o histórico de eventos do CloudTrail.

Para um registro contínuo de eventos em seu Conta da AWS, incluindo eventos do Nimble Studio, crie uma trilha. Uma trilha permite que o CloudTrail entregue arquivos de log a um bucket do Amazon S3. Por padrão, quando você cria uma trilha no console, ela é aplicada a todas as Regiões da AWS. A trilha loga eventos de todas as Regiões na partição da AWS e entrega os arquivos de log para o bucket do Amazon S3 especificado por você. Além disso, você pode configurar outros Serviços da AWS para analisar melhor e agir com base nos dados de eventos coletados nos logs do CloudTrail.

Para obter mais informações, consulte as informações a seguir:

Visão geral da criação de uma trilha

Serviços e integrações compatíveis com o CloudTrail

Configuração notificações do Amazon SNS para o CloudTrail

Receber arquivos de log do CloudTrail de várias regiões

Receber arquivos de log do CloudTrail de várias contas

As ações do Nimble Studio são registradas pelo CloudTrail e documentadas na referência de API do Amazon Nimble Studio. Por exemplo, chamadas para as ações CreateStudio, GetStudio e DeleteStudio geram entradas nos arquivos de log do CloudTrail.

Cada entrada de log ou evento contém informações sobre quem gerou a solicitação. As informações de identidade ajudam a determinar:

- Se a solicitação foi feita com credenciais de usuário raiz ou usuário do IAM AWS Identity and Access Management
- Se a solicitação foi feita com credenciais de segurança temporárias de um perfil ou de um usuário federado.
- Se a solicitação foi feita por outro serviço da .

Para obter mais informações, consulte CloudTrail userIdentity element.

## Noções básicas sobre entradas do arquivo de log do Nimble Studio

Uma trilha é uma configuração que permite a entrega de eventos como arquivos de log a um bucket do Amazon S3 especificado. Os arquivos de log CloudTrail contêm uma ou mais entradas de log. Um evento representa uma única solicitação de qualquer fonte, e inclui informações sobre a ação solicitada, data e hora da ação, parâmetros de solicitação e assim por diante. Os arquivos de log do CloudTrail não são um rastreamento de pilha ordenado das chamadas de API públicas, portanto, não aparecem em nenhuma ordem específica.

Esse exemplo de JSON mostra três ações:

- AÇÃO_1: CreateStudio
- AÇÃO_2: GetStudio
- AÇÃO_3: DeleteStudio


```
{
    "eventVersion": "0",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "EXAMPLE-PrincipalID:EXAMPLE-Session",
        "arn": "arn:aws:sts::111122223333:assumed-role/EXAMPLE-UserName/EXAMPLE-
Session",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE-accessKeyId",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "EXAMPLE-PrincipalID",
                "arn": "arn:aws:iam::111122223333:role/EXAMPLE-UserName",
                "accountId": "111122223333",
                "userName": "EXAMPLE-UserName"
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2021-03-08T23:25:49Z"
            }
        }
    },
    "eventTime": "2021-03-08T23:25:49Z",
    "eventSource": "nimble.amazonaws.com",
```

```
    "eventName": "CreateStudio",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "EXAMPLE-userAgent",
    "requestParameters": {
        "displayName": "Studio Name",
        "studioName": "EXAMPLE-studioName",
        "userRoleArn": "arn:aws:iam::111122223333:role/EXAMPLE-ServiceRole-User",
        "adminRoleArn": "arn:aws:iam::111122223333:role/EXAMPLE-ServiceRole-Admin"
    },
    "responseElements": {},
    "requestID": "EXAMPLE-requestID",
    "eventID": "EXAMPLE-eventID",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "111122223333"
},
{
    "eventVersion": "0",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "EXAMPLE-PrincipalID:EXAMPLE-Session",
        "arn": "arn:aws:sts::111122223333:assumed-role/EXAMPLE-UserName/EXAMPLE-
Session",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE-accessKeyId",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "EXAMPLE-PrincipalID",
                "arn": "arn:aws:iam::111122223333:role/EXAMPLE-UserName",
                "accountId": "111122223333",
                "userName": "EXAMPLE-UserName"
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2021-03-08T23:44:25Z"
            }
        }
    },
    "eventTime": "2021-03-08T23:44:25Z",
```

```
    "eventSource": "nimble.amazonaws.com",
    "eventName": "GetStudio",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "EXAMPLE-userAgent",
    "requestParameters": {
        "studioId": "us-west-2-EXAMPLE-studioId"
    },
    "responseElements": null,
    "requestID": "EXAMPLE-requestID",
    "eventID": "EXAMPLE-eventID",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "111122223333"
},
{
    "eventVersion": "0",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "EXAMPLE-PrincipalID:EXAMPLE-Session",
        "arn": "arn:aws:sts::111122223333:assumed-role/EXAMPLE-UserName/EXAMPLE-
Session",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE-accessKeyId",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "EXAMPLE-PrincipalID",
                "arn": "arn:aws:iam::111122223333:role/EXAMPLE-UserName",
                "accountId": "111122223333",
                "userName": "EXAMPLE-UserName"
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2021-03-08T23:45:14Z"
            }
        }
    },
    "eventTime": "2021-03-08T23:44:14Z",
    "eventSource": "nimble.amazonaws.com",
    "eventName": "DeleteStudio",
```

```
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "EXAMPLE-userAgent",
    "requestParameters": {
        "studioId": "us-west-2-EXAMPLE-studioId"
    },
    "responseElements": {
        "studio": {
            "adminRoleArn": "arn:aws:iam::111122223333:role/EXAMPLE-ServiceRole-Admin",
            "displayName": "My New Studio Name",
            "homeRegion": "us-west-2",
            "ssoClientId": "EXAMPLE-ssoClientId",
            "state": "DELETING",
            "statusCode": "DELETING_STUDIO",
            "statusMessage": "Deleting studio",
            "studioEncryptionConfiguration": {
                "keyType": "AWS_OWNED_CMK"
            },
            "studioId": "us-west-2-EXAMPLE-studioId",
            "studioName": "EXAMPLE-studioName",
            "studioUrl": "https://sso111122223333.us-
west-2.portal.nimble.amazonaws.com",
            "tags": {},
            "userRoleArn": "arn:aws:iam::111122223333:role/EXAMPLE-ServiceRole-User"
        }
    },
    "requestID": "EXAMPLE-requestID",
    "eventID": "EXAMPLE-eventID",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "111122223333"
}
```


No exemplo, você notará que os eventos mostram a região, o endereço IP e outros “requestParameters”, como “UserRolearn” e “AdminRoLearn”, que ajudarão você a identificar o evento. Você pode ver a hora e a data em “CreationDate” e a origem da solicitação, marcada como “EventSource”: “nimble.amazonaws.com”.

O CloudTrail é habilitado em sua Conta da AWS quando ela é criada. Quando ocorre atividade no IAM ou STS AWS, essa atividade é registrada em um evento do CloudTrail junto com outros

eventos AWS service (Serviço da AWS) em Histórico de eventos. Você pode exibir, pesquisar e baixar eventos recentes em sua Conta da AWS.

O AWS CloudTrail captura todas as chamadas de API para IAM e () como eventos, incluindo chamadas do console e chamadas de API. Para saber mais sobre como usar o CloudTrail com o IAM AWS STS e consulte Registrar chamadas de IAM e API AWS STS com AWS CloudTrail

Para obter mais informações sobre o CloudTrail, consulte o Guia do usuário AWS CloudTrail.

Para obter informações sobre outros serviços de monitoramento que a Amazon oferece, consulte o Guia do usuário do Amazon CloudWatch.

# Validação de conformidade do Amazon Nimble Studio

O Amazon Nimble Studio segue o modelo de responsabilidade compartilhada, e a conformidade é compartilhada entre AWS e nossos clientes.

Para saber se um AWS service (Serviço da AWS) está no escopo de programas de conformidade específicos, consulte Serviços da AWS no escopo por programa de conformidade em que você está interessado. Para obter informações gerais, consulteAWS Programas de conformidade.

É possível fazer download de relatórios de auditoria de terceiros usando o AWS Artifact. Para obter mais informações, consulte Downloading Reports inAWS Artifact.

Sua responsabilidade de conformidade ao usar o Serviços da AWS é determinada pela confidencialidade dos seus dados, pelos objetivos de conformidade da sua empresa e pelos regulamentos e leis aplicáveis. A AWS fornece os seguintes atributos para ajudar com a conformidade:

- Guias de referência rápida de conformidade e segurança - estes guias de implantação discutem considerações sobre arquitetura e fornecem as etapas para a implantação de ambientes de linha de base focados em segurança e conformidade na AWS.
- Architecting for HIPAA Security and Compliance on Amazon Web Services (Arquitetura para segurança e conformidade com HIPAA no Amazon Web Services): esse estudo técnico descreve como as empresas podem usar a AWS para criar aplicações adequadas aos padrões HIPAA.

> **Note**
>
> Nem todos os Serviços da AWS estão qualificados pela HIPAA. Para obter mais informações, consulte a Referência dos serviços qualificados pela HIPAA.

- atributos de conformidade da AWS: essa coleção de manuais e guias pode ser aplicada a seu setor e local.
- Guias de conformidade do cliente da AWS: entenda o modelo de responsabilidade compartilhada sob a ótica da conformidade. Os guias resumem as práticas recomendadas para proteção de Serviços da AWS e mapeiam as diretrizes para controles de segurança em várias estruturas (incluindo o Instituto Nacional de Padrões e Tecnologia (NIST), o Conselho de Padrões de Segurança do Setor de Cartões de Pagamento (PCI) e a Organização Internacional de Padronização (ISO)).
- Avaliar atributos com regras no AWS Config Guia do desenvolvedor: o serviço AWS Config avalia como as configurações de atributos estão em conformidade com práticas internas, diretrizes do setor e regulamentos.
- AWS Security Hub: este AWS service (Serviço da AWS) fornece uma visão abrangente do seu estado de segurança na AWS. O Security Hub usa controles de segurança para avaliar os atributos da AWS e verificar a conformidade com os padrões e as práticas recomendadas do setor de segurança. Para obter uma lista dos serviços e controles aceitos, consulte a Referência de controles do Security Hub.
- AWS Audit Manager: esse AWS service (Serviço da AWS) ajuda a auditar continuamente seu uso da para simplificar a forma como você gerencia os riscos e a conformidade com regulamentos e padrões do setor.

## Segurança da infraestrutura no Amazon Nimble Studio

Como serviço gerenciado, o Amazon Nimble Studio é protegido pela segurança de rede global AWS. Para obter informações sobre serviços de segurança da AWS e como a AWS protege a infraestrutura, consulte Segurança na nuvem da AWS. Para projetar seu ambiente da AWS usando as práticas recomendadas de segurança de infraestrutura, consulte Proteção de infraestrutura em Pilar de segurança: AWS Well-Architected Framework.

Você usa chamadas de API publicadas por AWS para acessar o Nimble Studio pela rede. Os clientes precisam oferecer suporte para:

- Transport Layer Security (TLS). Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Conjuntos de criptografia com sigilo de encaminhamento perfeito (perfect forward secrecy, ou PFS) como DHE (Ephemeral Diffie-Hellman, ou Efêmero Diffie-Hellman) ou ECDHE (Ephemeral Elliptic Curve Diffie-Hellman, ou Curva elíptica efêmera Diffie-Hellman). A maioria dos sistemas modernos, como Java 7 e versões posteriores, comporta esses modos.

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

# Melhores práticas de segurança do Nimble Studio

O Amazon Nimble Studio oferece vários atributos de segurança a serem considerados ao desenvolver e implementar suas próprias políticas de segurança. As melhores práticas a seguir são diretrizes gerais e não representam uma solução completa de segurança. Como essas melhores práticas podem não ser adequadas ou suficientes para o seu ambiente, trate-as como considerações úteis em vez de prescrições.

## Monitoramento

O monitoramento é uma parte importante para manter a confiabilidade, a disponibilidade e o desempenho do Nimble Studio e de suas soluções AWS. Para obter mais informações sobre monitoramento e resposta aos eventos, consulte Registro e monitoramento de eventos de segurança com o Nimble Studio.

## Proteção de dados

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

- Use uma autenticação multifator (MFA [multi-factor authentication]) com cada conta.
- Use SSL/TLS para se comunicar com os recursos da AWS. Recomendamos TLS 1.2 ou posterior.
- Configure o registro em log das atividades da API e do usuário com o .AWS CloudTrail

- Use AWS as soluções de criptografia da , juntamente com todos os controles de segurança padrão dos Serviços da AWS.
- Use serviços gerenciados de segurança avançada, como o Amazon Macie, que ajuda a localizar e proteger dados pessoais armazenados no Amazon S3.
- Se você precisar de módulos criptográficos validados pelo FIPS 140-2 ao acessar a AWS por meio de uma interface de linha de comando ou uma API, use um endpoint do FIPS. Para obter mais informações sobre endpoints do FIPS, consulte Federal Information Processing Standard (FIPS) 140-2.

É altamente recomendável que você nunca coloque informações de identificação confidenciais, como números de conta dos seus clientes, em campos de formato livre, como um campo Name (Nome). Isso inclui quando você trabalha com o Amazon Nimble Studio ou outro Serviços da AWS usando o console, API, AWS CLI ou SDKs AWS. Todos os dados inseridos no Amazon Nimble Studio ou em outros serviços podem ser coletados para inclusão em logs de diagnóstico. Ao fornecer um URL para um servidor externo, não inclua informações de credenciais no URL para validar a solicitação a esse servidor.

## Permissões

Gerencie o acesso aos recursos AWS usando usuários, funções do IAM e concedendo o mínimo de privilégios aos usuários. Estabeleça políticas e procedimentos de gerenciamento de credenciais para criar, distribuir, rotacionar e revogar credenciais de acesso da AWS. Para obter mais informações, consulte Melhores práticas do IAM no Guia do usuário do IAM.

# Suporte para o Nimble Studio

Esta seção fornece opções de suporte para o Nimble Studio, como obter ajuda ao implantar ou usar o serviço e suas aplicações relacionadas.

Índice



## Fórum do Nimble Studio

Se você tiver dúvidas sobre o Nimble Studio, visite o fórum do Nimble Studio. Lá você pode obter respostas da comunidade e dos moderadores do fórum AWS sobre os atributos, problemas técnicos e ajuda para solução de problemas do Nimble Studio.

## Suporte de aplicações

O Nimble Studio fornece documentação adicional para as seguintes aplicações.

### AWSThinkboxDeadline

Para obter ajuda com seu parque de renderização ou para saber como Deadline funciona, consulte a documentação AWSThinkboxDeadline.

### Nimble Studio File Transfer

Para saber como a transferência de arquivos funciona, consulte o Guia do usuário do Nimble Studio File Transfer.

## AWS Support Center

O Centro AWS Support é um centro para criar e gerenciar seus casos de suporte. Ele fornece acesso a uma variedade de recursos, incluindo soluções técnicas e de cobrança, um centro de

conhecimento, vídeos do centro de conhecimento, documentação AWS, além de treinamento e certificação.

## Planos do AWS Support

Os planos AWS Support ajudam você a otimizar o desempenho, permanecer seguro, evitar o tempo de inatividade e controlar os custos. Para obter mais informações sobre planos AWS Support, consulte Comparar planos AWS Support.

Para obter mais informações sobre como AWS pode ajudá-lo, acesse a página Fale conosco.

# Histórico do documentos

- Versão da API: mais recente
- Última atualização na documentação: 22 de setembro de 2023.

A tabela a seguir descreve as mudanças importantes em cada versão do Guia do administrador do Nimble.

| Alteração | Descrição | |
|---|---|---|
| Serviço e guia novos | Esta é a versão inicial do Amazon Nimble Studio e do Guia do Administrador do Amazon Nimble Studio. | 19 de junho de 2023 |
| Atualização da política gerenciada AWS | Atualizou as políticas `AmazonNimbleStudio-StudioUser` e `AmazonNimbleStudio-StudioAdmin` para usar a versão mais recente do serviço AWS IAM Identity Center. | 22 de setembro de 2023 |

# Glossário do AWS

Para obter a terminologia mais recente da AWS, consulte o glossário da AWS na Referência do Glossário da AWS.