



Manual do usuário

Migration Hub Strategy Recommendations



Migration Hub Strategy Recommendations: Manual do usuário

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

As marcas comerciais e imagens comerciais 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 são propriedade da Amazon pertencem aos respectivos proprietários, os quais podem ou não ser afiliados, estar conectados ou ser patrocinados pela Amazon.

Table of Contents

O que é o Migration Hub Strategy Recommendations?	1
Você está usando o Strategy Recommendations pela primeira vez?	1
Visão geral	2
Serviços relacionados	2
Configuração	4
Inscreva-se para um Conta da AWS	4
Criar um usuário com acesso administrativo	4
Strategy Recommendations: usuários e funções	6
Conceitos básicos	8
Pré-requisitos	8
Etapa 1: fazer download do coletor	10
Etapa 2: implantar o coletor	11
Implantar o coletor no vCenter	11
Implantar a AMI do coletor	12
Etapa 3: fazer login no coletor	14
Fazer login no coletor implantado no vCenter	14
Fazer login no coletor implantado como uma instância do Amazon EC2	14
Etapa 4: configurar o coletor	15
Configurações de AWS	16
Configurações do vCenter	17
Configurações do servidor remoto	20
Configurações de controle de versão	22
Preparar seus servidores remotos para a coleta de dados	24
Verifique a configuração para coleta de dados	27
Etapa 5: obter recomendações	29
Recomendações	32
Ver recomendações de estratégias	32
Recomendações de componentes de aplicações	33
Trabalho com componentes de aplicações	34
Análise de código-fonte	36
análise de banco de dados	37
Análise binária	39
Recomendações de servidor	40
Preferences	41

Fontes de dados	42
Ver fontes de dados	42
Coletor de dados de aplicações	42
Dados coletados pelo coletor	43
Atualizar o coletor	46
Como importar dados	47
Modelo de importação	47
Remover dados	52
Segurança	53
Proteção de dados	53
Criptografia em repouso	55
Criptografia em trânsito	55
Gerenciamento de identidade e acesso	55
Público	55
Autenticando com identidades	56
Gerenciamento do acesso usando políticas	60
Como o Migration Hub Strategy Recommendations funciona com o IAM	63
AWS políticas gerenciadas	70
Exemplos de políticas baseadas em identidade	76
Solução de problemas	80
Usar perfis vinculados ao serviço	84
VPC endpoints (AWS PrivateLink)	86
Validação de conformidade	88
Trabalhar com outros serviços da	90
AWS CloudTrail	90
Informações do Strategy Recommendations no CloudTrail	90
Noções básicas sobre as entradas de arquivos de log do Strategy Recommendations	92
Cotas	94
Notas de release	95
17 de novembro de 2023	95
12 de outubro de 2023	95
17 de abril de 2023	96
17 de março de 2023	96
7 de novembro de 2022	96
27 de setembro de 2022	96
30 de junho de 2022	97

18 de abril de 2022	97
25 de fevereiro de 2022	97
10 de fevereiro de 2022	97
28 de janeiro de 2022	98
14 de janeiro de 2022	98
21 de dezembro de 2021	98
15 de dezembro de 2021	98
25 de outubro de 2021	99
Histórico do documento	100
.....	cii

O que é o Migration Hub Strategy Recommendations?

O Migration Hub Strategy Recommendations ajuda você a planejar iniciativas de migração e modernização ao oferecer recomendações de estratégia de migração e modernização para caminhos de transformação viáveis para suas aplicações.

O Strategy Recommendations pode analisar seu inventário de servidores, ambiente de runtime e binários de aplicações para aplicações Microsoft IIS e Java Tomcat e Jboss para gerar relatórios antipadrões. Além disso, você pode configurar seu código-fonte para permitir que o Strategy Recommendations realize análises de código-fonte e banco de dados de todas as suas aplicações. O Strategy Recommendations compara essa análise com suas metas de negócios e com as preferências de transformação das aplicações e bancos de dados que você forneceu para recomendar:

- A estratégia de migração mais eficaz para cada uma das suas aplicações.
- Ferramentas ou serviços de migração e modernização que você pode usar.
- Incompatibilidades e antipadrões de aplicações a serem resolvidos para uma opção específica.

O Migration Hub Strategy Recommendations recomenda estratégias de migração e modernização para redefinição de hospedagem, redefinição de plataformas e refatoração com destinos de implantação, ferramentas e programas associados. Para obter informações sobre redefinição de hospedagem, redefinição de plataformas e refatoração, consulte [Termos de migração - 7 Rs](#) no glossário das Recomendações da AWS.

O Strategy Recommendations pode recomendar opções simples, como a redefinição de hospedagem no Amazon Elastic Compute Cloud (Amazon EC2) usando o AWS Application Migration Service (AWS MGN). Recomendações mais otimizadas podem incluir a redefinição de plataforma em contêineres usando o AWS App2Container ou a refatoração para tecnologias de código aberto, como o .NET Core e PostgreSQL.

Você está usando o Strategy Recommendations pela primeira vez?

Se esta for a primeira vez que você usa o Strategy Recommendations, recomendamos que você leia as seguintes seções:

- [Visão geral do Strategy Recommendations](#)

- [Configuração do Strategy Recommendations](#)
- [Conceitos básicos do Strategy Recommendations](#)

Visão geral do Strategy Recommendations

Você pode iniciar a avaliação do seu portfólio de servidores e aplicações usando o Migration Hub Strategy Recommendations no console do AWS Migration Hub. Você usa o console para configurar e realizar uma avaliação. Após a avaliação, você pode usar o console para visualizar os dados de avaliação de cada servidor e aplicação, junto com a ferramenta de transformação recomendada.

Para receber recomendações de refatoração e uma lista de incompatibilidades, você pode usar o Strategy Recommendations para avaliar o código-fonte e os bancos de dados da sua aplicação.

Você também pode baixar os dados de recomendações em um arquivo do Microsoft Excel.

Serviços relacionados

- [AWS Migration Hub](#) — Você usa o console do AWS Migration Hub para acessar o console do Migration Hub Strategy Recommendations. Ele também exibe informações sobre os servidores dos quais você está coletando dados.
- [AWS Application Discovery Service](#) — Você usa o Application Discovery Service para coletar dados sobre seus servidores e aplicações no console do AWS Migration Hub antes de usar o Strategy Recommendations.
- [AWS Application Migration Service](#) — O AWS Application Migration Service é o principal serviço de migração recomendado para migrações sem alterações (lift-and-shift) para a AWS.
- [AWS Database Migration Service](#) — O AWS Database Migration Service é um serviço web que você pode usar para migrar dados do seu banco de dados on-premises, em uma instância de banco de dados do Amazon Relational Database Service (Amazon RDS) ou em um banco de dados em uma instância do Amazon Elastic Compute Cloud (Amazon EC2) para um banco de dados em um produto do AWS.
- [AWS App2Container](#) — O AWS App2Container (A2C) é uma ferramenta da linha de comando para modernizar aplicações .NET e Java em aplicações em contêineres.
- [Assistente de Portabilidade para .NET](#) — Use para análise de código-fonte de .NET. O Assistente de Portabilidade para .NET é um scanner de compatibilidade que reduz o esforço manual necessário para fazer a portabilidade de aplicações do Microsoft .NET Framework para o .NET

Core. O Assistente de Portabilidade para .NET avalia o código-fonte da aplicação .NET e identifica APIs incompatíveis e pacotes de terceiros.

- [Programa de migração de fim de ciclo de suporte para Windows Server](#) — O Programa de migração de fim de ciclo de suporte (EMP) para Windows Server inclui ferramentas para migrar suas aplicações legadas do Windows Server 2003, 2008 e 2008 R2 para versões mais novas e compatíveis na AWS, sem qualquer refatoração.
- [AWS Schema Conversion Tool](#) — Você pode usar o AWS Schema Conversion Tool (AWS SCT) para converter seu esquema de banco de dados existente de um mecanismo de banco de dados para outro.
- [Windows Web Application Migration Assistant](#) — O Windows Web Application Migration Assistant para AWS Elastic Beanstalk é um utilitário PowerShell interativo que migra aplicações ASP.NET e ASP.NET Core dos servidores IIS Windows on-premises para o Elastic Beanstalk.
- [Babelfish para Aurora PostgreSQL](#) — O Babelfish para Aurora PostgreSQL é um novo recurso para a edição compatível com o Amazon Aurora PostgreSQL que permite que o Aurora compreenda comandos de aplicações criadas para o Microsoft SQL Server.

Configuração do Strategy Recommendations

Antes de usar o Migration Hub Strategy Recommendations pela primeira vez, execute as seguintes tarefas:

Tópicos

- [Inscreva-se para um Conta da AWS](#)
- [Criar um usuário com acesso administrativo](#)
- [Strategy Recommendations: usuários e funções](#)

Inscreva-se para um Conta da AWS

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

Para se inscrever em um Conta da AWS

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

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

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

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

Criar um usuário com acesso administrativo

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

Proteja seu Usuário raiz da conta da AWS

1. Faça login [AWS Management Console](#) como proprietário da conta escolhendo Usuário raiz e inserindo seu endereço de Conta da AWS e-mail. Na próxima página, digite sua senha.

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

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

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

Criar um usuário com acesso administrativo

1. Habilitar o IAM Identity Center.

Para obter instruções, consulte [Habilitar AWS IAM Identity Center](#) no Guia do usuário do AWS IAM Identity Center .

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

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

Iniciar sessão como o usuário com acesso administrativo

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

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

Atribuir acesso para usuários adicionais

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

Para obter instruções, consulte [Create a permission set](#) no Guia do usuário do AWS IAM Identity Center .

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

Para obter instruções, consulte [Add groups](#) no Guia do usuário do AWS IAM Identity Center .

Strategy Recommendations: usuários e funções

Recomendamos que você crie duas funções para o Strategy Recommendations:

- Para acessar o console, crie uma função com ambas as políticas gerenciadas anexadas `AWSMigrationHubFullAccess` e `AWSMigrationHubStrategyConsoleFullAccess`.
- Para acessar o coletor de dados de aplicações do Strategy Recommendations, crie uma função com a política gerenciada anexada `AWSMigrationHubStrategyCollector`.

As políticas gerenciadas do IAM definem o nível de acesso ao serviço por usuários.

A política AWS Migration Hub `AWSMigrationHubFullAccess` gerenciada concede acesso ao console do Migration Hub. Para obter mais informações, consulte [Funções e políticas do Migration Hub](#). Para obter mais informações sobre as políticas gerenciadas `AWSMigrationHubStrategyConsoleFullAccess` e `AWSMigrationHubStrategyCollector`, consulte [AWS políticas gerenciadas para recomendações estratégicas do Migration Hub](#).

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

- Usuários e grupos em AWS IAM Identity Center:

Crie um conjunto de permissões. Siga as instruções em [Criação de um conjunto de permissões](#) no Guia do usuário do AWS IAM Identity Center .

- Usuários gerenciados no IAM com provedor de identidades:

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

- Usuários do IAM:

- Crie um perfil que seu usuário possa assumir. Siga as instruções em [Criação de um perfil para um usuário do IAM](#) no Guia do usuário do IAM.

- (Não recomendado) Vincule uma política diretamente a um usuário ou adicione um usuário a um grupo de usuários. Siga as instruções em [Adição de permissões a um usuário \(console\)](#) no Guia do usuário do IAM.

Conceitos básicos do Strategy Recommendations

Esta seção descreve como começar a usar o Migration Hub Strategy Recommendations.

Tópicos

- [Pré-requisitos para o Strategy Recommendations](#)
- [Etapa 1: fazer download do coletor do Strategy Recommendations](#)
- [Etapa 2: implantar o coletor do Strategy Recommendations](#)
- [Etapa 3: fazer login no coletor do Strategy Recommendations](#)
- [Etapa 4: configurar o coletor do Strategy Recommendations](#)
- [Etapa 5: use o Strategy Recommendations no console do Migration Hub para obter recomendações](#)

Pré-requisitos para o Strategy Recommendations

A seguir estão os pré-requisitos para usar o Migration Hub Strategy Recommendations.

- Você deve ter uma ou mais AWS contas e usuários configurados para essas contas. Para ter mais informações, consulte [Configuração do Strategy Recommendations](#).
- O cliente do coletor de dados de aplicações do Strategy Recommendations deve ser capaz de coletar dados remotamente dos servidores. Isso requer que você use um conjunto de credenciais que funcione para todos os seus servidores Windows e um conjunto de credenciais que funcione para todos os seus servidores Linux. As credenciais devem ter permissões para criar e excluir diretórios em seus servidores.
- A versão do coletor que é implantada no vCenter oferece suporte ao VMware vCenter Server V6.0, V6.5, 6.7 ou 7.0.

Você também pode implantar o coletor em uma instância do Amazon EC2 usando a AMI do coletor.

- Verifique se o ambiente do sistema operacional (SO) é compatível:
 - Linux
 - Amazon Linux 2012.03, 2015.03
 - Amazon Linux 2 (atualização de 25/9/2018 e posteriores)
 - Ubuntu 12.04, 14.04, 16.04, 18.04, 20.04

- Red Hat Enterprise Linux 5.11, 6.10, 7.3, 7.7, 8.1
- CentOS 5.11, 6.9, 7.3
- SUSE 11 SP4, 12 SP5
- Windows
 - Windows Server 2008 R1 SP2, 2008 R2 SP1
 - Windows Server 2012 R1, 2012 R2
 - Windows Server 2016
 - Windows Server 2019
- Para análise do código-fonte, seus repositórios GitHub e o GitHub Enterprise devem ter um token de acesso pessoal com o escopo do repositório que possa ser compartilhado com o cliente coletor de Recomendações de Estratégia. Para obter mais informações sobre como criar um token de acesso pessoal com o escopo do repositório, consulte [Criação de um token de acesso pessoal](#) nos GitHubDocumentos.

Para analisar repositórios .NET para recomendações do Assistente de Portabilidade para .NET, você deve fornecer uma máquina Windows configurada com a ferramenta de avaliação de portabilidade do Assistente de Portabilidade para .NET. Para obter mais informações, consulte [Introdução ao Assistente de Portabilidade para .NET](#) no Guia do usuário do Assistente de Portabilidade para .NET.

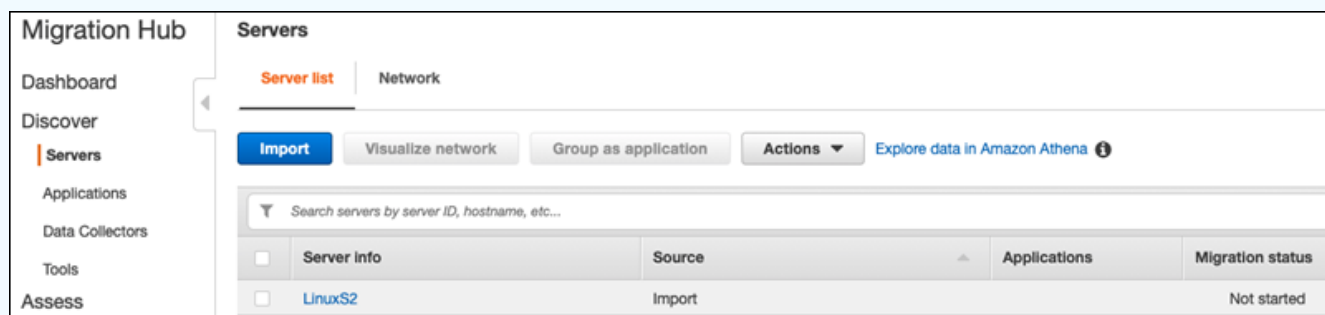
- Para habilitar o Strategy Recommendations para análise de banco de dados, você deve inserir credenciais no AWS Secrets Manager. Para ter mais informações, consulte [Análise do banco de dados do Strategy Recommendations](#).
- Você deve usar AWS Application Discovery Service para coletar dados sobre seus servidores e aplicativos no AWS Migration Hub console antes de usar as Recomendações de Estratégia. É possível usar um dos métodos a seguir para coletar os dados.
 - Importação do Migration Hub: com a importação do Migration Hub, você pode importar informações sobre seus servidores e aplicações on-premises para o Migration Hub. Para obter mais informações, consulte [Importação do Migration Hub](#) no Guia de usuário do Application Discovery Service.
 - AWS Application Discovery Service Agentless Collector: o Agentless Collector é um dispositivo VMware que coleta informações sobre máquinas virtuais (VMs) VMware. Para obter mais informações, consulte [Agentless Coletor](#) no Guia do usuário do Application Discovery Service.
 - AWS Application Discovery Agent — O Discovery Agent é um AWS software que você instala em seus servidores e VMs locais para capturar informações do sistema e detalhes das conexões

de rede entre os sistemas. Para obter mais informações, consulte [AWS Application Discovery Agent](#) no Guia do usuário do Application Discovery Service.

- Coletor de dados do Strategy Recommendations : se seus servidores estiverem hospedados no VMware vCenter e você fornecer acesso, o Strategy Recommendations poderá buscar automaticamente seu inventário de servidores. O console do Strategy Recommendations usará as informações coletadas para auxiliar na avaliação.

Note

Para verificar se a importação do Migration Hub foi concluída com êxito, no painel de navegação do console do Migration Hub, em Descobrir, escolha Servidores. Todos os servidores importados deve ser listados.



Etapa 1: fazer download do coletor do Strategy Recommendations

O coletor de dados de aplicações Migration Hub Strategy Recommendations é um dispositivo virtual que você pode instalar em seu ambiente VMware on-premises. O coletor de dados de aplicações do Strategy Recommendations também está disponível como uma imagem de máquina da Amazon (AMI). Se você quiser usar a versão AMI do coletor para avaliar AWS aplicativos ou por algum outro motivo, não precisa baixar o coletor. Você pode pular esta seção e ir para [Implantar o coletor do Strategy Recommendations em uma instância do Amazon EC2](#).

Esta seção descreve como baixar o arquivo Open Virtualization Archive (OVA) do coletor que você usa para implantar o coletor como uma máquina virtual (VM) em seu ambiente VMware.

Para fazer download do arquivo OVA do coletor

1. Usando a AWS conta que você criou [Configuração do Strategy Recommendations](#), entre AWS Management Console e abra o console do Migration Hub em <https://console.aws.amazon.com/migrationhub/>.
2. No painel de navegação do console Migration Hub, escolha Estratégia.
3. Na página Migration Hub Strategy Recommendations, escolha Fazer download do coletor de dados.
4. Você também pode escolher Fazer download do modelo de importação se quiser importar dados da aplicação. Para mais informações sobre como importar dados, consulte [Importar dados para o Strategy Recommendations](#).
5. Clique no botão Obter recomendações e escolha Concordar para permitir que o Migration Hub crie um perfil vinculado ao serviço (SLR) em sua conta. Ao configurar o Strategy Recommendations pela primeira vez, é necessário criar o SLR. Para ter mais informações, consulte [Usar perfis vinculados ao serviço do Strategy Recommendations](#).

Etapa 2: implantar o coletor do Strategy Recommendations

Esta seção descreve como implantar o coletor de dados de aplicações do Strategy Recommendations. Um coletor de dados de aplicações é um coletor de dados sem agente que identifica aplicações em execução em seus servidores, realiza análises de código-fonte e analisa seus bancos de dados.

Há duas maneiras de implantar o coletor:

- Implante-o como uma máquina virtual (VM) em seu VMware vCenter Server. Para ter mais informações, consulte [Implantar o coletor do Strategy Recommendations no vCenter](#).
- Se você tem AWS aplicativos que deseja avaliar, pode usar o coletor de recomendações estratégicas Amazon Machine Image (AMI). Para ter mais informações, consulte [Implantar o coletor do Strategy Recommendations em uma instância do Amazon EC2](#).

Implantar o coletor do Strategy Recommendations no vCenter

O coletor de dados de aplicações do Migration Hub Strategy Recommendations é um dispositivo virtual que você pode instalar em seu ambiente VMware on-premises. Esta seção descreve como

implantar o arquivo Open Virtualization Archive (OVA) do coletor como uma máquina virtual (VM) em seu ambiente VMware.

O procedimento a seguir descreve como implantar o coletor do Strategy Recommendations no ambiente do VMware vCenter Server.

Para implantar o coletor no vCenter

1. Faça login no vCenter como um administrador VMware.
2. Implante o arquivo OVA baixado na etapa 1. O arquivo OVA inclui o coletor e uma CLI que pode ser usada para acessar a API do Strategy Recommendations.

Você também pode fazer download do arquivo OVA pelo link a seguir:

<https://application-data-collector-release.s3.us-west-2.amazonaws.com/ova/latest/AWSMHubApplicationDataCollector.ova>

Recomendamos as seguintes especificações para a VM.

Especificações da VM do coletor do Strategy Recommendations

- RAM: um mínimo de 8 GB
- CPUs: pelo menos 4

Note

Para garantir que você esteja usando a versão mais recente do coletor com todos os novos atributos e correções de erros, atualize o coletor depois de implantar o arquivo OVA do coletor. Para obter instruções sobre como realizar um upgrade, consulte [Atualizar o coletor do Strategy Recommendations](#).

Implantar o coletor do Strategy Recommendations em uma instância do Amazon EC2

Se você tem AWS aplicativos que gostaria de avaliar, pode usar o coletor de dados do aplicativo Strategy Recommendations Amazon Machine Image (AMI).

O procedimento a seguir descreve como iniciar uma instância do Amazon EC2 com a AMI do coletor.

Para implantar a instância do Amazon EC2 do coletor

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. Na barra de navegação na parte superior da tela, a região atual é exibida [por exemplo, Leste dos EUA (Ohio)]. Escolha uma região que atenda às suas necessidades entre as regiões que o Strategy Recommendations usa. Para obter uma lista dessas regiões, consulte os [Endpoints de Strategy Recommendations](#) no Referência geral da AWS.
3. No painel de navegação, em Imagens, escolha AMIs.
4. Escolha Imagens públicas no menu suspenso De minha propriedade.
5. Escolha a barra de pesquisa e selecione Nome da AMI no menu.
6. Insira o nome AWSMHubApplicationDataCollector.
7. Para garantir que a AMI seja de uma fonte segura, verifique se o proprietário da conta é 703163444405.
8. Para executar uma instância baseada nesta AMI, selecione-a e escolha Iniciar. Para obter mais informações sobre como iniciar uma instância usando o console, consulte Como [iniciar sua instância a partir de uma AMI](#) no Guia do usuário do Amazon EC2.

Recomendamos as seguintes especificações para a instância do Amazon EC2.

Especificações da instância do Amazon EC2 do coletor do Strategy Recommendations

- RAM: um mínimo de 8 GB
- CPUs: pelo menos 4

A AMI do Strategy Recommendations inclui o coletor e uma CLI que podem ser usados para acessar a API do Strategy Recommendations.

Note

Para garantir que você esteja usando a versão mais recente do coletor com todos os novos atributos e correções de erros, atualize o coletor depois de implantar o coletor do Strategy Recommendations como uma instância do Amazon EC2. Para obter instruções sobre como realizar um upgrade, consulte [Atualizar o coletor do Strategy Recommendations](#).

Etapa 3: fazer login no coletor do Strategy Recommendations

Esta seção descreve como fazer login no coletor de dados de aplicações do Migration Hub Strategy Recommendations implantado. A forma como você faz login no coletor depende de como você implantou.

- [Fazer login no coletor implantado no ambiente baseado no vCenter](#)
- [Fazer login no coletor implantado como uma instância do Amazon EC2](#)

Fazer login no coletor implantado no ambiente baseado no vCenter

Para fazer login no coletor do Strategy Recommendations implantado no ambiente baseado no vCenter

1. Utilize o comando a seguir para se conectar ao coletor usando um cliente SSH.

```
ssh ec2-user@CollectorIPAddress
```

2. Quando for solicitada uma senha, insira a senha padrão `aq1@WSde3`. Você deverá alterar a senha no seu primeiro acesso à conta.

Fazer login no coletor implantado como uma instância do Amazon EC2

Para fazer login no coletor do Strategy Recommendations implantado como uma instância do Amazon EC2

- Utilize o comando a seguir para se conectar ao coletor usando um cliente SSH.

```
ssh -i "Keyname.pem" ec2-user@CollectorIPAddress
```

`Keyname.pem` é a chave privada que foi gerada quando você executou a instância do Amazon EC2 partindo do coletor AMI.

Etapa 4: configurar o coletor do Strategy Recommendations

Esta seção descreve como usar os comandos `collector setup` da linha de comando para configurar o coletor de dados de aplicações do Migration Hub Strategy Recommendations. Essas configurações são armazenadas localmente.

Antes de usar comandos do `collector setup`, você deve criar uma sessão bash shell no contêiner do Docker do coletor usando o comando `docker exec` a seguir.

```
docker exec -it application-data-collector bash
```

O comando `collector setup` executa todos os comandos a seguir em sequência, mas você pode executá-los individualmente:

- `collector setup --aws-configurations` — Defina as configurações da AWS.
- `collector setup --vcenter-configurations` — Defina as configurações do vCenter.

Note

A configuração do vCenter só estará disponível se o coletor estiver hospedado no vCenter. No entanto, você pode forçar a configuração do vCenter usando o comando `collector setup --vcenter-configurations`.

- `collector setup --remote-server-configurations` — Defina as configurações do servidor remoto.
- `collector setup --version-control-configurations` — Defina as configurações de controle de versão.

Para definir todas as configurações do coletor ao mesmo tempo

1. Insira o comando a seguir.

```
collector setup
```

2. Insira as informações para configurações da AWS conforme descrito em [Definir as configurações da AWS](#).
3. Insira as informações para configurações do vCenter conforme descrito em [Definir as configurações do vCenter](#).

4. Insira as informações para configurações do servidor remoto conforme descrito em [Definir configurações de servidor remoto](#).
5. Insira as informações para configurações do controle de versão conforme descrito em [Definir configurações de controle de versão](#).
6. Prepare seus servidores Windows e Linux para a coleta de dados do coletor seguindo as instruções em [Preparar seus servidores remotos Windows e Linux para a coleta de dados](#).

Definir as configurações da AWS

Para definir as configurações da AWS, ao usar o comando `collector setup` ou `collector setup --aws-configurations`.

1. Digite Y para sim à pergunta Você configurou as permissões do IAM... Você configura essas permissões ao criar um usuário para acessar o coletor usando a política gerenciada pela `AWSMigrationHubStrategyCollector` seguindo as etapas em [Strategy Recommendations: usuários e funções](#).
2. Insira a chave de acesso e a chave secreta da conta da AWS que tem o usuário que você criou para acessar o coletor seguindo as etapas em [Strategy Recommendations: usuários e funções](#).
3. Insira uma região, por exemplo, `us-west-2`. Escolha uma região que atenda às suas necessidades entre as regiões que o Strategy Recommendations usa. Para obter uma lista dessas regiões, consulte os [Endpoints de Strategy Recommendations](#) no Referência geral da AWS.
4. Insira Y para sim para a pergunta Carregar métricas relacionadas ao coletor para o serviço do Migration Hub Strategy?. As informações de métricas ajudam a AWS a fornecer o suporte adequado.
5. Insira Y para sim para a pergunta Carregar logs relacionados ao coletor para o serviço do Migration Hub Strategy?. As informações dos logs ajudam a AWS a fornecer o suporte adequado.

O exemplo a seguir mostra o que é exibido, incluindo entradas de exemplo para as configurações do AWS.

```
Have you setup IAM permissions in you AWS account as per the user guide? [Y/N]: Y
Choose one of the following options for providing user credentials:
1. Long term AWS credentials
```

2. Temporary AWS credentials

```
Enter your options [1-2]: 2
```

```
AWS session token:
```

```
AWS access key ID [None]:
```

```
AWS secret access Key [None]:
```

```
AWS region name [us-west-2]:
```

```
AWS configurations are saved successfully
```

```
Upload collector related metrics to migration hub strategy service? By default  
collector will upload metrics. [Y/N]: Y
```

```
Upload collector related logs to migration hub strategy service? By default collector  
will upload logs. [Y/N]: Y
```

```
Application data collector configurations are saved successfully
```

```
Start registering application data collector
```

```
Application data collector is registered successfully.
```

Definir as configurações do vCenter

Para definir as configurações do vCenter, ao usar o comando `collector setup` ou `collector setup --vcenter-configurations`:

1. Digite Y para sim para a pergunta Você gostaria de se autenticar usando as credenciais do VMware vCenter se quiser se autenticar usando as credenciais do VMware vCenter.

Note

A autenticação usando as credenciais do VMware vCenter exige que as ferramentas da VMware estejam instaladas nos servidores de destino.

Insira o URL do host, que pode ser o endereço IP ou o URL do vCenter. Em seguida, insira o Nome de usuário e a Senha do VMware vCenter.

2. Digite Y para sim na pergunta Você tem máquinas Windows gerenciadas pelo VMware vCenter, se quiser configurar servidores Windows.

Digite o Nome de usuário e a Senha para Windows.

Note

Se o Windows Remote Server pertencer a um domínio do Active Directory, você deverá inserir o nome de usuário como *nome-domínio\usuário* ao usar a CLI para fornecer configurações de servidor remoto. Por exemplo, se o nome do seu domínio for *exemplodomínio* e seu nome de usuário for *Administrador*, o nome de usuário inserido na CLI será *exemplodomínio\Administrador*.

3. Digite Y para sim na pergunta Configuração para Linux usando o VMware vCenter, se você quiser configurar servidores Linux.

Digite o Nome de usuário e a Senha para Linux.

4. Digite Y para sim nas perguntas Você gostaria de configurar credenciais para servidores fora do vCenter usando NTLM para Windows e SSH/Cert baseado em Linux, se quiser configurar credenciais de servidor remoto para servidores fora do vCenter.
5. Para a pergunta Você gostaria de usar as mesmas credenciais do Windows usadas durante a configuração do vCenter, digite Y para sim se as credenciais das máquinas Windows gerenciadas fora do vCenter forem as mesmas fornecidas ao configurar as credenciais para máquinas vCenter Windows. Caso contrário, insira N para não.

Se você responder Y para sim, as seguintes perguntas serão feitas.

- a. Digite Y para sim na caixa da pergunta Você concorda com o fato de o coletor aceitar e armazenar localmente certificados de servidor em seu nome durante a primeira interação com servidores Windows?
- b. Digite 1 para a pergunta Insira suas opções, se você quiser configurar a autenticação SSH.

Se você optar por usar a autenticação SSH, deverá copiar as credenciais da chave gerada para seus servidores Linux. Para obter mais informações, consulte [Configure a autenticação baseada em chaves em servidores Linux](#).

O exemplo a seguir mostra o que é exibido, incluindo entradas de exemplo para as configurações do VMware vCenter.

```
Your Linux remote server configurations are saved successfully.  
collector setup -vcenter-configurations
```

Start setting up vCenter configurations for remote execution

Note: Authenticating using VMware vCenter credentials requires VMware tools to be installed on the target servers

Would you like to authenticate using VMware vCenter credentials? [Y/N]: y

NOTE: Your vSphere user must have Guest Operations privileges enabled.

Host Url for VMware vCenter: *domain-name*

Username for VMware vCenter: *username*

Password for VMware vCenter: *password*

Reenter password for VMware vCenter: *password*

Successfully stored vCenter credentials...

Do you have Windows machines managed by VMware vCenter? [Y/N]: y

NOTE: For the best experience, we recommend that you create a new Active Directory user in the Domain Admins group.

Username for Windows (Domain\User): *username*

Password for Windows: *password*

Reenter password for Windows: *password*

Successfully stored windows credentials...

You can verify your setup for vCenter windows machines is correct with "collector diag-check"

Do you have Linux machines managed by VMware vCenter? [Y/N]: y

Username for Linux: *username*

Password for Linux: *password*

Reenter password for Linux: *password*

Successfully stored linux credentials...

You can verify your setup for vCenter linux machines is correct with "collector diag-check"

Would you like to setup credentials for servers not managed by vCenter using NTLM for windows and SSH/Cert based for Linux? [Y/N]: y

Setting up target server for remote execution:

Would you like to setup credentials for servers not managed by vCenter using NLTM for Windows [Y/N]: y

Would you like to use the same Windows credentials used during vCenter setup? [Y/N]: y

Are you okay with collector accepting and locally storing server certificates on your behalf during first interaction with windows servers? These certificates will be used by collector for secure communication with windows servers [Y/N]: y

Successfully stored windows server credentials...

Please note that all windows server certificates are stored in directory /opt/amazon/application-data-collector/remote-auth/windows/certs


```
Please note the IP address of the collector and run the script specified in the user
documentation on all the windows servers in your inventory
You can verify your setup for remote windows machines is correct with "collector diag-
check"
Would you like to setup credentials for servers not managed by vCenter using SSH/Cert
based for Linux? [Y/N]: y
Choose one of the following options for remote authentication:
1. SSH based authentication
2. Certificate based authentication
Enter your options [1-2]: 1
Would you like to use the same Linux credentials used during vCenter setup? [Y/N]: y
Generating SSH key on this machine...
Successfully generated SSH key pair

SSH key pair path: /opt/amazon/application-data-collector/remote-auth/linux/keys/
id_rsa_assessment
Please add the public key "id_rsa_assessment.pub" to the "$HOME/.ssh/authorized_keys"
file in your remote machines.
You can verify your setup for remote linux machines is correct with "collector diag-
check"
```

Definir configurações de servidor remoto

Para definir as configurações do servidor remoto, ao usar o comando `collector setup` ou o comando `collector setup --remote-server-configurations`:

1. Digite Y para sim na pergunta Você gostaria de configurar credenciais para servidores não gerenciados pelo vCenter usando NLTM para Windows, se quiser configurar servidores Windows.

Digite o Nome de usuário e a Senha para WinRM.

Note

Se o Windows Remote Server pertencer a um domínio do Active Directory, você deverá inserir o nome de usuário como *nome-domínio\usuário* ao usar a CLI para fornecer configurações de servidor remoto. Por exemplo, se o nome do seu domínio for *exemplodomínio* e seu nome de usuário for *Administrador*, o nome de usuário inserido na CLI será *exemplodomínio\Administrador*.

Digite Y para sim na caixa da pergunta Você concorda com o fato de o coletor aceitar e armazenar localmente certificados de servidor em seu nome durante a primeira interação com servidores Windows? Os certificados do Windows Server são armazenados no diretório `/opt/amazon/application-data-collector/remote-auth/windows/certs`.

Você deve copiar as credenciais do servidor geradas para seus servidores Windows. Para obter mais informações, consulte [Definir a configuração do servidor remoto em servidores Windows](#).

2. Digite Y para sim na pergunta Configuração para Linux usando SSH ou Cert, se você quiser configurar servidores Linux.
3. Digite 1 para a pergunta Insira suas opções, se você quiser configurar a autenticação baseada em chave SSH.

Se você optar por usar a autenticação SSH, deverá copiar as credenciais da chave gerada para seus servidores Linux. Para obter mais informações, consulte [Configure a autenticação baseada em chaves em servidores Linux](#).

4. Digite 2 para a pergunta Insira suas opções, se você quiser configurar a autenticação baseada em certificado.

Para obter informações sobre a autenticação baseada em certificado, consulte [Configurar a autenticação baseada em certificado em servidores Linux](#).

O exemplo a seguir mostra o que é exibido, incluindo entradas de exemplo para as configurações do servidor remoto.

```
Setting up target server for remote execution
Would you like to setup credentials for servers not managed by vCenter using NLTM for
Windows [Y/N]: y

NOTE: For the best experience, we recommend that you create a new Active Directory user
in the Domain Admins group.

Username for WinRM (Domain\User): username
Password for WinRM: password
Reenter password for WinRM: password
Are you okay with collector accepting and locally storing server certificates on your
behalf during first interaction with windows servers? These certificates will be used
by collector for secure communication with windows servers [Y/N]: Y
```

```
Successfully stored windows server credentials...
```

```
Please note that all windows server certificates are stored in directory /opt/amazon/application-data-collector/remote-auth/windows/certs
```

```
Please note the IP address of the collector and run the script specified in the user documentation on all the windows servers in your inventory
```

```
Would you like to setup credentials for servers not managed by vCenter using SSH/Cert based for Linux? [Y/N]: Y
```

```
Choose one of the following options for remote authentication:
```

1. SSH based authentication
2. Certificate based authentication

```
Enter your options [1-2]: 1
```

```
User name for remote server: username
```

```
Generating SSH key on this machine...
```

```
SSH key pair path: /opt/amazon/application-data-collector/remote-auth/linux/keys/id_rsa_assessment
```

```
Please add the public key "id_rsa_assessment.pub" to the "$HOME/.ssh/authorized_keys" file in your remote machines.
```

```
Your Linux remote server configurations are saved successfully.
```

Definir configurações de controle de versão

Para definir as configurações de controle de versão, ao usar o comando `collector setup` ou o comando `collector setup --version-control-configurations`:

1. Insira Y para sim a pergunta Configurar análise de código-fonte?.
2. Digite 1 para a pergunta Insira suas opções, se você quiser configurar o endpoint do servidor Git.

Digite `github.com` para o endpoint do servidor GIT.

3. Digite 2 para a pergunta Insira suas opções, se você quiser configurar o servidor do GitHub Enterprise.

*Insira o endpoint do Enterprise sem `https://`, da seguinte forma:
endpoint do servidor do GIT: `git-enterprise-endpoint`*

4. Digite seu *nome de usuário* e o *token* de acesso pessoal do Git.
5. Digite Y para sim para a pergunta Você tem algum repositório csharp que deva ser analisado em uma máquina Windows? se você quiser analisar o código C#.

Note

Para analisar repositórios .NET para recomendações do Assistente de Portabilidade para .NET, você deve fornecer uma máquina Windows configurada com a ferramenta de avaliação de portabilidade do Assistente de Portabilidade para .NET. Para obter mais informações, consulte [Introdução ao Assistente de Portabilidade para .NET](#) no Guia do usuário do Assistente de Portabilidade para .NET.

6. Para a pergunta Deseja reutilizar as credenciais existentes do Windows nesta máquina?
Insira Y para sim, se a máquina Windows para análise de código-fonte em C# usar as mesmas credenciais fornecidas anteriormente como parte da configuração de `--remote-server-configurations` ou `--vcenter-configurations`.

Digite N para não, se quiser inserir novas credenciais.
7. Para usar as credenciais do VMware vCenter Windows Machine, digite 1 em Escolher uma das seguintes opções para credenciais do Windows.
8. Insira o endereço IP da máquina Windows.

O exemplo a seguir mostra o que é exibido, incluindo entradas de exemplo para as configurações do controle de versão.

```
Set up for source code analysis [Y/N]: y
Choose one of the following options for version control type:
1. GIT
2. GIT Enterprise
3. Azure DevOps - Git
Enter your options [1-3]: 3
Your server endpoint: dev.azure.com (http://dev.azure.com/)
Your DevOps Organization name: <Your organization name>
Personal access token [None]:
Your version control credentials are saved successfully.
Do you have any csharp repositories that should be analyzed on a windows machine? [Y/N]: y
Would you like to reuse existing windows credentials on this machine? [Y/N]: y
Choose one of the following options for windows credentials:
1. VMWare vCenter Windows Machine
2. Standard Windows Machine
Enter your options [1-2]:
```

1

```
Windows machine IP Address: <Your windows machine IP address>
Using VMWare vCenter Windows Machine credentials
Successfully stored windows server credentials...
```

Preparar seus servidores remotos Windows e Linux para a coleta de dados

Note

Essa etapa não é necessária se você configurar o coletor de dados de aplicações do Strategy Recommendations usando as credenciais do vCenter.

Depois de definir as configurações do servidor remoto, se você estiver usando o comando `collector setup command` ou `collector setup --remote-server-configurations`, deverá preparar seus servidores remotos para que o coletor de dados de aplicações do Strategy Recommendations possa coletar dados deles.

Note

Você deve garantir que os servidores possam ser acessados usando seu endereço IP privado. Para obter mais instruções sobre como configurar o ambiente por meio de uma nuvem privada virtual (VPC) na AWS para execução remota, consulte o [Guia do usuário da Amazon Virtual Private Cloud](#).

Para preparar seus servidores Linux remotos, consulte [Preparar servidores Linux remotos](#).

Para preparar seus servidores Windows remotos, consulte [Definir a configuração do servidor remoto em servidores Windows](#).

Preparar servidores Linux remotos

Configure a autenticação baseada em chaves em servidores Linux

Se você optar por configurar a autenticação baseada em chave SSH para Linux ao definir configurações de servidor remoto, deverá executar as etapas a seguir para configurar a autenticação baseada em chave em seus servidores para que os dados possam ser coletados pelo coletor de dados de aplicações do Strategy Recommendations.

Para configurar a autenticação baseada em chaves em seus servidores Linux

1. Copie a chave pública gerada com o nome `id_rsa_assessment.pub` da seguinte pasta no contêiner:

`/opt/amazon/application-data-collector/remote-auth/linux/keys.`

2. Anexe a chave pública copiada ao arquivo `$HOME/.ssh/authorized_keys` para todas as máquinas remotas. Se não houver nenhum arquivo disponível, crie-o usando o comando `touch` ou `vim`.
3. Certifique-se de que a pasta inicial no servidor remoto tenha um nível de permissão 755 ou menos. Se for 777, não funcionará. Você pode usar o comando `chmod` para restringir as permissões.

Configurar a autenticação baseada em certificado em servidores Linux

Se você optar por configurar a autenticação baseada em certificado para Linux ao definir as configurações do servidor remoto, deverá executar as etapas a seguir para que os dados possam ser coletados pelo coletor de dados de aplicações do Strategy Recommendations.

Recomendamos essa opção se você já tiver uma Autoridade de Certificação (CA) configurada para seus servidores de aplicações.

Para configurar a autenticação baseada em certificados em seus servidores Linux

1. Copie o nome de usuário que funciona com todos os seus servidores remotos.
2. Copie a chave pública do coletor para a CA.

A chave pública do coletor pode ser encontrada no seguinte local:

`/opt/amazon/application-data-collector/remote-auth/linux/keys/id_rsa_assessment.pub`

Essa chave pública deve ser adicionada à sua CA para gerar o certificado.

3. Copie o certificado gerado na etapa anterior para o seguinte local no coletor:

`/opt/amazon/application-data-collector/remote-auth/linux/keys`

O nome do certificado deve ser `id_rsa_assessment-cert.pub`.

4. Forneça o nome do arquivo do certificado durante a etapa de configuração.

Definir a configuração do servidor remoto em servidores Windows

Se você optar por configurar o Windows ao definir as configurações do servidor remoto na configuração do coletor, deverá executar as etapas a seguir para que os dados possam ser coletados pelo Strategy Recommendations.

 Para entender mais sobre o script PowerShell executado no servidor remoto, leia esta nota.

O script ativa o PowerShell remoto e desativa todos os métodos de autenticação, exceto negociar. Isso é usado para o Windows NT LAN Manager (NTLM) e define o protocolo WSMAN "AllowUnencrypted" como falso para garantir que o receptor recém-criado aceite somente tráfego criptografado. Usando o script fornecido pela Microsoft, `New-SelfSignedCertificateEx.ps1`, ele cria um certificado autoassinado.

Qualquer instância WSMAN que tenha um receptor HTTP é removida junto com os receptores HTTPS existentes. Em seguida, ele cria um novo receptor HTTPS. Ele também cria uma regra de firewall de entrada para a porta TCP 5986. Na etapa final, o serviço WinRM é reiniciado.

Para configurar a coleta de dados por meio de uma conexão remota em seus servidores Windows 2008

1. Use o comando a seguir para verificar a versão do PowerShell instalada no seu servidor.

```
$PSVersionTable
```

2. Se a versão do PowerShell não for 5.1, baixe e instale o WMF 5.1 seguindo as instruções em [Instalar e configurar o WMF 5.1](#) na documentação da Microsoft.
3. Use o comando a seguir em uma nova janela do PowerShell para garantir que o PowerShell 5.1 esteja instalado.

```
$PSVersionTable
```

4. Siga o próximo conjunto de etapas, que descrevem como configurar a coleta de dados por meio de uma conexão remota no Windows 2012 e versões posteriores.

Para configurar a coleta de dados por meio de uma conexão remota em seus servidores Windows 2012 e mais recentes

1. Faça download do script de configuração do seguinte URL:

<https://application-data-collector-release.s3.us-west-2.amazonaws.com/scripts/WinRMSetup.ps1>

2. Faça o download `New-SelfSignedCertificateEx.ps1` do seguinte URL e cole o script na mesma pasta em que você baixou `WinRMSetup.ps1`:

<https://github.com/Azure/azure-libraries-for-net/blob/master/Samples/Asset/New-SelfSignedCertificateEx.ps1>

3. Para concluir a configuração, execute o script PowerShell baixado em todos os servidores de aplicações.

```
.\WinRMSetup.ps1
```

Note

Se o Gerenciamento Remoto do Windows (WinRM) não estiver configurado corretamente no Servidor Remoto do Windows, uma tentativa de coletar dados desse servidor falhará. Se isso acontecer, você deverá excluir o certificado que corresponde a esse servidor do seguinte local no contêiner:

```
/opt/amazon/application-data-collector/remote-auth/windows/certs/ads-server-id.cer
```

Depois de excluir o certificado, aguarde até que o processo de coleta de dados seja repetido.

Verifique se o coletor e os servidores estão configurados para coleta de dados

Verifique se o coletor e os servidores estão configurados corretamente para a coleta de dados usando o comando a seguir.

```
collector diag-check
```

Esse comando conduz um conjunto de verificações de diagnóstico nas configurações do servidor e fornece informações sobre falhas nas verificações.

Ao usar o comando no modo `-a`, você obtém a saída em um arquivo `DiagnosticCheckResult.txt` após a conclusão das verificações.

```
collector diag-check -a
```

Você pode realizar uma verificação de diagnóstico nas configurações do servidor de um único servidor com o endereço IP desse servidor.

Os exemplos a seguir mostram a saída de uma configuração bem-sucedida.

Servidor do Linux

```
Provide your test server IP address: IP address
-----
Start checking connectivity & credentials...
Connectivity and Credential Checks succeeded
-----
Start checking permissions...
Permission Check succeeded
-----
Start checking OS version...
OS version check succeeded
-----
Start checking Linux Bash installation...
Linux Bash installation check succeeded
-----
All diagnostic checks complete successfully.
This server is correctly set up and ready for data collection.
```

Servidor do Windows

```
Windows PowerShell Version Check succeeded
Provide your test server IP address: IP address
-----
Start checking connectivity & credentials...
Connectivity and Credential Checks succeeded
-----
Start checking permissions...
Permission Check succeeded
```

```
-----  
Start checking OS version...  
OS version check succeeded  
-----  
Start checking Windows architecture type...  
Windows Architecture Type Check succeeded  
-----  
All diagnostic checks complete successfully.  
This server is correctly set up and ready for data collection.
```

O exemplo a seguir mostra uma mensagem de erro que é exibida quando as credenciais do servidor remoto estão incorretas.

```
Unable to authenticate the server credentials with IP address ${IPAddress}.  
Ensure that your credentials are accurate and the server is configured correctly.  
Use the following command to reset incorrect credentials.  
collector setup --remote-server-configurations
```


Etapa 5: use o Strategy Recommendations no console do Migration Hub para obter recomendações

Esta seção descreve como usar o Strategy Recommendations no console do Migration Hub para obter recomendações de migração pela primeira vez.

Como obter recomendações

1. Usando a conta da AWS que você criou em [Configuração do Strategy Recommendations](#), faça login no AWS Management Console e abra o console do Migration Hub em <https://console.aws.amazon.com/migrationhub/>.
2. No painel de navegação do console Migration Hub, escolha Estratégia.
3. Na página Migration Hub Strategy Recommendations, escolha Obter recomendações.
4. Escolha Concordo se você concordar em permitir que o Migration Hub crie um perfil vinculado ao serviço (SLR) em sua conta. Para obter mais informações sobre o SLR, consulte [Usar perfis vinculados ao serviço do Strategy Recommendations](#).
5. Configurar a fonte de dados


- a. Na página Configurar fontes de dados, você deve escolher a fonte dos seus servidores para análise entre as seguintes opções:
 - i. Coletor de dados de aplicações do Strategy Recommendations: você pode usar o coletor do Strategy Recommendations para recuperar informações sobre VMs hospedadas no VMware vCenter automaticamente. Com essa opção, você não precisa realizar nenhuma configuração adicional.
 - ii. Importação manual: se você quiser trazer dados sobre seus servidores e aplicações de forma independente, você pode usar o modelo de importação do Strategy Recommendations. O modelo de importação é um arquivo JSON no qual você pode preencher as informações disponíveis para suas VMs.
 - iii. Application Discovery Service : você pode usar o Application Discovery Service para coletar informações sobre suas aplicações e servidores on-premises. No console do Migration Hub, na seção Ferramentas, você pode escolher entre várias opções em Ferramentas de descoberta. Por exemplo, você pode escolher Application Discovery Service Agentless Collector, AWSDiscovery Agent ou Importar (para arquivos CSV).
- b. A tabela Servidores lista todos os servidores disponíveis com base na sua seleção na seção de fonte de dados.
- c. Em Coletores de dados de aplicações registrados, os coletores de dados de aplicações que você configurou estão listados. Se você não configurou nenhum coletor de dados, pode fazer o download do coletor de dados e implantá-lo. Para obter mais informações, consulte [Etapa 2: implantar o coletor do Strategy Recommendations](#) e [Etapa 1: fazer download do coletor do Strategy Recommendations](#).

 Note

Para obter recomendações de estratégia, você deve configurar ao menos um coletor de dados de aplicações ou realizar uma importação de dados de aplicações. Se quiser adicionar seus dados no nível de aplicação sem configurar um coletor, você pode usar o modelo de importação de dados de aplicações. Você pode adicionar outras fontes de dados posteriormente.

- d. Se você selecionou Importação manual, em Detalhes da importação, escolha Adicionar nova importação.
- e. Em Nome da importação, insira um nome para a importação.

- f. Para o URI do bucket do S3, insira o URI do bucket do S3 para o qual seu arquivo JSON de importação será carregado.

 Important

O nome do bucket do S3 deve iniciar com o prefixo **migrationhub-strategy**.


- g. Escolha Próximo.

6. Especificar preferências

- a. Na página Especificar preferências, configure suas metas de negócios e preferências de migração. O Strategy Recommendations recomenda a estratégia ideal para migrar e modernizar suas aplicações e bancos de dados com base nas preferências que você especificar. Você poderá alterar essas preferências mais tarde.
- b. Escolha Próximo.

7. Revisar e enviar.

- a. Revise suas fontes de dados configuradas e suas preferências de migração.
- b. Se tudo estiver correto, escolha Iniciar análise de dados. Isso realizará uma análise do inventário do servidor e do ambiente de runtime e dos binários da aplicação para suas aplicações Microsoft IIS e Java.

 Note

O status da análise binária não é exibido no console. Quando a análise for concluída, você verá um link para o relatório antipadrão ou uma mensagem indicando que a análise não foi bem-sucedida.

Recomendações do Strategy Recommendations

Esta seção descreve como visualizar as recomendações de migração e modernização do Strategy Recommendations para servidores e aplicações em seu portfólio de migração.

Tópicos

- [Ver recomendações de estratégias no Strategy Recommendations](#)
- [Recomendações de estratégia da aplicação do Strategy Recommendations](#)
- [Recomendações de servidor do Strategy Recommendations](#)
- [Preferências do Strategy Recommendations](#)

Ver recomendações de estratégias no Strategy Recommendations

Esta seção descreve como usar as Recomendações de Estratégia no AWS Migration Hub console para visualizar as recomendações de estratégia de migração.

Para ver recomendações de estratégias

1. Usando a AWS conta que você criou [Configuração do Strategy Recommendations](#), entre AWS Management Console e abra o console do Migration Hub em <https://console.aws.amazon.com/migrationhub/>.
2. No painel de navegação do console do Migration Hub, escolha Estratégia e, em seguida, escolha Recomendações.
3. Na página Recomendações, você pode visualizar e exportar recomendações resumidas do seu portfólio e recomendações detalhadas da estratégia de migração "R". Você também pode visualizar ferramentas e destinos de migração e modernização, além de antipadrões para seus servidores e componentes de aplicações.

Os antipadrões são uma lista de problemas conhecidos encontrados em seu portfólio que são categorizados por gravidade. Antipadrões de alta gravidade representam incompatibilidades que precisam ser resolvidas, antipadrões de gravidade média representam avisos e antipadrões de baixa gravidade representam problemas de informação. Para obter informações sobre a estratégia "R", consulte [Termos de migração - 7 Rs](#) no glossário de AWS Prescriptive Guidance.

- Se ocorrer uma alteração em seu datacenter ou se você atualizar suas preferências, recomendamos reanalisar seus dados. Para reanalisar seus dados e obter novas recomendações, escolha Reanalisar dados.

Até que o processo de reanálise seja concluído, os resultados dos dados de recomendação podem ser uma mistura de dados anteriores e dados novos.

Para baixar um arquivo de relatório com as recomendações, escolha Exportar recomendações.

4. Na guia Componentes da aplicação, você pode ver as recomendações para componentes da aplicação em seu portfólio de migração. Para ter mais informações, consulte [Recomendações de estratégia da aplicação do Strategy Recommendations](#).
5. Na guia Servidores, você pode ver as recomendações para os servidores em seu portfólio de migração. Para ter mais informações, consulte [Recomendações de servidor do Strategy Recommendations](#).
6. Na guia Preferências, você pode editar as preferências especificadas em [Etapa 5: obter recomendações](#). Para obter informações sobre como editar suas preferências, consulte [Preferências do Strategy Recommendations](#).

Recomendações de estratégia da aplicação do Strategy Recommendations

Esta seção descreve como usar o Strategy Recommendations no console do Migration Hub para visualizar e analisar as recomendações de estratégia de migração para componentes de aplicações.

Tópicos

- [Trabalhar com componentes de aplicações no Strategy Recommendations](#)
- [Análise do código-fonte do Strategy Recommendations](#)
- [Análise do banco de dados do Strategy Recommendations](#)
- [Análise binária do Strategy Recommendations](#)

Trabalhar com componentes de aplicações no Strategy Recommendations

Esta seção descreve como usar o Migration Hub Strategy Recommendations no console do Migration Hub para visualizar e configurar as recomendações da estratégia de migração e modernização.

Tópicos

- [Visualizar recomendações de componentes de aplicações](#)
- [Configurar análise de código-fonte para um componente de aplicações](#)
- [Configurar análise de banco de dados para um componente de aplicações](#)

Visualizar recomendações de componentes de aplicações

Esta seção descreve como usar o Strategy Recommendations no console do Migration Hub para visualizar as recomendações de estratégia de migração para componentes de aplicações.

Para visualizar os detalhes das recomendações para os componentes de aplicações

1. Usando a AWS conta que você criou [Configuração do Strategy Recommendations](#), entre AWS Management Console e abra o console do Migration Hub em <https://console.aws.amazon.com/migrationhub/>.
2. No painel de navegação do console do Migration Hub, escolha Estratégia e, em seguida, escolha Recomendações.
3. Na página Recomendações, escolha a guia Componentes da aplicação.
 - a. Em Resumo dos componentes da aplicação, há uma visão geral dos vários tipos de componentes de aplicações que você está executando no seu portfólio de servidores.
 - b. Em Componentes da aplicação, você visualiza o nome do componente, o tipo de componente e as recomendações da estratégia “R” de migração. Você também pode visualizar o destino da migração e as ferramentas de migração e modernização a serem usadas em vários componentes de aplicações que estão sendo executados em seu portfólio de servidores. Para obter informações sobre a estratégia “R”, consulte [Termos de migração - 7 Rs](#) no glossário de AWS Prescriptive Guidance.
4. Para visualizar os detalhes de um componente de aplicações, selecione um componente de aplicações e escolha Exibir detalhes.

5. Na página de detalhes do componente de aplicações (a página com o nome do componente como título), em Resumo da recomendação, você pode visualizar as recomendações para o componente de aplicações. Você também pode ver os Antipadrões identificados. Os antipadrões são uma lista de problemas conhecidos encontrados em seu portfólio que são categorizados por gravidade.
6. Escolha a guia Opções de estratégia para ver a recomendação de migração para o componente de aplicações. Você pode substituir a estratégia recomendada selecionando uma estratégia diferente e, em seguida, escolhendo Definir como preferencial.
7. Dependendo do tipo de componente de aplicações que você está visualizando, há uma guia Configuração da origem ou de Configuração de banco de dados. Para obter mais informações sobre a Configuração da origem, consulte [Configurar análise de código-fonte para um componente de aplicações](#). Para obter mais informações sobre a Configuração de banco de dados, consulte [Configurar análise de banco de dados para um componente de aplicações](#).

Configurar análise de código-fonte para um componente de aplicações

Esta seção descreve como usar o Strategy Recommendations no console do Migration Hub para configurar a análise do código-fonte para um componente de aplicações.

Para configurar a análise de código-fonte de um componente de aplicações

1. No painel de navegação do console do Migration Hub, escolha Estratégia e, em seguida, escolha Recomendações.
2. Na página Recomendações, escolha a guia Componentes da aplicação.
3. Na lista de componentes em Componentes de aplicações, selecione um componente de aplicações com um tipo de componente java, dotnetframework ou IIS e escolha Exibir detalhes.
4. Na página de detalhes do componente de aplicações (a página com o nome do componente como título), escolha a guia Configuração do código-fonte.
5. Em Detalhes da configuração do código-fonte, escolha Analisar código-fonte.
6. Na página Analisar código-fonte, forneça o nome do repositório, o nome da ramificação e o nome do projeto (se aplicável) que armazenam o código-fonte do componente de aplicações. Selecione o tipo de controle de versão do GitHub código-fonte que você deseja usar e escolha Analisar.

Depois que a análise for concluída, você poderá visualizar as recomendações atualizadas na página de detalhes do componente de aplicações.

Para obter mais informações sobre análise de código-fonte, consulte [Análise do código-fonte do Strategy Recommendations](#).

Configurar análise de banco de dados para um componente de aplicações

Esta seção descreve como usar o Strategy Recommendations no console do Migration Hub para configurar a análise de bancos de dados para um componente de aplicações.

Para configurar a análise de banco de dados para um componente de aplicações

1. No painel de navegação do console do Migration Hub, escolha Estratégia e, em seguida, escolha Recomendações.
2. Na página Recomendações, escolha a guia Componentes da aplicação.
3. Na lista de componentes em Componentes de aplicações, selecione um componente de aplicações com o tipo de componente SQLServer e escolha Exibir detalhes.
4. Na página de detalhes do componente de aplicações (a página com o nome do componente como título), escolha a guia Configuração de banco de dados.
5. Em Detalhes da configuração do banco de dados, escolha Analisar detalhes do banco de dados.
6. Escolha um nome secreto no menu suspenso que você criou no AWS Secrets Manager para usar nas credenciais do banco de dados e escolha Analisar.

Depois que a análise for concluída, você poderá visualizar as recomendações atualizadas na página de detalhes do componente de aplicações.

Para obter mais informações sobre análise de banco de dados e configuração de um nome secreto, consulte [Análise do banco de dados do Strategy Recommendations](#).

Análise do código-fonte do Strategy Recommendations

O Migration Hub Strategy Recommendations identifica automaticamente as aplicações em seu portfólio e cria componentes de aplicações para eles. Por exemplo, se houver uma aplicação Java em seu portfólio, ela será identificada como um componente de aplicações com um tipo de componente java.

O Strategy Recommendations analisa o código-fonte dos componentes de aplicações se você configurá-lo para fazer isso. Para obter informações sobre como configurar um componente de aplicações para análise de código-fonte, consulte [Configurar análise de código-fonte para um componente de aplicações](#).

O Strategy Recommendations realiza a análise do código-fonte para as linguagens de programação Java e C#.

Para obter informações sobre os pré-requisitos para usar a análise do código-fonte do Strategy Recommendations, consulte. [Pré-requisitos para o Strategy Recommendations](#)

Análise do banco de dados do Strategy Recommendations

O Strategy Recommendations identifica automaticamente os servidores de banco de dados em seu portfólio e cria componentes de aplicações para eles. Por exemplo, se houver um banco de dados do SQL Server em seu portfólio, ele será identificado como componente de aplicações sqlservr.exe.

O Strategy Recommendations analisa bancos de dados individuais no componente do aplicativo SQL Server identificado, sqlservr.exe, usando a AWS Schema Conversion Tool. As recomendações de estratégia também identificam incompatibilidades na migração dos bancos de dados para AWS bancos de dados como Amazon Aurora MySQL Compatible Edition, Amazon Aurora PostgreSQL Compatible Edition, Amazon RDS for MySQL e Amazon RDS for PostgreSQL.

Atualmente, a análise de banco de dados do Strategy Recommendations está disponível somente para o SQL Server.

Para configurar o Strategy Recommendations para analisar seus bancos de dados, você deve fornecer credenciais para que o coletor de dados de aplicações do Strategy Recommendations se conecte aos seus bancos de dados. Para fazer isso, crie um segredo no AWS Secrets Manager em sua AWS conta.

Para obter informações sobre as permissões e privilégios das credenciais que você fornece, consulte [Privilégios necessários para as credenciais da AWS Schema Conversion Tool](#). Para obter informações sobre como criar um segredo com as credenciais, consulte [Criar um segredo no Secrets Manager para credenciais de banco de dados](#).

Depois de configurar as credenciais e o segredo, você pode configurar a análise do AWS Schema Conversion Tool no servidor do banco de dados. Para ter mais informações, consulte [Configurar análise de banco de dados para um componente de aplicações](#).

Depois de configurar a análise do banco de dados para o componente do aplicativo, uma tarefa de inventário do AWS Schema Conversion Tool é agendada. Depois que essa tarefa for concluída, você verá os novos componentes de aplicações sendo criados para cada banco de dados individual nesse servidor de banco de dados. Por exemplo, se o SQL Server tiver dois bancos de dados

(`exampledb1` e `exampledb2`), um componente de aplicação será criado para cada um dos bancos de dados com os nomes `exampledb1` e `exampledb2`.

Se você quiser ver antipadrões na migração de cada banco de dados identificado como bancos de dados da AWS, configure a análise para cada banco de dados seguindo as etapas em [Configurar análise de banco de dados para um componente de aplicações](#).

Privilégios necessários para as credenciais da AWS Schema Conversion Tool

As credenciais de login que você fornece ao AWS Secrets Manager somente necessitam de `VIEW SERVER STATE` e privilégios `VIEW ANY DEFINITION`. Também é possível criar um novo login usando o script disponível em https://gitlab.aws.dev/dmaf-pub/dmaf/-/blob/master/create_mssql_ro_user.sql.

Você pode fornecer qualquer nome de login e senha que desejar ao criar o login do SQL Server.

Criar um segredo no Secrets Manager para credenciais de banco de dados

Depois que as credenciais estiverem prontas para que o coletor de dados do aplicativo Strategy Recommendations se conecte a um banco de dados, crie um segredo no AWS Secrets Manager em sua AWS conta, conforme descrito no procedimento a seguir.

Para criar um segredo com o AWS Secrets Manager em sua AWS conta

1. Usando a AWS conta que você criou [Configuração do Strategy Recommendations](#), entre AWS Management Console e abra o console do AWS Secrets Manager em <https://console.aws.amazon.com/secretsmanager/>.
2. Selecione Armazenar um novo segredo.
3. Para o tipo de segredo, selecione Outro tipo de segredo.
4. Para Pares de chave/valor, insira o seguinte.

nome de usuário - *seu-nome de usuário*

Escolha + Adicionar linha e insira as informações a seguir.

senha - *sua-senha*

5. Selecione Next (Próximo).
6. Insira o nome do segredo como uma string com o prefixo `migrationhub-strategy-`. Por exemplo, `migrationhub-strategy-one`.

Note

Guarde o nome do segredo em um local seguro para uso posterior.

7. Selecione Próximo e Próximo novamente.
8. Escolha Armazenar.

Você pode usar o segredo criado para as credenciais do banco de dados ao configurar a análise do banco de dados no Strategy Recommendations.

Análise binária do Strategy Recommendations

O Migration Hub Strategy Recommendations identifica automaticamente as aplicações em seu portfólio e os componentes da aplicação que pertencem a elas. Por exemplo, se houver uma aplicação Java em seu portfólio, o Strategy Recommendations a identifica como um componente de aplicações com um tipo de componente java. Sem você configurar o acesso ao código-fonte, o Strategy Recommendations podem realizar análises binárias inspecionando as DLLs da aplicação IIS no Windows ou os arquivos JAR da aplicação no Linux e fornecer relatórios antipadrões ou relatórios de incompatibilidade. Um relatório antipadrão é uma lista de problemas conhecidos que o Strategy Recommendations encontram em seu portfólio, categorizados por gravidade. Um relatório de incompatibilidade contém um subconjunto dos antipadrões, que são compatibilidade de API, Nuget Package e Porting Action.

O Strategy Recommendations realiza análises para Windows IIS e aplicações Java Tomcat e Jboss. Se você tiver uma aplicação IIS, o Strategy Recommendations gera um relatório de incompatibilidade por padrão; você deve configurar o acesso ao código-fonte para receber o relatório antipadrão completo. Se você tiver uma aplicação Java, o Strategy Recommendations gera o relatório antipadrão completo por padrão.

O relatório de incompatibilidades ou antipadrão é exibido após a conclusão da análise. Se a análise não for bem-sucedida, você pode tentar executar uma análise de código-fonte fornecendo acesso ao código-fonte conforme descrito em [Definir configurações de controle de versão](#).

Recomendações de servidor do Strategy Recommendations

Esta seção descreve como usar o Migration Hub Strategy Recommendations no console do Migration Hub para visualizar as recomendações de estratégia de migração para os servidores em seu portfólio de migração.

Para ver recomendações para servidores

1. Usando a AWS conta que você criou [Configuração do Strategy Recommendations](#), entre AWS Management Console e abra o console do Migration Hub em <https://console.aws.amazon.com/migrationhub/>.
2. No painel de navegação do console do Migration Hub, escolha Estratégia e, em seguida, escolha Recomendações.
3. Na página Recomendações, escolha a guia Servidores.
 - a. Em Resumo do servidor, você vê uma visão geral dos vários tipos de servidores que está executando em seu portfólio.
 - b. Em Servidores, você vê os detalhes do servidor e do sistema operacional e as recomendações da estratégia “R” de migração. Você também pode ver o destino da migração e o número de antipadrões identificados em seus servidores, com base nas recomendações. Para obter informações sobre a estratégia “R”, consulte [Termos de migração - 7 Rs](#) no glossário de AWS Prescriptive Guidance.
4. Para ver mais detalhes das recomendações de um servidor, selecione o servidor na lista e escolha Exibir detalhes. Você pode visualizar os metadados coletados para o servidor, juntamente com análises detalhadas e recomendações para eles, que se baseiam nos componentes de aplicações encontrados em execução no servidor.
5. Na página de detalhes do servidor (a página com o nome do servidor como título), em Resumo da recomendação, você pode ver uma visão geral das recomendações de estratégia para o servidor. Você também pode ver os Antipadrões identificados. Os antipadrões são uma lista de problemas conhecidos encontrados em seu portfólio que são categorizados por gravidade.
6. Escolha a guia Opções de estratégia para ver a recomendação de migração para o servidor. Você pode substituir a estratégia recomendada selecionando uma estratégia diferente e, em seguida, escolhendo Definir como preferencial.
7. Escolha a guia Componentes da aplicação para ver a lista de componentes da aplicação associados ao servidor.

8. Para visualizar detalhes sobre o componente de aplicações, selecione o componente na lista e escolha Exibir detalhes. Para obter mais informações sobre componentes de aplicações, consulte [Trabalho com componentes de aplicações](#).

Preferências do Strategy Recommendations

Esta seção descreve como visualizar e editar as preferências do Migration Hub Strategy Recommendations no console do Migration Hub.

Você escolhe suas preferências de recomendação ao configurar pela primeira vez o Strategy Recommendations, conforme descrito em [Etapa 5: obter recomendações](#). Você pode editar essas preferências.

Para editar as preferências de recomendação

1. Usando a AWS conta que você criou [Configuração do Strategy Recommendations](#), entre AWS Management Console e abra o console do Migration Hub em <https://console.aws.amazon.com/migrationhub/>.
2. No painel de navegação do console do Migration Hub, escolha Estratégia e, em seguida, escolha Recomendações.
3. Na página Recomendações, escolha a guia Preferências.
4. Em Metas comerciais priorizadas, você pode arrastar e soltar as metas de negócios para reorganizá-las.
5. Escolha as Preferências da aplicação e as Preferências do banco de dados desejadas e, em seguida, escolha Salvar alterações.

Se você alterar suas preferências, um banner será exibido para lembrar você de escolher Reanalisar dados.

Fontes de dados de recomendações de estratégia

Esta seção descreve as fontes de dados que o Strategy Recommendations usa.

Tópicos

- [Ver as fontes de dados do Strategy Recommendations](#)
- [Coletor de dados de aplicações do Strategy Recommendations](#)
- [Importar dados para o Strategy Recommendations](#)
- [Remover seus dados do Strategy Recommendations](#)

Ver as fontes de dados do Strategy Recommendations

Esta seção descreve como visualizar as fontes de dados das Recomendações de Estratégia no AWS Management Console.

Para ver fontes de dados

1. Usando a AWS conta que você criou [Configuração do Strategy Recommendations](#), entre AWS Management Console e abra o console do Migration Hub em <https://console.aws.amazon.com/migrationhub/>.
2. No painel de navegação do console do Migration Hub, escolha Estratégia e, em seguida, escolha Fonte de dados.
3. Na guia Coletores, você pode visualizar os coletores de dados da aplicação do Strategy Recommendations que você configurou. Para obter mais informações sobre o coletor, consulte [Coletor de dados de aplicações do Strategy Recommendations](#).
4. Na guia Importações, você pode importar dados e visualizar suas importações de dados. Para ter mais informações, consulte [Importar dados para o Strategy Recommendations](#).
5. Na guia Ferramentas, você pode baixar o modelo de dados de importação do coletor e da aplicação.

Coletor de dados de aplicações do Strategy Recommendations

Esta seção descreve como usar o coletor de dados de aplicações do Strategy Recommendations.

Para obter informações sobre como baixar e configurar um coletor de dados de aplicações, consulte [Etapa 1: fazer download do coletor do Strategy Recommendations](#).

Tópicos

- [Dados coletados pelo coletor do Strategy Recommendations](#)
- [Atualizar o coletor do Strategy Recommendations](#)

Dados coletados pelo coletor do Strategy Recommendations

Esta seção descreve o tipo de dados que o coletor de dados de aplicações do Migration Hub Strategy Recommendations coleta. Um coletor de dados de aplicações é um coletor de dados sem agente que identifica aplicações em execução em seus servidores, realiza análises de código-fonte e analisa seus bancos de dados.

Campo de dados	Descrição
Tipo de SO	Windows ou Linux
Versão do SO	A versão específica do sistema operacional. Por exemplo, Windows Server 2003, RHEL 5.2.
Arquitetura do SO	SO de 32 bits ou 64 bits
É uma VM de servidor	O servidor é uma VM ou uma máquina física.
Software de virtualização	Por exemplo, vCenter, Hyper-V.
Local	Por exemplo, console Amazon Elastic Compute Cloud (Amazon EC2) ou on-premises.
É dualBoot	Permite a inicialização em vários sistemas operacionais
Tipo de firmware	BIOS, UEFI
Inicializador	GRUB, GRUB 2
Tipo de tabela de partição	MBR, GPT

Campo de dados	Descrição
Velocidade da CPU	Velocidade da CPU em GHz. Por exemplo, 2.4 GHz.
Windows OS data	
Edição do Windows	Standard, Data Center, Enterprise
Versão do .NET Framework	A versão do .NET Framework instalada.
Versão do .NET Core	A versão do .NET Core instalada.
Linux data	
Distribuição do SO do Linux	RHEL, CentOS, SUSE e assim por diante.
Versão do kernel	saída <code>uname -r</code> , como <code>4.9.217-0.1.ac.205.84.332.meta11.x86_64</code>
For each disk volume	
Tipo do sistema de arquivos	FAT32, NTFS, ReFS, ext4, jfs e assim por diante.
Tamanho do volume de disco	Espaço total em disco
Espaço livre do volume de disco	Espaço livre em disco
Formato de imagem de disco virtual	vmdk, vhd, vhdx
Tipo de disco (Windows)	Básico, dinâmico
Application level data	
Nome da aplicação	O nome do procedimento em execução. Por exemplo, <code>SQLSrvr.exe</code> , <code>MSdtssrvr.exe</code> e assim por diante.
Tipo de aplicativo	IIS, JBoss, Tomcat e assim por diante.
Linguagem de programação e versão	C#, Java

Campo de dados	Descrição
Versão JDK	A versão do JDK instalado.
O código-fonte está disponível	Se você fornecer um repositório de código-fonte, isso indica que o código-fonte está disponível.
Tamanho de bits da aplicação	16 bits, 32 bits, 64 bits
Windows	
Versão do .NET framework usada pela aplicação	A versão da DLL do .NET framework que está sendo carregada no runtime para a aplicação.
Versão do .NET Core	A versão DLL do .NET Core que está sendo carregada no runtime para a aplicação.
Usa a estrutura WPF?	Determina se a aplicação baseada em .NET é um tipo de aplicação WPF ou não.
Usa a estrutura WCF?	Determina se a aplicação baseada em .NET é um tipo de aplicação WCF ou não.
Versão ASP.NET	A versão do ASP.NET.
Versão do TLS	A versão do servidor IIS instalada na máquina Windows.
Tamanho de bits dos drivers do sistema operacional da aplicação	32 bits, 64 bits
Uso de registro do Windows	Consulta as chaves de registro da máquina para encontrar informações como versão do banco de dados, versão Java, versão do .NET e assim por diante.
Todas as DLLs usadas pela aplicação	Busca a lista de todas as DLLs carregadas no runtime por um processo do Windows.

Campo de dados	Descrição
PowerShell versão	Verifica a PowerShell versão instalada na máquina, que deve ser 5.1 ou posterior.
Linux	
Tipo de estruturas de aplicações	Tomcat, Spring Boot, JBoss, WebLogic WebSphere
Versão das estruturas de aplicações	A versão da estrutura de aplicações.
Database	
Tipo de banco de dados	MS SQL, Oracle, MySQL e assim por diante.
Versão do banco de dados	A versão do banco de dados.

Remova seus dados do Strategy Recommendations

Para remover todos os seus dados do Strategy Recommendations, entre em contato com o [AWS Support](#) e solicite a exclusão completa dos dados.

Atualizar o coletor do Strategy Recommendations

O coletor de dados de aplicações do Migration Hub Strategy Recommendations é atualizado automaticamente. Você pode usar o procedimento a seguir para atualizar manualmente o coletor, se necessário.

Para atualizar o coletor do Strategy Recommendations

1. Utilize o comando a seguir para se conectar à VM do coletor usando um cliente SSH.

```
ssh ec2-user@CollectorIPAddress
```

2. Altere para o diretório de atualização na VM do coletor conforme mostrado no exemplo a seguir.

```
cd /home/ec2-user/collector/upgrades
```

3. Insira o comando a seguir para executar o script de atualização.

```
bash application-data-collector-upgrade
```

Importar dados para o Strategy Recommendations

Como alternativa ao uso do coletor de dados de aplicações, você pode importar informações sobre os aplicativos e servidores para os quais deseja recomendações de migração e modernização.

Quando você importa dados, as recomendações não são tão detalhadas quanto quando você usa o coletor de dados. Por exemplo, você não pode usar a análise de código-fonte em dados importados.

Esta seção descreve como usar o modelo de importação de aplicações para importar dados para o Strategy Recommendations no console do Migration Hub.

Para importar dados

1. Usando a AWS conta que você criou [Configuração do Strategy Recommendations](#), entre AWS Management Console e abra o console do Migration Hub em <https://console.aws.amazon.com/migrationhub/>.
2. No painel de navegação do console do Migration Hub, escolha Estratégia e, em seguida, escolha Fonte de dados.
3. Escolha a guia Importações.
4. Escolha Baixar modelo de importação para baixar o modelo de importação da aplicação.
5. Preencha o modelo e faça upload dele para um bucket do Amazon S3. O nome do bucket deve começar com o prefixo migrationhub-strategy.
6. Volte para a guia Importações e escolha Importar.
7. Insira um nome para sua importação, insira o URI do objeto do Amazon S3 para seu modelo de dados preenchido e escolha Iniciar importação.

O modelo de importação do Strategy Recommendations

O modelo de importação que você baixa é um arquivo .json conforme mostrado no exemplo a seguir.

```
{  
  "ImportFormatVersion": 1,
```

```

"Resources": [
  {
    "ResourceType": "SERVER",
    "ResourceName": "",
    "ResourceId": "",
    "IpAddress": "",
    "OSDistribution": "",
    "OSType": "",
    "HostName": "",
    "OSVersion": "",
    "CPUArchitecture": ""
  },
  {
    "ResourceType": "PROCESS",
    "ResourceName": "",
    "ResourceId": "",
    "ApplicationType": "",
    "DotNetFrameworkVersion": "",
    "ApplicationVersion": "",
    "DotNetCoreVersion": "",
    "JdkVersion": "",
    "ProgrammingLanguage": "",
    "DatabaseType": "",
    "DatabaseVersion": "",
    "DatabaseEdition": "",
    "AssociatedServerIds": []
  }
]
}

```

Para ajudar você a preencher o modelo de importação, os valores válidos para os campos de dados estão listados nas tabelas a seguir.

Os campos obrigatórios para servidores estão listados na tabela a seguir.

Nome	Descrição	Tipo	Obrigatório	Valores válidos
ResourceId	Um ID exclusivo para o recurso	String	Sim	Qualquer string exclusiva

Nome	Descrição	Tipo	Obrigatório	Valores válidos
ResourceName	O nome do recurso	String	Sim	Qualquer string
ResourceType	O tipo do recurso a ser importado	String	Sim	"Servidor", "Processo"
OSDistribution	Windows, Windows Server, Ubuntu	String	Sim	Windows: "PC com Windows", "Servidor Windows" Linux: "Ubuntu", "RHEL", "Amazon Linux", "DEBIAN", "SLES", "CENT_OS", "ORACLE_LINUX", "FEDORA", "KALI"
OSType	O tipo de sistema operacional	String	Sim	"Windows", "Linux"
OSVersion	A versão do kernel	String	Sim	Veja a versão HTML da documentação.
CPUArchitecture	A arquitetura da CPU	String	Não	"32 bits", "64 bits"
IpAddress	O endereço IP do servidor	Array	Não	No formato xxx.xxx.xxx.xxx
MacAddresses	Os endereços Mac associados ao servidor	Array	Não	No formato xx:xx:xx:xx:xx:xx
Hostname	O nome do host	String	Não	Qualquer string

Os campos obrigatórios para processo estão listados na tabela a seguir.

Nome	Descrição	Tipo	Obrigatório	Valores válidos
ResourceId	Um ID exclusivo para o recurso	String	Sim	Qualquer string exclusiva
ResourceName	O nome do recurso	String	Sim	Qualquer string
ResourceType	O tipo do recurso a ser importado	String	Sim	"Servidor", "Processo"
AssociatedServerIds	Uma lista de IDs de servidor nos quais o processo está sendo executado.	String	Sim	O ResourceId do "Resource Type": "SERVIDOR" que você definiu.
ApplicationType	O tipo de aplicação	String	Sim	"Tomcat", "JBoss", "Spring", "IIS", "Mongo DB", "DB2", "Maria DB", "MySQL", "Oracle", "SQLServer", "Sybase", "PostgreSQLServer", "Cassandra", "IBM", "Oracle", "Java genérico" WebSphere WebLogic
ApplicationVersion	A versão da aplicação	String	Sim	"IIS 1.0", "IIS 2.0", "IIS 3.0", "IIS 4.0", "IIS 5.0", "IIS 5.1", "IIS 6.0", "IIS 7.0", "IIS 7.5", "IIS 8.0", "IIS 8.5", "IIS 10.0"

Nome	Descrição	Tipo	Obrigatório	Valores válidos
ProgrammingLanguage	A linguagem de programação para a aplicação	String	Não	"Java", "CSharp"
DotNetFrameworkVersion	A versão do .NET Framework, se a aplicação for baseada no .NET Framework	String	Não	"DotnetFramework 1.0"," DotnetFramework 1.0 SP1", "1.0 SP2", " DotnetFramework 1.0 SP3", "DotnetFramework 1.1", " DotnetFramework DotnetFramework 1.1 SP1", "DotnetFramework2.0", " 2.0 SP1", "DotnetFramework 2.0 SP2", " 3.0", "3.0 SP1", " DotnetFramework 3.0 SP2", "DotnetFramework 3.5", " DotnetFramework DotnetFramework 3.5 SP1", "4.5", " 4.5.1", "DotnetFramework 4,5,2", " 4,6", "DotnetFramework4,6", " 4,6", "4,7", " 4,7", "4,7", " DotnetFramework 4,7", "4,8" DotnetFramework DotnetFramework DotnetFramework DotnetFramework DotnetFramework DotnetFramework DotnetFramework DotnetFramework DotnetFramework DotnetFramework DotnetFramework

Nome	Descrição	Tipo	Obrigatório	Valores válidos
DotNetCoreVersion	A versão do .NET Core, se a aplicação for baseada no .NET Core	String	Não	".NET Core 1.0", ".NET Core 1.1", ".NET Core 2.0", ".NET Core 2.1", ".NET Core 2.2", ".NET Core 3.0", ".NET Core 3.1"
JdkVersion	A versão do JDK, se a aplicação usar o JDK	String	Não	"JDK1.0", "JDK2.0", "JDK3.0", ..., "JDK11.0"
DatabaseType	O tipo do banco de dados	String	Não	"SQLServer", "Oracle", "Sybase", "Mongo DB", "Maria DB", "Apache Cassandra", "MySQL", "IBM DB2", "PostgreSQLServer"
DatabaseEdition	A edição do banco de dados	String	Não	
DatabaseVersion	A versão do banco de dados	String	Não	Veja a versão HTML da documentação.

Remover seus dados do Strategy Recommendations

Para remover todos os seus dados do Migration Hub Strategy Recommendations, entre em contato com o [AWS Support](#).

Segurança no Migration Hub Strategy Recommendations

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 compartilhada](#) descreve isso como a segurança da nuvem e segurança na nuvem:

- **Segurança da nuvem:** AWS é responsável pela proteção da infraestrutura que executa AWS 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 [AWS Programas de conformidade](#). Para saber mais sobre os programas de compatibilidade que se aplicam ao Migration Hub Strategy Recommendations, consulte [Serviços da AWS em escopo por programa de compatibilidade](#).
- **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.

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

Tópicos

- [Proteção de dados no Migration Hub Strategy Recommendations](#)
- [Gerenciamento de identidade e acesso do Migration Hub Strategy Recommendations](#)
- [Validação de conformidade para o Migration Hub Strategy Recommendations](#)

Proteção de dados no Migration Hub Strategy Recommendations

O AWS [modelo de responsabilidade compartilhada](#) é aplicado à proteção de dados no Migration Hub Strategy Recommendations. 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 as Conta 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 Name (Nome). Essa recomendação inclui quando você trabalha com o Strategy Recommendations ou com outros serviços da Serviços da AWS usando o console, a API, a AWS CLI ou os SDKs da AWS. 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, recomendamos fortemente que não sejam incluídas informações de credenciais no URL para validar a solicitação a esse servidor.

Criptografia em repouso

Todos os dados armazenados no banco de dados do Strategy Recommendations são criptografados.

Criptografia em trânsito

As comunicações entre redes do Strategy Recommendations oferecem suporte à criptografia TLS 1.2 entre todos os componentes e clientes.

Gerenciamento de identidade e acesso do Migration Hub Strategy Recommendations

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

Tópicos

- [Público](#)
- [Autenticando com identidades](#)
- [Gerenciamento do acesso usando políticas](#)
- [Como o Migration Hub Strategy Recommendations funciona com o IAM](#)
- [AWS políticas gerenciadas para recomendações estratégicas do Migration Hub](#)
- [Exemplos de políticas baseadas em identidade para o Migration Hub Strategy Recommendations](#)
- [Resolução de problemas de identidade e acesso do Migration Hub Strategy Recommendations](#)
- [Usar perfis vinculados ao serviço do Strategy Recommendations](#)
- [Migration Hub Strategy Recommendations e endpoints da VPC de interface \(AWS PrivateLink\)](#)

Público

A forma como você usa AWS Identity and Access Management (IAM) difere, dependendo do trabalho que você faz nas Recomendações de Estratégia.

Usuário do serviço: se você usar o serviço Strategy Recommendations para fazer seu trabalho, o administrador fornecerá as credenciais e as permissões necessárias. À medida que usar mais atributos do Strategy Recommendations para fazer seu trabalho, você poderá precisar de permissões adicionais. Entender como o acesso é gerenciado pode ajudá-lo a solicitar as permissões corretas ao seu administrador. Se não conseguir acessar um atributo no Strategy Recommendations, consulte [Resolução de problemas de identidade e acesso do Migration Hub Strategy Recommendations](#).

Administrador do serviço: se você for o responsável pelos recursos do Strategy Recommendations na empresa, provavelmente terá acesso total ao Strategy Recommendations. Cabe a você determinar quais atributos e recursos do Strategy Recommendations os usuários do serviço devem acessar. Assim, você deve enviar solicitações ao administrador do IAM para alterar as permissões dos usuários de seu serviço. Revise as informações nesta página para entender a introdução ao IAM. Para saber mais sobre como sua empresa pode usar o IAM com o Strategy Recommendations, consulte [Como o Migration Hub Strategy Recommendations funciona com o IAM](#).

Administrador do IAM: se você for um administrador do IAM, talvez queira saber detalhes sobre como pode criar políticas para gerenciar o acesso ao Strategy Recommendations. Para visualizar exemplos de políticas baseadas em identidade do Strategy Recommendations que podem ser usadas no IAM, consulte [Exemplos de políticas baseadas em identidade para o Migration Hub Strategy Recommendations](#).

Autenticando com identidades

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

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

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

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

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

Conta da AWS usuário root

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

Identidade federada

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

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

Para o gerenciamento de acesso centralizado, recomendamos usar o AWS IAM Identity Center. Você pode criar usuários e grupos no IAM Identity Center ou pode se conectar e sincronizar com um conjunto de usuários e grupos em sua própria fonte de identidade para uso em todos os seus Contas

da AWS aplicativos. Para obter mais informações sobre o Centro de Identidade do IAM, consulte [O que é o Centro de Identidade do IAM?](#) no Guia do usuário do AWS IAM Identity Center .

Grupos e usuários do IAM

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

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

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

Perfis do IAM

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

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

- **Acesso de usuário federado:** para atribuir permissões a identidades federadas, você pode criar um perfil e definir permissões para ele. Quando uma identidade federada é autenticada, essa identidade é associada ao perfil e recebe as permissões definidas pelo mesmo. Para obter

mais informações sobre perfis para federação, consulte [Criar uma função para um provedor de identidade de terceiros](#) no Guia do usuário do IAM. Se você usar o IAM Identity Center, deverá configurar um conjunto de permissões. Para controlar o que suas identidades podem acessar após a autenticação, o IAM Identity Center correlaciona o conjunto de permissões a um perfil no IAM. Para obter informações sobre conjuntos de permissões, consulte [Conjuntos de permissões](#) no Guia do usuário do AWS IAM Identity Center .

- Permissões temporárias para usuários do IAM: um usuário ou um perfil do IAM pode assumir um perfil do IAM para obter temporariamente permissões diferentes para uma tarefa específica.
- Acesso entre contas: é possível usar um perfil do IAM para permitir que alguém (uma entidade principal confiável) em outra conta acesse recursos em sua conta. Os perfis são a principal forma de conceder acesso entre contas. No entanto, com alguns Serviços da AWS, você pode anexar uma política diretamente a um recurso (em vez de usar uma função como proxy). Para saber a diferença entre perfis e políticas baseadas em recurso para acesso entre contas, consulte [Como os perfis do IAM diferem das políticas baseadas em recurso](#) no Guia do usuário do IAM.
- Acesso entre serviços — Alguns Serviços da AWS usam recursos em outros Serviços da AWS. Por exemplo, quando você faz uma chamada em um serviço, é comum que esse serviço execute aplicações no Amazon EC2 ou armazene objetos no Amazon S3. Um serviço pode fazer isso usando as permissões da entidade principal da chamada por meio de um perfil de serviço ou um perfil vinculado ao serviço.
 - Sessões de acesso direto (FAS) — Quando você usa um usuário ou uma função do IAM para realizar ações AWS, você é considerado principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O FAS usa as permissões do diretor chamando um AWS service (Serviço da AWS), combinadas com a solicitação AWS service (Serviço da AWS) para fazer solicitações aos serviços posteriores. As solicitações do FAS são feitas somente quando um serviço recebe uma solicitação que requer interações com outros Serviços da AWS ou com recursos para ser concluída. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte [Encaminhar sessões de acesso](#).
- Perfil de serviço: é um [perfil do IAM](#) que um serviço assume para realizar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para obter mais informações, consulte [Criar uma função para delegar permissões a um AWS service \(Serviço da AWS\)](#) no Guia do usuário do IAM.
- Função vinculada ao serviço — Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um AWS service (Serviço da AWS) O serviço pode assumir o perfil para executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS

e são de propriedade do serviço. Um administrador do IAM pode exibir, mas não pode editar as permissões para perfis vinculados ao serviço.

- Aplicativos em execução no Amazon EC2 — Você pode usar uma função do IAM para gerenciar credenciais temporárias para aplicativos que estão sendo executados em uma instância do EC2 e fazendo AWS CLI solicitações de API. É preferível fazer isso e armazenar chaves de acesso na instância do EC2. Para atribuir uma AWS função a uma instância do EC2 e disponibilizá-la para todos os seus aplicativos, você cria um perfil de instância anexado à instância. Um perfil de instância contém o perfil e permite que os programas em execução na instância do EC2 obtenham credenciais temporárias. Para mais informações, consulte [Uso de uma função do IAM para conceder permissões a aplicações em execução em instâncias do Amazon EC2](#) no Guia do usuário do IAM.

Para saber se deseja usar perfis do IAM ou usuários do IAM, consulte [Quando criar uma função do IAM \(em vez de um usuário\)](#) no Guia do usuário do IAM.

Gerenciamento do acesso usando políticas

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

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

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

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

Políticas baseadas em identidade

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

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

Políticas baseadas em recurso

Políticas baseadas em recurso são documentos de políticas JSON que você anexa a um recurso. São exemplos de políticas baseadas em 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 que condições. Você precisa [especificar uma entidade principal](#) em uma política baseada em recurso. Os diretores podem incluir contas, usuários, funções, usuários federados ou. Serviços da AWS

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

Listas de controle de acesso (ACLs)

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

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

Outros tipos de política

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

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

Vários tipos de política

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

Como o Migration Hub Strategy Recommendations funciona com o IAM

Antes de usar o IAM para gerenciar o acesso ao Strategy Recommendations, saiba quais recursos do IAM estão disponíveis para uso com o Strategy Recommendations.

Recursos do IAM que podem ser usados com o Migration Hub Strategy Recommendations

Recurso do IAM	Suporte do Strategy Recommendations
Políticas baseadas em identidade	Sim
Políticas baseadas em recurso	Não
Ações de políticas	Sim
Recursos de políticas	Não
Chaves de condição de políticas	Não
ACLs	Não
ABAC (tags em políticas)	Não
Credenciais temporárias	Sim
Permissões de entidade principal	Sim
Perfis de serviço	Não
Funções vinculadas ao serviço	Sim

Para ter uma visão de alto nível de como as recomendações estratégicas e outros AWS serviços funcionam com a maioria dos recursos do IAM, consulte [AWS os serviços que funcionam com o IAM](#) no Guia do usuário do IAM.

Políticas baseadas em identidade para o Strategy Recommendations

É compatível com políticas baseadas em identidade	Sim
---	-----

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

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

Exemplos de políticas baseadas em identidade para o Strategy Recommendations

Para visualizar exemplos de políticas baseadas em identidade do Strategy Recommendations, consulte [Exemplos de políticas baseadas em identidade para o Migration Hub Strategy Recommendations](#).

Políticas baseadas em recursos no Strategy Recommendations

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

Políticas baseadas em recurso são documentos de políticas JSON que você anexa a um recurso. 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 que condições. Você precisa [especificar uma entidade principal](#) em uma política baseada em recurso. Os diretores podem incluir contas, usuários, funções, usuários federados ou. Serviços da AWS

Para permitir o acesso entre contas, você pode especificar uma conta inteira ou as entidades do IAM em outra conta como a entidade principal em uma política baseada em recurso. Adicionar uma entidade principal entre contas à política baseada em recurso é apenas metade da tarefa de estabelecimento da relação de confiança. Quando o principal e o recurso são diferentes Contas da

AWS, um administrador do IAM na conta confiável também deve conceder permissão à entidade principal (usuário ou função) para acessar o recurso. Eles concedem permissão ao anexar uma política baseada em identidade para a entidade. No entanto, se uma política baseada em recurso conceder acesso a uma entidade principal na mesma conta, nenhuma outra política baseada em identidade será necessária. Para obter mais informações, consulte [Como os perfis do IAM diferem de políticas baseadas em recursos](#) no Guia do usuário do IAM.

Ações políticas para o Strategy Recommendations

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

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

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

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

Para ver uma lista das ações do Strategy Recommendations, consulte [Ações definidas pelo Migration Hub Strategy Recommendations](#) na Referência de Autorização de Serviço.

As ações de política no Strategy Recommendations usam o seguinte prefixo antes da ação:

```
migrationhub-strategy
```

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

```
"Action": [  
  "migrationhub-strategy:action1",  
  "migrationhub-strategy:action2"  
]
```

Para visualizar exemplos de políticas baseadas em identidade do Strategy Recommendations, consulte [Exemplos de políticas baseadas em identidade para o Migration Hub Strategy Recommendations](#).

Recursos de políticas para o Strategy Recommendations

Oferece suporte a recursos de políticas Não

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

O elemento 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 recurso usando seu [nome do recurso da Amazon \(ARN\)](#). Isso pode ser feito para ações que oferecem suporte a um tipo de recurso específico, conhecido como permissões em nível de recurso.

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

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

Para ver uma lista dos tipos de recursos e seus ARNs do Strategy Recommendations, consulte [Recursos definidos pelo Migration Hub Strategy Recommendations](#) na Referência de Autorização de Serviço. Para saber com quais ações você pode especificar o ARN de cada recurso, consulte [Ações definidas pelo Migration Hub Strategy Recommendations](#).

Para visualizar exemplos de políticas baseadas em identidade do Strategy Recommendations, consulte [Exemplos de políticas baseadas em identidade para o Migration Hub Strategy Recommendations](#).

Chaves de condição de políticas para o Strategy Recommendations

Compatível com chaves de condição de política específicas do serviço Não

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

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

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

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

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

Para ver uma lista das chaves de condições do Strategy Recommendations, consulte [Chaves de condições do Migration Hub Strategy Recommendations](#) na Referência de Autorização de Serviço. Para saber com quais ações e recursos é possível usar uma chave de condição, consulte [Ações definidas pelo Migration Hub Strategy Recommendations](#).

Para visualizar exemplos de políticas baseadas em identidade do Strategy Recommendations, consulte [Exemplos de políticas baseadas em identidade para o Migration Hub Strategy Recommendations](#).

Listas de controle de acesso (ACLs) no Strategy Recommendations

Oferece suporte a ACLs

Não

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

Controle de acesso por atributo (ABAC) com o Strategy Recommendations

Oferece suporte a ABAC (tags em políticas) Não

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

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

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

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

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

Usar credenciais temporárias com o Strategy Recommendations

Oferece suporte a credenciais temporárias Sim

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

Você está usando credenciais temporárias se fizer login AWS Management Console usando qualquer método, exceto um nome de usuário e senha. Por exemplo, quando você acessa AWS

usando o link de login único (SSO) da sua empresa, esse processo cria automaticamente credenciais temporárias. Você também cria automaticamente credenciais temporárias quando faz login no console como usuário e, em seguida, alterna perfis. Para obter mais informações sobre como alternar perfis, consulte [Alternar para uma função \(console\)](#) no Guia do usuário do IAM.

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

Permissões de entidade principal entre serviços para o Strategy Recommendations

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

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

Perfis de serviço para o Strategy Recommendations

Oferece suporte a perfis de serviço	Não
-------------------------------------	-----

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

⚠ Warning

A alteração das permissões de um perfil de serviço pode interromper a funcionalidade do Strategy Recommendations. Edite perfis de serviço somente quando o Strategy Recommendations fornecer orientação para tal.

Perfis vinculados ao serviço para o Strategy Recommendations

Oferece suporte a funções vinculadas ao serviço Sim

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

Para obter detalhes sobre como criar ou gerenciar perfis vinculados ao serviço do Strategy Recommendations, consulte [Usar perfis vinculados ao serviço do Strategy Recommendations](#).

AWS políticas gerenciadas para recomendações estratégicas do Migration Hub

Para adicionar permissões a usuários, grupos e funções, é mais fácil usar políticas AWS gerenciadas do que escrever políticas você mesmo. 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 AWS gerenciadas. Essas políticas abrangem casos de uso comuns e estão disponíveis na sua Conta da AWS. Para obter mais informações sobre políticas AWS gerenciadas, consulte [políticas AWS gerenciadas](#) no Guia do usuário do IAM.

AWS os serviços mantêm e atualizam as políticas AWS gerenciadas. Você não pode alterar as permissões nas políticas AWS gerenciadas. Ocasionalmente, os serviços adicionam permissões adicionais a uma política AWS gerenciada para oferecer suporte a novos recursos. 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 AWS gerenciada quando um novo recurso é lançado ou quando novas operações são disponibilizadas. Os serviços não removem as permissões de uma política AWS gerenciada, portanto, as atualizações de políticas não violarão suas permissões existentes.

Além disso, AWS oferece suporte a políticas gerenciadas para funções de trabalho que abrangem vários serviços. Por exemplo, a política `ReadOnlyAccess` AWS gerenciada fornece acesso somente de leitura a todos os AWS serviços e recursos. Quando um serviço lança um novo recurso, AWS adiciona permissões somente de 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.

AWS política gerenciada: `AWSMigrationHubStrategyConsoleFullAccess`

É possível anexar a política `AWSMigrationHubStrategyConsoleFullAccess` a suas identidades do IAM.

A política `AWSMigrationHubStrategyConsoleFullAccess` concede acesso total a um usuário ao serviço Strategy Recommendations por meio do AWS Management Console.

Detalhes das permissões

Esta política inclui as seguintes permissões:

- `discovery`: concede ao usuário acesso para obter o resumo da descoberta no Application Discovery Service.
- `iam`: permite que uma função vinculada ao serviço seja criada para o usuário, o que é um requisito para usar o Strategy Recommendations.
- `migrationhub-strategy`: concede ao usuário acesso total ao Strategy Recommendations.
- `s3`: permite que o usuário crie e leia os buckets do S3 usados pelo Strategy Recommendations.
- `secretsmanager`: permite que o usuário liste o acesso aos segredos no Secrets Manager.

Para ver as permissões dessa política, consulte o Guia [AWSMigrationHubStrategyConsoleFullAccess](#) de referência de políticas AWS gerenciadas.

AWS política gerenciada: AWSMigrationHubStrategyCollector

É possível anexar a política AWSMigrationHubStrategyCollector a suas identidades do IAM.

Detalhes das permissões

Esta política inclui as seguintes permissões:

- `application-transformation`— concede permissões para carregar dados de log e métricas para operações de transformação de aplicativos e trabalhar com avaliações e recomendações de compatibilidade de portabilidade.
- `execute-api`: permite que o usuário acesse o Amazon API Gateway para fazer upload de logs e métricas para a AWS.
- `migrationhub-strategy`— Concede ao usuário acesso para registrar mensagens, enviar mensagens, carregar dados de registro e fazer upload de dados métricos para as Recomendações de Estratégia.
- `s3`— Concede ao usuário acesso aos compartimentos da lista e suas localizações. Os usuários também têm acesso para gravar, recuperar objetos, adicionar objetos, retornar a lista de controle de acesso (ACL), criar, acessar, configurar a criptografia, modificar a configuração, definir o estado de versão e criar ou substituir uma `PublicAccessBlock` configuração de ciclo de vida para os buckets do S3 usados pelas Recomendações de Estratégia.
- `secretsmanager`: permite que o usuário acesse segredos no Secrets Manager que são usados pelo Strategy Recommendations.

Para ver as permissões dessa política, consulte o Guia [AWSMigrationHubStrategyCollector](#) de referência de políticas AWS gerenciadas.

Recomendações de estratégia: atualizações das políticas AWS gerenciadas

Veja detalhes sobre as atualizações das políticas AWS gerenciadas das Recomendações de Estratégia desde que esse serviço começou a rastrear essas alterações. Para receber alertas automáticos sobre alterações feitas nesta página, inscreva-se no feed de RSS na página de Histórico do documento do Strategy Recommendations.

Alteração	Descrição	Data
<p>AWSMigrationHubStrategyCollector: atualizar para uma política existente</p>	<p>Essa política foi atualizada para incluir as ações de transformação de <code>GetPortingRecommendationAssessment</code> aplicativos <code>PutLogData</code> <code>StartPortingCompatibilityAssessment</code> <code>GetPortingCompatibilityAssessment</code>, <code>StartPortingRecommendationAssessment</code> e permitir que o serviço de transformação de aplicativos envie registros e métricas para o serviço. Os <code>ListBucket</code> e <code>GetBucketLocation</code> foram adicionados ao Amazon Simple Storage Service (Amazon S3) para suportar uploads de registros e métricas. Os <code>PutLogData</code> e também <code>PutMetricData</code> foram adicionados para permitir que o coletor de recomendações estratégicas envie registros e métricas para o endpoint do serviço.</p>	<p>1 de abril de 2024</p>
<p>AWSMigrationHubStrategyCollector: atualização para uma política existente</p>	<p>Esta política é atualizada com <code>PutMetricData</code> as <code>PutLogData</code> ações e. Essas ações permitem o upload de dados de registros e métricas para operações de transform</p>	<p>5 de fevereiro de 2024</p>

Alteração	Descrição	Data
	<p>ação de aplicativos. Essa atualização também adiciona condições para garantir que <code>aws:ResourceAccount</code> seja igual à permissão <code>aws:PrincipalAccount</code> para usar o Amazon Simple Storage Service e AWS Secrets Manager as ações incluídas.</p>	
<p>AWSMigrationHubStrategyCollector: atualização para uma política existente</p>	<p>Esta política é atualizada com as seguintes APIs do Amazon S3: <code>CreateBucket</code> , <code>PutEncryptionConfiguration</code> , <code>PutBucketPublicAccessBlock</code> , <code>PutBucketPolicy</code> , <code>PutBucketVersioning</code> e <code>PutLifecycleConfiguration</code> .</p>	<p>15 de setembro de 2023</p>
<p>AWSMigrationHubStrategyCollector: atualização para uma política existente</p>	<p>Esta atualização de política concede permissões que permitem a análise do código-fonte.</p>	<p>8 de março de 2023</p>
<p>AWSMigrationHubStrategyConsoleFullAccess: atualização para uma política existente</p>	<p>Essa política é atualizada com três AWS Application Discovery Service APIs — <code>DescribeConfigurations</code> <code>DescribeTags</code> , e. <code>ListConfigurations</code></p>	<p>10 de novembro de 2022</p>

Alteração	Descrição	Data
<p>AWSMigrationHubStrategyCollector: atualização para uma política existente</p>	<p>Esta política é atualizada com a <code>UpdateCollectorConfiguration</code> ação. Esta ação armazena a configuração do seu coletor para facilitar a recuperação.</p>	<p>7 de setembro de 2022</p>
<p>AWSMigrationHubStrategyConsoleFullAccess— Nova política disponibilizada no lançamento</p>	<p>A política <code>AWSMigrationHubStrategyConsoleFullAccess</code> concede acesso total a um usuário ao serviço <code>Strategy Recommendations</code> por meio do <code>AWS Management Console</code>.</p>	<p>25 de outubro de 2021</p>
<p>AWSMigrationHubStrategyCollector— Nova política disponibilizada no lançamento</p>	<p>A política <code>AWSMigrationHubStrategyCollector</code> concede ao usuário acesso ao serviço <code>Strategy Recommendations</code> e acesso de leitura/gravação aos buckets do S3 relacionados ao serviço. Também concede ao <code>Amazon API Gateway</code> acesso para fazer upload de registros e métricas AWS, e ao <code>AWS Secrets Manager</code> acesso para buscar credenciais.</p>	<p>25 de outubro de 2021</p>

Alteração	Descrição	Data
AWSMigrationHubStrategyServiceRolePolicy — Nova política disponibilizada no lançamento	A política AWSMigrationHubStrategyServiceRolePolicy de função vinculada ao serviço fornece acesso a e. AWS Migration Hub AWS Application Discovery Service Esta política também concede permissões para armazenar relatórios no Amazon Simple Storage Service (Amazon S3).	25 de outubro de 2021
O Strategy Recommendations começou a monitorar alterações	A Strategy Recommendations começou a monitorar as mudanças em suas políticas AWS gerenciadas.	25 de outubro de 2021

Exemplos de políticas baseadas em identidade para o Migration Hub Strategy Recommendations

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

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

Para obter detalhes sobre ações e tipos de recurso definidos pelo Strategy Recommendations, incluindo o formato dos ARNs para cada tipo de recurso, consulte [Ações, recursos e chaves de condição para o Strategy Recommendations](#) na Referência de autorização do serviço.

Tópicos

- [Práticas recomendadas de políticas](#)
- [Usando o console do Strategy Recommendations](#)
- [Permitir que os usuários visualizem suas próprias permissões](#)
- [Acessar um bucket do Amazon S3](#)

Práticas recomendadas de políticas

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

- Comece com as políticas AWS gerenciadas e avance para as permissões de privilégios mínimos — Para começar a conceder permissões aos seus usuários e cargas de trabalho, use as políticas AWS gerenciadas que concedem permissões para muitos casos de uso comuns. Eles estão disponíveis no seu Conta da AWS. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo AWS cliente que sejam específicas para seus casos de uso. Para obter mais informações, consulte [Políticas gerenciadas pela AWS](#) ou [Políticas gerenciadas pela AWS para perfis de trabalho](#) no Guia do usuário do IAM.
- Aplique permissões de privilégio mínimo: ao definir permissões com as políticas do IAM, conceda apenas as permissões necessárias para executar uma tarefa. Você faz isso definindo as ações que podem ser executadas em recursos específicos sob condições específicas, também conhecidas como permissões de privilégio mínimo. Para obter mais informações sobre como usar o IAM para aplicar permissões, consulte [Políticas e permissões no IAM](#) no Guia do usuário do IAM.
- Use condições nas políticas do IAM para restringir ainda mais o acesso: você pode adicionar uma condição às políticas para limitar o acesso a ações e recursos. Por exemplo, você pode escrever uma condição de política para especificar que todas as solicitações devem ser enviadas usando SSL. Você também pode usar condições para conceder acesso às ações de serviço se elas forem usadas por meio de uma ação específica AWS service (Serviço da AWS), como AWS CloudFormation. Para obter mais informações, consulte [Elementos de política JSON do IAM: Condition](#) no Guia do usuário do IAM.
- Use o IAM Access Analyzer para validar suas políticas do IAM a fim de garantir permissões seguras e funcionais: o IAM Access Analyzer valida as políticas novas e existentes para que elas sigam a linguagem de política do IAM (JSON) e as práticas recomendadas do IAM. O IAM Access Analyzer oferece mais de cem verificações de política e recomendações acionáveis para ajudar você a criar políticas seguras e funcionais. Para obter mais informações, consulte [Validação de políticas do IAM Access Analyzer](#) no Guia do usuário do IAM.

- Exigir autenticação multifator (MFA) — Se você tiver um cenário que exija usuários do IAM ou um usuário root, ative Conta da AWS a MFA para obter segurança adicional. Para exigir a MFA quando as operações de API forem chamadas, adicione condições de MFA às suas políticas. Para obter mais informações, consulte [Configuração de acesso à API protegido por MFA](#) no Guia do usuário do IAM.

Para obter mais informações sobre as práticas recomendadas do IAM, consulte [Práticas recomendadas de segurança no IAM](#) no Guia do usuário do IAM.

Usando o console do Strategy Recommendations

Para acessar o console do Migration Hub Strategy Recommendations, você precisa ter um conjunto mínimo de permissões. Essas permissões devem permitir que você liste e visualize detalhes sobre os recursos de Recomendações de Estratégia em seu Conta da AWS. Se você criar uma política baseada em identidade que seja mais restritiva do que as permissões mínimas necessárias, o console não funcionará como pretendido para entidades (usuários ou perfis) com essa política.

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

Para garantir que usuários e funções ainda possam usar o console de Recomendações de Estratégia, anexe também as Recomendações de Estratégia ConsoleAccess ou a política ReadOnly AWS gerenciada às entidades. Para obter mais informações, consulte [Adicionando Permissões a um Usuário](#) no Guia do Usuário do IAM.

Permitir que os usuários visualizem suas próprias permissões

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

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

```

        "iam:GetUserPolicy",
        "iam:ListGroupsForUser",
        "iam:ListAttachedUserPolicies",
        "iam:ListUserPolicies",
        "iam:GetUser"
    ],
    "Resource": ["arn:aws:iam::*:user/${aws:username}"]
},
{
    "Sid": "NavigateInConsole",
    "Effect": "Allow",
    "Action": [
        "iam:GetGroupPolicy",
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam:ListAttachedGroupPolicies",
        "iam:ListGroupPolicies",
        "iam:ListPolicyVersions",
        "iam:ListPolicies",
        "iam:ListUsers"
    ],
    "Resource": "*"
}
]
}

```

Acessar um bucket do Amazon S3

Neste exemplo, você deseja conceder a um usuário do IAM seu Conta da AWS acesso a um dos seus buckets do Amazon S3, `examplebucket`. Você também deseja permitir que o usuário adicione, atualize e exclua objetos.

Além de conceder as permissões `s3:PutObject`, `s3:GetObject` e `s3:DeleteObject` ao usuário, a política também concede as permissões `s3:ListAllMyBuckets`, `s3:GetBucketLocation` e `s3:ListBucket`. Estas são permissões adicionais, exigidas pelo console. As ações `s3:PutObjectAcl` e `s3:GetObjectAcl` também são necessárias para copiar, recortar e colar objetos no console. Para obter uma demonstração de exemplo que concede permissões aos usuários e testa-os ao usar o console, consulte [Demonstração de exemplo: Usar políticas de usuário para controlar o acesso a seu bucket](#).

```

{
    "Version": "2012-10-17",

```

```
"Statement":[
  {
    "Sid":"ListBucketsInConsole",
    "Effect":"Allow",
    "Action":[
      "s3:ListAllMyBuckets"
    ],
    "Resource":"arn:aws:s3:::*"
  },
  {
    "Sid":"ViewSpecificBucketInfo",
    "Effect":"Allow",
    "Action":[
      "s3:ListBucket",
      "s3:GetBucketLocation"
    ],
    "Resource":"arn:aws:s3:::examplebucket"
  },
  {
    "Sid":"ManageBucketContents",
    "Effect":"Allow",
    "Action":[
      "s3:PutObject",
      "s3:PutObjectAcl",
      "s3:GetObject",
      "s3:GetObjectAcl",
      "s3:DeleteObject"
    ],
    "Resource":"arn:aws:s3:::examplebucket/*"
  }
]
```

Resolução de problemas de identidade e acesso do Migration Hub Strategy Recommendations

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

Tópicos

- [Não tenho autorização para executar uma ação no Strategy Recommendations](#)
- [Não estou autorizado a realizar iam: PassRole](#)
- [Quero visualizar minhas chaves de acesso](#)
- [Sou administrador e desejo permitir que outras pessoas tenham acesso ao Strategy Recommendations](#)
- [Quero permitir que pessoas fora da minha acessem meus recursos Conta da AWS de Recomendações de Estratégia](#)

Não tenho autorização para executar uma ação no Strategy Recommendations

Se isso AWS Management Console indicar que você não está autorizado a realizar uma ação, entre em contato com o administrador para obter ajuda. O administrador é a pessoa que forneceu o seu nome de usuário e senha.

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

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

Neste caso, Mateo pede ao administrador para atualizar suas políticas para permitir a ele o acesso ao recurso `my-example-widget` usando a ação `migrationhub-strategy:GetWidget`.

Não estou autorizado a realizar iam: PassRole

Se você receber uma mensagem de erro informando que não tem autorização para executar a ação `iam:PassRole`, será necessário atualizar suas políticas para permitir a transmissão de um perfil para o Strategy Recommendations.

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

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

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

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

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

Quero visualizar minhas chaves de acesso

Depois de criar suas chaves de acesso de usuário do IAM, é possível visualizar seu ID da chave de acesso a qualquer momento. No entanto, você não pode visualizar sua chave de acesso secreta novamente. Se você perder sua chave secreta, crie um novo par de chaves de acesso.

As chaves de acesso consistem em duas partes: um ID de chave de acesso (por exemplo, AKIAIOSFODNN7EXAMPLE) e uma chave de acesso secreta (por exemplo, wJalrXUtnFEMI/K7MDENG/bPxrFiCYEXAMPLEKEY). Como um nome de usuário e uma senha, você deve usar o ID da chave de acesso e a chave de acesso secreta em conjunto para autenticar suas solicitações. Gerencie suas chaves de acesso de forma tão segura quanto você gerencia seu nome de usuário e sua senha.

Important

Não forneça as chaves de acesso a terceiros, mesmo que seja para ajudar a [encontrar o ID de usuário canônico](#). Ao fazer isso, você pode dar a alguém acesso permanente ao seu Conta da AWS.

Ao criar um par de chaves de acesso, você é solicitado a guardar 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, será necessário adicionar novas chaves de acesso para seu usuário do IAM. Você pode ter no máximo duas chaves de acesso. Se você já tiver duas, você deverá excluir um par de chaves para poder criar um novo. Para visualizar as instruções, consulte [Gerenciar chaves de acesso](#) no Guia do usuário do IAM.

Sou administrador e desejo permitir que outras pessoas tenham acesso ao Strategy Recommendations

Para permitir que outros usuários acessem o Strategy Recommendations, crie uma entidade do IAM (usuário ou função) para a pessoa ou a aplicação que precisa do acesso. Elas usarão as credenciais dessa entidade para acessar a AWS. Você deve anexar uma política à entidade que concede a eles as permissões corretas no Strategy Recommendations.

Para começar a usar imediatamente, consulte [Criar os primeiros usuário e grupo delegados pelo IAM](#) no Guia do usuário do IAM.

Quero permitir que pessoas fora da minha acessem meus recursos Conta da AWS de Recomendações de Estratégia

Você pode criar um perfil que os usuários de outras contas ou pessoas fora da organização podem usar para acessar seus recursos. Você pode especificar quem é confiável para assumir o perfil. Para serviços que oferecem suporte a políticas baseadas em 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 Strategy Recommendations é compatível com esses atributos, consulte [Como o Migration Hub Strategy Recommendations funciona com o IAM](#).
- Para saber como fornecer acesso aos seus recursos em todos os Contas da AWS que você possui, consulte [Como fornecer acesso a um usuário do IAM em outro Conta da AWS que você possui](#) no Guia do usuário do IAM.
- Para saber como fornecer acesso aos seus recursos a terceiros Contas da AWS, consulte [Como fornecer acesso Contas da AWS a terceiros](#) no Guia do usuário do IAM.
- Para saber como conceder acesso por meio da federação de identidades, consulte [Conceder acesso a usuários autenticados externamente \(federação de identidades\)](#) no Guia do usuário do IAM.
- Para saber a diferença entre usar perfis e políticas baseadas em recursos para acesso entre contas, consulte [Como os perfis do IAM diferem de políticas baseadas em recursos](#) no Guia do usuário do IAM.

Usar perfis vinculados ao serviço do Strategy Recommendations

O Migration Hub Strategy Recommendations usa funções [vinculadas ao serviço AWS Identity and Access Management \(IAM\)](#). O perfil vinculado ao serviço é um tipo exclusivo de perfil do IAM vinculado diretamente ao Strategy Recommendations. As funções vinculadas ao serviço são predefinidas pelas Recomendações de Estratégia e incluem todas as permissões que o serviço exige para chamar outros AWS serviços em seu nome.

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

Para obter informações sobre outros serviços compatíveis com funções vinculadas a serviços, consulte [Serviços da AWS compatíveis com o IAM](#) e procure os serviços que contenham Sim na coluna Função vinculada a serviço. Escolha um Sim com um link para visualizar a documentação do perfil vinculado a esse serviço.

Permissões de perfis vinculados ao serviço para o Strategy Recommendations

O Strategy Recommendations usa a função vinculada ao serviço nomeada `AWSServiceRoleForMigrationHubStrategy` e a associa à política `AWSMigrationHubStrategyServiceRolePolicy` do IAM — Fornece acesso a e. AWS Migration Hub AWS Application Discovery Service Esta política também concede permissões para armazenar relatórios no Amazon Simple Storage Service (Amazon S3).

A função vinculada ao serviço `AWSServiceRoleForMigrationHubStrategy` confia nos seguintes serviços para aceitar a função:

- `migrationhub-strategy.amazonaws.com`

A política de permissões de perfil permite que o Strategy Recommendations realize as seguintes ações.

AWS Application Discovery Service ações

`discovery:ListConfigurations`

```
discovery:DescribeConfigurations
```

AWS Migration Hub ações

```
mgh:GetHomeRegion
```

Ações do Amazon S3

```
s3:GetBucketAcl
```

```
s3:GetBucketLocation
```

```
s3:GetObject
```

```
s3:ListAllMyBuckets
```

```
s3:ListBucket
```

```
s3:PutObject
```

```
s3:PutObjectAcl
```

Para ver as permissões dessa política, consulte o Guia [AWSMigrationHubStrategyServiceRolePolicy](#) de referência de políticas AWS gerenciadas.

Para ver o histórico de atualizações dessa política, consulte [Recomendações de estratégia: atualizações das políticas AWS gerenciadas](#).

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

Criar um perfil vinculado ao serviço para o Strategy Recommendations

Não é necessário criar manualmente um perfil vinculado ao serviço. Quando você concorda em permitir que o Migration Hub crie uma função vinculada ao serviço (SLR) em sua conta no AWS Management Console, o Strategy Recommendations cria a função vinculada ao serviço para você.

Se excluir esse perfil vinculado ao serviço e precisar criá-lo novamente, você poderá usar esse mesmo processo para recriar o perfil em sua conta. Quando você concorda em permitir que o Migration Hub crie um perfil vinculado ao serviço (SLR) em sua conta, o Strategy Recommendations cria novamente o perfil vinculado ao serviço para você.

Editar um perfil vinculado ao serviço para o Strategy Recommendations

O Strategy Recommendations não permite que você edite a função `AWSServiceRoleForMigrationHubStrategy` vinculada ao serviço. Depois de criar um perfil vinculado ao serviço, você não poderá alterar o nome do perfil, pois várias entidades podem fazer referência a ele. No entanto, você pode editar a descrição da função usando o console, a CLI ou a API do Strategy Recommendations.

Excluir um perfil vinculado ao serviço para o Strategy Recommendations

Como excluir manualmente o perfil vinculado ao serviço usando o IAM

Use o console do IAM AWS CLI, o ou a AWS API para excluir a função `AWSServiceRoleForMigrationHubStrategy` vinculada ao serviço. Para obter mais informações, consulte [Excluir um perfil vinculado ao serviço](#) no Guia do usuário do IAM.

Ao excluir recursos de Recomendações de Estratégia usados pela `AWSServiceRoleForMigrationHubStrategySLR`, você não pode ter nenhuma avaliação em execução (tarefas para gerar recomendações). Também não é possível realizar nenhuma avaliação em segundo plano. Se as avaliações estiverem em execução, a exclusão do SLR falhará no console do IAM. Se a exclusão do SLR falhar, você poderá tentar a exclusão novamente após a conclusão de todas as tarefas em segundo plano. Você não precisa limpar nenhum recurso criado antes de excluir o SLR.

Regiões compatíveis com perfis vinculados ao serviço do Strategy Recommendations

O Strategy Recommendations oferece suporte a perfis vinculados ao serviço em todas as regiões em que o serviço está disponível. Para obter mais informações, consulte [Regiões e endpoints da AWS](#).

Migration Hub Strategy Recommendations e endpoints da VPC de interface (AWS PrivateLink)

É possível estabelecer uma conexão privada entre a VPC e o Migration Hub Strategy Recommendations criando um endpoint da VPC de interface. Os endpoints de interface são desenvolvidos pelo AWS PrivateLink. Com AWS PrivateLink, você pode acessar as operações de API do Strategy Recommendations de modo privado, sem um gateway da Internet, um dispositivo NAT, uma conexão VPN ou uma conexão do AWS Direct Connect. As instâncias na VPC não precisam de endereços IP públicos para a comunicação com as operações de API do Strategy

Recommendations. O tráfego entre sua VPC e o Strategy Recommendations permanece na rede da Amazon.

Cada endpoint de interface é representado por uma ou mais [interfaces de rede elástica](#) nas sub-redes.

Para obter mais informações, consulte [VPC endpoints de interface \(AWS PrivateLink\)](#) no Guia do usuário da Amazon VPC.

Considerações sobre o Strategy Recommendations (endpoints da VPC)

Antes de configurar um endpoint da VPC de interface para o Strategy Recommendations, certifique-se de revisar as [propriedades e limitações do endpoint de interface](#) e [cotas do AWS PrivateLink](#) no Guia do usuário da Amazon VPC.

O Strategy Recommendations oferece suporte a chamadas para todas as ações de API da VPC. Para usar tudo no Strategy Recommendations, você deve criar um endpoint da VPC.

Criar um endpoint da VPC de interface para o Strategy Recommendations

É possível criar um endpoint da VPC para o Strategy Recommendations usando o console da Amazon VPC ou a AWS Command Line Interface (AWS CLI). Para obter mais informações, consulte [Criar um endpoint de interface](#) no Guia do usuário da Amazon VPC.

Criar um endpoint da VPC para o Strategy Recommendations usando o seguinte nome de serviço:

- `com.amazonaws.region.migrationhub-strategy`

Se você habilitar o DNS privado para o endpoint, poderá fazer solicitações de API para o Strategy Recommendations usando seu nome DNS padrão para a região. Por exemplo, você pode usar o nome `migrationhub-strategy.us-east-1.amazonaws.com`.

Para obter mais informações, consulte [Acessar um serviço por um endpoint de interface](#) no Guia do usuário da Amazon VPC.

Criar uma política de endpoint da VPC para o Strategy Recommendations

É possível anexar uma política de endpoint ao endpoint da VPC que controla o acesso ao Strategy Recommendations. Essa política especifica as seguintes informações:

- A entidade principal que pode executar ações.

- As ações que podem ser executadas.
- Os atributos no quais as ações podem ser executadas.

Para obter mais informações, consulte [Controlar o acesso a serviços com VPC endpoints](#) no Guia do usuário da Amazon VPC.

Exemplo: ações de uma política de endpoint da VPC para o Strategy Recommendations

Veja a seguir um exemplo de uma política de endpoint para o Strategy Recommendations. Quando anexada a um endpoint, essa política concede acesso às ações indicadas do Strategy Recommendations para todos os principais em todos os recursos.

```
{
  "Statement": [
    {
      "Principal": "*",
      "Effect": "Allow",
      "Action": [
        "migrationhub-strategy:ListContacts",
      ],
      "Resource": "*"
    }
  ]
}
```


Validação de conformidade para o Migration Hub Strategy Recommendations

Para saber se um AWS service (Serviço da AWS) está dentro do escopo de programas de conformidade específicos, consulte [Serviços da AWS Escopo por Programa de Conformidade](#) [Serviços da AWS](#) e escolha o programa de conformidade em que você está interessado. Para obter informações gerais, consulte Programas de [AWS conformidade Programas AWS](#) de .

Você pode baixar relatórios de auditoria de terceiros usando AWS Artifact. Para obter mais informações, consulte [Baixar relatórios em AWS Artifact](#) .

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

- [Guias de início rápido sobre segurança e conformidade](#) — Esses guias de implantação discutem considerações arquitetônicas e fornecem etapas para a implantação de ambientes básicos AWS focados em segurança e conformidade.
- [Arquitetura para segurança e conformidade com a HIPAA na Amazon Web Services](#) — Este whitepaper descreve como as empresas podem usar AWS para criar aplicativos qualificados para a HIPAA.

 Note

Nem todos Serviços da AWS são elegíveis para a HIPAA. Para obter mais informações, consulte [Referência dos Serviços Qualificados pela HIPAA](#).

- AWS Recursos de <https://aws.amazon.com/compliance/resources/> de conformidade — Essa coleção de pastas de trabalho e guias pode ser aplicada ao seu setor e local.
- [AWS Guias de conformidade do cliente](#) — Entenda o modelo de responsabilidade compartilhada sob a ótica da conformidade. Os guias resumem as melhores práticas de proteção Serviços da AWS e mapeiam as diretrizes para controles de segurança em várias estruturas (incluindo o Instituto Nacional de Padrões e Tecnologia (NIST), o Conselho de Padrões de Segurança do Setor de Cartões de Pagamento (PCI) e a Organização Internacional de Padronização (ISO)).
- [Avaliação de recursos com regras](#) no Guia do AWS Config desenvolvedor — O AWS Config serviço avalia o quão bem suas configurações de recursos estão em conformidade com as práticas internas, as diretrizes e os regulamentos do setor.
- [AWS Security Hub](#)— Isso AWS service (Serviço da AWS) fornece uma visão abrangente do seu estado de segurança interno AWS. O Security Hub usa controles de segurança para avaliar os atributos da AWS e verificar a conformidade com os padrões e as práticas recomendadas do setor de segurança. Para obter uma lista dos serviços com suporte e controles aceitos, consulte a [Referência de controles do Security Hub](#).
- [Amazon GuardDuty](#) — Isso AWS service (Serviço da AWS) detecta possíveis ameaças às suas cargas de trabalho Contas da AWS, contêineres e dados monitorando seu ambiente em busca de atividades suspeitas e maliciosas. GuardDuty pode ajudá-lo a atender a vários requisitos de conformidade, como o PCI DSS, atendendo aos requisitos de detecção de intrusões exigidos por determinadas estruturas de conformidade.
- [AWS Audit Manager](#)— Isso AWS service (Serviço da AWS) ajuda você a auditar continuamente seu AWS uso para simplificar a forma como você gerencia o risco e a conformidade com as regulamentações e os padrões do setor.

Trabalhar com outros serviços da

Esta seção descreve outros produtos da AWS que interagem com o Migration Hub Strategy Recommendations.

Tópicos

- [Registrar chamadas da API do Strategy Recommendations com o AWS CloudTrail](#)

Registrar chamadas da API do Strategy Recommendations com o AWS CloudTrail

O Migration Hub Strategy Recommendations é integrado ao AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, um perfil ou um produto da AWS no Strategy Recommendations. O CloudTrail captura as chamadas de API do Strategy Recommendations como eventos. As chamadas capturadas incluem as chamadas do console do Strategy Recommendations e as chamadas de código para as operações da API do Strategy Recommendations.

Se você criar uma trilha, poderá habilitar a entrega contínua de eventos do CloudTrail para um bucket do Amazon S3, incluindo eventos para o Strategy Recommendations. Se você não configurar uma trilha, ainda poderá visualizar os eventos mais recentes no console do CloudTrail em Event history (Histórico de eventos). Usando as informações coletadas pelo CloudTrail, é possível determinar a solicitação feita para o Strategy Recommendations, o endereço IP do qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita e outros detalhes.

Para saber mais sobre o CloudTrail, consulte o [Guia do usuário do AWS CloudTrail](#).

Informações do Strategy Recommendations no CloudTrail

O CloudTrail é habilitado em sua Conta da AWS quando ela é criada. Quando ocorre atividade no Strategy Recommendations, essa atividade é registrada em um evento do CloudTrail junto com outros eventos de serviços da AWS no Event history (Histórico de eventos). Você pode visualizar, pesquisar e baixar eventos recentes em sua Conta da AWS. Para obter mais informações, consulte [Viewing events with CloudTrail Event history](#) (Como visualizar eventos com o histórico de eventos do CloudTrail).

Para ter um registro de eventos contínuo em sua Conta da AWS, incluindo eventos do Strategy Recommendations, crie uma trilha. Uma trilha permite que o CloudTrail entregue arquivos de log

a um bucket do Amazon S3. Por padrão, quando você cria uma trilha no console, ela é aplicada a todas as Regiões da AWS. A trilha registra em log eventos de todas as regiões na partição da AWS e entrega os arquivos de log para o bucket do Amazon S3 especificado por você. Além disso, é possível configurar outros serviços da AWS para analisar mais ainda mais e agir com base nos dados de eventos coletados nos logs do CloudTrail. Para obter mais informações, consulte:

- [Visão geral da criação de uma trilha](#)
- [Serviços e integrações compatíveis com o CloudTrail](#)
- [Configurar notificações do Amazon SNS para o CloudTrail](#)
- [Receber arquivos de log do CloudTrail de várias regiões](#) e [Receber arquivos de log do CloudTrail de várias contas](#)

O Strategy Recommendations é compatível com as seguintes ações como eventos nos arquivos de log do CloudTrail:

- [GetApplicationComponentStrategies](#)
- [GetApplicationComponentDetails](#)
- [GetAssesment](#)
- [GetImportFileTask](#)
- [GetPortfolioPreferences](#)
- [GetPortfolioSummary](#)
- [GetServerDetails](#)
- [GetServerStrategies](#)
- [ListApplicationComponents](#)
- [ListCollectors](#)
- [ListImportFileTask](#)
- [ListServers](#)
- [PutPortfolioPreferences](#)
- [StartAssessment](#)
- [StartImportFileTask](#)
- [StopAssessment](#)
- [UpdateApplicationComponetConfig](#)
- [UpdateServerConfig](#)

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

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

Para obter mais informações, consulte [Elemento userIdentity do CloudTrail](#).

Noções básicas sobre as entradas de arquivos de log do Strategy Recommendations

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

O exemplo a seguir mostra uma entrada de log do CloudTrail que demonstra a ação [GetServerDetails](#).

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "777777777777",
    "arn": "arn:aws:sts::111122223333:assumed-role/myUserName/...",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "777777777777",
        "arn": "arn:aws:iam::111122223333:role/myUserName",
        "accountId": "111122223333",
        "userName": "myUserName"
      }
    }
  }
}
```

```
    },
    "webIdFederationData": {},
    "attributes": {
      "creationDate": "2021-09-20T01:07:16Z",
      "mfaAuthenticated": "false"
    }
  }
},
"eventTime": "2021-09-20T01:07:43Z",
"eventSource": "migrationhub-strategy.amazonaws.com",
"eventName": "GetServerDetails",
"awsRegion": "us-west-2",
"sourceIPAddress": "",
"userAgent": "",
"requestParameters": {
  "serverId": "ads-server-006"
},
"responseElements": null,
"requestID": "07D681279BD94AED",
"eventID": "cdc4b7ed-e171-4cef-975a-ad829d4123e8",
"readOnly": true,
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "111122223333",
"eventCategory": "Management"
}
```

Cotas para o Migration Hub Strategy Recommendations

Sua conta da AWS possui cotas padrão, anteriormente chamadas de limites, para cada produto da AWS. A menos que especificado de outra forma, cada cota é específica da região. Você pode solicitar aumentos para algumas cotas e outras cotas não podem ser aumentadas.

Para ver uma lista das cotas do Migration Hub Strategy Recommendations, consulte as [Cotas de serviço do Strategy Recommendations](#).

Você também pode visualizar as cotas para o Strategy Recommendations abrindo o console [Service Quotas](#). No painel de navegação, escolha Produtos da AWS e selecione Migration Hub Strategy Recommendations.

Para solicitar o aumento da cota, consulte [Requesting a Quota Increase](#) (Solicitação de aumento de cota) no Guia do usuário do Service Quotas. Se a cota ainda não estiver disponível no Service Quotas, use o [formulário de aumento de limite](#).

Notas de release

Tópicos

- [17 de novembro de 2023](#)
- [12 de outubro de 2023](#)
- [17 de abril de 2023](#)
- [17 de março de 2023](#)
- [7 de novembro de 2022](#)
- [27 de setembro de 2022](#)
- [30 de junho de 2022](#)
- [18 de abril de 2022](#)
- [25 de fevereiro de 2022](#)
- [10 de fevereiro de 2022](#)
- [28 de janeiro de 2022](#)
- [14 de janeiro de 2022](#)
- [21 de dezembro de 2021](#)
- [15 de dezembro de 2021](#)
- [25 de outubro de 2021](#)

17 de novembro de 2023

Novos atributos

- Coletor v1.1.47
- Support para aplicativos.NET 8.

12 de outubro de 2023

Novos atributos

- Coletor v1.1.45
- Support para fontes de dados múltiplos.

17 de abril de 2023

Novos atributos

- Collector v1.1.22
- Melhorias no script de atualização. Isso requer a versão mais recente do Collector.

17 de março de 2023

Novo atributo

Análise binária adicionada, que fornece detecção de antipadrões e incompatibilidades sem código-fonte.

7 de novembro de 2022

Novo atributo

- Filtragem de aplicações para aplicações
- Filtragem de servidores por tags do AWS Application Discovery Service

27 de setembro de 2022

Novo atributo

- Collector v1.1.12
 - SCT versão 667
 - eMPAnalyzer 2.2.0.368
- Comandos de `diag check` adicionados para insights do servidor.
- Suporte adicionado para recomendações potenciais.
- Interface de usuário aprimorada para verificar a configuração e o status da avaliação.

Correções de erros

- Portabilidade, tradutor assistente e outras correções.

30 de junho de 2022

Novo atributo

- Collector v1.1.11
 - Suporte adicionado para API do VMware.
 - O A2C solicitou alterações para adicionar o cabeçalho do usuário ao baixar o arquivo binário.
 - Caminho inicial do Linux, shell padrão e terminação remota de todos os shells foram adicionados.
- Binário público A2C v1.17
 - Foi adicionado suporte para o Azure DevOps como destino de implantação do pipeline.

18 de abril de 2022

Novo atributo

- Collector v1.1.7
- Capacidade adicionada de baixar dinamicamente o binário A2C do URL público.

Correções de erros

- A2C v1.1.5

25 de fevereiro de 2022

Correções de erros

- SCT v5.6.9
- A2C v1.1.2
- Collector v1.1.4

10 de fevereiro de 2022

Correções de erros

- SCT v5.6.8
- A2C v1.1.1
 - Verificação adicionada para o comando tar no Linux.
 - Corrigido o problema de verificação das imagens de aplicações no Amazon ECR.
 - Corrigido o problema que exigia a remoção do contêiner para pré-validação.
- Collector v1.1.3
 - Corrigido o erro 4xx para máquina remota de 32 bits.
 - Os códigos de erro do A2C foram atualizados.
 - Endereço IP validado no C# para análise do código-fonte da máquina remota.

28 de janeiro de 2022

Novo atributo

- Collector v1.1.2
- Foi adicionado suporte ao repositório DevOps Git do Azure para análise de código-fonte.

14 de janeiro de 2022

Novo atributo

- Collector v1.1.1
- Recomendações do Babelfish adicionadas para bancos de dados SQL.

21 de dezembro de 2021

Problema resolvido

- Collector v1.1.0
- A análise de banco de dados foi restaurada.

15 de dezembro de 2021

Problema conhecido

- Collector v1.0.4
- Atualmente, a análise de banco de dados não é compatível (CVE-2021-44228).

25 de outubro de 2021

Novo atributo

- Collector v1.0.0
- Versão inicial do Guia do usuário do Migration Hub Strategy Recommendations.

Histórico do documento e da versão

A tabela a seguir descreve as versões de documentação para o Strategy Recommendations. Para ter mais informações, consulte [Notas de release](#).

Alteração	Descrição	Data
AWS atualizações de políticas gerenciadas - atualizar para AWSMigrationHubStrategyCollector	Atualizou a AWSMigrationHubStrategyCollector política para incluir novas <code>s3application-transformation</code> , e <code>migration-hub-strategy</code> ações.	1 de abril de 2024
AWS atualizações de políticas gerenciadas - atualizar para AWSMigrationHubStrategyCollector	Atualizou a AWSMigrationHubStrategyCollector política para incluir novas <code>application-transformation</code> ações. Essa atualização também adiciona condições para restringir várias ações onde <code>aws:ResourceAccount</code> devem ser iguais à <code>aws:PrincipalAccount</code> .	5 de fevereiro de 2024
Novo atributo	O cliente coletor de dados do aplicativo Strategy Recommendations v1.1.47 está disponível com suporte para aplicativos.NET 8.	17 de novembro de 2023
Novo atributo	O cliente coletor de dados do aplicativo Strategy Recommendations v1.1.45	12 de outubro de 2023

	está disponível com suporte para várias fontes de dados.	
AWS atualizações de políticas gerenciadas - atualizar para AWSMigrationHubStrategyCollector	Atualizou a AWSMigrationHubStrategyCollector política para incluir novas APIs do Amazon S3.	15 de setembro de 2023
AWS atualizações de políticas gerenciadas - atualizar para AWSMigrationHubStrategyCollector	Atualizou a AWSMigrationHubStrategyCollector política para incluir novos analisadores de código-fonte.	8 de março de 2023
Atualizações de práticas recomendadas do IAM	Para obter mais informações, consulte Práticas recomendadas de segurança no IAM.	25 de fevereiro de 2023
AWS atualizações de políticas gerenciadas - atualização de uma política existente	As recomendações de estratégia do Migration Hub adicionaram três AWS Application Discovery Service APIs a uma política existente.	10 de novembro de 2022
Atualizações de segurança	Estabeleça uma conexão privada com a interface de endpoint da VPC.	7 de março de 2022
Novo atributo	Foi adicionado suporte ao repositório DevOps Git do Azure para análise de código-fonte.	28 de janeiro de 2022
Novo atributo	Recomendações do Babelfish adicionadas para bancos de dados SQL.	14 de janeiro de 2022
Lançamento inicial	Versão inicial do Guia do usuário do Migration Hub Strategy Recommendations.	25 de outubro de 2021

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.