



Manual do usuário

AWS Application Discovery Service



AWS Application Discovery Service: 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 desprestige a Amazon. Todas as outras marcas comerciais que não pertencem à Amazon pertencem a seus respectivos proprietários, que podem ou não ser afiliados, patrocinados pela Amazon ou ter conexão com ela.

Table of Contents

O que é o AWS Application Discovery Service?	1
Descoberta de VMware	2
Descoberta de banco	3
Compare o Agentless Collector e o Discovery Agent	3
Pressuposições	4
Configuração	6
Cadastre-se na Amazon Web Services	6
Criar usuários do IAM	6
Criação de um usuário administrativo do IAM	7
Criação de um usuário não administrativo do IAM	7
Faça login no Migration Hub e escolha uma região de origem	8
Agente Discovery	9
Pré-requisitos	10
Instale no Linux	12
Requisitos em plataformas Linux mais antigas	15
Gerencie o processo do Discovery Agent no Linux	16
Desinstalar um agente	17
Solução de problemas do Linux Discovery Ag	18
Instalar o no Windows	19
Assinatura de pacotes e atualizações automáticas	23
Gerencie o processo do Discovery Agent no Windows	23
Solução de problemas no Windows	25
Dados coletados	26
Iniciar ou interromper a coleta de dados	29
Colecionador sem agente	32
Introdução	33
Pré-requisitos	33
Etapa 1: criar um usuário do IAM	36
Etapa 2: baixar o coletor	38
Etapa 3: implantar o coletor	39
Etapa 4: acessar o console do coletor	40
Etapa 5: Configurar o coletor	40
Etapa 6: Configurar módulos de coleta de dados	47
Etapa 7: Visualizar os dados coletados	62

Dados coletados	63
Dados coletados pelo módulo VMware	64
Dados coletados pelo módulo de banco de dados e análise	68
Usar o console	70
Painel do Coletor	70
Editar configurações do coletor	72
Editar credenciais do vCenter	73
Atualizações	74
Solução de problemas	75
Corrigindo que o Agentless Collector não pode ser alcançado durante a configuração AWS	76
Corrigindo problemas de certificação autoassinada ao se conectar ao host proxy	78
Encontrando colecionadores insalubres	78
Corrigindo problemas de endereço IP	79
Corrigindo problemas de credenciais do vCenter	80
Corrigindo problemas de encaminhamento de dados	80
Corrigindo problemas de conexão	81
Suporte autônomo ao host ESX	83
Como entrar em contato com o AWS Support	83
Importar	85
Campos de arquivos de importação compatíveis	86
Configuração de permissões de importação	91
Carregar o arquivo de importação para o Amazon S3	94
Importação de dados	95
Acompanhando suas solicitações de importação Migration Hub	98
Visualize, exporte e explore dados	100
Exibir dados coletados	100
Lógica de combinação	101
A tabela deve estar vazia	102
Exploração de dados no Athena	104
Habilitar a exploração de dados no Amazon Athena	105
Trabalhando com exploração de dados no Amazon Athena	107
Demonstrações do console	117
Painel principal	117
Painel principal	117
Ferramentas de coleta de dados	118

Iniciando e interrompendo coletores de dados	118
Visualização e classificação de coletores de dados	119
Visualize, exporte e explore dados	123
Visualização e classificação de servidores	124
Marcar servidores	125
Exportando dados do servidor	126
Exploração de dados no Athena	127
Aplicações	128
Usando a API para consultar itens descobertos	129
Usando a DescribeConfigurations ação	129
Usando a ListConfigurations ação	133
Consistência eventual	149
Segurança	150
Identity and Access Management	151
Público	151
Autenticação com identidades	152
Gerenciamento do acesso usando políticas	155
Como AWS Application Discovery Service funciona com o IAM	158
AWS políticas gerenciadas	161
Exemplos de políticas baseadas em identidade	166
Understanding and Using Service-Linked Roles (Noções básicas e uso de funções vinculadas ao serviço)	173
Solução de problemas	181
Registrar em log e monitorar no AWS Application Discovery Service	182
Registro de chamadas de API do Application Discovery Service com AWS CloudTrail	182
Cotas	186
Solução de problemas	187
Pare a coleta de dados por meio da exploração de dados	187
Remova os dados coletados pela exploração de dados	188
Corrija problemas comuns com a exploração de dados no Amazon Athena	190
A exploração de dados no Amazon Athena não é iniciada porque as funções vinculadas ao serviço e os recursos necessários AWS não podem ser criados	190
Os dados do novo agente não aparecem no Amazon Athena	190
Você não tem permissões suficientes para acessar o Amazon S3, o Amazon Data Firehose ou AWS Glue	192
Solução de problemas de registros de importação com falha	192

Histórico do documento	195
Glossário do AWS	199
Apêndice	200
.....	200
Apêndice: Discovery Connector	200
Dados coletados pelo Discovery Connector	201
Coleta de dados do conector	205
Solução de problemas do Discovery Connector	206
.....	ccxi

O que é o AWS Application Discovery Service?

AWS Application Discovery Service ajuda você a planejar a migração para a AWS Nuvem coletando dados de configuração e uso sobre seus servidores on-premises. O Application Discovery Service é integrado com o AWS Migration Hub e o AWS Database Migration Service Fleet Advisor. O Migration Hub simplifica o rastreamento da migração, pois agrega suas informações de status de migração em um único console. Você pode visualizar os servidores descobertos, agrupá-los em aplicativos e, em seguida, rastrear o status da migração de cada aplicativo a partir do console do Migration Hub em sua região de origem. Você pode usar o DMS Fleet Advisor para avaliar as opções de migração para cargas de trabalho do banco de dados.

Todos os dados descobertos são armazenados na sua região de origem do AWS Migration Hub. Portanto, você deve definir sua região de origem no console do Migration Hub ou com comandos da CLI antes de realizar qualquer atividade de descoberta e migração. Seus dados podem ser exportados para análise no Microsoft Excel ou em ferramentas de análise de AWS, como Amazon Athena e Amazon QuickSight.

Usando as APIs do Application Discovery Service, você pode exportar os dados de desempenho e utilização do sistema para seus servidores descobertos. Insira esses dados em seu modelo de custo para calcular o custo de execução desses servidores AWS. Além disso, é possível exportar dados sobre as conexões de rede que existem entre servidores. Essas informações ajudam a determinar as dependências de rede entre servidores e a agrupá-las em aplicativos para planejar a migração.

Note

Sua região de origem deve ser configurada no AWS Migration Hub antes de você iniciar o processo de descoberta, pois seus dados serão armazenados em sua região de origem. Para obter mais informações sobre como trabalhar com uma região de origem, consulte [Região de origem](#).

O Application Discovery Service oferece duas maneiras de realizar a descoberta e coletar dados sobre seus servidores locais:

- A descoberta sem agente pode ser realizada implantando o Application Discovery Service Agentless Collector (Agentless Collector) (arquivo OVA) por meio do VMware vCenter. Depois que o Agentless Collector é configurado, ele identifica máquinas virtuais (VMs) e hosts associados ao vCenter. O Agentless Collector coleta os seguintes dados de configuração estática: nomes

de host do servidor, endereços IP, endereços MAC, alocações de recursos de disco, versões do mecanismo de banco de dados e esquemas de banco de dados. Além disso, ele coleta os dados de utilização de cada VM e banco de dados, fornecendo a utilização média e máxima de métricas como CPU, RAM e E/S de disco.

- A descoberta baseada em agente pode ser realizada implantando o AWS Application Discovery Agent em cada uma de suas VMs e servidores físicos. O instalador do agente está disponível para os sistemas operacionais Windows e Linux. Ela coleta dados de configuração estáticos, informações detalhadas de séries temporais sobre o desempenho do sistema, conexões de rede de entrada e de saída e processos em execução.

O Application Discovery Service se integra às soluções de descoberta de aplicativos dos parceiros da AWS Partner Network (APN). Essas soluções de terceiros podem ajudá-lo a importar detalhes sobre seu ambiente local diretamente para o Migration Hub, sem usar nenhum coletor ou agente de descoberta sem agente. Ferramentas de descoberta de aplicativos de terceiros podem consultar o AWS Application Discovery Service e gravar no banco de dados do Application Discovery Service usando a API pública. Dessa forma, é possível importar dados para o Migration Hub e visualizá-los, para poder associar aplicativos a servidores e rastrear migrações.

Descoberta de VMware

Se você tiver máquinas virtuais (VMs) em execução no ambiente VMware vCenter, poderá usar o Agentless Collector para coletar informações do sistema sem precisar instalar um agente em cada VM. Em vez disso, você carrega esse dispositivo local para o vCenter e permite que ele descubra todos os hosts e VMs.

O Agentless Collector captura as informações de desempenho do sistema e a utilização de recursos para cada VM em execução no vCenter, independentemente do sistema operacional em uso. No entanto, ele não pode analisar cada VM "por dentro" e, portanto, não pode descobrir quais processos estão em execução em cada VM nem quais são as conexões de rede existentes. Portanto, se você precisar desse nível de detalhe e quiser examinar mais de perto algumas de suas VMs existentes para ajudar no planejamento de sua migração, você pode instalar o Discovery Agent conforme necessário.

Além disso, para VMs hospedadas no VMware, você pode usar o Agentless Collector e o Discovery Agent para realizar a descoberta simultaneamente. Para obter detalhes sobre quais tipos exatos de dados cada ferramenta de descoberta coletará, consulte [Dados coletados pelo Agentless Collector](#) e [Dados coletados pelo Discovery Agent](#).

Descoberta de banco

Se você tiver servidores de banco de dados e análise em seu ambiente local, poderá usar o Agentless Collector para descobrir e inventariar esses servidores. Em seguida, você pode coletar métricas de desempenho para cada servidor de banco de dados sem a necessidade de instalar o Agentless Collector em cada computador do seu ambiente.

O módulo de coleta de dados analíticos e de banco de dados do Agentless Collector captura metadados e métricas de desempenho que fornecem informações sobre sua infraestrutura de dados. O módulo de coleta de dados de banco de dados e análise usa o LDAP no Microsoft Active Directory para coletar informações sobre o sistema operacional, o banco de dados e os servidores de análise em sua rede. Em seguida, o módulo de coleta de dados executa periodicamente consultas para coletar métricas reais de utilização da CPU, memória e capacidade de disco dos bancos de dados e servidores de análise. Para obter detalhes sobre as métricas coletadas, consulte [Dados coletados pelo módulo de banco de dados e análise](#).

Depois que o Agentless Collector concluir a coleta de dados do seu ambiente, você poderá usar o AWS DMS console para análises adicionais e planejar sua migração. Por exemplo, para escolher um destino de migração ideal no Nuvem AWS, você pode gerar recomendações de destino para seus bancos de dados de origem. Para obter mais informações, consulte [Módulo de coleta de dados de banco de dados e análise](#).

Compare o Agentless Collector e o Discovery Agent

A tabela a seguir fornece uma comparação rápida das ferramentas de coleta de dados do Application Discovery Service.

	Coletor sem agente	Discovery Agent
Supported server types		
Máquina virtual da VMware	Sim	Sim
Servidor físico	Não	Sim
Deployment		
Por servidor	Não	Sim

	Coletor sem agente	Discovery Agent
Por vCenter	Sim	Não
Collected data		
Dados de configuração do servidor estático	Yes	Yes
Dados de configuração do banco	Yes	No
Métricas de utilização da VM	Yes	No
Métricas de utilização do banco de dados	Yes	No
Informações de séries temporais sobre desempenho	No	Yes (Export only)
Conexões de rede de entrada/saída	No	Yes (Export only)
Processos em execução	No	Yes (Export only)
SO com suporte	Any OS running in VMware vCenter V5.5+	Para obter a lista de sistemas operacionais Linux e Windows compatíveis, consulte Pré-requisitos para o Discovery Agent .
Bancos de dados compatíveis	Oracle, SQL Server, MySQL, and PostgreSQL	Nenhum

Pressuposições

Para usar o Application Discovery Service, presume-se o seguinte:

- Você se inscreveu para AWS. Para obter mais informações, consulte [Configurando o Application Discovery Service](#).

- Você selecionou uma região de origem do Migration Hub. Para obter mais informações, consulte [a documentação sobre as regiões on-premises](#).

Veja o que esperar:

- A região de origem do Migration Hub é a única região em que o Application Discovery Service armazena seus dados de descoberta e planejamento.
- Agentes, conectores e importações de descoberta podem ser usados somente na região de origem selecionada do Migration Hub.
- Para obter uma lista das AWS regiões em que você pode usar o Application Discovery Service, consulte [Referência geral da Amazon Web Services](#).

Configurando o Application Discovery Service

Antes de usar AWS Application Discovery Service pela primeira vez, conclua as seguintes tarefas:

[Cadastre-se na Amazon Web Services](#)

[Criar usuários do IAM](#)

[Faça login no console do Migration Hub e escolha uma região de origem](#)

Cadastre-se na Amazon Web Services

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 prática recomendada de segurança, atribua acesso administrativo a um usuário e use somente o usuário raiz para realizar [tarefas que exijam acesso do usuário raiz](#).

Criar usuários do IAM

Ao criar uma AWS conta, você obtém uma identidade de login única que tem acesso completo a todos os AWS serviços e recursos da conta. Essa identidade é chamada de usuário raiz da AWS conta. Fazer login AWS Management Console usando o endereço de e-mail e a senha que você usou para criar a conta oferece acesso completo a todos os AWS recursos da sua conta.

É altamente recomendável que você não use o usuário raiz para tarefas diárias, nem mesmo as administrativas. Em vez disso, siga a prática recomendada de segurança [Criar usuários individuais do IAM](#) e crie um usuário administrador AWS Identity and Access Management (IAM). Depois, guarde as credenciais do usuário raiz em um lugar seguro e utilize-as para executar somente algumas tarefas de gerenciamento de contas e serviços.

Além de criar um usuário administrativo, você também precisará criar usuários não administrativos do IAM. Os tópicos a seguir explicam como criar os dois tipos de usuários do IAM.

Tópicos

- [Criação de um usuário administrativo do IAM](#)
- [Criação de um usuário não administrativo do IAM](#)

Criação de um usuário administrativo do IAM

Por padrão, uma conta de administrador herda todas as políticas necessárias para acessar o Application Discovery Service.

Para criar um usuário administrador

- Crie um usuário administrador em sua AWS conta. Para obter instruções, consulte [Criar seu primeiro grupo de administradores e usuário do IAM](#) no Guia do usuário do IAM.

Criação de um usuário não administrativo do IAM

Ao criar usuários não administrativos do IAM, siga a prática recomendada de segurança [Grant Least Privilege, concedendo permissões mínimas](#) aos usuários.

Use políticas gerenciadas do IAM para definir o nível de acesso ao Application Discovery Service por usuários não administrativos do IAM. Para obter informações sobre as políticas gerenciadas do Application Discovery Service, consulte [AWS políticas gerenciadas para AWS Application Discovery Service](#).

Para criar um usuário do IAM não administrador

1. Em AWS Management Console, navegue até o console do IAM.
2. Crie um usuário do IAM não administrador seguindo as instruções para criar um usuário com o console, conforme descrito em Como [criar um usuário do IAM em sua AWS conta](#) no Guia do usuário do IAM.

Ao seguir as instruções no Guia do usuário do IAM:

- Quando estiver na etapa de seleção do tipo de acesso, selecione Acesso programático. Observe que, embora não seja recomendado, selecione o acesso ao AWS Management

Console somente se você planeja usar as mesmas credenciais de usuário do IAM para acessar o AWS console.

- Na etapa sobre a página Definir permissão, escolha a opção Anexar políticas existentes diretamente ao usuário. Em seguida, selecione uma política gerenciada do IAM para o Application Discovery Service na lista de políticas. Para obter informações sobre as políticas gerenciadas do Application Discovery Service, consulte [AWS políticas gerenciadas para AWS Application Discovery Service](#).
- Quando estiver na etapa de visualização das chaves de acesso do usuário (IDs da chave de acesso e chaves de acesso secretas), siga as orientações na Nota importante sobre como salvar a nova ID da chave de acesso e a chave de acesso secreta do usuário em um local seguro e protegido.

Faça login no console do Migration Hub e escolha uma região de origem

Você precisa escolher uma região de AWS Migration Hub origem na AWS conta que está usando para AWS Application Discovery Service o.

Para escolher a região de origem

1. Usando sua AWS conta, faça login 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 Configurações e escolha uma região de origem.

Seus dados do Migration Hub são armazenados em sua região de origem para fins de descoberta, planejamento e rastreamento de migração. Para obter mais informações, consulte [The Migration Hub Home Region](#).

AWS Agente de descoberta de aplicativos

O AWS Application Discovery Agent (Discovery Agent) é um software que você instala em servidores e VMs locais destinados à descoberta e migração. Os agentes coletam informações sobre configuração do sistema, o desempenho do sistema, os processos em execução e detalhes das conexões de rede entre sistemas. Os agentes oferecem suporte à maioria dos sistemas operacionais Linux e Windows, e você pode implantá-los em servidores físicos locais, instâncias do Amazon EC2 e máquinas virtuais.

Note

Antes de implantar o Discovery Agent, você deve escolher uma [região de origem do Migration Hub](#). Registre seu agente em sua região de origem.

O Discovery Agent é executado em seu ambiente local e requer privilégios de root. Quando você inicia o Discovery Agent, ele se conecta com segurança à sua região de origem e se registra no Application Discovery Service.

- Por exemplo, se `eu-central-1` for sua região de origem, ela se registra no `arsenal-discovery.eu-central-1.amazonaws.com` no Application Discovery Service.
- Ou substitua sua região de origem conforme necessário para todas as outras regiões, exceto `us-west-2`.
- Se `us-west-2` for sua região de origem, ela se registra no `arsenal.us-west-2.amazonaws.com` no Application Discovery Service.

Como funciona

Após o registro, o agente começa a coletar dados para o host ou a VM em que reside. O agente envia um ping ao Application Discovery Service em intervalos de 15 minutos para obter informações de configuração.

Os dados coletados incluem especificações do sistema, utilização de séries temporais ou dados de desempenho, conexões de rede e dados de processamento. Você pode usar essas informações para mapear os ativos da TI e as dependências de rede. Todos esses pontos de dados podem ajudá-lo a determinar o custo de execução desses servidores AWS e também a planejar a migração.

Os dados são transmitidos com segurança pelos Discovery Agents para o Application Discovery Service usando a criptografia TLS (Transport Layer Security). Os agentes estão configurados para atualizar automaticamente quando as novas versões se tornam disponíveis. Se você desejar, é possível alterar essa definição de configuração.

Tip

Antes de baixar e iniciar a instalação do Discovery Agent, certifique-se de ler todos os pré-requisitos exigidos em [Pré-requisitos para o Discovery Agent](#)

Tópicos

- [Pré-requisitos para o Discovery Agent](#)
- [Instale o Discovery Agent no Linux](#)
- [Instalar o no Windows](#)
- [Dados coletados pelo Discovery Agent](#)
- [Iniciar ou interromper a coleta de dados do Discovery Agent](#)

Pré-requisitos para o Discovery Agent

A seguir estão os pré-requisitos e as tarefas que você deve executar antes de instalar com êxito o AWS Application Discovery Agent (Discovery Agent).

- Você deve definir uma [região de AWS Migration Hub origem](#) antes de começar a instalar o Discovery Agent.
- Se você tiver uma versão 1.x do agente instalado, ela deve ser removida antes da instalação da versão mais recente.
- Se o host no qual o agente está sendo instalado executa Linux, verifique se o host suporta pelo menos a arquitetura de CPU Intel i686 (também conhecida como microarquitetura P6).
- 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 2003 R2 SP2

Windows Server 2008 R1 SP2, 2008 R2 SP1

Windows Server 2012 R1, 2012 R2

Windows Server 2016

Windows Server 2019

Windows Server 2022

- Se as conexões de saída da sua rede forem restritas, será necessário atualizar as configurações do firewall. Os agentes requerem acesso ao `arsenal` pela porta TCP 443. Eles não requerem que nenhuma porta de entrada esteja aberta.

Por exemplo, se a sua região de origem for `eu-central-1`, você usará `https://arsenal-discovery.eu-central-1.amazonaws.com:443`

- O acesso ao Amazon S3 em sua região de origem é necessário para que o upgrade automático funcione.
- Crie um usuário AWS Identity and Access Management (IAM) no console e anexe a política gerenciada existente `AWSApplicationDiscoveryAgentAccess` do IAM. Essa política permite que o usuário execute as ações necessárias do agente em seu nome. Para obter mais informações sobre políticas gerenciadas, consulte [AWS políticas gerenciadas para AWS Application Discovery Service](#).
- Verifique o tempo de distorção dos servidores Network Time Protocol (NTP) e o corrija se necessário. A sincronização de hora incorreta faz com que a chamada de registro do agente falhe.

Note

O Discovery Agent tem um agente executável de 32 bits, que funciona em sistemas operacionais de 32 e 64 bits. O número de pacotes de instalação necessários para a implantação é reduzido ao ter um único agente executável. Esse agente executável funciona para SO Linux e Windows. Isso é abordado nas respectivas seções de instalação que se seguem.

Instale o Discovery Agent no Linux

Execute o procedimento a seguir no Linux. Certifique-se de que sua [região de origem do Migration Hub](#) tenha sido definida antes de iniciar esse procedimento.

Note

Se você estiver usando uma versão desatualizada do Linux, consulte [Requisitos em plataformas Linux mais antigas](#).

Para instalar o AWS Application Discovery Agent em seu data center

1. Faça login em seu servidor ou VM baseado em Linux e crie um novo diretório para conter os componentes do seu agente.
2. Alterne para o novo diretório e faça download do script de instalação na linha de comando ou no console.
 - a. Para fazer download na linha de comando, execute o comando a seguir:

```
curl -o ./aws-discovery-agent.tar.gz https://s3-us-west-2.amazonaws.com/aws-discovery-agent.us-west-2/linux/latest/aws-discovery-agent.tar.gz
```

- b. Para fazer o download do console do Migration Hub, faça o seguinte:
 - i. Abra o console e vá para a página [Discovery Tools \(Ferramentas de descoberta\)](#).
 - ii. Na caixa Discovery Agent (Agente de descoberta), selecione Download agent (Fazer download do agente) e, em seguida, Linux na caixa de listagem exibida. O download começará imediatamente.
3. Verifique a assinatura de criptografia do pacote de instalação com estes três comandos:

```
curl -o ./agent.sig https://s3.us-west-2.amazonaws.com/aws-discovery-agent.us-west-2/linux/latest/aws-discovery-agent.tar.gz.sig
```

```
curl -o ./discovery.gpg https://s3.us-west-2.amazonaws.com/aws-discovery-agent.us-west-2/linux/latest/discovery.gpg
```

```
gpg --no-default-keyring --keyring ./discovery.gpg --verify agent.sig aws-
discovery-agent.tar.gz
```

A impressão digital da chave pública do agente (discovery.gpg) é 7638 F24C 6717 F97C 4F1B 3BC0 5133 255E 4DF4 2DA2.

4. Extraia do tarball como exibido abaixo.

```
tar -xzf aws-discovery-agent.tar.gz
```

5. Para instalar o agente, escolha um dos seguintes métodos de instalação.

Para...	Fazer isso...
Instale Discovery Agent	<p>Para instalar o agente, execute o comando <code>agent install</code> conforme mostrado no exemplo a seguir. No exemplo, <i>your-home-region</i> substitua pelo nome da sua região de origem, <i>aws-access-key-id</i> pelo ID da chave de acesso e <i>aws-secret-access-key</i> pela chave de acesso secreta.</p> <pre>sudo bash install -r <i>your-home-region</i> -k <i>aws-access-key-id</i> -s <i>aws-secret-access-key</i></pre> <p>Por padrão, os agentes baixam e aplicam automaticamente as atualizações à medida que elas se tornam disponíveis.</p> <p>Recomendamos o uso desta configuração padrão.</p> <p>No entanto, se você não quiser que os agentes baixem e apliquem atualizações automaticamente, inclua o <code>-u false</code></p>

Para...	Fazer isso...
<p>(Opcional) Instale o Discovery Agent e configure um proxy não transparente</p>	<p>parâmetro ao executar o comando de instalação do agente.</p> <p>Para configurar um proxy não transparente, adicione os seguintes parâmetros ao comando de instalação do agente:</p> <ul style="list-style-type: none"> • -e A senha do proxy. • -f O número da porta do proxy. • -g O esquema de proxy. • -i O nome de usuário do proxy. <p>Veja a seguir um exemplo do comando <code>agent install</code> usando os parâmetros de proxy não transparentes.</p> <pre data-bbox="862 968 1507 1241"> sudo bash install -r <i>your-home-region</i> -k <i>aws-access-key-id</i> -s <i>aws-secret-access-key</i> -d <i>myproxy.mycompany.com</i> -e <i>mypassword</i> -f <i>proxy-port-number</i> -g https -i <i>myusername</i> </pre> <p>Se seu proxy não exigir autenticação, omita <code>-i</code> os parâmetros <code>-e</code> e <code>-i</code>.</p> <p>O exemplo de comando <code>install</code> usa <code>https</code>, se seu proxy usa HTTP, especifique <code>http</code> o valor do <code>-g</code> parâmetro.</p>

6. Se as conexões de saída da sua rede forem restritas, será necessário atualizar as configurações do firewall. Os agentes requerem acesso ao `arsenal` pela porta TCP 443. Eles não requerem que nenhuma porta de entrada esteja aberta.

Por exemplo, se a sua região de origem for `eu-central-1`, você usará `https://arsenal-discovery.eu-central-1.amazonaws.com:443`

Tópicos

- [Requisitos em plataformas Linux mais antigas](#)
- [Gerencie o processo do Discovery Agent no Linux](#)
- [Desinstale o Discovery Agent no Linux](#)
- [Solução de problemas do Linux Discovery Ag](#)

Requisitos em plataformas Linux mais antigas

Algumas plataformas Linux mais antigas, como SUSE 10, CentOS 5 e RHEL 5, estão no fim da vida útil ou são apenas minimamente compatíveis. Essas plataformas podem sofrer com pacotes de out-of-date criptografia que impedem que o script de atualização do agente baixe os pacotes de instalação.

Curl

O agente do Application Discovery exige `curl` comunicações seguras com o AWS servidor. Algumas versões antigas de `curl` não conseguem se comunicar com segurança com um serviço moderno da web.

Para usar a versão do `curl` incluída no Application Discovery Agent para todas as operações, execute o script de instalação com o parâmetro `-c true`.

Pacote de autoridade de certificação

Os sistemas Linux mais antigos podem ter um pacote de Autoridade out-of-date Certificadora (CA), que é essencial para proteger a comunicação pela Internet.

Para usar o pacote CA incluído no Application Discovery Agent para todas as operações, execute o script de instalação com o parâmetro `-b true`.

Essas opções de script de instalação podem ser usadas juntas. No exemplo de comando a seguir, os dois parâmetros do script são passados para o script de instalação:

```
sudo bash install -r your-home_region -k aws-access-key-id -s aws-secret-access-key -c true -b true
```

Gerencie o processo do Discovery Agent no Linux

Você pode gerenciar o comportamento do Discovery Agent no nível do sistema usando as System V `init` ferramentas `systemd` `Upstart`, ou. As seguintes guias descrevem os comandos para as tarefas compatíveis em cada uma das respectivas ferramentas.

systemd

Comandos de gerenciamento para o Application Discovery Agent

Tarefa	Command
Verifique que o agente está sendo executado	<code>sudo systemctl status aws-discovery-daemon.service</code>
Iniciar um agente	<code>sudo systemctl start aws-discovery-daemon.service</code>
Interromper um agente	<code>sudo systemctl stop aws-discovery-daemon.service</code>
Reiniciar um agente	<code>sudo systemctl restart aws-discovery-daemon.service</code>

Upstart

Comandos de gerenciamento para o Application Discovery Agent

Tarefa	Command
Verifique que o agente está sendo executado	<code>sudo initctl status aws-discovery-daemon</code>
Iniciar um agente	<code>sudo initctl start aws-discovery-daemon</code>
Interromper um agente	<code>sudo initctl stop aws-discovery-daemon</code>
Reiniciar um agente	<code>sudo initctl restart aws-discovery-daemon</code>

System V init

Comandos de gerenciamento para o Application Discovery Agent

Tarefa	Command
Verifique que o agente está sendo executado	<code>sudo /etc/init.d/aws-discovery-daemon status</code>
Iniciar um agente	<code>sudo /etc/init.d/aws-discovery-daemon start</code>
Interromper um agente	<code>sudo /etc/init.d/aws-discovery-daemon stop</code>
Reiniciar um agente	<code>sudo /etc/init.d/aws-discovery-daemon restart</code>

Desinstale o Discovery Agent no Linux

Esta seção descreve como desinstalar o Discovery Agent no Linux.

Para desinstalar um agente se você estiver usando o gerenciador de pacotes yum

- Use o comando a seguir para desinstalar um agente se estiver usando o yum.

```
rpm -e --nodeps aws-discovery-agent
```

Para desinstalar um agente se você estiver usando o gerenciador de pacotes apt-get

- Use o comando a seguir para desinstalar um agente se estiver usando o apt-get.

```
apt-get remove aws-discovery-agent:i386
```

Para desinstalar um agente se você estiver usando o gerenciador de pacotes zypper

- Use o comando a seguir para desinstalar um agente se estiver usando o zypper.

```
zypper remove aws-discovery-agent
```

Solução de problemas do Linux Discovery Ag

Se você encontrar problemas ao instalar ou usar o Discovery Agent no Linux, consulte as orientações a seguir sobre registro e configuração. Ao ajudar a solucionar possíveis problemas com o agente ou sua conexão com o Application Discovery Service, o AWS Support geralmente solicita esses arquivos.

- Arquivos de log

Os arquivos de log do Discovery Agent estão localizados no seguinte diretório.

```
/var/log/aws/discovery/
```

Os arquivos de log são nomeados para indicar se são gerados pelo daemon principal, pelo atualizador automático ou pelo instalador.

- Arquivos de configuração

Os arquivos de configuração do Discovery Agent versão 2.0.1617.0 ou mais recente estão localizados no diretório a seguir.

```
/etc/opt/aws/discovery/
```

Os arquivos de configuração das versões do Discovery Agent anteriores à 2.0.1617.0 estão localizados no diretório a seguir.

```
/var/opt/aws/discovery/
```

- Para obter instruções sobre como remover versões mais antigas do Discovery Agent, consulte [Pré-requisitos para o Discovery Agent](#).

Instalar o no Windows

Conclua o procedimento a seguir para instalar um agente no Windows. Certifique-se de que sua [região de origem do Migration Hub](#) tenha sido definida antes de iniciar esse procedimento.

Para instalar o AWS Application Discovery Agent em seu data center

1. Baixe o [instalador do agente do Windows](#), mas não clique duas vezes para executar o instalador no Windows.

Important


Não clique duas vezes para executar o instalador no Windows, pois ele falhará na instalação. A instalação do agente funciona apenas a partir do prompt de comando. (Se você já clicou duas vezes no instalador, acesse Adicionar ou remover programas e desinstale o agente antes de continuar com as demais etapas de instalação.)

Se o instalador do agente do Windows não detectar nenhuma versão do tempo de execução do Visual C++ x86 no host, ele instalará automaticamente o tempo de execução do Visual C++ x86 2015—2019 antes de instalar o software do agente.

2. Abra o prompt de comando como um administrador e navegue até o local no qual você salvou o pacote instalação.
3. Para instalar o agente, escolha um dos seguintes métodos de instalação.

Para...	Fazer isso...
Instale Discovery Agent	<p>Para instalar o agente, execute o comando <code>agent install</code> conforme mostrado no exemplo a seguir. No exemplo, <i>your-home-region</i> substitua pelo nome da sua região de origem, <i>aws-access-key-id</i> pelo ID da chave de acesso e <i>aws-secret-access-key</i> pela chave de acesso secreta.</p> <p>Opcionalmente, você pode definir o local de instalação do agente especificando o caminho da pasta <i>C:\install-location</i> para o parâmetro <code>INSTALLLOCATION</code>.</p>

Para...	Fazer isso...
	<p>Por exemplo, <code>INSTALLLOCATION=" C:\install-location "</code>. A hierarquia de pastas resultante será [caminho <code>INSTALLLOCATION</code>]\AWS Discovery. Por padrão, o local de instalação é a Program Files pasta.</p> <p>Opcionalmente, você pode usar <code>LOGANDCONFIGLOCATION</code> para substituir o diretório padrão (ProgramData) da pasta de registros do agente e do arquivo de configuração. A hierarquia de pastas resultante é [<code>LOGANDCONFIGLOCATION path</code>]\AWS Discovery .</p> <pre data-bbox="862 888 1507 1129">.\AWSDiscoveryAgentInstaller.exe REGION=" your-home-region " KEY_ID="aws-access-key-id " KEY_SECRET=" aws-secret-access-key " /quiet</pre> <p>Por padrão, os agentes baixam e aplicam automaticamente as atualizações à medida que elas se tornam disponíveis.</p> <p>Recomendamos o uso desta configuração padrão.</p> <p>No entanto, se você não quiser que os agentes baixem e apliquem atualizações automaticamente, inclua o seguinte parâmetro ao executar o comando de instalação do agente: <code>AUTO_UPDATE=false</code></p>

Para...	Fazer isso...
	<div data-bbox="862 212 1507 520" style="border: 1px solid #f08080; border-radius: 10px; padding: 10px;"><p> Warning</p><p>A desativação das atualizações automáticas impede que os patches de segurança mais recentes sejam instalados.</p></div>

Para...	Fazer isso...
(Opcional) Instale o Discovery Agent e configure um proxy não transparente	<p>Para configurar um proxy não transparente, adicione as seguintes propriedades públicas ao comando de instalação do agente:</p> <ul style="list-style-type: none">• PROXY_HOST — O nome do host proxy• PROXY_SCHEME — O esquema de proxy• PROXY_PORT — O número da porta proxy• PROXY_USER — O nome de usuário do proxy• PROXY_PASSWORD — A senha do usuário proxy <p>Veja a seguir um exemplo do comando <code>agent install</code> usando as propriedades de proxy não transparentes.</p> <pre data-bbox="862 1052 1507 1451">.\AWSDiscoveryAgentInstall.exe REGION=" <i>your-home-region</i> " KEY_ID=" <i>aws-access-key-id</i> " KEY_SECRET=" <i>aws-secret-access-key</i> " PROXY_HOST=" <i>myproxy.mycompany.com</i> " PROXY_SCHEME="http s" PROXY_PORT=" <i>proxy-port-number</i> " PROXY_USER=" <i>myusername</i> " PROXY_PASSWORD=" <i>mypassword</i> " /quiet</pre> <p>Se seu proxy não exigir autenticação, omita as <code>PROXY_PASSWORD</code> e <code>PROXY_USER</code> propriedades. O exemplo de comando <code>install</code> usa <code>https</code>. Se seu proxy usa HTTP, especifique o <code>PROXY_SCHEME</code> valor.</p>

4. Se as conexões de saída da sua rede forem restritas, você deverá atualizar as configurações do firewall. Os agentes requerem acesso ao `arsenal` pela porta TCP 443. Eles não requerem que nenhuma porta de entrada esteja aberta.

Por exemplo, se sua região de origem foreu `eu-central-1`, você usaria o seguinte: `https://arsenal-discovery.eu-central-1.amazonaws.com:443`

Assinatura de pacotes e atualizações automáticas

Para o Windows Server 2008 e versões posteriores, a Amazon assina criptograficamente o pacote de instalação do agente do Application Discovery Service com um certificado SHA256. Para atualizações automáticas assinadas por SHA2 no Windows Server 2008 SP2, certifique-se de que os hosts tenham um hotfix instalado para oferecer suporte à autenticação de assinatura SHA2. O [hotfix](#) de suporte mais recente da Microsoft ajuda a oferecer suporte à autenticação SHA2 no Windows Server 2008 SP2.

Note

Os hotfixes para suporte a SHA256 para o Windows 2003 não estão mais disponíveis publicamente na Microsoft. Se essas correções ainda não estiverem instaladas em seu host Windows 2003, atualizações manuais serão necessárias.

Para realizar atualizações manualmente

1. Baixe o [Windows Agent Updater](#).
2. Abra o prompt de comando como administrador.
3. Navegue até o local em que o atualizador foi salvo.
4. Execute o seguinte comando .

```
AWSDiscoveryAgentUpdater.exe /Q
```

Gerencie o processo do Discovery Agent no Windows

Você pode gerenciar o comportamento do Discovery Agent no nível do sistema por meio do console do Windows Server Manager Services. A tabela a seguir fornece orientações.

Tarefa	Nome do serviço	Status dos serviços/ação
Verifique que o agente está sendo executado	AWS Agente Discovery	Started
	AWS Atualizador Discovery	
Iniciar um agente	AWS Agente Discovery	Escolha Iniciar
	AWS Atualizador Discovery	
Interromper um agente	AWS Agente Discovery	Escolha Stop
	AWS Atualizador Discovery	
Reiniciar um agente	AWS Agente Discovery	Selecione Reiniciar.
	AWS Atualizador Discovery	

Para desinstalar um agente de descoberta no Windows

1. Abra o Painel de Controle no Windows.
2. Clique em Programas.
3. Selecione Programas e Recursos.
4. Selecione AWS Discovery Agent.
5. Clique em Desinstalar.

Note

Se você optar por reinstalar o agente depois de desinstalá-lo, execute o comando a seguir com as opções `/repair` e `/norestart`

```
.\AWSDiscoveryAgentInstaller.exe REGION="your-home-region" KEY_ID="aws-access-key-id" KEY_SECRET="aws-secret-access-key" /quiet /repair /norestart
```

Para desinstalar um agente de descoberta no Windows usando a linha de comando

1. Clique com o botão direito em Iniciar.
2. Escolha o prompt de comando.
3. Use o comando a seguir para desinstalar um agente de descoberta no Windows.

```
wmic product where name='AWS Discovery Agent' call uninstall
```

Solução de problemas do Discovery Agent no Windows

Se você encontrar problemas ao instalar ou usar o AWS Application Discovery Agent no Windows, consulte as orientações a seguir sobre registro e configuração. AWS Support geralmente solicita esses arquivos ao ajudar a solucionar possíveis problemas com o agente ou sua conexão com o Application Discovery Service.

- Registro da instalação

Em alguns casos, o comando de instalação do agente parece falhar. Por exemplo, uma falha pode ocorrer com o Windows Services Manager informando que os serviços de descoberta não estão sendo criados. Nesse caso, adicione `/log install.log` ao comando para gerar um log de instalação detalhado.

- Registro operacional

No Windows Server 2008 e posterior, os arquivos de log do agente podem ser encontrados neste diretório:

```
C:\ProgramData\AWS\AWS Discovery\Logs
```

No Windows Server 2003, os arquivos de log do agente podem ser encontrados neste diretório:

```
C:\Documents and Settings\All Users\Application Data\AWS\AWS Discovery\Logs
```

Os arquivos de log são nomeados para indicar se são gerados pelo serviço principal, pelas atualizações automáticas ou pelo instalador.

- Arquivo de configuração

No Windows Server 2008 e posterior, o arquivo de configuração do agente pode ser encontrado neste local:

```
C:\ProgramData\AWS\AWS Discovery\config
```

No Windows Server 2003, o arquivo de configuração do agente pode ser encontrado neste local:

```
C:\Documents and Settings\All Users\Application Data\AWS\AWS Discovery\config
```

- Para obter instruções sobre como remover versões anteriores do Discovery Agent, consulte [Pré-requisitos para o Discovery Agent](#).

Dados coletados pelo Discovery Agent

AWS O Application Discovery Agent (Discovery Agent) é um software que você instala em servidores e VMs locais. O Discovery Agent coleta dados de configuração do sistema, dados de desempenho ou utilização de séries temporais, dados de processo e conexões de rede TCP (Transmission Control Protocol). Esta seção descreve os dados coletados.

Legenda da tabela dos dados coletados do Discovery Agent:

- O termo host refere-se a um servidor físico ou uma VM.
- Os dados coletados estão em Kilobytes (KB), a menos que especificado de outra forma.
- Dados equivalentes no console do Migration Hub são reportados em megabytes (MB).
- O período de votação ocorre em intervalos de aproximadamente 15 segundos e é enviado a AWS cada 15 minutos.
- Os campos de dados indicados com um asterisco (*) só estão disponíveis nos .csv arquivos produzidos pela função de exportação da API do agente.

Campo de dados	Descrição
agentAssignedProcessIdentificação *	ID dos processos descobertos pelo agente
agentId	ID exclusivo do agente

Campo de dados	Descrição
agentProvidedTime ^{Carimbo *}	Data e hora da observação do agente (mm/dd/aaaa hh:mm:ss am/pm)
cmdLine [*]	Processo inserido na linha de comando
cpuType	Tipo de CPU (unidade de processamento central) usada no host
destinationIp [*]	Endereço IP do dispositivo para o qual o pacote está sendo enviado
destinationPort [*]	O número da porta para a qual os dados/a solicitação estão sendo enviados
family [*]	Protocolo da família de roteamento
freeRAM (MB)	RAM livre e RAM armazenado em cache que podem ser disponibilizados imediatamente para aplicativos, medidos em MB
gateway [*]	Endereço de rede do nó
hostName	Nome do host no qual os dados foram coletados
hypervisor	Tipo de hypervisor
ipAddress	Endereço IP do host
ipVersion [*]	Número da versão do IP
isSystem [*]	Atributo booleano para indicar se um processo é de propriedade do SO
macAddress	Endereço MAC do host
name [*]	Nome do host, da rede, das métricas, etc., os dados estão sendo coletados para

Campo de dados	Descrição
netMask [*]	Prefixo do Endereço IP ao qual um host de rede pertence
osName	Nome do sistema operacional no host
osVersion	Versão do sistema operacional no host
caminho	Caminho do comando originado na linha de comando
sourceIp [*]	Endereço IP do dispositivo que está enviando o pacote IP
sourcePort [*]	Número da porta a partir da qual a solicitação/ os dados foram gerados
timestamp [*]	Data e hora do atributo relatado registrados pelo agente
totalCpuUsagePct	Porcentagem de uso da CPU no host durante o período de sondagem
totalDiskBytesReadPerSecond (Kbps)	Total de kilobits lidos por segundo em todos os discos
totalDiskBytesWrittenPerSecond (Kbps)	Total de kilobits gravados por segundo em todos os discos
totalDiskFreeTamanho (GB)	Espaço livre no disco em GB
totalDiskReadOpsPerSecond	Total de operações de E/S de leitura por segundo
totalDiskSize (GB)	Capacidade total do disco em GB
totalDiskWriteOpsPerSecond	Total de operações de E/S de gravação por segundo

Campo de dados	Descrição
totalNetworkBytesReadPerSecond (Kbps)	Total de throughput de bytes lidos por segundo
totalNetworkBytesWrittenPerSecond (Kbps)	Total da taxa de transferência de bytes gravados por segundo
totalNumCores	Total de unidades de processamento independente dentro da CPU
totalNumCpus	Total de unidades de processamento central
totalNumDisks	O número de discos rígidos físicos em um host
totalNumLogicalProcessadores *	Total de núcleos físicos vezes o número de threads que podem ser executados em cada núcleo
totalNumNetworkCartões	Total de cartões de rede no servidor
totalRAM (MB)	Total de RAM disponível no host
transportProtocol *	Tipo de protocolo de transporte usado

Iniciar ou interromper a coleta de dados do Discovery Agent

Depois que o Discovery Agent for implantado e configurado, se as coletas de dados pararem, você poderá reiniciá-lo. Você pode iniciar ou interromper a coleta de dados por meio do console ou fazendo chamadas de API por meio do AWS CLI. Ambos os métodos são descritos nos procedimentos a seguir.

Using the Migration Hub console

O procedimento a seguir mostra como iniciar ou interromper o processo de coleta de dados do Discovery Agent, na página Coletores de Dados do console do Migration Hub.

Para iniciar ou interromper a coleta de dados

1. No painel de navegação, selecione Data Collectors (Coletores de dados).

2. Clique na guia Agents (Agentes).
3. Marque a caixa de seleção do agente que você deseja iniciar ou interromper.

 Tip

Se você instalou vários agentes, mas só deseja iniciar ou interromper a coleta de dados em determinados hosts, a coluna Nome do host na linha do agente identifica o host no qual o agente está instalado.

4. Selecione Start data collection (Iniciar coleta de dados) ou Stop data collection (Interromper coleta de dados).

Using the AWS CLI

Para iniciar ou interromper o processo de coleta de dados do Discovery Agent a partir do AWS CLI, você deve primeiro instalar o AWS CLI em seu ambiente e, em seguida, definir a CLI para usar a região [inicial do Migration Hub](#) selecionada.

Para instalar AWS CLI e iniciar ou interromper a coleta de dados

1. Se você ainda não fez isso, instale o AWS CLI apropriado para o seu tipo de sistema operacional (Windows ou Mac/Linux). Consulte o [Guia AWS Command Line Interface do usuário](#) para obter instruções.
2. Abra o prompt de comando (Windows) ou o Terminal (MAC/Linux).
 - a. Digite `aws configure` e pressione Enter.
 - b. Insira o ID da chave de AWS acesso e a chave de acesso AWS secreta.
 - c. Insira a região de origem no nome da região padrão, por exemplo, `us-west-2`. (Estamos supondo que `us-west-2` seja a região de origem neste exemplo.)
 - d. Digite `text` no Default Output Format (Formato padrão de saída).
3. Para encontrar a ID do agente para o qual você deseja interromper ou iniciar a coleta de dados, digite o seguinte comando:

```
aws discovery describe-agents
```

4. Para iniciar a coleta de dados pelo agente, digite o seguinte comando:

```
aws discovery start-data-collection-by-agent-ids --agent-ids <agent ID>
```

Para interromper a coleta de dados pelo agente, digite o seguinte comando:

```
aws discovery stop-data-collection-by-agent-ids --agent-ids <agent ID>
```

Coletor sem agente do Application Discovery Service

O Application Discovery Service Agentless Collector (Agentless Collector) é um aplicativo local que coleta informações por meio de métodos sem agente sobre seu ambiente local, incluindo informações do perfil do servidor (por exemplo, sistema operacional, número de CPUs, quantidade de RAM), metadados do banco de dados e métricas de utilização. Você pode instalar o Agentless Collector como uma máquina virtual (VM) em seu ambiente do VMware vCenter Server usando um arquivo de virtualização aberto (OVA).

O Agentless Collector tem uma arquitetura modular, que permite o uso de vários métodos de coleta sem agente. Atualmente, o Agentless Collector oferece suporte a módulos para coleta de dados de VMs VMware e de servidores de banco de dados e análises. Os módulos futuros oferecerão suporte à coleta de conexões de rede, à coleta de plataformas de virtualização adicionais e à coleta em nível de sistema operacional.

O Agentless Collector oferece suporte à coleta de dados para o AWS Application Discovery Service (Application Discovery Service), que ajuda você a planejar sua migração para o Nuvem AWS coletando dados de uso e configuração sobre seus servidores e bancos de dados locais.

O Application Discovery Service é integrado ao AWS Migration Hub, o que simplifica o rastreamento da migração, pois agrega as informações do status da migração em um único console. Você pode visualizar os servidores descobertos, obter recomendações do Amazon EC2, visualizar conexões de rede, agrupar servidores em aplicativos e, em seguida, rastrear o status de migração de cada aplicativo a partir do console do Migration Hub em sua região de origem.

O módulo de coleta de dados analíticos e de banco de dados do Agentless Collector está integrado com AWS Database Migration Service (AWS DMS). Essa integração ajuda a planejar sua migração para Nuvem AWS. Você pode usar o módulo de coleta de dados de banco de dados e análises para descobrir servidores de banco de dados e análise em seu ambiente e criar um inventário dos servidores que você deseja migrar para o Nuvem AWS. Esse módulo de coleta de dados coleta metadados do banco de dados e métricas reais de utilização de CPU, memória e capacidade de disco. Depois de coletar essas métricas, você pode usar o AWS DMS console para gerar recomendações de destino para seus bancos de dados de origem.

Tópicos

- [Introdução ao Agentless Collector](#)
- [Dados coletados pelo Agentless Collector](#)

- [Usando o console Agentless Collector](#)
- [Atualizando manualmente o Agentless Collector](#)
- [Solução de problemas do Agentless Collector](#)

Introdução ao Agentless Collector

Esta seção descreve como começar a usar o Application Discovery Service Agentless Collector (Agentless Collector).

Tópicos

- [Pré-requisitos para o Agentless Collector](#)
- [Etapa 1: criar um usuário do IAM para o Agentless Collector](#)
- [Etapa 2: Baixe o Agentless Collector](#)
- [Etapa 3: implantar o Agentless Collector](#)
- [Etapa 4: acessar o console do Agentless Collector](#)
- [Etapa 5: Configurar o Agentless Collector](#)
- [Etapa 6: Configurar os módulos de coleta de dados do Agentless Collector](#)
- [Etapa 7: Visualizar os dados coletados](#)


Pré-requisitos para o Agentless Collector

A seguir estão os pré-requisitos para usar o Application Discovery Service Agentless Collector (Agentless Collector):

- Uma ou mais AWS contas.
- Uma AWS conta com a região de AWS Migration Hub origem definida, consulte [Faça login no console do Migration Hub e escolha uma região de origem](#). Seus dados do Migration Hub são armazenados em sua região de origem para fins de descoberta, planejamento e rastreamento de migração.
- Um usuário do IAM da AWS conta configurado para usar a política AWS gerenciada `AWSApplicationDiscoveryAgentlessCollectorAccess`. Para usar o módulo de coleta de dados de banco de dados e análises, esse usuário do IAM também deve usar duas políticas do IAM gerenciadas pelo cliente `DMSCollectorPolicy` `FleetAdvisorS3Policy` e. Para obter mais informações, consulte [Etapa 1: criar um usuário do IAM para o Agentless](#)

[Collector](#). O usuário do IAM deve ser criado em uma AWS conta com a região de origem do Migration Hub definida.

- VMware vCenter Server V5.5, V6, V6.5, 6.7 ou 7.0.

 Note

O Agentless Collector oferece suporte a todas essas versões do VMware, mas atualmente testamos com as versões 6.7 e 7.0.

- Para a configuração do VMware vCenter Server, certifique-se de fornecer credenciais do vCenter com as permissões de leitura e visualização definidas para o grupo Sistema.
- O Agentless Collector requer acesso de saída pela porta TCP 443 para vários domínios. AWS Para obter uma lista desses domínios, consulte [Configurar o firewall para acesso externo aos domínios AWS](#).
- Para usar o módulo de coleta de dados de banco de dados e análises, crie um bucket Amazon S3 no Região da AWS que você definiu como sua região de origem do Migration Hub. Os módulos de coleta de dados analíticos e de banco de dados armazenam metadados de inventário nesse bucket do Amazon S3. Para obter mais informações, consulte [Criação de um bucket](#) no Guia do usuário do Amazon S3.

Configurar o firewall para acesso externo aos domínios AWS

Se as conexões de saída da sua rede forem restritas, você deverá atualizar as configurações do firewall para permitir o acesso de saída aos AWS domínios exigidos pelo Agentless Collector. AWSOs domínios que exigem acesso de saída dependem se sua região de origem do Migration Hub é a região Oeste dos EUA (Oregon), us-west-2 ou alguma outra região.

Os domínios a seguir exigem acesso externo se a região inicial da sua AWS conta for us-west-2:

- `arsenal-discovery.us-west-2.amazonaws.com`— O coletor usa esse domínio para validar se ele está configurado com as credenciais de usuário do IAM necessárias. O coletor também o usa para enviar e armazenar dados coletados, já que a região de origem é us-west-2.
- `migrationhub-config.us-west-2.amazonaws.com`— O coletor usa esse domínio para determinar para qual região de origem o coletor envia dados com base nas credenciais de usuário do IAM fornecidas.
- `api.ecr-public.us-east-1.amazonaws.com`— O coletor usa esse domínio para descobrir as atualizações disponíveis.

- `public.ecr.aws`— O coletor usa esse domínio para baixar as atualizações.
- `dms.your-migrationhub-home-region.amazonaws.com`— O coletor usa esse domínio para se conectar ao coletor de AWS DMS dados.
- `s3.amazonaws.com`— O coletor usa esse domínio para carregar dados coletados pelo módulo de coleta de dados de análise e banco de dados para o seu bucket do Amazon S3.

Os seguintes domínios exigem acesso externo se a região de origem AWS da sua conta não for: **us-west-2**

- `arsenal-discovery.us-west-2.amazonaws.com`— O coletor usa esse domínio para validar se ele está configurado com as credenciais de usuário do IAM necessárias.
- `arsenal-discovery.your-migrationhub-home-region.amazonaws.com`— O coletor usa esse domínio para enviar e armazenar dados coletados.
- `migrationhub-config.us-west-2.amazonaws.com`— O coletor usa esse domínio para determinar para qual região de origem o coletor deve enviar dados com base nas credenciais de usuário do IAM fornecidas.
- `api.ecr-public.us-east-1.amazonaws.com`— O coletor usa esse domínio para descobrir as atualizações disponíveis.
- `public.ecr.aws`— O coletor usa esse domínio para baixar as atualizações.
- `dms.your-migrationhub-home-region.amazonaws.com`— O coletor usa esse domínio para se conectar ao coletor de AWS DMS dados.
- `s3.amazonaws.com`— O coletor usa esse domínio para carregar dados coletados pelo módulo de coleta de dados de análise e banco de dados para o seu bucket do Amazon S3.

Ao configurar o Agentless Collector, você pode receber erros como Falha na instalação — Verifique suas credenciais e tente novamente ou AWS não será possível entrar em contato. Verifique as configurações de rede. Esses erros podem ser causados por uma tentativa fracassada do Agentless Collector de estabelecer uma conexão HTTPS com um dos AWS domínios aos quais ele precisa de acesso de saída.

Se uma conexão AWS não puder ser estabelecida, o Agentless Collector não poderá coletar dados do seu ambiente local. Para obter informações sobre como corrigir a conexão com AWS, consulte [Corrigindo que o Agentless Collector não pode ser alcançado durante a configuração AWS](#).

Etapa 1: criar um usuário do IAM para o Agentless Collector

Para usar o Agentless Collector, na AWS conta em que você usou [Faça login no console do Migration Hub e escolha uma região de origem](#), você deve criar um usuário AWS Identity and Access Management (IAM). Em seguida, configure esse usuário do IAM para usar a seguinte política AWS gerenciada [AWSApplicationDiscoveryAgentlessCollectorAccess](#). Você anexa essa política do IAM ao criar o usuário do IAM.

Para usar o módulo de coleta de dados de banco de dados e análises, crie duas políticas de IAM gerenciadas pelo cliente. Essas políticas fornecem acesso ao seu bucket do Amazon S3 e à AWS DMS API. Para obter mais informações, consulte [Criar uma política gerenciada pelo cliente](#) no Guia do usuário do IAM.

- Use o código JSON a seguir para criar a **DMSCollectorPolicy** política.

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "dms:DescribeFleetAdvisorCollectors",
      "dms:ModifyFleetAdvisorCollectorStatuses",
      "dms:UploadFileMetadataList"
    ],
    "Resource": "*"
  }]
}
```

- Use o código JSON a seguir para criar a **FleetAdvisorS3Policy** política.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject*",
        "s3:GetBucket*",
        "s3:List*",
        "s3:DeleteObject*",
        "s3:PutObject*"
      ]
    }
  ],
}
```

```
        "Resource": [
            "arn:aws:s3:::bucket_name",
            "arn:aws:s3:::bucket_name/*"
        ]
    }
]
```

No exemplo anterior, *bucket_name* substitua pelo nome do bucket do Amazon S3 que você criou na etapa de pré-requisitos.

Recomendamos que você crie um usuário não administrativo do IAM para usar com o Agentless Collector. Ao criar usuários não administrativos do IAM, siga a prática recomendada de segurança [Grant Least Privilege, concedendo permissões mínimas](#) aos usuários.

Para criar um usuário do IAM não administrador para usar com o Agentless Collector

1. Em AWS Management Console, navegue até o console do IAM usando a AWS conta que você usou para definir a região de origem [Faça login no console do Migration Hub e escolha uma região de origem](#).
2. Crie um usuário do IAM não administrador seguindo as instruções para criar um usuário com o console, conforme descrito em Como [criar um usuário do IAM em sua AWS conta](#) no Guia do usuário do IAM.

Ao seguir as instruções no Guia do usuário do IAM:

- Quando estiver na etapa de seleção do tipo de acesso, selecione Acesso programático. Observe que, embora não seja recomendado, selecione o acesso ao AWS Management Console somente se você planeja usar as mesmas credenciais de usuário do IAM para acessar o AWS console.
- Na etapa sobre a página Definir permissão, escolha a opção Anexar políticas existentes diretamente ao usuário. Em seguida, selecione a política `AWSApplicationDiscoveryAgentlessCollectorAccess` AWS gerenciada na lista de políticas.

Em seguida, selecione as políticas `DMSCollectorPolicy` de IAM gerenciadas pelo `FleetAdvisorS3Policy` cliente.

- Quando estiver na etapa de visualização das chaves de acesso do usuário (IDs da chave de acesso e chaves de acesso secretas), siga as orientações na Nota importante sobre como salvar a nova ID da chave de acesso e a chave de acesso secreta do usuário em um local seguro e protegido. Você precisará dessas chaves de acesso [Etapa 5: Configurar o Agentless Collector](#).

É uma prática recomendada AWS de segurança alternar as chaves de acesso. Para obter informações sobre a rotação de chaves, consulte Alternar [chaves de acesso regularmente para casos de uso que exigem credenciais de longo prazo](#) no Guia do usuário do IAM.

Etapa 2: Baixe o Agentless Collector

Para configurar o Application Discovery Service Agentless Collector (Agentless Collector), você deve baixar e implantar o arquivo Agentless Collector Open Virtualization Archive (OVA). O Agentless Collector é um dispositivo virtual que você instala em seu ambiente VMware local. Esta etapa descreve como baixar o arquivo OVA do coletor e a próxima etapa descreve como implantá-lo.

Para baixar o arquivo OVA do coletor e verificar sua soma de verificação

1. Entre no vCenter como administrador do VMware e alterne para o diretório em que você deseja baixar o arquivo OVA do Agentless Collector.
2. Baixe o arquivo OVA do seguinte URL:

[Coletor OVA sem agente](#)

3. Dependendo do algoritmo de hash que você usa no ambiente do seu sistema, faça download do [MD5](#) ou do [SHA256](#) para obter o arquivo que contém o valor de soma de verificação. Use o valor baixado para verificar o `ApplicationDiscoveryServiceAgentlessCollector` arquivo baixado na etapa anterior.
4. Dependendo da sua variação do Linux, execute o comando SHA256 ou MD5 apropriado para a versão para verificar se a assinatura criptográfica do arquivo `ApplicationDiscoveryServiceAgentlessCollector.ova` corresponde ao valor no respectivo arquivo MD5/SHA256 que você baixou.

```
$ md5sum ApplicationDiscoveryServiceAgentlessCollector.ova
```

```
$ sha256sum ApplicationDiscoveryServiceAgentlessCollector.ova
```

Etapa 3: implantar o Agentless Collector

O Application Discovery Service Agentless Collector (Agentless Collector) é um dispositivo virtual que você instala em seu ambiente VMware local. Esta seção descreve como implantar o arquivo Open Virtualization Archive (OVA) que você baixou na etapa anterior, em seu ambiente VMware.

Especificações da máquina virtual Agentless Collector

- Sistema operacional — Amazon Linux 2
- RAM — 16 GB
- CPU — 4 núcleos

O procedimento a seguir orienta você na implantação do arquivo OVA do Agentless Collector em seu ambiente VMware.

Para implantar o Agentless Collector

1. Faça login no vCenter como um administrador VMware.
2. Use uma das seguintes formas de instalar o arquivo OVA:
 - Use a interface do usuário: escolha Arquivo, escolha Implantar modelo OVF, selecione o arquivo OVA do coletor que você baixou na seção anterior e, em seguida, conclua o assistente.
 - Use a linha de comando: Para instalar o arquivo OVA do coletor a partir da linha de comando, baixe e use a Ferramenta de Formato de Virtualização Aberta da VMware (ovftool). Para baixar o ovftool, selecione uma versão na página de [documentação da ferramenta OVF](#).

Veja a seguir um exemplo do uso da ferramenta de linha de comando ovftool para instalar o arquivo OVA do coletor.

```
ovftool --acceptAllEulas --name=AgentlessCollector --datastore=datastore1  
-dm=thin ApplicationDiscoveryServiceAgentlessCollector.ovf  
'vi://username:password@vcenterurl/Datacenter/host/esxi/'
```

A seguir, descrevemos os valores **substituíveis** no exemplo:

- O nome é o nome que você deseja usar para sua VM do Agentless Collector.
- O armazenamento de dados é o nome do armazenamento de dados em seu vCenter.

- O nome do arquivo OVA é o nome do arquivo OVA do coletor baixado.
 - O nome de usuário/senha são suas credenciais do vCenter.
 - O vcenterurl é o URL do seu vCenter.
 - O caminho vi é o caminho para seu host VMware ESXi.
3. Localize o Agentless Collector implantado em seu vCenter. Clique com o botão direito do mouse na VM e escolha Ligar, Ligar.
 4. Depois de alguns minutos, o endereço IP do coletor é exibido no vCenter. Você usa esse endereço IP para se conectar ao coletor.

Etapa 4: acessar o console do Agentless Collector

O procedimento a seguir descreve como acessar o console do Application Discovery Service Agentless Collector (Agentless Collector).

Para acessar o console do Agentless Collector

1. Abra um navegador da Web e digite o seguinte URL na barra de endereço: **https://** /<ip_address>, de onde <ip_address>vem o endereço IP do coletor. [Etapa 3: implantar o Agentless Collector](#)
2. Escolha Começar na primeira vez que acessar o Agentless Collector. Depois disso, você será solicitado a fazer login.

Se você estiver acessando o console Agentless Collector pela primeira vez, em seguida você acessará. [Etapa 5: Configurar o Agentless Collector](#) Caso contrário, a seguir você verá [O painel do Agentless Collector](#).

Etapa 5: Configurar o Agentless Collector

O Application Discovery Service Agentless Collector (Agentless Collector) é uma máquina virtual (VM) baseada no Amazon Linux 2. A seção a seguir descreve como configurar uma VM coletora na página Configure Agentless Collector do console Agentless Collector.

Para configurar uma VM coletora na página Configurar coletor sem agente

1. Em Nome do coletor, insira um nome para o coletor identificá-lo. O nome pode conter espaços, mas não pode conter caracteres especiais.

2. Em Sincronização de dados, insira a chave de AWS acesso e a chave secreta da AWS conta que o usuário do IAM deve especificar como a conta de destino para receber os dados descobertos pelo coletor. Para obter informações sobre os requisitos para o usuário do IAM, consulte [Etapa 1: criar um usuário do IAM para o Agentless Collector](#).
 - a. Em AWSChave de acesso, insira a chave de acesso do usuário do IAM da AWS conta que você está especificando como a conta de destino.
 - b. Em AWSChave secreta, insira a chave secreta do usuário do IAM da AWS conta que você está especificando como a conta de destino.
 - c. (Opcional) Se sua rede exigir o uso de um proxy para acessarAWS, insira o host do proxy, a porta do proxy e, opcionalmente, as credenciais necessárias para se autenticar com o servidor proxy existente.
3. Em Senha do Agentless Collector, configure uma senha a ser usada para autenticar o acesso ao Agentless Collector.
 - As senhas diferenciam maiúsculas de minúsculas
 - As senhas devem ter entre 8 e 64 caracteres
 - A senha deve conter pelo menos um caractere de cada uma das quatro seguintes categorias:
 - Letras minúsculas (a-z)
 - Letras maiúsculas (A-Z)
 - Números (0-9)
 - Caracteres não alfanuméricos (@\$! #%*? &)
 - As senhas não podem conter caracteres especiais além dos seguintes: @\$! #%*? &
 - a. Em Senha do Agentless Collector, insira uma senha a ser usada para autenticar o acesso ao coletor.
 - b. Para inserir novamente a senha do Agentless Collector, para verificação, insira a senha novamente.
4. Em Outras configurações, leia o Contrato de Licença. Se você concordar em aceitá-lo, marque a caixa de seleção.
5. Para ativar as atualizações automáticas do Agentless Collector, em Outras configurações, selecione Atualizar automaticamente o Agentless Collector. Se você não marcar essa caixa de seleção, precisará atualizar manualmente o Agentless Collector conforme descrito em [Atualizando manualmente o Agentless Collector](#)

6. Escolha Salvar configurações.

Os tópicos a seguir descrevem as tarefas opcionais de configuração do coletor.

Tarefas de configuração opcionais

- [\(Opcional\) Configurar um endereço IP estático para a VM Agentless Collector](#)
- [\(Opcional\) Redefina a VM do Agentless Collector para usar DHCP](#)
- [\(Opcional\) Configurar o protocolo de autenticação Kerberos](#)

(Opcional) Configurar um endereço IP estático para a VM Agentless Collector

As etapas a seguir descrevem como configurar um endereço IP estático para a VM do Application Discovery Service Agentless Collector (Agentless Collector). Quando instalada pela primeira vez, a VM coletora é configurada para usar o Dynamic Host Configuration Protocol (DHCP).

Note

O Agentless Collector suporta IPv4. Ele não suporta IPv6.

Para configurar um endereço IP estático para a VM coletora

1. Colete as seguintes informações de rede do VMware vCenter:

- Endereço IP estático — Um endereço IP não assinado na sub-rede. Por exemplo, 192.168.1.138.
- Máscara de rede — Isso pode ser obtido verificando a configuração do endereço IP do host VMware vCenter que hospeda a VM coletora. Por exemplo, 255.255.255.0.
- Gateway padrão — Isso pode ser obtido verificando a configuração do endereço IP do host VMware vCenter que hospeda a VM coletora. Por exemplo, 192.168.1.1.
- DNS primário — Isso pode ser obtido verificando a configuração do endereço IP do host VMware vCenter que hospeda a VM coletora. Por exemplo, 192.168.1.1.
- (Opcional) DNS secundário
- (Opcional) Nome de domínio local — Isso permite que o coletor acesse a URL do host do vCenter sem o nome do domínio.

- Abra o console da VM do coletor e faça login **ec2-user** usando a senha, **collector** conforme mostrado no exemplo a seguir.

```
username: ec2-user
password: collector
```

- Desative a interface de rede digitando o seguinte comando no terminal remoto.

```
sudo /sbin/ifdown eth0
```

- Atualize a configuração da interface eth0 usando as etapas a seguir.

- Abra ifcfg-eth0 no editor vi usando o comando a seguir.

```
sudo vi /etc/sysconfig/network-scripts/ifcfg-eth0
```

- Atualize os valores da interface, conforme mostrado no exemplo a seguir, com as informações coletadas na etapa Coletar informações da rede.

```
DEVICE=eth0
BOOTPROTO=static
ONBOOT=yes
IPADDR=static-ip-value
NETMASK=netmask-value
GATEWAY=gateway-value
TYPE=Ethernet
USERCTL=yes
PEERDNS=no
RES_OPTIONS="timeout:2 attempts:5"
```

- Atualize o Sistema de Nomes de Domínio (DNS) usando as etapas a seguir.

- Abra o `resolv.conf` arquivo no vi usando o comando a seguir.

```
sudo vi /etc/resolv.conf
```

- Atualize o `resolv.conf` arquivo no vi usando o comando a seguir.

```
search localdomain-name
options timeout:2 attempts:5
nameserver dnsserver-value
```

O exemplo a seguir mostra um `resolv.conf` arquivo editado.

```
search vsphere.local
options timeout:2 attempts:5
nameserver 192.168.1.1
```

6. Ative a interface de rede digitando o seguinte comando.

```
sudo /sbin/ifup eth0
```

7. Reinicialize a VM conforme mostrado no exemplo a seguir.

```
sudo reboot
```

8. Verifique suas configurações de rede usando as etapas a seguir.

- a. Verifique se o endereço IP está configurado corretamente, digitando os seguintes comandos.

```
ifconfig
ip addr show
```

- b. Verifique se o gateway foi adicionado corretamente, digitando o seguinte comando.

```
route -n
```

A saída deve ser semelhante ao exemplo a seguir.

```
Kernel IP routing table
Destination      Gateway          Genmask         Flags Metric Ref    Use Iface
0.0.0.0          192.168.1.1    0.0.0.0         UG    0      0      0 eth0
172.17.0.0       0.0.0.0        255.255.0.0     U    0      0      0 docker0
192.168.1.0      0.0.0.0        255.255.255.0   U    0      0      0
```

- c. Verifique se você pode executar ping em uma URL pública digitando o comando a seguir.

```
ping www.google.com
```

- d. Verifique se você pode fazer ping no endereço IP ou no nome do host do vCenter, conforme mostrado no exemplo a seguir.

```
ping vcenter-host-url
```

(Opcional) Redefina a VM do Agentless Collector para usar DHCP

As etapas a seguir descrevem como reconfigurar a VM do Agentless Collector para usar DHCP.

Para configurar a VM coletora para usar DHCP

1. Desative a interface de rede digitando o seguinte comando no terminal remoto.

```
sudo /sbin/ifdown eth0
```

2. Atualize a configuração de rede usando as etapas a seguir.

- a. Abra o `ifcfg-eth0` arquivo no editor vi usando o comando a seguir.

```
sudo /sbin/ifdown eth0
```

- b. Atualize os valores no `ifcfg-eth0` arquivo conforme mostrado no exemplo a seguir.

```
DEVICE=eth0
BOOTPROTO=dhcp
ONBOOT=yes
TYPE=Ethernet
USERCTL=yes
PEERDNS=yes
DHCPV6C=yes
DHCPV6C_OPTIONS=-nw
PERSISTENT_DHCLIENT=yes
RES_OPTIONS="timeout:2 attempts:5"
```

3. Redefina a configuração de DNS digitando o seguinte comando.

```
echo "" | sudo tee /etc/resolv.conf
```

4. Ative a interface de rede digitando o seguinte comando.

```
sudo /sbin/ifup eth0
```

5. Reinicialize a VM do coletor conforme mostrado no exemplo a seguir.

```
sudo reboot
```

(Opcional) Configurar o protocolo de autenticação Kerberos

Se o servidor do sistema operacional suportar o protocolo de autenticação Kerberos, você poderá usar esse protocolo para se conectar ao seu servidor. Para fazer isso, você deve configurar a VM do Application Discovery Service Agentless Collector.

As etapas a seguir descrevem como configurar o protocolo de autenticação Kerberos em sua VM do Application Discovery Service Agentless Collector.

Para configurar o protocolo de autenticação Kerberos em sua VM coletora

1. Abra o console da VM do coletor e faça login **ec2-user** usando a senha, **collector** conforme mostrado no exemplo a seguir.

```
username: ec2-user  
password: collector
```

2. Abra o arquivo de `krb5.conf` configuração na `/etc` pasta. Para fazer isso, você pode usar o exemplo de código a seguir.

```
cd /etc  
sudo nano krb5.conf
```

3. Atualize o arquivo de `krb5.conf` configuração com as seguintes informações.

```
[libdefaults]  
    forwardable = true  
    dns_lookup_realm = true  
    dns_lookup_kdc = true  
    ticket_lifetime = 24h  
    renew_lifetime = 7d  
    default_realm = default_Kerberos_realm
```

```
[realms]
  default_Kerberos_realm = {
    kdc = KDC_hostname
    server_name = server_hostname
    default_domain = domain_to_expand_hostnames
  }

[domain_realm]
  .domain_name = default_Kerberos_realm
  domain_name = default_Kerberos_realm
```

Salve o arquivo e saia do editor de texto.

4. Reinicialize a VM do coletor conforme mostrado no exemplo a seguir.

```
sudo reboot
```

Etapa 6: Configurar os módulos de coleta de dados do Agentless Collector

Na página do painel do console do Application Discovery Service Agentless Collector (Agentless Collector), em Coleta de dados, você configura o módulo de coleta de dados para coletar dados de inventário, perfil e utilização de seus servidores.

Atualmente, o Agentless Collector oferece suporte à coleta de dados de VMs VMware e de servidores de banco de dados e análises. Os módulos futuros oferecerão suporte à coleta de plataformas de virtualização adicionais e à coleta em nível de sistema operacional.

Tópicos

- [Módulo de coleta de dados do VMware vCenter Agentless Collector](#)
- [Módulo de coleta de dados de banco de dados e análise](#)

Módulo de coleta de dados do VMware vCenter Agentless Collector

Esta seção descreve o módulo de coleta de dados VMware vCenter do Application Discovery Service Agentless Collector (Agentless Collector), que é usado para coletar dados de inventário, perfil e utilização do servidor de suas VMs VMware.


Tópicos

- [Como configurar o módulo de coleta de dados do Agentless Collector para o VMware vCenter](#)

- [coleta de dados VMware coleta de dados VMware](#)
- [Controle o escopo da coleta de dados do vCenter](#)

Como configurar o módulo de coleta de dados do Agentless Collector para o VMware vCenter

Esta seção descreve como configurar o módulo de coleta de dados VMware vCenter do Agentless Collector para coletar dados de inventário, perfil e utilização do servidor de suas VMs VMware.

 Note

Antes de iniciar a configuração do vCenter, certifique-se de fornecer credenciais do vCenter com as permissões de leitura e visualização definidas para o grupo Sistema.

Para configurar o módulo de coleta de dados do VMware vCenter

1. Na página do painel do Agentless Collector, em Coleta de dados, escolha Configurar na seção VMware vCenter.
2. Na página Configurar a coleta de dados do VMware vCenter, faça o seguinte:
 - a. Em credenciais do vCenter:
 - i. Para URL/IP do vCenter, insira o endereço IP do seu host do VMware vCenter Server.
 - ii. Em Nome de usuário do vCenter, insira o nome de um usuário local ou de domínio que o coletor usa para se comunicar com o vCenter. Para usuários de domínio, use o formato domínio\nome do usuário ou nome do usuário@domínio.
 - iii. Em vCenter Password (Senha vCenter), insira a senha de usuário de domínio ou local.
 - b. Em Preferências de coleta de dados:
 - Para começar a coletar dados automaticamente imediatamente após uma configuração bem-sucedida, selecione Iniciar coleta de dados automaticamente.
 - c. Escolha Set up (Configurar).

Em seguida, você verá a página de detalhes da coleta de dados da VMware, descrita no próximo tópico.

coleta de dados VMware coleta de dados VMware

A página de detalhes da coleta de dados da VMware mostra detalhes sobre o vCenter em que você configurou [Como configurar o módulo de coleta de dados do Agentless Collector para o VMware vCenter](#).

Em Servidores vCenter descobertos, o vCenter que você configurou está listado com as seguintes informações sobre o vCenter:

- O endereço IP do servidor vCenter.
- O número de servidores no vCenter.
- O status coleta de dados.
- Quanto tempo passou desde a última atualização.

Escolha Remover servidor vCenter para remover o servidor vCenter exibido e retornar à página Configurar coleta de dados do VMware vCenter.

Se você não tiver optado por iniciar a coleta de dados automaticamente, poderá iniciar a coleta de dados usando o botão Iniciar coleta de dados nesta página. Depois que a coleta de dados é iniciada, o botão Iniciar muda para Interromper coleta de dados.

Se a coluna Status da coleção mostrar Coleta, a coleta de dados foi iniciada.

Você visualiza os dados coletados no AWS Migration Hub console. Se você estiver coletando dados para um inventário de servidores VMware vCenter, poderá acessar os dados que aparecem no console aproximadamente 15 minutos depois de ativar a coleta de dados.

Você pode escolher Exibir servidores no Migration Hub nesta página para abrir o console do Migration Hub, caso seu acesso à Internet não esteja bloqueado. Se você escolher esse botão ou não, para obter informações sobre como acessar o console do Migration Hub, consulte [Etapa 7: Visualizar os dados coletados](#).

A seguir estão as diretrizes para a duração recomendada da coleta de dados de acordo com as atividades de planejamento da migração:

- TCO (custo total de propriedade) - 2 a 4 semanas
- Planejamento de migração - 2 a 6 semanas

Controle o escopo da coleta de dados do vCenter

O usuário do vCenter exige permissões somente de leitura em cada host ESX ou VM para inventariar usando o Application Discovery Service. Usando as configurações de permissão, você pode controlar quais hosts e VMs são incluídos na coleta de dados. Você pode permitir que todos os hosts e VMs do vCenter atual sejam inventariados ou conceder permissões case-by-case com base nisso.

Note

Como prática recomendada de segurança, não conceda permissões adicionais e desnecessárias para o usuário do vCenter do Application Discovery Service.

Os procedimentos seguintes descrevem os cenários de configuração pedidos do menos ao mais granular. Esses procedimentos são para o vSphere Client v6.7.0.2. Os procedimentos para outras versões do cliente podem ser diferentes, dependendo da versão do cliente vSphere que você está usando.

Para descobrir dados sobre todos os hosts ESX e VMs no vCenter atual

1. No cliente VMware vSphere, escolha vCenter e escolha Hosts and Clusters ou VMs and Templates.
2. Escolha um recurso de data center e escolha Permissões.
3. Escolha o usuário vCenter e escolha o símbolo para adicionar, editar ou remover uma função de usuário.
4. Escolha Somente leitura no menu Função.
5. Escolha Propagar para crianças e escolha OK.

Para descobrir dados sobre um host ESX específico e todos os seus objetos filhos

1. No cliente VMware vSphere, escolha vCenter e escolha Hosts and Clusters ou VMs and Templates.
2. Escolha Related Objects, Hosts.
3. Abra o menu de contexto (botão direito do mouse) no nome de host e escolha All vCenter Actions, Add Permission.
4. Em Add Permission, adicione o usuário do vCenter no host. Em Assigned Role, escolha Read-only.

5. Escolha Propagate to children, OK.

Para descobrir dados sobre um host ESX específico ou uma VM secundária

1. No cliente VMware vSphere, escolha vCenter e escolha Hosts and Clusters ou VMs and Templates.
2. Escolha Related Objects.
3. Escolha Hosts (que mostra uma lista de host ESX conhecidos do vCenter) ou Virtual Machines (que mostra uma lista de VMs em todos os hosts ESX).
4. Abra o menu de contexto (botão direito do mouse) no nome de host ou VM e escolha All vCenter Actions, Add Permission.
5. Em Add Permission, adicione o usuário do vCenter no host ou na VM. Em Assigned Role, escolha Read-only, .
6. Escolha OK.

Note

Se você escolheu Propagar para crianças, ainda poderá remover a permissão somente de leitura dos hosts e VMs do ESX case-by-case com base nisso. Essa opção não afeta as permissões herdadas aplicando-se ao host ESX e VMs.

Módulo de coleta de dados de banco de dados e análise

Esta seção descreve como configurar, configurar e usar um módulo de coleta de dados de banco de dados e análise. Você pode usar esse módulo de coleta de dados para se conectar ao seu ambiente de dados e coletar metadados e métricas de desempenho de seus bancos de dados e servidores de análise locais. Para obter informações sobre as métricas que você pode coletar com este módulo, consulte [Dados coletados pelo banco de dados Agentless Collector e pelo módulo de coleta de dados analíticos](#).

Em alto nível, ao usar o módulo de coleta de dados de banco de dados e análises, você executa as seguintes etapas.

1. Conclua as etapas de pré-requisitos, configure seu usuário do IAM e crie o coletor de AWS DMS dados.

2. Configure o encaminhamento de dados para garantir que seu módulo de coleta de dados possa enviar os metadados coletados e as métricas de desempenho para AWS.
3. Adicione seus servidores LDAP e use-os para descobrir servidores de sistema operacional em seu ambiente de dados. Como alternativa, adicione seus servidores de sistema operacional manualmente ou use [Módulo de coleta de dados VMware coleta de dados VMware](#).
4. Configure as credenciais de conexão para os servidores do sistema operacional e use-as para descobrir servidores de banco de dados.
5. Configure as credenciais de conexão para seus servidores de banco de dados e análise e, em seguida, execute a coleta de dados. Para obter mais informações, consulte [Coleta de dados de banco de dados e análises](#).
6. Visualize os dados coletados no AWS DMS console e use-os para gerar recomendações de metas para uma migração para Nuvem AWS. Para obter mais informações, consulte [Coleta de dados de banco de dados e análises](#).

Tópicos

- [Servidores de sistema operacional, banco de dados e análise compatíveis](#)
- [Crie o coletor de AWS DMS dados](#)
- [Configurar o encaminhamento de dados](#)
- [Adicione seus servidores LDAP e OS](#)
- [Descubra seus servidores de banco de dados](#)

Servidores de sistema operacional, banco de dados e análise compatíveis

O módulo de coleta de dados de banco de dados e análise no Agentless Collector oferece suporte aos servidores LDAP do Microsoft Active Directory.

Esse módulo de coleta de dados oferece suporte aos seguintes servidores de sistema operacional.

- Amazon Linux 2
- CentOS Linux versão 6 e superior
- Debian versão 10 posterior
- Red Hat Enterprise Linux versão 7 posterior
- SUSE Linux Enterprise Server versão 12 e posterior

- Ubuntu versão 16.01 e superior
- Windows Server 2012 e posterior
- Windows XP e superior

Além disso, o módulo de coleta de dados de banco de dados e análise oferece suporte aos seguintes servidores de banco de dados.

- Versão 2012 do Microsoft SQL Server até 2019
- MySQL versão 5.6 e até 8
- Oracle versão 11g Release 2 e até 12c, 19c e 21c
- PostgreSQL versão 9.6 e até 13

Crie o coletor de AWS DMS dados

Seu módulo de coleta de dados de análise e banco de AWS DMS dados usa um coletor de dados para interagir com o AWS DMS console. Você pode visualizar os dados coletados no AWS DMS console ou usá-los para determinar o mecanismo AWS alvo do tamanho certo. Para obter mais informações, consulte [Usando o recurso de recomendações de metas do AWS DMS Fleet Advisor](#).

Antes de criar um coletor de AWS DMS dados, crie uma função do IAM que seu coletor de AWS DMS dados usa para acessar seu bucket do Amazon S3. Você criou esse bucket do Amazon S3 ao preencher os pré-requisitos em [Pré-requisitos para o Agentless Collector](#).

Criar uma função do IAM para seu coletor de AWS DMS dados acessar o Amazon S3

1. Faça login no AWS Management Console e abra o console do IAM em <https://console.aws.amazon.com/iam/>.
2. No painel de navegação, escolha Roles depois depois depois depois depois depois depois Create role.
3. Na página Selecionar entidade confiável, em Tipo de entidade confiável, escolha AWSServiço. Para Casos de uso de outros AWS serviços, escolha DMS.
4. Marque a caixa de seleção DMS e escolha Avançar.
5. Na página Adicionar permissões, escolha FleetAdvisorS3Policy que você criou antes. Escolha Próximo.
6. Na página Nome, revisão e criação, digite **FleetAdvisorS3Role** para Nome da função e escolha Criar função.

7. Abra a função que você criou e escolha a guia Relações de confiança. Escolha Edit trust policy (Editar política de confiança).
8. Na página Editar política de confiança, cole o seguinte JSON no editor, substituindo o código existente.

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "",
    "Effect": "Allow",
    "Principal": {
      "Service": [
        "dms.amazonaws.com",
        "dms-fleet-advisor.amazonaws.com"
      ]
    },
    "Action": "sts:AssumeRole"
  }]
}
```

9. Escolha Update policy.

Agora, crie um coletor de dados no AWS DMS console.

Para criar um coletor de dados AWS DMS

1. Faça login no AWS Management Console e abra o AWS DMS console em <https://console.aws.amazon.com/dms/v2/>.
2. Escolha a Região da AWS que você definiu como sua região de origem do Migration Hub. Para obter mais informações, consulte [Faça login no Migration Hub e escolha uma região de origem](#).
3. No painel de navegação, escolha Coletores de dados em Descobrir. A página Coletores de dados é aberta.
4. Escolha Criar coletor de dados. A página Criar coletor de dados é aberta.
5. Em Nome na seção Configuração geral, insira o nome do seu coletor de dados.
6. Na seção Conectividade, escolha Browse S3. Escolha o bucket do Amazon S3 que você criou antes na lista.
7. Para a função do IAM, escolha FleetAdvisorS3Role a que você criou antes.
8. Escolha Criar coletor de dados.

Configurar o encaminhamento de dados

Depois de criar os AWS recursos necessários, configure o encaminhamento de dados do módulo de coleta de dados de análise e banco de dados para seu AWS DMS coletor.

Para configurar o encaminhamento de dados

1. Abra o console do Agentless Collector. Para obter mais informações, consulte [Etapa 4: acessar o console do coletor](#).
2. Escolha Exibir banco de dados e coletor de análises.
3. Na página Painel, escolha Configurar encaminhamento de dados na seção Encaminhamento de dados.
4. Para Região da AWS, ID da chave de acesso do IAM e chave de acesso secreta do IAM, seu Agentless Collector usa os valores que você configurou anteriormente. Para ter mais informações, consulte [Faça login no Migration Hub e escolha uma região de origem](#) e [Etapa 1: criar um usuário do IAM](#).
5. Para o coletor de dados Connected DMS, escolha o coletor de dados que você criou no AWS DMS console.
6. Escolha Save (Salvar).

Depois de configurar o encaminhamento de dados, verifique a seção Encaminhamento de dados na página do Painel. Certifique-se de que seu módulo de coleta de dados de análise e banco de dados exiba



for Access to DMS e Access to S3.


Adicione seus servidores LDAP e OS

O módulo de coleta de dados de banco de dados e análise usa o LDAP no Microsoft Active Directory para coletar informações sobre o sistema operacional, o banco de dados e os servidores de análise em sua rede. O Lightweight Directory Access Protocol (LDAP) é um protocolo de aplicativo de padrão aberto. Você pode usar esse protocolo para acessar e manter serviços de informações de diretório distribuídos em sua rede IP.

Você pode adicionar um servidor LDAP existente ao seu banco de dados e módulo de coleta de dados analíticos para descobrir automaticamente os servidores do sistema operacional em sua rede. Se você não usa o LDAP, pode adicionar servidores do sistema operacional manualmente.

Para adicionar um servidor LDAP ao seu módulo de coleta de dados de análise e banco de dados

1. Abra o console do Agentless Collector. Para obter mais informações, consulte [Etapa 4: acessar o console do coletor](#).
2. Escolha Exibir banco de dados e coletor de análises e, em seguida, escolha servidores LDAP em Discovery no painel de navegação.
3. Escolha Adicionar servidor LDAP. A página Adicionar servidor LDAP é aberta.
4. Em Nome do host, insira o nome do host do seu servidor LDAP.
5. Em Porta, insira o número da porta usada para solicitações LDAP.
6. Em Nome de usuário, insira o nome de usuário que você usa para se conectar ao servidor LDAP.
7. Em Senha, digite a senha que você usa para se conectar ao seu servidor LDAP.
8. (Opcional) Escolha Verificar conexão para garantir que você adicionou suas credenciais do servidor LDAP corretamente. Como alternativa, você pode verificar suas credenciais de conexão do servidor LDAP posteriormente, na lista na página de servidores LDAP.
9. Escolha Adicionar servidor LDAP.
10. Na página Servidores LDAP, selecione seu servidor LDAP na lista e escolha Discover OS servers.

 Important

Para a descoberta do sistema operacional, o módulo de coleta de dados precisa de credenciais para que o servidor de domínio execute solicitações usando o protocolo LDAP.

O módulo de coleta de dados de banco de dados e análise se conecta ao seu servidor LDAP e descobre seus servidores de sistema operacional. Depois que o módulo de coleta de dados concluir a descoberta dos servidores do sistema operacional, você poderá ver a lista de servidores do sistema operacional descobertos escolhendo Exibir servidores do sistema operacional.

Como alternativa, você pode adicionar seus servidores do sistema operacional manualmente ou importar a lista de servidores de um arquivo de valores separados por vírgula (CSV). Além disso,

you can use the data collection module of the VMware vCenter Agentless Collector to discover your operational system servers. For more information, consult [Mócoleta de dados VMware coleta de dados VMware](#).

To add an operational system server to your data store and data collection module of analytical data

1. On the data collector page of data and analysis, choose Operational Servers in Discovered in the navigation panel.
2. Choose Add operational system server. The Add operational system server page is open.
3. Provide your operational system server credentials.
 - a. For the operational system type, choose the operational system of your server.
 - b. In Hostname/IP, enter the host name or IP address of your operational system server.
 - c. In Port, enter the port number used for remote queries.
 - d. In Authentication type, choose the authentication type that your operational system server uses.
 - e. In Username, enter the user name that you use to connect to your operational system server.
 - f. In Password, enter the password that you use to connect to your operational system server.
 - g. Choose Verify to ensure that you have added the operational system server credentials correctly.
4. (Optional) Add several operational system servers starting from a CSV file.
 - a. Choose Import in bulk operational system servers from CSV.
 - b. Choose Download model to save a CSV file that includes a model that you can customize.
 - c. Enter the connection credentials of the operational system servers in the file according to the model. The example below shows how you can provide connection credentials of the operational system server in a CSV file.

```
OS type,Hostname/IP,Port,Authentication type,Username>Password
Linux,192.0.2.0,22,Key-based authentication,USER-EXAMPLE,ANPAJ2UCCR6DPCEXAMPLE
Windows,203.0.113.0,,NTLM,USER2-EXAMPLE,AKIAIOSFODNN7EXAMPLE
```

Salve seu arquivo CSV depois de adicionar credenciais para todos os servidores do sistema operacional.

- d. Escolha Procurar e, em seguida, escolha seu arquivo CSV.
5. Escolha Adicionar servidor do sistema operacional.
6. Depois de adicionar credenciais para todos os servidores do sistema operacional, selecione seus servidores de sistema operacional e escolha Descobrir servidores de banco de dados.

Descubra seus servidores de banco de dados

Para a descoberta de bancos de dados, crie usuários para seus bancos de dados de origem com as permissões mínimas necessárias para o módulo de coleta de dados. Para obter mais informações, consulte [Criação de usuários de banco de dados para o AWS DMS Fleet Advisor](#) no Guia AWS DMS do usuário.

Para descobrir os bancos de dados em execução nos servidores OS adicionados anteriormente, o módulo de coleta de dados requer acesso ao sistema operacional e aos servidores de banco de dados. Certifique-se de que seu banco de dados seja acessível na porta especificada nas configurações de conexão. Em seguida, ative a autenticação remota em seu servidor de banco de dados. Além disso, forneça ao seu módulo de coleta de dados as seguintes permissões.

Para descobrir servidores de banco de dados no Windows

1. Forneça credenciais com concessões para executar consultas do Windows Management Instrumentation (WMI) e do WMI Query Language (WQL) e ler o registro.
2. Adicione o usuário do Windows que você especificou nas credenciais de conexão do servidor OS aos seguintes grupos: Usuários COM distribuídos, Usuários de registro de desempenho, usuários do monitor de desempenho e leitores do registro de eventos. Para fazer isso, use o exemplo de código a seguir.

```
net localgroup "Distributed COM Users" username /ADD
net localgroup "Performance Log Users" username /ADD
net localgroup "Performance Monitor Users" username /ADD
net localgroup "Event Log Readers" username /ADD
```

No exemplo anterior, *username* substitua pelo nome do usuário do Windows que você especificou nas credenciais de conexão do servidor do sistema operacional.

3. Conceda as permissões necessárias para o usuário do Windows que você especificou nas credenciais de conexão do servidor do sistema operacional.
 - Para Propriedades de gerenciamento e instrumentação do Windows, escolha Inicialização local e ativação remota.
 - Para Controle de WMI, escolha as permissões Executar Métodos, Ativar Conta, Ativação Remota e Segurança de Leitura para os WMI namespaces CIMV2DEFAULTStandartCimv2,, e.
 - Para o plug-in WMI, execute `winrm configsddl default` e escolha Ler e executar.
4. Configure seu host do Windows usando o exemplo de código a seguir.

```
netsh advfirewall firewall add rule name="Open Ports for WinRM incoming traffic"
  dir=in action=allow protocol=TCP localport=5985, 5986 # Opens ports for WinRM
netsh advfirewall firewall add rule name="All ICMP V4" protocol=icmpv4:any,any
  dir=in action=allow # Allows ICMP traffic

Enable-PSRemoting -Force # Enables WinRM
Set-Service WinRM -StartMode Automatic # Allows WinRM service to run on host
  startup
Set-Item WSMan:\localhost\Client\TrustedHosts -Value {IP} -Force # Sets the
  specific IP from which the access to WinRM is allowed

winrm set winrm/config/service '{@Negotiation="true"}' # Allow Negotiate auth usage
winrm set winrm/config/service '{@AllowUnencrypted="true"}' # Allow unencrypted
  connection
```

Para descobrir servidores de banco de dados no Linux

1. Forneça acesso sudo aos `netstat` comandos e.

O exemplo de código a seguir concede ao sudo acesso aos `netstat` comandos e.

```
sudo bash -c "cat << EOF >> /etc/sudoers.d/username
username ALL=(ALL) NOPASSWD: /usr/bin/ss
username ALL=(ALL) NOPASSWD: /usr/bin/netstat
EOF"
```

No exemplo anterior, *username* substitua pelo nome do usuário Linux que você especificou nas credenciais de conexão do servidor do sistema operacional.

O exemplo anterior usa `o/usr/bin/` caminho para `osnetstat` comandos e. Esse caminho pode ser diferente em seu ambiente. Para determinar o caminho para `osnetstat` comandos e, execute `oswhich` `sswhich` `netstat` comandos e.

2. Configure seus servidores Linux para permitir a execução de scripts SSH remotos e permitir o tráfego do Internet Control Message Protocol (ICMP).

Para iniciar a descoberta de seus servidores de banco de dados

1. Na página do coletor de banco de dados e análises, escolha Servidores do sistema operacional em Descoberta no painel de navegação.
2. Selecione os servidores do sistema operacional que incluem seus servidores de banco de dados e análise e escolha Verificar conexão no menu Ações.
3. Para servidores com o status de conectividade de Falha, edite as credenciais de conexão.
 - a. Selecione um único servidor ou vários servidores quando eles tiverem credenciais idênticas e escolha Editar no menu Ações. A página Editar servidor do sistema operacional é aberta.
 - b. Em Porta, insira o número da porta usada para consultas remotas.
 - c. Em Tipo de autenticação, escolha o tipo de autenticação que seu servidor do sistema operacional usa.
 - d. Em Nome de usuário, insira o nome de usuário que você usa para se conectar ao servidor do sistema operacional.
 - e. Em Senha, digite a senha que você usa para se conectar ao servidor do sistema operacional.
 - f. Escolha Verificar conexão para verificar se você atualizou as credenciais do servidor do sistema operacional corretamente. Em seguida, escolha Salvar.
4. Depois de atualizar as credenciais de todos os servidores do sistema operacional, selecione seus servidores de sistema operacional e escolha Descobrir servidores de banco de dados.

O módulo de coleta de dados de banco de dados e análises se conecta aos servidores do sistema operacional e descobre os servidores de banco de dados e análise suportados. Depois que o módulo de coleta de dados concluir a descoberta, você poderá ver a lista de servidores de banco de dados e análise descobertos escolhendo Exibir servidores de banco de dados.

Como alternativa, você pode adicionar seus servidores de banco de dados e análise ao inventário manualmente. Além disso, você pode importar a lista de servidores de um arquivo CSV. Você pode

ignorar esta etapa se já tiver adicionado todos os seus servidores de banco de dados e análise ao inventário.

Para adicionar manualmente um banco de dados ou servidor de análise

1. Na página Coletor de banco de dados e análises, escolha Coleta de dados no painel de navegação.
2. Escolha Adicionar servidor de banco de dados. A página Adicionar servidor de banco de dados é aberta.
3. Forneça suas credenciais do servidor de banco de dados.
 - a. Para Mecanismo de banco de dados, escolha o mecanismo de banco de dados do seu servidor. Para obter mais informações, consulte [Servidores de sistema operacional, banco de dados e análise compatíveis](#).
 - b. Em Hostname /IP, insira o nome do host ou endereço IP do seu banco de dados ou servidor de análise.
 - c. Em Porta, insira a porta em que seu servidor é executado.
 - d. Em Tipo de autenticação, escolha o tipo de autenticação que seu banco de dados ou servidor de análise usa.
 - e. Em Nome de usuário, insira o nome de usuário que você usa para se conectar ao servidor.
 - f. Em Senha, digite a senha que você usa para se conectar ao seu servidor.
 - g. Escolha Verificar para garantir que você adicionou suas credenciais de banco de dados ou servidor de análise corretamente.
4. (Opcional) Adicione vários servidores de um arquivo CSV.
 - a. Escolha Importar servidores de banco de dados em massa do CSV.
 - b. Escolha Baixar modelo para salvar um arquivo CSV que inclui um modelo que você pode personalizar.
 - c. Insira as credenciais de conexão do seu banco de dados e servidores de análise no arquivo de acordo com o modelo. O exemplo a seguir mostra como você pode fornecer credenciais de conexão do banco de dados ou do servidor de análise em um arquivo CSV.

```
Database engine,Hostname/IP,Port,Authentication type,Username>Password,Oracle  
service name,Database,Allow public key retrieval,Use SSL,Trust server  
certificate
```

```
Oracle,192.0.2.1,1521,Login/Password authentication,USER-  
EXAMPLE,AKIAI44QH8DHBEXAMPLE,orcl,,,,  
PostgreSQL,198.51.100.1,1533,Login/Password authentication,USER2-  
EXAMPLE,bPxRfiCYEXAMPLE,,postgre,,TRUE,  
MSSQL,203.0.113.1,1433,Login/Password authentication,USER3-  
EXAMPLE,h3yCo8nvnBEXAMPLE,,,,,TRUE  
MySQL,2001:db8:4006:812:ffff:200e,8080,Login/Password authentication,USER4-  
EXAMPLE,APKAEIVFHP46CEXAMPLE,,mysql,TRUE,TRUE,
```

Salve seu arquivo CSV depois de adicionar credenciais para todos os seus servidores de banco de dados e análises.

- d. Escolha Procurar e, em seguida, escolha seu arquivo CSV.
5. Escolha Adicionar servidor de banco de dados.
6. Depois de adicionar credenciais para todos os servidores do sistema operacional, selecione seus servidores de sistema operacional e escolha Descobrir servidores de banco de dados.

Depois de adicionar todos os seus servidores de banco de dados e análises ao módulo de coleta de dados, adicione-os ao inventário. O módulo de coleta de dados de banco de dados e análises pode se conectar aos servidores a partir do inventário e coletar metadados e métricas de desempenho.

Para adicionar seu banco de dados e servidores de análise ao inventário

1. Na página Coletor de banco de dados e análises, escolha Servidores de banco de dados em Descoberta no painel de navegação.
2. Selecione os servidores de banco de dados e análise para os quais você deseja coletar metadados e métricas de desempenho.
3. Escolha Adicionar ao inventário.

Depois de adicionar todos os servidores de banco de dados e análises ao seu inventário, você pode começar a coletar metadados e métricas de desempenho. Para obter mais informações, consulte [Coleta de dados de banco de dados e análises](#).

Etapa 7: Visualizar os dados coletados

Você pode visualizar os dados que seu Coletor Sem Agente do Application Discovery Service (Agentless Collector) coletou no console do Migration Hub. Você pode visualizar as métricas coletadas para servidores de banco de dados e análises no AWS DMS console.

Para visualizar os dados descobertos pelo módulo de coleta de dados do VMware vCenter Agentless Collector

1. Faça login AWS Management Console e abra o console do Migration Hub em <https://console.aws.amazon.com/migrationhub/>. Para essa tarefa, recomendamos que você use uma conta de usuário do IAM diferente do usuário do IAM que você criou para configurar e acessar o Agentless Collector.
2. No painel de navegação do console do Migration Hub, em Discover, escolha Servers.
3. Para ver detalhes sobre um servidor, escolha o nome do host do servidor na coluna Informações do servidor. A página de detalhes do servidor exibe informações sobre o servidor, como nome do host, endereço IP, métricas de desempenho e assim por diante.

Para visualizar os dados descobertos pelo módulo de coleta de dados de banco de dados e análise

1. Faça login no AWS Management Console e abra o AWS DMS console em <https://console.aws.amazon.com/dms/v2/>.
2. Escolha Inventário em Descobrir. A página Inventário é aberta.
3. Escolha Analisar inventários para determinar as propriedades do esquema do banco de dados, como semelhança e complexidade.
4. Escolha a guia Esquemas para ver os resultados da análise.

Você pode usar o AWS DMS console para identificar esquemas duplicados, determinar a complexidade da migração e exportar as informações de inventário para análise futura. Para obter mais informações, consulte [Usando inventários para análise no AWS DMS Fleet Advisor](#).

Dados coletados pelo Agentless Collector

Você configura o módulo de coleta de dados do Application Discovery Service Agentless Collector (Agentless Collector) para coletar dados de inventário, perfil e utilização de seus servidores.

Atualmente, o Agentless Collector oferece suporte à coleta de dados de VMs VMware e de servidores de banco de dados e análises. Os módulos futuros oferecerão suporte à coleta de plataformas de virtualização adicionais e à coleta em nível de sistema operacional. Para obter informações sobre como configurar a coleta de dados, consulte [Etapa 6: Configurar os módulos de coleta de dados do Agentless Collector](#).

Os tópicos a seguir descrevem os dados coletados pelos módulos de coleta de dados do Application Discovery Service Agentless Collector (Agentless Collector).

Tópicos

- [Dados coletados pelo módulo de coleta de dados Agentless Collector VMware vCenter](#)
- [Dados coletados pelo banco de dados Agentless Collector e pelo módulo de coleta de dados analíticos](#)

Dados coletados pelo módulo de coleta de dados Agentless Collector VMware vCenter

As informações a seguir descrevem os dados coletados pelo módulo de coleta de dados do VMware vCenter do Application Discovery Service Agentless Collector (Agentless Collector). Para obter informações sobre como configurar a coleta de dados, consulte [Como configurar o módulo de coleta de dados do Agentless Collector para o VMware vCenter](#).

Legenda da tabela dos dados coletados do Agentless Collector VMware vCenter:

- Os dados coletados estão em Kilobytes (KB), a menos que especificado de outra forma.
- Dados equivalentes no console do Migration Hub são reportados em megabytes (MB).
- Os campos de dados indicados com um asterisco (*) estão disponíveis somente nos arquivos.csv produzidos a partir da função de exportação da API Application Discovery Service.

O Agentless Collector oferece suporte à exportação de dados usando a CLI. AWS Para exportar dados coletados usando a AWS CLI, siga as instruções descritas em Exportar dados de desempenho do sistema para todos os servidores na página [Exportar dados coletados](#) no Guia do usuário do Application Discovery Service.

- O período de sondagem ocorre em intervalos de aproximadamente 60 minutos.
- Os campos de dados indicados com um asterisco duplo (**) retornam atualmente um valor nulo.

Campo de dados	Descrição
applicationConfigurationId*	ID do aplicativo de migração em que a VM está agrupada.

Campo de dados	Descrição
avgCpuUsagePct	Porcentagem média de uso da CPU durante o período de pesquisa.
avgDiskBytesReadPerSecond	Número médio de bytes lidos do disco durante o período de pesquisa.
avgDiskBytesWrittenPerSecond	Número médio de bytes gravados em disco durante o período de pesquisa.
avgDiskReadOpsPerSecond**	Número médio de operações de E/S de leitura por segundo nulo.
avgDiskWriteOpsPerSecond**	Número médio de operações de E/S de gravação por segundo.
avgFreeRAM	RAM livre média expressa em MB.
avgNetworkBytesReadPerSecond	Quantidade média de taxa de transferência de bytes lidos por segundo.
avgNetworkBytesWrittenPerSecond	Quantidade média de taxa de transferência de bytes gravados por segundo.
Fabricante de computadores	Fornecedor relatado pelo host ESXi.
Modelo de computador	Modelo de computador relatado pelo host ESXi.
configId	ID atribuída pelo Application Discovery Service à VM descoberta.
configType	Tipo de recurso descoberto.
connectorId	ID do dispositivo virtual.
cpuType	vCPU para uma VM, modelo real para um host.
datacenterId	ID do vCenter.

Campo de dados	Descrição
hostId*	ID do host da VM.
hostName	Nome do host que executa o software de virtualização.
hypervisor	Tipo de hipervisor.
id	ID do servidor.
lastModifiedTime ^{Carimbo *}	Data e hora mais recentes da coleta de dados antes da exportação dos dados.
macAddress	Endereço MAC da VM.
manufacturer	Criador do software de virtualização.
maxCpuUsagePct	Porcentagem máxima de uso da CPU durante o período de pesquisa.
maxDiskBytesReadPerSecond	Número máximo de bytes lidos do disco durante o período de pesquisa.
maxDiskBytesWrittenPerSecond	Número máximo de bytes gravados no disco durante o período de pesquisa.
maxDiskReadOpsPerSecond**	Número máximo de operações de E/S de leitura por segundo.
maxDiskWriteOpsPerSecond**	Número máximo de operações de E/S de gravação por segundo.
maxNetworkBytesReadPerSecond	Quantidade máxima de taxa de transferência de bytes lidos por segundo.
maxNetworkBytesWrittenPerSecond	Quantidade máxima de taxa de transferência de bytes gravados por segundo.

Campo de dados	Descrição
memoryReservation [*]	Limite para evitar o comprometimento excessivo da memória na VM.
moRefId	ID de referência exclusiva do vCenter Managed Object.
name [*]	Nome da VM ou da rede (especificado pelo usuário).
numCores	Número de núcleos de CPU atribuídos à VM.
numCpus	Número de soquetes de CPU no host ESXi.
numDisks ^{**}	Número de discos na VM.
numNetworkCards ^{**}	Número de placas de rede na VM.
osName	Nome do sistema operacional na VM.
osVersion	Versão do sistema operacional na VM.
portGroupId [*]	ID do grupo de portas membros da VLAN.
portGroupName [*]	Nome do grupo de portas membros da VLAN.
powerState [*]	Status do poder.
serverId	O Application Discovery Service atribuiu o ID à VM descoberta.
smBiosId [*]	ID/versão do BIOS de gerenciamento do sistema.
estado [*]	Status do dispositivo virtual.
toolsStatus	Estado operacional das ferramentas VMware

Campo de dados	Descrição
totalDiskFreeTamanho	Espaço livre em disco expresso em MB. Disponível para vCenter Server 7.0 e versões posteriores.
totalDiskSize	Capacidade total do disco expressa em MB.
totalRAM	Quantidade total de RAM disponível na VM em MB.
type	Tipo de hospedeiro.
vCenterId	Número de identificação exclusivo de uma VM.
vCenterName*	Nome do host do vCenter.
virtualSwitchName*	Nome do switch virtual.
vmFolderPath	Caminho do diretório dos arquivos da VM.
vmName	Nome da máquina virtual.

Dados coletados pelo banco de dados Agentless Collector e pelo módulo de coleta de dados analíticos

O módulo de coleta de dados analíticos e banco de dados do Application Discovery Service Agentless Collector (Agentless Collector) coleta as seguintes métricas do seu ambiente de dados. Para obter informações sobre como configurar a coleta de dados, consulte [Módulo de coleta de dados de banco de dados e análise](#).

Quando você usa o módulo de coleta de dados de banco de dados e análise para coletar metadados e a capacidade do banco de dados, ele captura as seguintes métricas.

- Memória disponível nos servidores do sistema operacional
- Armazenamento disponível em seus servidores de sistema operacional
- Versão e edição do banco de dados
- Número de CPUs em seus servidores de sistema operacional

- Número de esquemas
- O número de procedimentos armazenados
- Número de tabelas
- Número de gatilhos
- Número de visualizações
- Estrutura do esquema

Depois de iniciar a análise do esquema no AWS DMS console, seu módulo de coleta de dados analisa e exibe as seguintes métricas.

- Datas de suporte ao banco de
- Número de linhas de código
- Complexidade do esquema
- Similaridade de esquemas

Quando você usa o módulo de coleta de dados de banco de dados e análise para coletar metadados, capacidade do banco de dados e utilização de recursos, ele captura as seguintes métricas.

- Taxa de transferência de E/S em seus servidores de banco de dados
- O número de operações de entrada e saída por segundo (IOPS) nos servidores de banco de dados
- Número de CPUs que seus servidores de sistema operacional usam
- Uso de memória em seus servidores de sistema operacional
- Uso de armazenamento em seus servidores de sistema operacional

Você pode usar o módulo de coleta de dados de banco de dados e análise para coletar metadados, capacidade e métricas de utilização de seus bancos de dados Oracle e SQL Server. Ao mesmo tempo, para bancos de dados PostgreSQL e MySQL, o módulo de coleta de dados pode coletar somente metadados.

Usando o console Agentless Collector

Esta seção descreve como usar o console do Application Discovery Service Agentless Coletor (Agentless Coletor).

Tópicos

- [O painel do Agentless Collector](#)
- [Editando as configurações do Agentless Collector](#)
- [Editando credenciais do VMware vCenter](#)

O painel do Agentless Collector

Na página do painel do Application Discovery Service Agentless Collector (Agentless Collector), você pode ver o status do coletor e escolher um método de coleta de dados conforme descrito nos tópicos a seguir.

Tópicos

- [Status do coletor](#)
- [Coleta de dados](#)

Status do coletor

O status do coletor fornece informações de status sobre o coletor. O nome do coletor, o status da conexão do coletor com a AWS, a região de origem do Migration Hub e a versão.

Se você tiver problemas de AWS conexão, talvez precise editar as configurações do Agentless Coletor.

Para editar as configurações do coletor, escolha Editar configurações do coletor e siga as instruções descritas em [Editando as configurações do Agentless Collector](#).

Coleta de dados

Em Coleta de dados, você pode escolher um método de coleta de dados. O Application Discovery Service Agentless Collector (Agentless Collector) atualmente oferece suporte à coleta de dados de VMs da VMware e de servidores de banco de dados e análise. Os módulos futuros oferecerão suporte à coleta de plataformas de virtualização adicionais e à coleta em nível de sistema operacional.

Tópicos

- [Coletor de dados do VMware vCenter](#)
- [Coleta de dados de banco de dados e análises](#)

Coletor de dados do VMware vCenter

Para coletar dados de inventário, perfil e utilização de servidores de suas VMs VMware, configure conexões com seus servidores vCenter. Para configurar as conexões, escolha Configurar na seção VMware vCenter e siga as instruções descritas em [Etapa 6: Configurar os módulos de coleta de dados do Agentless Collector](#).

Depois de configurar a coleta de dados do vCenter, no painel, você pode realizar o seguinte:

- Exibir o status da coleta de dados
- Iniciar coleta de dados
- Interromper a coleta de dados

Note

Na página do painel, depois de configurar a coleta de dados do vCenter, o botão Configurar na seção VMware vCenter é substituído por informações de status da coleta de dados, um botão Interromper coleta de dados e um botão Exibir e editar.

Coleta de dados de banco de dados e análises

Você pode executar seu módulo de coleta de dados de análise e banco de dados nos dois modos a seguir.

Capacidade de metadados e banco de dados

O módulo de coleta de dados coleta informações como esquemas, versões, edições, CPU, memória e capacidade de disco do seu banco de dados e servidores de análise. Você pode usar essas informações coletadas para calcular as recomendações de metas noAWS DMS console. Se seu banco de dados de origem estiver superprovisionado ou subprovisionado, as recomendações de destino também serão provisionadas em excesso ou subprovisionamento.

Esse é o modo padrão.

Metadados, capacidade do banco de dados e utilização de recursos

Além das informações de metadados e da capacidade do banco de dados, o módulo de coleta de dados coleta métricas reais de utilização da CPU, memória e capacidade de disco dos bancos de dados e servidores de análise. Esse modo fornece recomendações de metas mais precisas do que o modo padrão porque as recomendações são baseadas nas cargas de trabalho reais do banco de dados. Nesse modo, o módulo de coleta de dados coleta métricas de desempenho a cada minuto.

Para começar a coletar metadados e métricas de desempenho do seu banco de dados e servidores de análise

1. Na página Coletor de banco de dados e análises, escolha Coleta de dados no painel de navegação.
2. Na lista Inventário do banco de dados, selecione os servidores de banco de dados e análise para os quais você deseja coletar metadados e métricas de desempenho.
3. Escolha Executar coleta de dados. A caixa de diálogo Tipo de coleta de dados é aberta.
4. Escolha como coletar dados para análise.

Se você escolher a opção Metadados, capacidade do banco de dados e utilização de recursos, defina o período da coleta de dados. Você pode coletar dados durante os próximos 7 dias ou definir o intervalo personalizado de 1 a 60 dias.

5. Escolha Executar coleta de dados. A página de coleta de dados é aberta.
6. Escolha a guia Integridade da coleção para ver o status da coleta de dados.

Depois de concluir a coleta de dados, seu módulo de coleta de dados carrega os dados coletados em seu bucket do Amazon S3. Em seguida, você pode visualizar esses dados coletados conforme descrito em [Etapa 7: Visualizar os dados coletados](#).

Editando as configurações do Agentless Collector

Você configurou o coletor ao configurar pela primeira vez o Application Discovery Service Agentless Collector (Agentless Collector) conforme descrito em [Etapa 5: Configurar o Agentless Collector](#). O procedimento a seguir descreve como editar as configurações do Agentless Coletor.

Para editar as configurações do coletor

- Escolha o botão Editar configurações do coletor no painel do Agentless Collector.

Na página Editar configurações do coletor, faça o seguinte:

- a. Em Nome do coletor, insira um nome para identificar o coletor. O nome pode conter espaços, mas não pode conter caracteres especiais.
- b. Em AWSConta de destino para dados de descoberta, insira a chave deAWS acesso e a chave secreta daAWS conta a ser especificada como a conta de destino para receber os dados descobertos pelo coletor. Para obter informações sobre os requisitos para o usuário do IAM, consulte [Etapa 1: criar um usuário do IAM para o Agentless Collector](#).
 - i. Para AWSchave de acesso, insira a chave de acesso do usuário do IAM daAWS conta que você está especificando como a conta de destino.
 - ii. Para AWSchave secreta, insira a chave secreta do usuário do IAM daAWS conta que você está especificando como a conta de destino.
- c. Em Senha do Agentless Collector, altere a senha a ser usada para autenticar o acesso ao Agentless Collector.
 - i. Para a senha do Agentless Collector, insira uma senha a ser usada para autenticar o acesso ao Agentless Collector.
 - ii. Para reinserir a senha do Agentless Collector, para verificação, insira a senha novamente.
- d. Escolha Salvar configurações.

Em seguida, você verá [O painel do Agentless Collector](#).

Editando credenciais do VMware vCenter

Para coletar dados de inventário, perfil e utilização de servidores de suas VMs VMware, configure conexões com seus servidores vCenter. Para obter informações sobre como configurar conexões do VMware vCenter, consulte [Etapa 6: Configurar os módulos de coleta de dados do Agentless Collector](#).

Esta seção descreve como editar as credenciais do vCenter.

Note

Antes de editar as credenciais do vCenter, certifique-se de poder fornecer às credenciais do vCenter as permissões de leitura e visualização definidas para o grupo Sistema.

Para editar as credenciais do VMware vCenter

Na [coleta de dados VMware coleta de dados VMware](#) página, escolha Editar servidores vCenter.

- Na página Editar vCenter, faça o seguinte:
 - a. Em credenciais do vCenter:
 - i. Para URL/IP do vCenter, insira o endereço IP do seu host do VMware vCenter Server.
 - ii. Em vCenter Username (Nome de usuário do vCenter), insira o nome de um local ou usuário de domínio que o conector usa para se comunicar com o vCenter. Para usuários de domínio, use o formato domínio\nome do usuário ou nome do usuário@domínio.
 - iii. Em vCenter Password (Senha vCenter), insira a senha de usuário de domínio ou local.
 - b. Escolha Save (Salvar).

Atualizando manualmente o Agentless Collector

Ao configurar o Application Discovery Service Agentless Collector (Agentless Collector), você pode optar por ativar as atualizações automáticas conforme descrito em [Etapa 5: Configurar o Agentless Collector](#). Se você não ativar as atualizações automáticas, precisará atualizar manualmente o Agentless Collector.

O procedimento a seguir descreve como atualizar manualmente o Agentless Collector.

Para atualizar manualmente o Agentless Collector

1. Obtenha o arquivo Agentless Collector Open Virtualization Archive (OVA) mais recente.
2. (Opcional) Recomendamos que você exclua o arquivo OVA anterior do Agentless Collector antes de implantar o mais recente.
3. Na [Introdução ao Agentless Collector](#) seção, siga as etapas a [Etapa 3: implantar o Agentless Collector](#) seguir [Etapa 6: Configurar os módulos de coleta de dados do Agentless Collector](#).

O procedimento anterior atualiza somente o Agentless Collector. É sua responsabilidade manter o sistema operacional atualizado.

Para atualizar sua instância do Amazon EC2

1. Obtenha o endereço IP do Agentless Collector do VMware vCenter.
2. Abra o console da VM do coletor e faça login **ec2-user** usando a senha, **collector** conforme mostrado no exemplo a seguir.

```
username: ec2-user
password: collector
```

3. Siga as instruções em [Atualizar o software da instância em sua instância AL2](#) no Guia do usuário do Amazon Linux 2.

Correção dinâmica do Kernel no Amazon Linux 2

A máquina virtual Agentless Collector usa o Amazon Linux 2 conforme descrito em. [Etapa 3: implantar o Agentless Collector](#)

Para habilitar e usar a aplicação de patches ao vivo para o Amazon Linux 2, consulte [Kernel Live Patching no Amazon Linux 2](#) no Guia do usuário do Amazon EC2.

Solução de problemas do Agentless Collector

Esta seção contém tópicos que podem ajudá-lo a solucionar problemas conhecidos com o Application Discovery Service Agentless Collector (Agentless Collector).

Tópicos

- [Corrigindo que o Agentless Collector não pode ser alcançado durante a configuração AWS](#)
- [Corrigindo problemas de certificação autoassinada ao se conectar ao host proxy](#)
- [Encontrando colecionadores insalubres](#)
- [Corrigindo problemas de endereço IP](#)
- [Corrigindo problemas de credenciais do vCenter](#)
- [Corrigindo problemas de encaminhamento de dados no módulo de coleta de dados de banco de dados e análises](#)
- [Corrigindo problemas de conexão no módulo de coleta de dados de banco de dados e análise](#)

- [Suporte autônomo ao host ESX](#)
- [Entrar em contato com AWS o Support em caso de problemas com o Agentless Collector](#)

Corrigindo que o Agentless Collector não pode ser alcançado durante a configuração AWS

O Agentless Collector requer acesso de saída pela porta TCP 443 para vários domínios. AWS Ao configurar o Agentless Collector no console, você pode receber a seguinte mensagem de erro.

Não foi possível alcançar AWS

AWS não pode ser alcançado. Verifique as configurações de rede.

Esse erro ocorre devido a uma tentativa fracassada do Agentless Collector de estabelecer uma conexão HTTPS com um AWS domínio com o qual o coletor precisa se comunicar durante o processo de configuração. A configuração do Agentless Collector falhará se uma conexão não puder ser estabelecida.

Para corrigir a conexão com AWS

1. Verifique com seu administrador de TI se o firewall da sua empresa está bloqueando o tráfego de saída na porta 443 para qualquer um dos AWS domínios que exigem acesso de saída. AWS Os domínios que exigem acesso externo dependem se sua região de origem é a região Oeste dos EUA (Oregon), us-west-2 ou alguma outra região.

Os domínios a seguir exigem acesso externo se a região de origem da sua AWS conta for us-west-2:

- `arsenal-discovery.us-west-2.amazonaws.com`
- `migrationhub-config.us-west-2.amazonaws.com`
- `api.ecr-public.us-east-1.amazonaws.com`
- `public.ecr.aws`

Os seguintes domínios exigem acesso externo se a região de origem AWS da sua conta não for: **us-west-2**

- `arsenal-discovery.us-west-2.amazonaws.com`
- `arsenal-discovery.your-home-region.amazonaws.com`
- `migrationhub-config.us-west-2.amazonaws.com`
- `api.ecr-public.us-east-1.amazonaws.com`
- `public.ecr.aws`

Se seu firewall estiver bloqueando o acesso de saída aos AWS domínios com os quais o Agentless Collector precisa se comunicar, configure um host proxy na seção Sincronização de dados em Configuração do Collector.

2. Se a atualização do firewall não resolver o problema de conexão, use as etapas a seguir para garantir que a máquina virtual coletora tenha conectividade de rede de saída com os domínios listados na etapa anterior.
 - a. Obtenha o endereço IP do Agentless Collector do VMware vCenter.
 - b. Abra o console da VM do coletor e faça login **ec2-user** usando a senha, **collector** conforme mostrado no exemplo a seguir.

```
username: ec2-user
password: collector
```

- c. Teste a conexão com os domínios listados executando o telnet nas portas 443, conforme mostrado no exemplo a seguir.

```
telnet migrationhub-config.us-west-2.amazonaws.com 443
```

3. Se o telnet não conseguir resolver o domínio, tente configurar um servidor DNS estático usando as instruções [para o Amazon Linux 2](#).
4. Se o erro persistir, para obter mais suporte, consulte [Entrar em contato com AWS o Support em caso de problemas com o Agentless Collector](#).

Corrigindo problemas de certificação autoassinada ao se conectar ao host proxy

Se a comunicação com o proxy fornecido opcionalmente for via HTTPS e o proxy tiver um certificado autoassinado, talvez seja necessário fornecer um certificado.

1. Obtenha o endereço IP do Agentless Collector do VMware vCenter.
2. Abra o console da VM do coletor e faça login `ec2-user` com a senha, `collector` conforme mostrado no exemplo a seguir.

```
username: ec2-user
password: collector
```

3. Cole o corpo do certificado associado ao proxy seguro, incluindo ambos `-----BEGIN CERTIFICATE-----` e `-----END CERTIFICATE-----`, no seguinte arquivo:

```
/etc/pki/ca-trust/source/anchors/https-proxy-ca.pem
```

4. Para instalar o novo certificado, execute os seguintes comandos:

```
sudo update-ca-trust
```

5. Reinicie o Agentless Collector executando o seguinte comando:

```
sudo shutdown -r now
```

Encontrando colecionadores insalubres

As informações de status de cada coletor são encontradas na página [Coletores de dados](#) do console AWS Migration Hub (Migration Hub). Você pode identificar coletores com problemas encontrando qualquer coletor com o status `Requer atenção`.

O procedimento a seguir descreve como acessar o console do Agentless Collector para identificar problemas de saúde.

Para acessar o console do Agentless Collector

1. Usando sua AWS conta, faça login 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, em Discover, escolha Coletores de dados.
3. Na guia Coletores sem agente, anote o endereço IP de cada conector com o status Requer atenção.
4. Para abrir o console do Agentless Collector, abra um navegador da web. Em seguida, digite o seguinte URL na barra de endereço: **https://<ip_address>**, onde ip_address é o endereço IP de um coletor não íntegro.
5. Escolha Login e, em seguida, insira a senha do Agentless Collector, que foi configurada quando o coletor foi configurado em. [Etapa 5: Configurar o Agentless Collector](#)
6. Na página do painel do Agentless Collector, em Coleta de dados, escolha Exibir e editar na seção VMware vCenter.
7. Siga as instruções [Editando credenciais do VMware vCenter](#) para corrigir o URL e as credenciais.

Depois de corrigir os problemas de saúde, o coletor restabelecerá a conectividade com o servidor vCenter e o status do coletor mudará para o estado de coleta. Se os problemas persistirem, consulte [Entrar em contato com AWS o Support em caso de problemas com o Agentless Collector](#).

As causas mais comuns de coletores não íntegros são problemas de endereço IP e credenciais. [Corrigindo problemas de endereço IP](#) e [Corrigindo problemas de credenciais do vCenter](#) pode ajudá-lo a resolver esses problemas e devolver um coletor a um estado saudável.

Corrigindo problemas de endereço IP

Um coletor pode entrar em um estado não íntegro se o endpoint do vCenter fornecido durante a configuração do coletor estiver malformatado, inválido ou se o servidor vCenter estiver inativo no momento e não puder ser acessado. Nesse caso, você receberá uma mensagem de erro de conexão.

O procedimento a seguir pode ajudar a resolver problemas de endereço IP.

Para corrigir problemas de endereço IP do coletor

1. Obtenha o endereço IP do Agentless Collector do VMware vCenter.
2. Abra o console do Agentless Collector abrindo um navegador da web e, em seguida, digite a seguinte URL na barra de endereço: **https://<ip_address>**, onde ip_address é o endereço IP do coletor. [Etapa 3: implantar o Agentless Collector](#)

3. Escolha Login e, em seguida, insira a senha do Agentless Collector, que foi configurada quando o coletor foi configurado em. [Etapa 5: Configurar o Agentless Collector](#)
4. Na página do painel do Agentless Collector, em Coleta de dados, escolha Exibir e editar na seção VMware vCenter.
5. Na página de detalhes da coleta de dados da VMware, em Servidores vCenter descobertos, anote o endereço IP na coluna vCenter.
6. Usando uma ferramenta de linha de comando separada, como ping ou traceroute, valide se o servidor vCenter associado está ativo e se o IP pode ser acessado pela VM do coletor.
 - Se o endereço IP estiver incorreto e o serviço vCenter estiver ativo, atualize o endereço IP no console do coletor e escolha Avançar.
 - Se o endereço IP estiver correto, mas o servidor vCenter estiver inativo, ative-o.
 - Se o endereço IP estiver correto e o servidor vCenter estiver ativo, verifique se ele está bloqueando conexões de rede de entrada devido a problemas de firewall. Se sim, atualize suas configurações de firewall para permitir conexões de entrada da VM coletora.

Corrigindo problemas de credenciais do vCenter

Os coletores podem entrar em um estado não íntegro se as credenciais de usuário do vCenter fornecidas ao configurar um coletor forem inválidas ou não tiverem privilégios de conta de leitura e exibição do vCenter.

Se você tiver problemas relacionados às credenciais do vCenter, verifique se você tem as permissões de leitura e exibição do vCenter definidas para o grupo Sistema.

Para obter informações sobre a edição de credenciais do vCenter, consulte. [Editando credenciais do VMware vCenter](#)

Corrigindo problemas de encaminhamento de dados no módulo de coleta de dados de banco de dados e análises

A página inicial do módulo de coleta de dados de banco de dados e análises no Agentless Collector exibe o status da conexão para Access to DMS e Access to S3. Se você ver Sem acesso para acesso ao DMS e Acesso ao S3, configure o encaminhamento de dados. Para ter mais informações, consulte [Configurar o encaminhamento de dados](#).

Se você tiver esse problema depois de configurar o encaminhamento de dados, verifique se o módulo de coleta de dados pode acessar a Internet. Em seguida, certifique-se de ter adicionado as políticas DMS CollectorPolicy e FleetAdvisorS3Policy ao seu usuário do IAM. Para ter mais informações, consulte [Etapa 1: criar um usuário do IAM para o Agentless Collector](#).

Se seu módulo de coleta de dados não conseguir se conectar AWS, forneça acesso externo aos seguintes domínios.

- `dms.your-home-region.amazonaws.com`
- `s3.amazonaws.com`

Corrigindo problemas de conexão no módulo de coleta de dados de banco de dados e análise

O módulo de coleta de dados de banco de dados e análises no Agentless Collector se conecta aos seus servidores LDAP para descobrir servidores de sistema operacional em seu ambiente de dados. Em seguida, o módulo de coleta de dados se conecta aos servidores do sistema operacional para descobrir servidores de banco de dados e análises. A partir desses servidores de banco de dados, o módulo de coleta de dados reúne métricas de capacidade e desempenho. Se o módulo de coleta de dados não conseguir se conectar a esses servidores, verifique se você pode se conectar aos seus servidores.

Nos exemplos a seguir, substitua os valores *substituíveis* pelos seus valores.

- Para verificar se você pode se conectar ao seu servidor LDAP, instale o `ldap-util` pacote. Para fazer isso, execute o comando a seguir.

```
sudo apt-get install ldap-util
```

Em seguida, execute o comando a seguir.

```
ldapsearch -x -D "CN=user,CN=Users,DC=example,DC=com" -w "password" -b  
"dc=example,dc=com" -h
```

- Para verificar se você pode se conectar a um servidor do sistema operacional Linux, use os comandos a seguir.

```
ssh -i C:\Users\user\private_key.pem -p 22 username@my-linux-host.domain.com
```

Execute o exemplo anterior como administrador no Windows.

```
ssh username@my-linux-host.domain.com
```

Execute o exemplo anterior no Linux.

- Para verificar se você pode se conectar a um servidor do sistema operacional Windows, use os comandos a seguir.

```
winrs -r:[hostname or ip] -u:username -p:password cmd
```

Execute o exemplo anterior como administrador no Windows.

```
sudo apt install -y winrm  
winrm --user=username --password=password [http or https]://[hostname or ip]:[port]  
"[cmd.exe or any other CLI command]"
```

Execute o exemplo anterior no Linux.

- Para verificar se você pode se conectar a um banco de dados do SQL Server, use os comandos a seguir.

```
sqlcmd -S [hostname or IP] -U username -P 'password'  
SELECT GETDATE() AS sysdate
```

- Para verificar se você pode se conectar a um banco de dados MySQL, use os comandos a seguir.

```
mysql -u username -p 'password' -h [hostname or IP] -P [port]  
SELECT NOW() FROM DUAL
```

- Para verificar se você pode se conectar a um banco de dados Oracle, use os comandos a seguir.

```
sqlplus username/password@[hostname or IP]:port/servicename  
SELECT SYSDATE FROM DUAL
```

- Para verificar se você pode se conectar a um banco de dados PostgreSQL, use os comandos a seguir.

```
psql -U username -h [hostname or IP] -p port -d database  
SELECT CURRENT_TIMESTAMP AS sysdate
```


Se você não conseguir se conectar aos seus servidores de banco de dados e análise, certifique-se de fornecer as permissões necessárias. Para ter mais informações, consulte [Descubra seus servidores de banco de dados](#).

Suporte autônomo ao host ESX

O Agentless Collector não oferece suporte a um host ESX autônomo. O host ESX deve fazer parte da instância do vCenter Server.

Entrar em contato com AWS o Support em caso de problemas com o Agentless Collector

Se você encontrar problemas com o Application Discovery Service Agentless Collector (Agentless Collector) e precisar de ajuda, entre em contato com o [AWS Suporte](#). Você será contatado e talvez seja solicitado que envie os registros do coletor.

Para obter registros do Agentless Collector

1. Obtenha o endereço IP do Agentless Collector do VMware vCenter.
2. Abra o console da VM do coletor e faça login **ec2-user** usando a senha, **collector** conforme mostrado no exemplo a seguir.

```
username: ec2-user
password: collector
```

3. Use o comando a seguir para navegar até a pasta de registro.

```
cd /var/log/aws/collector
```

4. Compacte os arquivos de log usando os comandos a seguir.

```
sudo cp /local/agentless_collector/compose.log .
docker inspect $(docker ps --format {{.Names}}) | sudo tee docker_inspect.log >/dev/null
sudo tar czf logs_$(date '+%d-%m-%Y_%H.%M.%S').tar.gz * --exclude='db.mv*'
```

5. Copie o arquivo de log da VM do Agentless Collector.

```
scp logs*.tar.gz targetuser@targetaddress
```

6. Entregue o tar.gz arquivo ao AWS Enterprise Support.

Importação

AWS Migration HubA importação do (Migration Hub) permite importar detalhes de seu ambiente no local diretamente para o Migration Hub sem usar o Application Discovery Service Agentless Collector (Agentless Collector) ouAWSApplication Discovery Agent (Discovery Agent), para que seja possível executar a avaliação e o planejamento da migração diretamente dos dados importados. Também é possível agrupar os dispositivos como aplicativos e acompanhar o status de migração deles.

Para iniciar uma solicitação de importação

- Baixe o modelo de importação especialmente formatado, de valor separado por vírgula (CSV).
- Preencha-o com os dados do servidor local existente.
- Faça upload para o Migration Hub usando o console do Migration HubAWS CLIou uma deAWSSDKs.

Você pode enviar várias solicitações de importação. Cada solicitação é processada sequencialmente. Você pode verificar o status de suas solicitações de importação a qualquer momento, através do console ou das APIs de importação.

Depois de concluída uma solicitação de importação, você pode exibir os detalhes de registros importados individuais. Exiba dados de utilização, tags e mapeamentos de aplicativo diretamente de dentro do console do Migration Hub. Caso sejam encontrados erros durante a importação, você poderá revisar a contagem de registros bem-sucedidos e com falha e ver os detalhes do erro de cada registro com falha.

Tratamento de erros: Um link é fornecido para fazer download do log de erros e arquivos de registros com falha como arquivos CSV em um arquivo compactado. Use esses arquivos para reenviar a solicitação de importação depois de corrigir os erros.

São aplicados limites ao número de registros importados, servidores importados e registros excluídos que você pode manter. Para obter mais informações, consulte [Cotas do AWS Application Discovery Service](#)

Campos de arquivos de importação compatíveis

A importação do Migration Hub permite importar dados de qualquer fonte. Os dados fornecidos devem estar no formato compatível para um arquivo CSV e devem conter somente os campos compatíveis com os intervalos compatíveis com esses campos.

Um asterisco ao lado de um nome de campo de importação na tabela a seguir indica que é um campo obrigatório. Cada registro do arquivo de importação deve ter, pelo menos, um ou mais desses campos obrigatórios preenchidos para identificar um servidor ou aplicativo de forma exclusiva. Caso contrário, não ocorrerá a importação de um registro sem nenhum dos campos obrigatórios.

Note


Se você estiver usando qualquer um dos `VMware.MoRefId` ou `VMware.vCenterId`, para identificar um registro, deverá ter os dois campos no mesmo registro.

Nome do campo de importação	Descrição	Exemplos
ExternalId*	Identificador personalizado que permite que você marque cada registro como exclusivo. Por exemplo, ExternalId pode ser o ID do inventário do servidor em seu datacenter.	ID de inventário 1 Servidor 2 ID CMBD 3
SMBiosId	ID de BIOS de gerenciamento de sistema (SMBIOS).	
IPAddress*	Lista delimitada por vírgulas de endereços IP do servidor, entre aspas.	192.0.0.2 "10.12.31.233, 10.12.32.11"
MACAddress*	Lista delimitada por vírgulas do endereço MAC do servidor, entre aspas.	00:1B:44:11:3A:B7 "00-15-E9-2B-99-3C, 00-14-22-01-23-45"

Nome do campo de importação	Descrição	Exemplos
HostName*	O nome de host do servidor. É recomendável usar o nome de domínio totalmente qualificado (FQDN) para esse valor.	ip-1-2-3-4 localhost.domain
VMware.MoRefId*	O ID de referência do objeto gerenciado Deve ser fornecido com um VMware.CenterId.	
VMware.vCenterId*	Identificador exclusivo da máquina virtual. Deve ser fornecido com um VMware.MoRefId.	
CPU.NumberOfProcessors	O número de CPUs.	4
CPU.NumberOfCores	O número total de núcleos físicos.	8
CPU.NumberOfLogicalCores	O número total de threads que podem ser executados simultaneamente em todas as CPUs em um servidor. Algumas CPUs oferecem suporte à execução simultânea de vários threads em um único núcleo de CPU. Nesses casos, esse número será maior do que o número de núcleos físicos (ou virtuais).	16
OS.Name	O nome do sistema operacional.	Linux Windows.Hat

Nome do campo de importação	Descrição	Exemplos
OS.Version	A versão do sistema operacional.	16.04.3 NT 6.2.8
VMware.VMName	O nome da máquina virtual.	Corp1
RAMTotalSizeInMB	O total de RAM disponível no servidor, em MB.	64 128
RAMUsedSizeInMB.avg	A quantidade média de RAM usada no servidor, em MB.	64 128
RAMUsedSizeInMB.máx	A quantidade máxima de RAM usada disponível no servidor, em MB.	64 128
CPU.UsagePct.AVG	A utilização média da CPU quando a ferramenta de descoberta estava coletando dados.	45 23.9
CPU.UsagePct.Máximo	A utilização máxima da CPU quando a ferramenta de descoberta estava coletando dados.	55.34 24
DiskReadsPerSecondInKB.avg	O número médio de leituras de disco por segundo, em KB.	1159 84506
DiskWritesPerSecondInKB.avg	O número médio de gravações de disco por segundo, em KB.	199 6197

Nome do campo de importação	Descrição	Exemplos
DiskReadsPerSecondInKB.máx	O número máximo de leituras de disco por segundo, em KB.	37892 869962
DiskWritesPerSecondInKB.máx	O número máximo de gravações de disco por segundo, em KB.	18436 1808
DiskReadsOpsPerSecond.AVG	O número médio de operações de leitura de disco por segundo.	45 28
DiskWritesOpsPerSecond.AVG	O número médio de operações de gravação de disco por segundo.	8 3
DiskReadsOpsPerSecond.Máximo	O número máximo de operações de leitura de disco por segundo.	1083 176
DiskWritesOpsPerSecond.Máximo	O número máximo de operações de gravação de disco por segundo.	535 71
NetworkReadsPerSecondInKB.avg	O número médio de operações de leitura de rede por segundo, em KB.	45 28
NetworkWritesPerSecondInKB.avg	O número médio de operações de gravação de rede por segundo, em KB.	8 3
NetworkReadsPerSecondInKB.máx	O número máximo de operações de leitura de rede por segundo, em KB.	1083 176

Nome do campo de importação	Descrição	Exemplos
NetworkWritesPerSecondInKB.máx	O número máximo de operações de gravação de rede por segundo, em KB.	535 71
Aplicações	Uma lista delimitada por vírgulas de aplicativos que incluem esse servidor, entre aspas. Esse valor pode incluir aplicativos existentes e/ou novos aplicativos que são criados na importação.	Application1 "Application2, Application3"
Etiquetas	Uma lista delimitada por vírgulas de tags formatadas como nome:valor. <div style="border: 1px solid #f08080; border-radius: 10px; padding: 10px; background-color: #fff9f9;"> <p> Important Não armazene informações confidenciais (como dados pessoais) em tags.</p> </div>	"zone:1, critical:yes" "zone:3, critical:no, zone:1"

Você pode importar dados mesmo se não tiver dados preenchidos para todos os campos definidos no modelo de importação, desde que cada registro tenha pelo menos um dos campos obrigatórios. As duplicações são gerenciadas entre várias solicitações de importação usando uma chave de correspondência externa ou interna. Se você preencher sua própria chave de correspondência, External ID, esse campo será usado para identificar os registros de forma exclusiva e importá-los. Se nenhuma chave de correspondência for especificada, a importação usará uma chave de correspondência gerada internamente derivada de algumas das colunas no modelo de importação. Para obter mais informações sobre essa correspondência, consulte [Lógica correspondente para servidores e aplicativos descobertos](#).

Note

A importação do Migration Hub não é compatível com campos fora dos definidos no modelo de importação. Todos os campos personalizados fornecidos serão ignorados e não serão importados.

Configuração de permissões de importação

Para poder importar os dados, o usuário do IAM deve ter as permissões necessárias do Amazon S3 para fazer upload (`s3:PutObject`) seu arquivo de importação para o Amazon S3 e para ler o objeto (`s3:GetObject`). Você também deve estabelecer acesso programático (para o AWS CLI) ou acesso ao console criando uma política do IAM e anexando-a ao usuário do IAM que executa importações no AWS conta.

Console Permissions

Use o procedimento a seguir para editar a política de permissões para o usuário do IAM do que fará solicitações de importação em AWS conta usando o console.

Para editar as políticas gerenciadas anexadas a um usuário

1. Faça login no AWS Management Console e abra o console do IAM em <https://console.aws.amazon.com/iam/>.
2. No painel de navegação, escolha Usuários.
3. Escolha o nome do usuário cuja política de permissões você deseja alterar.
4. Selecione a guia Permissions (Permissões) e escolha Add permissions (Adicionar permissões).
5. Selecione Attach existing policies directly (Associar políticas existentes diretamente) e Create policy (Criar política).
 - a. Na página Create policy (Criar política) aberta, escolha JSON e cole-a na seguinte política. Lembre-se de substituir o nome do bucket pelo nome real do bucket para o qual o usuário do IAM fará upload dos arquivos de importação.

```
{  
  "Version": "2012-10-17",  
  "Statement": [  

```

```

{
  "Effect": "Allow",
  "Action": [
    "s3:GetBucketLocation",
    "s3:ListAllMyBuckets"
  ],
  "Resource": "*"
},
{
  "Effect": "Allow",
  "Action": ["s3:ListBucket"],
  "Resource": ["arn:aws:s3:::importBucket"]
},
{
  "Effect": "Allow",
  "Action": [
    "s3:PutObject",
    "s3:GetObject",
    "s3:DeleteObject"
  ],
  "Resource": ["arn:aws:s3:::importBucket/*"]
}
]
}

```

- b. Escolha Review policy (Revisar política).
 - c. Forneça à sua política um novo Name (Nome) e uma descrição opcional antes de revisar o resumo da política.
 - d. Escolha Create policy (Criar política).
6. Retorne para oConceda permissõesPágina do console do IAM para o usuário do que fará solicitações de importação emAWSconta.
 7. Atualize a tabela de políticas e procure o nome da política que você acabou de criar.
 8. Selecione Next (Próximo): Análise.
 9. Escolha Add permissions (Adicionar permissões).

Agora que você adicionou a política ao usuário do IAM, você está pronto para iniciar o processo de importação.

AWS CLI Permissions

Use o procedimento a seguir para criar as políticas gerenciadas necessárias para conceder a um usuário do IAM as permissões para fazer solicitações de importação de dados usando a AWS CLI.

Para criar e anexar as políticas gerenciadas

1. Usar `aws iam create-policy` AWS CLI para criar uma política do IAM com as permissões a seguir. Lembre-se de substituir o nome do bucket pelo nome real do bucket para o qual o usuário do IAM fará upload dos arquivos de importação.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": ["s3:ListBucket"],
      "Resource": ["arn:aws:s3:::importBucket"]
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject"
      ],
      "Resource": ["arn:aws:s3:::importBucket/*"]
    }
  ]
}
```

Para obter mais informações sobre o uso desse comando, consulte [create-policy](#) no AWS CLI Referência de comando.

2. Usar `aws iam create-policy` AWS CLI para criar uma política adicional do IAM com as permissões a seguir.

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

```

    "Action": [
      "discovery:ListConfigurations",
      "discovery:CreateApplication",
      "discovery:UpdateApplication",
      "discovery:AssociateConfigurationItemsToApplication",
      "discovery:DisassociateConfigurationItemsFromApplication",
      "discovery:GetDiscoverySummary",
      "discovery:StartImportTask",
      "discovery:DescribeImportTasks",
      "discovery:BatchDeleteImportData"
    ],
    "Resource": "*"
  }
]
}

```

3. Usar `aaws iam attach-user-policy` AWS CLI para associar as políticas que você criou nas duas etapas anteriores ao usuário do IAM que executará solicitações de importação em AWS conta usando o AWS CLI. Para obter mais informações sobre o uso desse comando, consulte [attach-user-policy](#) no AWS CLI Referência de comando.

Agora que você adicionou as políticas ao usuário do IAM, você está pronto para iniciar o processo de importação.

Lembre-se de que, quando o usuário do IAM faz upload de objetos para o bucket do Amazon S3 especificado, ele deve deixar as permissões padrão para os objetos definidos para que o usuário possa ler o objeto.

Carregar o arquivo de importação para o Amazon S3

Em seguida, você deve fazer upload do arquivo de importação em formato CSV para o Amazon S3 para que ele possa ser importado. Antes de começar, você deve ter um bucket do Amazon S3 que armazenará o arquivo de importação criado e/ou escolhido antecipadamente.

Console S3 Upload

Para carregar o arquivo de importação para o Amazon S3

1. Faça login no AWS Management Console e abra o console do Amazon S3 em <https://console.aws.amazon.com/s3/>.

2. Na lista Bucket name (Nome do bucket), escolha o nome do bucket no qual você deseja fazer upload do objeto.
3. Escolha Upload (Carregar).
4. Na caixa de diálogo Upload (Fazer upload), escolha Add files (Adicionar arquivos) para escolher o arquivo a ser carregado.
5. Escolha um arquivo para carregar e, em seguida, escolha Open (Abrir).
6. Escolha Upload (Carregar).
7. Assim que o arquivo tiver sido carregado, escolha o nome do seu objeto de arquivo de dados do painel do bucket.
8. Na guia Overview (Visão geral) da página de detalhes do objeto, copie o Object URL (URL do objeto). Você precisará disso ao criar sua solicitação de importação.
9. Vá para a importação no console do Migration Hub, conforme descrito em [Importação de dados](#). Em seguida, cole o URL do objeto no campo URL do objeto do Amazon S3 campo.

AWS CLI S3 Upload

Para carregar o arquivo de importação para o Amazon S3

1. Abra uma janela de terminal e navegue até o diretório onde o arquivo de importação está salvo.
2. Digite o comando

```
aws s3 cp ImportFile.csv s3://BucketName/ImportFile.csv
```

3. Isso retorna os seguintes resultados:

```
upload: .\ImportFile.csv to s3://BucketName/ImportFile.csv
```

4. Copie o caminho completo do objeto Amazon S3 do Amazon S3 que foi retornado. Você precisará disso ao criar sua solicitação de importação.

Importação de dados

Depois de fazer download do modelo de importação do console do Migration Hub e preenchê-lo com os dados existentes do servidor no local, você está pronto para começar a importar os dados para o

Migration Hub. As instruções a seguir descrevem duas maneiras de fazer isso, usando o console ou chamadas de API por meio da AWS CLI.

Console Import

Inicie a importação de dados no Ferramentas do console do Migration Hub.

Para iniciar a importação de dados

1. No painel de navegação, em Discover (Descobrir), selecione Tools (Ferramentas).
2. Se você ainda não tiver um modelo de importação preenchido, faça download do modelo escolhendo import template (importar modelo) na caixa Import (Importar). Abra o modelo baixado e preencha-o com seus dados existentes de servidor no local. Você também pode fazer download do modelo de importação do nosso bucket do Amazon S3 do em https://s3.us-west-2.amazonaws.com/templates-7cfcf56-bd96-4b1c-b45b-a5b42f282e46/import_template.csv
3. Para abrir o Importação página, escolha Importação no Importação (Criar snapshot final?).
4. Under Nome da importação, especifique um nome para a importação.
5. Preencha o URL do objeto do Amazon S3 campo. Para executar essa etapa, você precisará fazer upload do arquivo de dados de importação para o Amazon S3. Para obter mais informações, consulte [Carregar o arquivo de importação para o Amazon S3](#)
6. Selecione Import (Importar) na área inferior direita. Isso abrirá a página Imports (Importações) onde você pode ver sua importação e o status listado na tabela.

Depois de seguir o procedimento anterior para iniciar a importação de dados, a página Imports (Importações) mostrará detalhes de cada solicitação de importação, incluindo seu status de andamento, a hora de conclusão e o número de registros bem-sucedidos ou com falha com a capacidade de fazer download desses registros. Nessa tela, você também pode navegar até a página Servers (Servidores) em Discover (Descobrir) para ver os dados importados reais.

Na página Servers (Servidores), você pode ver uma lista de todos os servidores (dispositivos) que são descobertos junto com o nome de importação. Quando você navega a partir do Importações (histórico de importação) selecionando o nome da importação listada na Name (Nome), você será direcionado para o Servidores página em que um filtro é aplicado com base no conjunto de dados da importação selecionada. Então, você só vê os dados pertencentes a essa importação específica.

O arquivo está em um formato .zip e contém dois arquivos, `errors-file` e `failed-entries-file`. O arquivo de erros contém uma lista de mensagens de erro associadas a cada linha com falha e o nome da coluna associado de seu arquivo de dados que não foi importado. Você pode usar esse arquivo para identificar rapidamente os problemas ocorridos. O arquivo de entradas com falha inclui cada linha e todas as colunas fornecidas que falharam. Você pode fazer as alterações destacadas no arquivo de erros nesse arquivo e tentar importá-lo novamente com as informações corrigidas.

AWS CLI Import

Para iniciar o processo de importação de dados da AWS CLI, primeiro é necessário instalar a AWS CLI em seu ambiente. Para obter mais informações, consulte [Instalar o AWS Interface da linha de comando](#) no AWS Command Line Interface Guia do usuário do.

Note

Se você ainda não tiver um modelo de importação preenchido, faça download do modelo de importação de nosso bucket do Amazon S3 do aqui: https://s3.us-west-2.amazonaws.com/templates-7cfcf56-bd96-4b1c-b45b-a5b42f282e46/import_template.csv

Para iniciar a importação de dados

1. Abra uma janela do terminal e digite o seguinte comando:

```
aws discovery start-import-task --import-url s3://BucketName/ImportFile.csv --  
name ImportName
```

2. Isso criará a tarefa de importação e retornará as seguintes informações de status:

```
{  
  "task": {  
    "status": "IMPORT_IN_PROGRESS",  
    "applicationImportSuccess": 0,  
    "serverImportFailure": 0,  
    "serverImportSuccess": 0,  
    "name": "ImportName",  
    "importRequestTime": 1547682819.801,  
    "applicationImportFailure": 0,  
    "clientRequestToken": "EXAMPLE1-abcd-1234-abcd-EXAMPLE1234",
```

```
    "importUrl": "s3://BucketName/ImportFile.csv",  
    "importTaskId": "import-task-EXAMPLE1229949eabfEXAMPLE03862c0"  
  }  
}
```

Acompanhando suas solicitações de importação Migration Hub

Você pode acompanhar o status de suas solicitações de importação do Migration Hub usando o console, AWS CLI, ou um dos AWS SDKs.

Console Tracking

Do Importações no console do Migration Hub, você encontrará os seguintes elementos.

- **Name (Nome)**— O nome da solicitação de importação.
- **ID de importação**— O ID exclusivo da solicitação de importação.
- **Horário de importação**— a data e a hora em que a solicitação de importação foi criada.
- **Status da importação**— O status da solicitação de importação. Pode ter um dos valores a seguir:
 - **Importação de**— Este arquivo de dados está sendo importado no momento.
 - **Importado**— O arquivo de dados inteiro foi importado com êxito.
 - **Importado com erros**— Um ou mais registros do arquivo de dados não foram importados. Para resolver seus registros com falha, escolha **Download failed records** (Fazer download de registros com falha) para a tarefa de importação e corrija os erros no arquivo csv de entradas com falha e faça a importação novamente.
 - **Falha na importação**— Nenhum registro do arquivo de dados foi importado. Para resolver seus registros com falha, escolha **Download failed records** (Fazer download de registros com falha) para a tarefa de importação e corrija os erros no arquivo csv de entradas com falha e faça a importação novamente.
- **Registros importados**— O número de registros em um arquivo de dados específico que foram importados com êxito.
- **Registros com falha**— o número de registros em um arquivo de dados específico que não foram importados.

CLI Tracking

Você pode monitorar o status de suas tarefas de importação com o comando `aws discovery describe-import-tasks` da AWS CLI.

1. Abra uma janela do terminal e digite o seguinte comando:

```
aws discovery describe-import-tasks
```

2. Isso retornará uma lista de todas as suas tarefas de importação no formato JSON completas com status e outras informações relevantes. Você também pode filtrar resultados para retornar um subconjunto de suas tarefas de importação.

Ao monitorar suas tarefas de importação, você pode descobrir que o valor `serverImportFailure` retornado é maior do que zero. Quando isso acontece, o arquivo de importação tinha uma ou mais entradas que não puderam ser importadas. Isso pode ser resolvido com o download de arquivo de registros com falha, revisando os arquivos e outra solicitação de importação com o arquivo `failed-entries.csv` modificado.

Depois de criar sua tarefa de importação, você pode executar ações adicionais para ajudar a gerenciar e monitorar a migração de dados. Por exemplo, é possível fazer download de um arquivo de registros com falha para uma solicitação específica. Para obter informações sobre como usar o arquivo de registros com falha para resolver problemas de importação, consulte [Solução de problemas de registros de importação com falha](#).

Visualize, exporte e explore os dados descobertos

Coletor sem agente do Application Discovery Service (coletor sem agente) eAWSO Discovery Agent (Discovery Agent) fornece dados de desempenho do sistema com base na média e no pico de utilização. Você pode usar os dados de desempenho do sistema coletados para realizar um alto nível de custo total de propriedade (TCO). Os agentes de descoberta coletam dados mais detalhados, incluindo dados de séries temporais para informações de desempenho do sistema, conexões de rede de entrada e saída e processos em execução no servidor. Você pode usar esses dados para saber quais são as dependências de rede entre servidores, bem como agrupar os servidores relacionados como aplicativos para planejamento de migração.

Nesta seção, você encontrará instruções sobre como visualizar e trabalhar com dados descobertos pelo Agentless Collector e pelo Discovery Agent a partir do console e doAWS CLI.

Tópicos

- [Visualize os dados coletados usando o console do Migration Hub](#)
- [A tabela deve estar vazia](#)
- [Exploração de dados no Amazon Athena](#)

Visualize os dados coletados usando o console do Migration Hub

Tanto para o Application Discovery Service Agentless Collector (Agentless Collector) quanto para oAWS Discovery Agent (Discovery Agent), após o início do processo de coleta de dados, você pode usar o console para visualizar os dados coletados sobre seus servidores e VMs. Os dados aparecem no console aproximadamente 15 minutos após o início da coleta de dados. Você também pode visualizar esses dados no formato CSV exportando os dados coletados fazendo chamadas de API usandoAWS CLI o. A exportação de dados coletados é abordada na próxima seção [A tabela deve estar vazia](#).

Como exibir dados coletados de servidores descobertos

1. No painel de navegação do console, selecione Servers (Servidores). Os servidores descobertos aparecem na lista de servidores.
2. Para obter detalhes sobre os dados coletados, clique no link do nome do servidor na coluna Server info (Informações do servidor). Em seguida, será exibida uma tela que descreve informações detalhadas, como informações do sistema, métricas de desempenho e muito mais.

Para saber mais sobre como usar o console para visualizar, classificar e marcar servidores descobertos por seus Agentless Collectors ou Discovery Agents, consulte [AWS Application Discovery Service Demonstrações do console](#).

O banco de dados Agentless Collector e o módulo de coleta de dados analíticos carregam os dados coletados para o bucket do Amazon S3. Você pode visualizar os dados desse bucket no console do AWS DMS.

Para visualizar os dados coletados sobre bancos de dados e servidores de análise descobertos

1. Faça login no AWS Management Console e abra o console do AWS DMS em <https://console.aws.amazon.com/dms/v2/>.
2. Escolha Inventário em Descobrir. A página Inventário é aberta e exibe uma lista dos servidores de banco de dados e análise descobertos.

Lógica correspondente para servidores e aplicativos descobertos

AWS Application Discovery Service (Application Discovery Service) tem uma lógica de correspondência integrada que identifica quando os servidores que ele descobre correspondem às entradas existentes. Quando essa lógica encontra uma correspondência, ela atualiza as informações do servidor descoberto já existente com novos valores.

Essa lógica de correspondência manipula servidores duplicados de várias fontes, incluindo importação AWS Migration Hub (Migration Hub), Application Discovery Service Agentless Collector (Agentless Collector), AWS Application Discovery Agent (Discovery Agent) e outras ferramentas de migração. Para obter mais informações sobre a importação do Migration Hub, consulte [Importação do Migration Hub](#).

Quando ocorre a descoberta de um servidor, cada entrada é comparada com registros importados anteriormente para garantir que o servidor importado ainda não exista. Se nenhuma correspondência for encontrada, um novo registro será criado e um novo identificador exclusivo do servidor será atribuído. Se uma correspondência for encontrada, uma nova entrada ainda será criada, mas será atribuído o mesmo identificador exclusivo que o do servidor existente. Ao visualizar esse servidor no console do Migration Hub, você só encontra uma entrada exclusiva para o servidor.

Os atributos do servidor associados a essa entrada são mesclados para mostrar valores de atributo de um registro anteriormente disponível, bem como o registro recém-importado. Se houver mais de um valor para um determinado atributo de servidor de várias fontes, por exemplo, dois valores diferentes no Total RAM associados a um determinado servidor descoberto com importação e

também pelo Discovery Agent, o valor que foi atualizado mais recentemente será mostrado no registro correspondente do servidor.

Campos correspondentes

Os seguintes campos são usados para fazer a correspondência de servidores quando ferramentas de descoberta são usadas.

- `ExternalId`— Esse é o campo principal usado para combinar servidores. Se o valor nesse campo for idêntico a outro `ExternalId` em outra entrada, o Application Discovery Service corresponderá às duas entradas, independentemente de os outros campos coincidirem ou não.
- `IPAddress`
- `HostName`
- `MacAddress`
- `VMware.MoRefId` e `VMware.vCenterId`— Esses dois valores devem ser idênticos aos respectivos campos em outra entrada para que o Application Discovery Service realize uma correspondência.

A tabela deve estar vazia

Tanto para o Application Discovery Service Agentless Collector (Agentless Collector) quanto para o AWS Application Discovery Agent (Discovery Agent), após o início do processo de coleta de dados, você pode exportar os dados coletados sobre seus servidores e VMs. Esses dados podem ser exportados interagindo com o console ou fazendo chamadas de API por meio do AWS CLI, dependendo da ferramenta de descoberta usada para coletar dados.

Clique no método de sua preferência abaixo para visualizar instruções sobre essas duas maneiras.

Exporte os dados coletados para todos os servidores usando o AWS CLI

Os dados coletados de todos os coletores sem agente e agentes de descoberta em execução em seus hosts e VMs podem ser exportados em massa usando o AWS Command Line Interface (AWS CLI). Eles devem ser instalados em seu ambiente antes de exportar os dados.

Como instalar a AWS CLI e exportar dados coletados

1. Se você ainda não tiver feito isso, instale a AWS CLI adequada ao seu tipo de SO (Windows ou Mac/Linux). Para obter instruções de instalação, consulte o [Guia AWS Command Line Interface do usuário](#).

2. Abra o prompt de comando (Windows) ou o Terminal (MAC/Linux).
 - a. Digite `aws configure` e pressione Enter.
 - b. Insira seu ID de chave de acesso AWS e chave de acesso AWS secreta.
 - c. Digite `us-west-2` no Default Region Name (Nome padrão da região).
 - d. Digite `text` no Default Output Format (Formato padrão de saída).
3. Digite o seguinte comando para gerar um ID de exportação:

```
aws discovery start-export-task
```

4. Com o ID de exportação gerado na etapa anterior, digite o seguinte comando para gerar um URL do S3 como um valor do parâmetro "configurationsDownloadUrl":

```
aws discovery describe-export-tasks --export-ids <export ID>
```

5. Copie o URL gerado na etapa anterior e cole-o em um navegador para fazer download do arquivo compactado com dados coletados sobre os servidores descobertos.

Agente de exportação coletou dados usando o console

A exportação dos dados coletados pelo agente do console é limitada a um agente, quando você está na página de detalhes de um servidor específico. Na página de detalhes, você pode encontrar os trabalhos de exportação do servidor listados na parte inferior da tela, abaixo de Exportações. Se não houver nenhuma tarefa de exportação, a tabela estará em branco. Você pode executar até cinco exportações de dados do servidor por vez.

Como exportar dados coletados de um servidor descoberto

1. No painel de navegação, selecione Servers (Servidores).
2. Na coluna Server info (Informações do servidor), clique no link do servidor para o qual você deseja exportar os dados.
3. Na seção Exports (Exportações), na parte inferior da tela, selecione Export server details (Exportar detalhes do servidor).
4. Em Export server details (Exportar detalhes do servidor), preencha os campos Start date (Data de início) e Time (Hora).

Note

O horário de início não pode ser mais de 72 horas antes da hora atual.

5. Selecione Export para iniciar o trabalho. O status inicial será In-progress (Em andamento). Para atualizá-lo, clique no ícone de atualização na seção Exports (Exportações).
6. Quando o trabalho de exportação for concluído, clique em Download (Fazer download) e salve o arquivo .zip.
7. Descompacte o arquivo salvo. Um conjunto de arquivos.csv contém os dados de exportação.

Você pode abrir os arquivos .csv no Microsoft Excel e analisar os dados exportados do servidor.

Entre os arquivos, você pode encontrar um arquivo JSON que contém dados sobre a tarefa de exportação e seus resultados.

Note

Para obter informações sobre como gerar e exportar recomendações de instâncias do Amazon Elastic Compute Cloud (Amazon EC2) no AWS Migration Hub console, consulte [Recomendações de instâncias do Amazon EC2](#) no Guia AWS Migration Hub do usuário.

Exploração de dados no Amazon Athena

A exploração de dados no Amazon Athena permite que você analise os dados coletados de todos os servidores locais descobertos pelos agentes de descoberta em um só lugar. Depois que a exploração de dados no Amazon Athena estiver habilitada no console do Migration Hub (ou usando o StartContinuousExport API) e a coleta de dados para agentes é ativada, os dados coletados pelos agentes são automaticamente armazenados em seu bucket do S3 em intervalos regulares.

Em seguida, você pode visitar o Amazon Athena para executar consultas predefinidas para analisar o desempenho do sistema de séries temporais para cada servidor, o tipo de processos que estão sendo executados em cada servidor e as dependências de rede entre servidores diferentes. Além disso, você pode escrever suas próprias consultas personalizadas usando o Amazon Athena, fazer upload de outras fontes de dados existentes, como exportações do banco de dados de gerenciamento de configuração (CMDB) e associar os servidores descobertos aos aplicativos de

negócios reais. Você também pode integrar o banco de dados do Athena com a Amazon QuickSight para visualizar as saídas da consulta e realizar análises adicionais

Etapas

1. [Habilitar a exploração de dados no Amazon Athena](#)
2. [Trabalhando com exploração de dados no Amazon Athena](#)

Habilitar a exploração de dados no Amazon Athena

A exploração de dados no Amazon Athena é habilitada ao ativar a exportação contínua usando o console do Migration Hub ou uma chamada de API do AWS CLI. Você deve ativar a exploração de dados antes de poder ver e começar a explorar seus dados descobertos no Amazon Athena.

Quando você executa a Exportação contínua da função vinculada ao serviço `AWS::ServiceRoleForApplicationDiscoveryServiceContinuousExport` é usado automaticamente pela sua conta. Para obter mais informações sobre essa função vinculada ao serviço, consulte [Permissões de função vinculada ao serviço do Application Discovery Service](#).

As instruções a seguir mostram como habilitar a exploração de dados no Amazon Athena usando o console e o AWS CLI.

Enable with the console

A exploração de dados no Amazon Athena é habilitada pela ativação implícita da exportação contínua quando você escolhe “Iniciar coleta de dados” ou clica no botão “Exploração de dados no Amazon Athena” no Coletores de dados página do console do Migration Hub.

Para permitir a exploração de dados no Amazon Athena a partir do console

1. No painel de navegação, selecione Data Collectors (Coletores de dados).
2. Clique na guia Agents (Agentes).
3. Escolha Iniciar coleta de dados, ou se você já tiver a coleta de dados ativada, clique no Exploração de dados no Amazon Athena alternar.
4. Na caixa de diálogo gerada a partir da etapa anterior, clique na caixa de seleção para concordar com os custos associados e selecione Continue (Continuar) ou Enable (Habilitar).

Note

Seus agentes agora estão trabalhando no modo de “exportação contínua”, o que permitirá que você veja e trabalhe com os dados descobertos no Amazon Athena. Na primeira vez em que isso é ativado, pode levar até 30 minutos para que seus dados apareçam no Amazon Athena.

Enable with the AWS CLI

A exploração de dados no Amazon Athena é habilitada pela ativação explícita da exportação contínua por meio de uma chamada de API do AWS CLI. Para fazer isso, a AWS CLI deve estar instalada em seu ambiente.

Para instalar o AWS CLI e habilitar a exploração de dados no Amazon Athena

1. Instale a AWS CLI no sistema operacional (Linux, macOS ou Windows). Consulte o [AWS Command Line Interface Guia do usuário do](#) para obter instruções.
2. Abra o prompt de comando (Windows) ou o Terminal (macOS/Linux).
 - a. Digite `aws configure` e pressione Enter.
 - b. Insira seu AWS ID da chave de acesso e a AWS Chave de acesso secreta.
 - c. Digite `us-west-2` no Default Region Name (Nome padrão da região).
 - d. Digite `text` no Default Output Format (Formato padrão de saída).
3. Digite o seguinte comando:

```
aws discovery start-continuous-export
```

Note

Seus agentes agora estão trabalhando no modo de “exportação contínua”, o que permitirá que você veja e trabalhe com os dados descobertos no Amazon Athena. Na primeira vez em que isso é ativado, pode levar até 30 minutos para que seus dados apareçam no Amazon Athena.

Trabalhando com exploração de dados no Amazon Athena

Depois de habilitar a exploração de dados no Amazon Athena, você pode começar a explorar e trabalhar com dados atuais detalhados que foram descobertos por seus agentes consultando os dados diretamente no Athena. Você pode usar os dados para gerar planilhas, realizar análises de custo, migrar a consulta para um programa de visualização com o objetivo de diagramar as dependências da rede e muito mais.

Os tópicos desta seção descrevem as maneiras pelas quais você pode trabalhar com seus dados no Athena para avaliar e planejar a migração de seu ambiente local para AWS.

Tópicos

- [Explorar dados diretamente no Amazon Athena](#)
- [Visualizar dados do Amazon Athena](#)
- [Consultas predefinidas para usar no Athena](#)

Explorar dados diretamente no Amazon Athena

As instruções a seguir explicam como explorar os dados do agente diretamente no console do Athena. Se você não tiver nenhum dado no Athena ou não tiver habilitado a exploração de dados no Amazon Athena, você será solicitado por uma caixa de diálogo para habilitar a exploração de dados no Amazon Athena, conforme explicado em [Habilitar a exploração de dados no Amazon Athena](#).

Para explorar os dados descobertos pelo agente diretamente no Athena

1. No console do AWS Migration Hub, escolha Servers (Servidores) no painel de navegação.
2. Para abrir o console do Amazon Athena, escolha Explore dados no Amazon Athena.
3. Na página Editor de consultas, no painel de navegação, em Banco de dados, verifique se `application_discovery_service_database` está selecionado.

Note

Em Tabelas, as tabelas a seguir representam os conjuntos de dados agrupados pelos agentes.

- `os_info_agent`
- `network_interface_agent`

- `sys_performance_agent`
- `processes_agent`
- `inbound_connection_agent`
- `outbound_connection_agent`
- `id_mapping_agent`

4. Consulte os dados no console do Amazon Athena escrevendo e executando consultas SQL no Athena Query Editor. Por exemplo, é possível usar a consulta a seguir para ver todos os endereços IP do servidor descobertos.

```
SELECT * FROM network_interface_agent;
```

Para obter mais consultas de exemplo, consulte [Consultas predefinidas para usar no Athena](#).

Visualizar dados do Amazon Athena

Para visualizar seus dados, uma consulta pode ser transferida para um programa de visualização como o Amazon QuickSight ou outras ferramentas de visualização de código aberto, como Cytoscape, yEd ou Gephi. Use essas ferramentas para renderizar diagramas de rede, gráficos de resumo e outras representações gráficas. Quando esse método é usado, você se conecta ao Athena por meio do programa de visualização para que ele possa acessar os dados coletados como uma fonte para produzir a visualização.

Para visualizar seus dados do Amazon Athena usando a Amazon QuickSight

1. Faça login no [Amazônia QuickSight](#).
2. Escolha Connect to another data source or upload a file (Conecte-se a outra fonte de dados ou faça upload de um arquivo).
3. Escolha Athena. A Nova origem de dados do Athena A caixa de diálogo é exibida.
4. Insira um nome no campo Data source name (Nome da fonte de dados).
5. Escolha Create data source.
6. Saída de seleção UMAgents-servers-ostabela no Escolha sua tabela caixa de diálogo e escolha Select.
7. Na caixa de diálogo Finalizar a criação do conjunto de dados, selecione Importar para SPICE para acelerar a análise e Visualizar.

A visualização é renderizada.

Consultas predefinidas para usar no Athena

Esta seção contém um conjunto de consultas predefinidas que executam casos de uso típicos, como análise de TCO e visualização de rede. Você pode usar essas consultas como estão ou adequá-las às suas necessidades.

Como usar uma consulta predefinida

1. No console do AWS Migration Hub, escolha Servers (Servidores) no painel de navegação.
2. Para abrir o console do Amazon Athena, escolha Explore dados no Amazon Athena.
3. Na página Editor de consultas, no painel de navegação, em Banco de dados, verifique se `application_discovery_service_database` está selecionado.
4. Escolha o sinal de adição (+) no Editor de consultas para criar uma guia para uma nova consulta.
5. Copie uma das consultas de [Consultas predefinidas](#).
6. Cole a consulta no painel de consultas da guia de nova consulta que você acabou de criar.
7. Escolha Run Query.

Consultas predefinidas

Escolha um título para ver informações sobre a consulta.

Obtenha endereços IP e nomes de host para servidores

Essa função auxiliar de exibição recupera endereços IP e nomes de host para um determinado servidor. Você pode usar essa exibição em outras consultas. Para obter informações sobre como criar uma visualização, consulte [CRIAR VISUALIZAÇÃO](#) na Guia do usuário do Amazon Athena.

```
CREATE OR REPLACE VIEW hostname_ip_helper AS
SELECT DISTINCT
  "os"."host_name"
, "nic"."agent_id"
, "nic"."ip_address"
FROM
  os_info_agent os
```

```
, network_interface_agent nic
WHERE ("os"."agent_id" = "nic"."agent_id");
```

Identifique servidores com ou sem agentes

Essa consulta pode ajudar você a realizar a validação de dados. Se você implantou agentes em uma série de servidores em sua rede, poderá usar essa consulta para saber se há outros servidores na sua rede sem agentes implantados neles. Nessa consulta, examinamos o tráfego de rede de entrada e de saída e filtramos o tráfego apenas para endereços IP privados. Ou seja, endereços IP que começam com 192, 10 ou 172.

```
SELECT DISTINCT "destination_ip" "IP Address" ,
  (CASE
    WHEN (
      (SELECT "count"(*)
      FROM network_interface_agent
      WHERE ("ip_address" = "destination_ip") ) = 0) THEN
      'no'
    WHEN (
      (SELECT "count"(*)
      FROM network_interface_agent
      WHERE ("ip_address" = "destination_ip") ) > 0) THEN
      'yes' END) "agent_running"
  FROM outbound_connection_agent
WHERE (((("destination_ip" LIKE '192.%')
  OR ("destination_ip" LIKE '10.%'))
  OR ("destination_ip" LIKE '172.%'))
UNION
SELECT DISTINCT "source_ip" "IP ADDRESS" ,
  (CASE
    WHEN (
      (SELECT "count"(*)
      FROM network_interface_agent
      WHERE ("ip_address" = "source_ip") ) = 0) THEN
      'no'
    WHEN (
      (SELECT "count"(*)
      FROM network_interface_agent
      WHERE ("ip_address" = "source_ip") ) > 0) THEN
      'yes' END) "agent_running"
  FROM inbound_connection_agent
WHERE (((("source_ip" LIKE '192.%')
  OR ("source_ip" LIKE '10.%'))
```

```
OR ("source_ip" LIKE '172.%')));
```

Analise dados de desempenho do sistema para servidores com agentes

É possível usar essa consulta para analisar o desempenho do sistema e o dados de padrão de utilização para seus servidores locais que têm agentes instalados. A consulta combina as tabelas `system_performance_agent` e `os_info_agent` para identificar o nome do host de cada servidor. Essa consulta retorna os dados de utilização de séries temporais (em intervalos de 15 minutos) para todos os servidores nos quais os agentes estão em execução.

```
SELECT "OS"."os_name" "OS Name" ,
       "OS"."os_version" "OS Version" ,
       "OS"."host_name" "Host Name" ,
       "SP"."agent_id" ,
       "SP"."total_num_cores" "Number of Cores" ,
       "SP"."total_num_cpus" "Number of CPU" ,
       "SP"."total_cpu_usage_pct" "CPU Percentage" ,
       "SP"."total_disk_size_in_gb" "Total Storage (GB)" ,
       "SP"."total_disk_free_size_in_gb" "Free Storage (GB)" ,
       ("SP"."total_disk_size_in_gb" - "SP"."total_disk_free_size_in_gb") "Used
Storage" ,
       "SP"."total_ram_in_mb" "Total RAM (MB)" ,
       ("SP"."total_ram_in_mb" - "SP"."free_ram_in_mb") "Used RAM (MB)" ,
       "SP"."free_ram_in_mb" "Free RAM (MB)" ,
       "SP"."total_disk_read_ops_per_sec" "Disk Read IOPS" ,
       "SP"."total_disk_bytes_written_per_sec_in_kbps" "Disk Write IOPS" ,
       "SP"."total_network_bytes_read_per_sec_in_kbps" "Network Reads (kbps)" ,
       "SP"."total_network_bytes_written_per_sec_in_kbps" "Network Write (kbps)"
FROM "sys_performance_agent" "SP" , "OS_INFO_agent" "OS"
WHERE ("SP"."agent_id" = "OS"."agent_id") limit 10;
```

Rastreie a comunicação de saída entre servidores com base no número da porta e nos detalhes do processo

Esta consulta obtém os detalhes sobre o tráfego de saída para cada serviço, juntamente com o número da porta e os detalhes do processo.

Antes de executar a consulta, caso ainda não tenha feito isso, você deve criar a tabela `iana_service_ports_import` que contém o banco de dados de registro de porta IANA baixado da IANA. Para obter informações sobre como criar essa tabela, consulte [Criando a tabela de importação do registro de portas IANA](#).

Depois que a tabela `iana_service_ports_import` for criada, crie duas funções auxiliares de visualização para rastrear o tráfego de saída. Para obter informações sobre como criar uma visualização, consulte [CRIAR VISUALIZAÇÃO](#) na Guia do usuário do Amazon Athena.

Como criar funções auxiliares de controle de saída

1. Abra o console do Athena em <https://console.aws.amazon.com/athena/>.
2. Criar `valid_outbound_ips_helperview`, usando a seguinte função auxiliar que lista todos os endereços IP de destino de saída distintos.

```
CREATE OR REPLACE VIEW valid_outbound_ips_helper AS
SELECT DISTINCT "destination_ip"
FROM outbound_connection_agent;
```

3. Crie a visualização `outbound_query_helper` usando a função auxiliar a seguir que determina a frequência de comunicação para o tráfego de saída.

```
CREATE OR REPLACE VIEW outbound_query_helper AS
SELECT "agent_id" ,
       "source_ip" ,
       "destination_ip" ,
       "destination_port" ,
       "agent_assigned_process_id" ,
       "count"(*) "frequency"
FROM outbound_connection_agent
WHERE (("ip_version" = 'IPv4')
       AND ("destination_ip" IN
           (SELECT *
            FROM valid_outbound_ips_helper )))
GROUP BY "agent_id", "source_ip", "destination_ip", "destination_port",
         "agent_assigned_process_id";
```

4. Depois de criar a tabela `iana_service_ports_import` e suas duas funções auxiliares, você poderá executar a seguinte consulta para obter os detalhes do tráfego de saída de cada serviço, juntamente com o número da porta e os detalhes do processo.

```
SELECT hip1.host_name "Source Host Name",
       outbound_connections_results0.source_ip "Source IP Address",
       hip2.host_name "Destination Host Name",
       outbound_connections_results0.destination_ip "Destination IP Address",
       outbound_connections_results0.frequency "Connection Frequency",
```

```

        outbound_connections_results0.destination_port "Destination Communication
Port",
        outbound_connections_results0.servicename "Process Service Name",
        outbound_connections_results0.description "Process Service Description"
FROM
    (SELECT DISTINCT o.source_ip,
        o.destination_ip,
        o.frequency,
        o.destination_port,
        ianap.servicename,
        ianap.description
    FROM outbound_query_helper o, iana_service_ports_import ianap
    WHERE o.destination_port = TRY_CAST(ianap.portnumber AS integer)) AS
outbound_connections_results0 LEFT OUTER
JOIN hostname_ip_helper hip1
    ON outbound_connections_results0.source_ip = hip1.ip_address LEFT OUTER
JOIN hostname_ip_helper hip2
    ON outbound_connections_results0.destination_ip = hip2.ip_address

```

Rastreie a comunicação de entrada entre servidores com base no número da porta e nos detalhes do processo

Esta consulta obtém informações sobre o tráfego de entrada para cada serviço, juntamente com o número da porta e os detalhes do processo.

Antes de executar esta consulta, caso ainda não tenha feito isso, você deve criar a tabela `iana_service_ports_import` que contém o banco de dados de registro de porta IANA baixado da IANA. Para obter informações sobre como criar essa tabela, consulte [Criando a tabela de importação do registro de portas IANA](#).

Depois que a tabela `iana_service_ports_import` for criada, crie duas funções auxiliares de visualização para rastrear o tráfego de entrada. Para obter informações sobre como criar uma visualização, consulte [CRIAR VISUALIZAÇÃO](#) na Guia do usuário do Amazon Athena.

Como criar funções auxiliares de controle de entrada

1. Abra o console do Athena em <https://console.aws.amazon.com/athena/>.
2. Crie a visualização `valid_inbound_ips_helper` usando a função auxiliar a seguir que lista todos os endereços IP de origem de entrada distintos.

```
CREATE OR REPLACE VIEW valid_inbound_ips_helper AS
```

```
SELECT DISTINCT "source_ip"
FROM inbound_connection_agent;
```

3. Crie a visualização `inbound_query_helper` usando a função auxiliar a seguir que determina a frequência de comunicação do tráfego de entrada.

```
CREATE OR REPLACE VIEW inbound_query_helper AS
SELECT "agent_id" ,
       "source_ip" ,
       "destination_ip" ,
       "destination_port" ,
       "agent_assigned_process_id" ,
       "count"(*) "frequency"
FROM inbound_connection_agent
WHERE (("ip_version" = 'IPv4')
      AND ("source_ip" IN
          (SELECT *
           FROM valid_inbound_ips_helper )))
GROUP BY "agent_id", "source_ip", "destination_ip", "destination_port",
         "agent_assigned_process_id";
```

4. Depois de criar a tabela `iana_service_ports_import` e suas duas funções auxiliares, você poderá executar a seguinte consulta para obter os detalhes do tráfego de entrada de cada serviço, juntamente com o número da porta e os detalhes do processo.

```
SELECT hip1.host_name "Source Host Name",
       inbound_connections_results0.source_ip "Source IP Address",
       hip2.host_name "Destination Host Name",
       inbound_connections_results0.destination_ip "Destination IP Address",
       inbound_connections_results0.frequency "Connection Frequency",
       inbound_connections_results0.destination_port "Destination Communication
Port",
       inbound_connections_results0.servicename "Process Service Name",
       inbound_connections_results0.description "Process Service Description"
FROM
  (SELECT DISTINCT i.source_ip,
                  i.destination_ip,
                  i.frequency,
                  i.destination_port,
                  ianap.servicename,
                  ianap.description
   FROM inbound_query_helper i, iana_service_ports_import ianap
```



```

WHERE i.destination_port = TRY_CAST(ianap.portnumber AS integer)) AS
inbound_connections_results0 LEFT OUTER
JOIN hostname_ip_helper hip1
  ON inbound_connections_results0.source_ip = hip1.ip_address LEFT OUTER
JOIN hostname_ip_helper hip2
  ON inbound_connections_results0.destination_ip = hip2.ip_address

```

Identifique o software em execução pelo número da porta

Esta consulta identifica o software em execução com base nos números de porta.

Antes de executar esta consulta, caso ainda não tenha feito isso, você deve criar a tabela `iana_service_ports_import` que contém o banco de dados de registro de porta IANA baixado da IANA. Para obter informações sobre como criar essa tabela, consulte [Criando a tabela de importação do registro de portas IANA](#).

Execute a consulta a seguir para identificar o software em execução com base nos números de porta.

```

SELECT o.host_name "Host Name",
       ianap.servicename "Service",
       ianap.description "Description",
       con.destination_port,
       con.cnt_dest_port "Destination Port Count"
FROM   (SELECT agent_id,
              destination_ip,
              destination_port,
              Count(destination_port) cnt_dest_port
        FROM   inbound_connection_agent
        GROUP  BY agent_id,
                 destination_ip,
                 destination_port) con,
       (SELECT agent_id,
              host_name,
              Max("timestamp")
        FROM   os_info_agent
        GROUP  BY agent_id,
                 host_name) o,
       iana_service_ports_import ianap
WHERE  ianap.transportprotocol = 'tcp'
       AND con.destination_ip NOT LIKE '172%'
       AND con.destination_port = ianap.portnumber

```

```

    AND con.agent_id = o.agent_id
ORDER BY cnt_dest_port DESC;

```

Criando a tabela de importação do registro de portas IANA

Algumas das consultas predefinidas exigem uma tabela chamada `iana_service_ports_import` que contém informações baixadas da IANA (Internet Assigned Numbers Authority).

Como criar a tabela `iana_service_ports_import`

1. Faça download do arquivo CSV do banco de dados de registro de porta IANA de [Service Name and Transport Protocol Port Number Registry](#) em [iana.org](#).
2. Faça upload do arquivo no Amazon S3. Para obter mais informações, consulte [Como fazer upload de arquivos e pastas em um bucket do S3?](#)
3. Crie uma nova tabela no Athena chamada `iana_service_ports_import`. Para obter instruções, consulte [Criar uma tabela](#) na Guia do usuário do Amazon Athena. No exemplo a seguir, você precisa substituir `my_bucket_name` pelo nome do bucket do S3 para o qual você fez upload do arquivo CSV na etapa anterior.

```

CREATE EXTERNAL TABLE IF NOT EXISTS iana_service_ports_import (
    ServiceName STRING,
    PortNumber INT,
    TransportProtocol STRING,
    Description STRING,
    Assignee STRING,
    Contact STRING,
    RegistrationDate STRING,
    ModificationDate STRING,
    Reference STRING,
    ServiceCode STRING,
    UnauthorizedUseReported STRING,
    AssignmentNotes STRING
)
ROW FORMAT SERDE 'org.apache.hadoop.hive.serde2.lazy.LazySimpleSerDe'
WITH SERDEPROPERTIES (
    'serialization.format' = ',',
    'quoteChar' = '"',
    'field.delim' = ','
) LOCATION 's3://my_bucket_name/'
TBLPROPERTIES ('has_encrypted_data'='false',"skip.header.line.count"="1");

```

AWS Application Discovery Service Demonstrações do console

AWS Application Discovery Service (Application Discovery Service) está integrado com AWS Migration Hub (Migration Hub) e os clientes podem visualizar e gerenciar seus coletores de dados, servidores e aplicativos no Migration Hub. Ao usar o console do Application Discovery Service, você é redirecionado para o console do Migration Hub. Trabalhar com o console do Migration Hub não requer etapas ou configurações adicionais de sua parte.

Nesta seção, você pode descobrir como gerenciar e monitorar o Application Discovery Service Agentless Collector (Agentless Collector) e AWS Agente de descoberta de aplicativos (Agente de descoberta) usando o console.

Tópicos

- [Painel principal](#)
- [Ferramentas de coleta de dados](#)
- [Visualize, exporte e explore dados do servidor](#)

Painel principal

Para ver o painel principal, escolha [Painel do AWS Migration Hub](#) no painel de navegação do console (Migration Hub). No painel principal do Migration Hub, você pode visualizar estatísticas de alto nível sobre servidores, aplicativos e coletores de dados, como o Application Discovery Service Agentless Collector (Agentless Collector) e AWS Agente de descoberta de aplicativos (agente de descoberta).

Painel principal

O painel principal reúne dados dos painéis Discover (Descobrir) e Migrate (Migrar) em um local central. Ele tem quatro painéis de informações e status e uma lista de links para acesso rápido. Com os painéis, você pode ver um resumo do status dos aplicativos atualizados mais recentemente. Você também pode obter acesso rápido a qualquer um dos seus aplicativos, obter uma visão geral dos aplicativos em diferentes estados e acompanhar o progresso da migração ao longo do tempo.

Para ver o painel principal, escolha [Painel do painel de navegação](#), do lado esquerdo da página inicial do console do Migration Hub.

Ferramentas de coleta de dados

Coletor sem agente do Application Discovery Service (coletor sem agente) e AWS Application Discovery Agent (Discovery Agent) são as ferramentas de coleta de dados que o AWS Application Discovery Service (Application Discovery Service) é usado para ajudar você a descobrir sua infraestrutura existente. Os seguintes tópicos explicam como baixar e implantar essas ferramentas de coleta de dados de descoberta, [Introdução ao Agentless Collector](#) e [AWS Agente de descoberta de aplicativos](#).

Essas ferramentas de coleta de dados armazenam seus dados no repositório do Application Discovery Service, fornecendo detalhes sobre cada servidor e os processos em execução neles. Quando qualquer uma dessas ferramentas é implantada, você pode iniciar, interromper e visualizar os dados coletados do AWS Migration Hub Console (Migration Hub).

Tópicos

- [Iniciando e interrompendo coletores de dados](#)
- [Visualização e classificação de coletores de dados](#)

Iniciando e interrompendo coletores de dados

Depois do AWS Application Discovery Agent (Discovery Agent) está implantado, você pode iniciar ou interromper o processo de coleta de dados no Coletor de dados página do AWS Migration Hub Console (Migration Hub).

Como iniciar ou interromper ferramentas de coleta de dados

1. Usar a conta da 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, em Descubra, escolha Coletor de dados.
3. Clique na guia Agents (Agentes).
4. Marque a caixa de seleção da ferramenta de coleta que você deseja iniciar ou interromper.
5. Selecione Start data collection (Iniciar coleta de dados) ou Stop data collection (Interromper coleta de dados).

Visualização e classificação de coletores de dados

Se você implantou muitos coletores de dados, poderá classificar a lista exibida de coletores implantados na página do console do Coletor de dados. Você classifica a lista aplicando filtros na barra de pesquisa. Você pode pesquisar e filtrar usando a maioria dos critérios especificados na lista Data Collectors (Coletores de dados).

A tabela a seguir mostra os critérios de pesquisa que você pode usar, incluindo operadores, valores e uma definição dos valores.

Critério de pesquisa	Operador	Valor: Definição
ID do Agente	==	Qualquer ID de agente selecionada na lista pré-preenchida da qual uma ferramenta de coleta está instalada.
Hostname	==	De agentes; qualquer nome de host selecionado na lista pré-preenchida em que um agente foi instalado.
	!=	
Collection status	==	Iniciado: Os dados estão sendo coletados e enviados para o Application Discovery Service
	!=	Início agendado: A coleta de dados está programada para iniciar. Os dados serão enviados para o Application Discovery Service no próximo ping, e o status mudará para Iniciado.
		Interrompido: Os dados não estão sendo coletados ou enviados para o Application Discovery Service.

Critério de pesquisa	Operador	Valor: Definição
		Interromper A coleta de dados está programada para ser interrompida. Os dados deixarão de ser enviados para o Application Discovery Service no próximo ping e o status mudará para Interrompido.

Critério de pesquisa	Operador	Valor: Definição
Integridade	== !=	<p>Integridade A coleta de dados não está ativada. A ferramenta está funcionando normalmente.</p> <p>Inintegridade A ferramenta está em estado de erro. Os dados não estão sendo coletados ou não relatados.</p> <p>Desconhecido Nenhuma conexão estabelecida em mais de uma hora.</p> <p>Desligamento A ferramenta comunicou “desligamento” pela última vez devido ao desligamento de um sistema, serviço ou daemon. Se uma reinicialização ou atualização de ferramenta ocorreu, o status será alterado para outro estado no primeiro ciclo de relatórios.</p> <p>Execução do: A coleta de dados está ativada. A ferramenta está funcionando normalmente.</p>
IP address	== !=	<p>Qualquer endereço IP selecionado na lista pré-preenchida em que uma ferramenta de coleta foi instalada.</p>

A tabela a seguir mostra os critérios de pesquisa que você pode usar Coletor etor sem agentes, incluindo operadores, valores e uma definição dos valores.

Critério de pesquisa	Operador	Valor: Definição
ID	==	Qualquer ID de coletor sem agente selecionada na lista pré-preenchida da qual uma ferramenta de coleta está instalada.
Hostname	== !=	Para coletores sem agente, qualquer nome de host selecionado na lista pré-preenchida de hosts em que um coletor sem agente está instalado.
Status	== !=	<p>Coletor de dados A coleta de dados está ativada. A ferramenta está funcionando normalmente.</p> <p>Pronto para configurar — A coleta de dados não está ativada. A ferramenta está funcionando normalmente.</p> <p>Requer atenção— A ferramenta está em um estado de erro e precisa de atenção.</p> <p>Desconhecido Nenhuma conexão estabelecida em mais de uma hora.</p> <p>Desligar: A ferramenta comunicou “desligamento” pela última vez devido ao</p>

Critério de pesquisa	Operador	Valor: Definição
		desligamento de um sistema, serviço ou daemon. Se uma reinicialização ou atualização de ferramenta ocorreu, o status será alterado para outro estado no primeiro ciclo de relatórios.
IP address	== !=	Qualquer endereço IP selecionado na lista pré-preenchida em que uma ferramenta de coleta foi instalada.

Como classificar coletores de dados aplicando filtros de pesquisa

1. Usar a doAWSconta daAWS Management Console abra o console do Migration Hub em <https://console.aws.amazon.com/migrationhub/>.
2. No painel de navegação do console do Migration Hub, em Descubra, escolha Coletor etor etor de dados.
3. Escolha entre os Coletor etor sem agentes ou Agentes Guia.
4. Clique dentro da barra de pesquisa e escolha um critério de pesquisa da lista.
5. Escolha um operador da lista seguinte.
6. Escolha um valor da última lista.

Visualize, exporte e explore dados do servidor

A página Servers (Servidores) fornece dados da configuração e do desempenho do sistema sobre cada instância de servidor conhecida nas ferramentas de coleta de dados. Você pode visualizar informações do servidor, classificar servidores com filtros, marcar com tags servidores com pares de chave/valor e exportar informações detalhadas do sistema e do servidor.

Tópicos

- [Visualização e classificação de servidores](#)

- [Marcar servidores](#)
- [Exportando dados do servidor](#)
- [Exploração de dados no Athena](#)
- [Aplicações](#)

Visualização e classificação de servidores

Você pode visualizar informações sobre os servidores descobertos pelas ferramentas de coleta de dados e classificá-los usando filtros.

Visualizando servidores

Você pode obter uma visão geral e uma visão detalhada dos servidores descobertos pelas ferramentas de coleta de dados.

Como visualizar servidores descobertos

1. Usar a doAWSconta daAWS Management Consolee abra o console do Migration Hub em <https://console.aws.amazon.com/migrationhub/>.
2. No painel de navegação do console do Migration Hub, emDescubra, escolhade aplicativos. Os servidores descobertos aparecem na lista de servidores.
3. Para obter mais detalhes sobre um servidor, escolha o link dele na coluna Server info (Informações do servidor). Desse modo, uma tela que descreve o servidor será exibida.

A tela de detalhes do servidor exibe informações do sistema e métricas de desempenho. Você também pode encontrar um botão para exportar as dependências de rede e informações de processos. Para exportar informações detalhadas sobre servidores, consulte [Exportando dados do servidor](#).

Classificando servidores com filtros de pesquisa

Para encontrar servidores específicos facilmente, aplique filtros de pesquisa para classificar todos os servidores descobertos pelas ferramentas de coleta. Você pode pesquisar e filtrar vários critérios.

Como classificar servidores aplicando filtros de pesquisa

1. Usar a doAWSconta daAWS Management Consolee abra o console do Migration Hub em <https://console.aws.amazon.com/migrationhub/>.

2. No painel de navegação do console do Migration Hub, em **Descubra**, escolha aplicativos.
3. Clique dentro da barra de pesquisa e escolha um critério de pesquisa da lista.
4. Escolha um operador da lista seguinte.
5. Digite um valor, com distinção entre letras maiúsculas e minúsculas, para o critério de pesquisa selecionado e pressione **Enter**.
6. Vários filtros podem ser aplicados repetindo as etapas 2 a 4.

Marcar servidores

Para ajudar no planejamento da migração e na organização, crie várias tags para cada servidor. As Tags são os pares de chave/valor definidos pelo usuário que podem armazenar quaisquer dados ou metadados personalizados sobre servidores. Você pode marcar um servidor individual ou vários servidores em uma única operação. AWS Application Discovery Service As tags (Application Discovery Service) são semelhantes às AWS tags, mas os dois tipos de tag não podem ser usados de forma intercambiável.

É possível adicionar ou remover várias tags de um ou mais servidores na página principal de Servers (Servidores). Em uma página de detalhes do servidor, você pode adicionar ou remover uma ou mais tags do servidor selecionado. Você pode fazer qualquer tipo de tarefa de marcação com tags que envolva vários servidores ou tags em uma única operação. Também é possível remover as tags.

Como adicionar tags a um ou mais servidores

1. Usar a conta da 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, em **Descubra**, escolha aplicativos.
3. Na coluna **Server info** (Informações do servidor), clique no link do servidor ao qual você deseja adicionar tags. Para adicionar tags a mais de um servidor por vez, clique em dentro das caixas de seleção de vários servidores.
4. Escolha **Adicione tag** e, em seguida, escolha **Adicione um novo tag**.
5. Na caixa de diálogo, digite uma chave no campo **Chave** e, opcionalmente, um valor no campo **Valor**.

Adicione mais tags escolhendo **Adicione um novo tag** adicionando mais informações.

6. Escolha **Save** (Salvar).

Como remover tags de um ou mais servidores

1. Usar a doAWSconta daAWS Management Consoleabra o console do Migration Hub em<https://console.aws.amazon.com/migrationhub/>.
2. No painel de navegação do console do Migration Hub, emDescubra, escolhade aplicativos.
3. Na coluna Server info (Informações do servidor), clique no link do servidor do qual você deseja remover tags. Marque as caixas de seleção de vários servidores para remover tags de mais de um servidor por vez.
4. EscolhaRemover tags.
5. Selecione cada etiqueta que você deseja remover.
6. Selecione a opção Confirm (Confirmar).

Exportando dados do servidor

Para exportar as dependências de rede e as informações do processo de um servidor por vez, use a tela de detalhes desse servidor. Você pode encontrar os trabalhos de exportação de um servidor em uma tabela localizada na seção Exports (Exportações) da tela de detalhes do servidor. Se ainda não houver trabalhos de exportação, a tabela estará vazia. É possível exportar simultaneamente até cinco conjuntos de dados.


Note

A exportação de dados do servidor do console só está disponível para dados coletados por um agente em execução nesse servidor. Se você quiser exportar dados em massa para todos os servidores em que os agentes foram instalados, consulte[Exploração de dados no Amazon Athena](#).

Como exportar dados detalhados do servidor

1. Usar a doAWSconta daAWS Management Consoleabra o console do Migration Hub em<https://console.aws.amazon.com/migrationhub/>.
2. No painel de navegação do console do Migration Hub, emDescubra, escolhade aplicativos.
3. Na coluna Server info (Informações do servidor), clique no ID do servidor para o qual você deseja exportar os dados.

4. Na seção Exports (Exportações), na parte inferior da tela, selecione Export server details (Exportar detalhes do servidor).
5. Em Export server details (Exportar detalhes do servidor), preencha os campos Start date (Data de início) e Time (Hora).

 Note

O horário de início não pode ser mais de 72 horas antes do horário atual.

6. Selecione Export para iniciar o trabalho. O status inicial será In-progress (Em andamento). Para atualizá-lo, clique no ícone de atualização na seção Exports (Exportações).
7. Quando o trabalho de exportação for concluído, clique em Download (Fazer download) e salve o arquivo .zip.
8. Descompacte o arquivo salvo. Os dados exportados estão contidos em um conjunto de arquivos .csv, semelhante a:
 - *<AWSID da conta da_destinationProcessConnection.csv*
 - *<AWSID da conta da_networkInterface.csv*
 - *<AWSID da conta da_osInfo.csv*
 - *<AWSID da conta da_process.csv*
 - *<AWSID da conta da_sourceProcessConnection.csv*
 - *<AWSID da conta da_systemPerformance.csv*

Você pode abrir os arquivos .csv no Microsoft Excel e analisar os dados exportados do servidor.

Entre os arquivos, você pode encontrar um arquivo JSON que contém dados sobre a tarefa de exportação e seus resultados.

Exploração de dados no Athena

A exploração de dados no Amazon Athena permite que você analise os dados coletados de todos os servidores locais descobertos pelo Discovery Agent em um só lugar. Depois que a exploração de dados no Amazon Athena estiver habilitada no console do Migration Hub (ou usando o StartContinuousExport API) e a coleta de dados para agentes é ativada, os dados coletados pelos

agentes são automaticamente armazenados em seu bucket do S3 em intervalos regulares. Para obter mais informações, consulte [Exploração de dados no Amazon Athena](#)

Aplicações

É possível que alguns de seus servidores descobertos precisem ser migrados juntos para permanecerem funcionais. Neste caso, você pode definir e agrupar logicamente os servidores descobertos em aplicativos.

Como parte do processo de agrupamento, você pode pesquisar, filtrar e adicionar tags.

Como agrupar servidores em um aplicativo novo ou existente

1. Usar a doAWSconta daAWS Management Consolee abra o console do Migration Hub em <https://console.aws.amazon.com/migrationhub/>.
2. No painel de navegação do console do Migration Hub, emDescubra, escolhede aplicativos.
3. Na lista de servidores, selecione todos os servidores que você deseja agrupar em um aplicativo novo ou existente.

Para ajudar a escolher servidores para o seu grupo, você pode pesquisar e filtrar qualquer critério especificado na lista de servidores. Clique dentro da barra de pesquisa e escolha um item da lista. Em seguida, selecione um operador da próxima lista e digite seus critérios.

4. Opcional Para cada de aplicativos selecionadosAdicione tag, digite um valor paraChavee, em seguida, opcionalmente, digite um valor paraValor.
5. Clique em Group as application (Agrupar como aplicativo), para criar seu aplicativo, ou adicioná-lo a um existente.
6. Na caixa de diálogo Group as application (Agrupar como aplicativo), selecione Group as a new application (Agrupar como um novo aplicativo) ou Add to an existing application (Adicionar a um aplicativo existente).
 - a. Se você escolher Group as a new application (Agrupar como um novo aplicativo), digite um Application name (Nome do aplicativo). Como alternativa, você pode inserir uma Application description (Descrição do aplicativo).
 - b. Se você escolher Add to an existing application (Adicionar a um aplicativo existente), selecione o nome do aplicativo a ser adicionado à lista.
7. Escolha Save (Salvar).

Usando a API Application Discovery Service para consultar itens de configuração descobertos

Um item de configuração é um ativo de TI que foi descoberto em seu data center por um agente ou por uma importação. Ao usar AWS Application Discovery Service (Application Discovery Service), você usa a API para especificar filtros e consultar itens de configuração específicos para ativos de servidor, aplicativo, processo e conexão. Para obter informações sobre a API, consulte [Application Discovery Service API Reference](#).

As tabelas nas seções a seguir listam os filtros de entrada e as opções de classificação de saída disponíveis para duas ações do Application Discovery Service:

- `DescribeConfigurations`
- `ListConfigurations`

As opções de filtragem e classificação são organizadas pelo tipo de ativo ao qual se aplicam (servidor, aplicativo, processo ou conexão).

Important

Os resultados retornados por `DescribeConfigurations`, `ListConfigurations`, e `StartExportTask` podem não conter atualizações recentes. Para ter mais informações, consulte [Consistência eventual](#).

Usando a `DescribeConfigurations` ação

A ação `DescribeConfigurations` recupera atributos para uma lista de IDs de configuração. Todos os IDs fornecidos devem ser para o mesmo tipo de ativo (servidor, aplicativo, processo ou conexão). Os campos de saída são específicos ao tipo de ativo selecionado. Por exemplo, a saída de um item da configuração do servidor inclui uma lista de atributos sobre o servidor, como nome do host, o sistema operacional e o número de placas de rede. Para obter mais informações sobre a sintaxe do comando, consulte [DescribeConfigurations](#).

A ação `DescribeConfigurations` não é compatível com filtragem.

Campos de saída para `DescribeConfigurations`

As tabelas a seguir, organizadas por tipo de ativo, listam os campos de saída compatíveis da ação DescribeConfigurations. Os marcados como obrigatórios estão sempre presentes na saída.

Ativos do servidor

Campo	Obrigatório
<code>server.agentId</code>	
<code>server.applications</code>	
<code>server.applications.hasMoreValues</code>	
<code>server.configurationId</code>	x
<code>server.cpuType</code>	
<code>server.hostName</code>	
<code>server.hypervisor</code>	
<code>server.networkInterfaceInfo</code>	
<code>server.networkInterfaceInfo.hasMoreValues</code>	
<code>server.osName</code>	
<code>server.osVersion</code>	
<code>server.tags</code>	
<code>server.tags.hasMoreValues</code>	
<code>server.timeOfCreation</code>	x
<code>server.type</code>	
<code>server.performance.avgCpuUsagePct</code>	

Campo	Obrigatório
<code>server.performance.avgDiskReadIOPS</code>	
<code>server.performance.avgDiskReadsPerSecondInKB</code>	
<code>server.performance.avgDiskWriteIOPS</code>	
<code>server.performance.avgDiskWritesPerSecondInKB</code>	
<code>server.performance.avgFreeRAMInKB</code>	
<code>server.performance.avgNetworkReadsPerSecondInKB</code>	
<code>server.performance.avgNetworkWritesPerSecondInKB</code>	
<code>server.performance.maxCpuUsagePct</code>	
<code>server.performance.maxDiskReadIOPS</code>	
<code>server.performance.maxDiskReadsPerSecondInKB</code>	
<code>server.performance.maxDiskWriteIOPS</code>	
<code>server.performance.maxDiskWritesPerSecondInKB</code>	
<code>server.performance.maxNetworkReadsPerSecondInKB</code>	

Campo	Obrigatório
<code>server.performance.maxNetworkWritesPerSecondInKB</code>	
<code>server.performance.minFreeRAMInKB</code>	
<code>server.performance.numCores</code>	
<code>server.performance.numCpus</code>	
<code>server.performance.numDisks</code>	
<code>server.performance.numNetworkCards</code>	
<code>server.performance.totalRAMInKB</code>	

Processar ativos

Campo	Obrigatório
<code>process.commandLine</code>	
<code>process.configurationId</code>	x
<code>process.name</code>	
<code>process.path</code>	
<code>process.timeOfCreation</code>	x

Ativos do aplicativo

Campo	Obrigatório
<code>application.configurationId</code>	x

Campo	Obrigatório
<code>application.description</code>	
<code>application.lastModifiedTime</code>	x
<code>application.name</code>	x
<code>application.serverCount</code>	x
<code>application.timeOfCreation</code>	x

Usando a **ListConfigurations** ação

A ação `ListConfigurations` recupera uma lista de itens de configuração de acordo com os critérios especificados em um filtro. Para obter mais informações sobre a sintaxe do comando, consulte [ListConfigurations](#).

Campos de saída para **ListConfigurations**

As tabelas a seguir, organizadas por tipo de ativo, listam os campos de saída compatíveis da ação `ListConfigurations`. Os marcados como obrigatórios estão sempre presentes na saída.

Ativos do servidor

Campo	Obrigatório
<code>server.configurationId</code>	x
<code>server.agentId</code>	
<code>server.hostName</code>	
<code>server.osName</code>	
<code>server.osVersion</code>	
<code>server.timeOfCreation</code>	x
<code>server.type</code>	

Processar ativos

Campo	Obrigatório
<code>process.commandLine</code>	
<code>process.configurationId</code>	x
<code>process.name</code>	
<code>process.path</code>	
<code>process.timeOfCreation</code>	x
<code>server.agentId</code>	
<code>server.configurationId</code>	x

Ativos do aplicativo

Campo	Obrigatório
<code>application.configurationId</code>	x
<code>application.description</code>	
<code>application.name</code>	x
<code>application.serverCount</code>	x
<code>application.timeOfCreation</code>	x
<code>application.lastModifiedTime</code>	x

Ativos de conexão

Campo	Obrigatório
<code>connection.destinationIp</code>	x
<code>connection.destinationPort</code>	x
<code>connection.ipVersion</code>	x
<code>connection.latestTimestamp</code>	x
<code>connection.occurrence</code>	x
<code>connection.sourceIp</code>	x
<code>connection.transportProtocol</code>	
<code>destinationProcess.configurationId</code>	
<code>destinationProcess.name</code>	
<code>destinationServer.configurationId</code>	
<code>destinationServer.hostName</code>	
<code>sourceProcess.configurationId</code>	
<code>sourceProcess.name</code>	
<code>sourceServer.configurationId</code>	
<code>sourceServer.hostName</code>	

Filtros compatíveis para **ListConfigurations**

As tabelas a seguir, organizadas por tipo de ativo, listam os filtros compatíveis para a ação `ListConfigurations`. Os filtros e os valores estão em uma relação chave/valor definida por uma das condições lógicas compatíveis. A saída dos filtros indicados pode ser classificada.

Ativos do servidor

Filtro	Condições compatíveis	Valores com suporte	Classificação compatível
<code>server.configurationId</code>	<ul style="list-style-type: none"> EQUALS NOT_EQUALS EQ NE 	<ul style="list-style-type: none"> Qualquer ID de configuração de servidor válido 	Nenhum
<code>server.hostName</code>	<ul style="list-style-type: none"> EQUALS NOT_EQUALS EQ NE CONTAINS NOT_CONTAINS 	<ul style="list-style-type: none"> String 	<ul style="list-style-type: none"> ASC DESC
<code>server.osName</code>	<ul style="list-style-type: none"> EQUALS NOT_EQUALS EQ NE CONTAINS NOT_CONTAINS 	<ul style="list-style-type: none"> String 	<ul style="list-style-type: none"> ASC DESC
<code>server.osVersion</code>	<ul style="list-style-type: none"> EQUALS NOT_EQUALS EQ NE CONTAINS NOT_CONTAINS 	<ul style="list-style-type: none"> String 	<ul style="list-style-type: none"> ASC DESC
<code>server.agentId</code>	<ul style="list-style-type: none"> EQUALS NOT_EQUALS EQ NE 	<ul style="list-style-type: none"> String 	Nenhum

Filtro	Condições compatíveis	Valores com suporte	Classificação compatível
<code>server.connectorId</code>	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE 	<ul style="list-style-type: none"> • String 	Nenhum
<code>server.type</code>	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE 	String com um dos seguintes valores: <ul style="list-style-type: none"> • EC2 • OUTRO • VMWARE_VM • VMWARE_HOST • VMWARE_VM_TEMPLATE 	Nenhum
<code>server.vmWareInfo.morefId</code>	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS 	<ul style="list-style-type: none"> • String 	Nenhum
<code>server.vmWareInfo.vcenterId</code>	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS 	<ul style="list-style-type: none"> • String 	Nenhum

Filtro	Condições compatíveis	Valores com suporte	Classificação compatível
<code>server.vmWareInfo.hostId</code>	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS 	<ul style="list-style-type: none"> • String 	Nenhum
<code>server.networkInterfaceInfo.portGroupId</code>	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS 	<ul style="list-style-type: none"> • String 	Nenhum
<code>server.networkInterfaceInfo.portGroupName</code>	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS 	<ul style="list-style-type: none"> • String 	Nenhum
<code>server.networkInterfaceInfo.virtualSwitchName</code>	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS 	<ul style="list-style-type: none"> • String 	Nenhum

Filtro	Condições compatíveis	Valores com suporte	Classificação compatível
<code>server.networkInterfaceInfo.ipAddress</code>	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS 	<ul style="list-style-type: none"> • String 	Nenhum
<code>server.networkInterfaceInfo.macAddress</code>	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS 	<ul style="list-style-type: none"> • String 	Nenhum
<code>server.performance.avgCpuUsagePct</code>	<ul style="list-style-type: none"> • GE • LE • GT • LT 	<ul style="list-style-type: none"> • Porcentagem 	Nenhum
<code>server.performance.totalDiskFreeSizeInKB</code>	<ul style="list-style-type: none"> • GE • LE • GT • LT 	<ul style="list-style-type: none"> • Double 	Nenhum
<code>server.performance.avgFreeRAMInKB</code>	<ul style="list-style-type: none"> • GE • LE • GT • LT 	<ul style="list-style-type: none"> • Double 	Nenhum

Filtro	Condições compatíveis	Valores com suporte	Classificação compatível
<code>server.tag.value</code>	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS 	<ul style="list-style-type: none"> • String 	Nenhum
<code>server.tag.key</code>	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS 	<ul style="list-style-type: none"> • String 	Nenhum
<code>server.application.name</code>	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS 	<ul style="list-style-type: none"> • String 	Nenhum
<code>server.application.description</code>	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS 	<ul style="list-style-type: none"> • String 	Nenhum

Filtro	Condições compatíveis	Valores com suporte	Classificação compatível
<code>server.application.configurationId</code>	<ul style="list-style-type: none"> EQUALS NOT_EQUALS EQ NE 	<ul style="list-style-type: none"> Qualquer ID de configuração de aplicativo válido 	Nenhum
<code>server.process.configurationId</code>	<ul style="list-style-type: none"> EQUALS NOT_EQUALS EQ NE 	<ul style="list-style-type: none"> ProcessId 	Nenhum
<code>server.process.name</code>	<ul style="list-style-type: none"> EQUALS NOT_EQUALS EQ NE CONTAINS NOT_CONTAINS 	<ul style="list-style-type: none"> String 	Nenhum
<code>server.process.commandLine</code>	<ul style="list-style-type: none"> EQUALS NOT_EQUALS EQ NE CONTAINS NOT_CONTAINS 	<ul style="list-style-type: none"> String 	Nenhum

Ativos do aplicativo

Filtro	Condições compatíveis	Valores com suporte	Classificação compatível
<code>application.configurationId</code>	<ul style="list-style-type: none"> EQUALS NOT_EQUALS EQ NE 	<ul style="list-style-type: none"> ApplicationId 	Nenhum
<code>application.name</code>	<ul style="list-style-type: none"> EQUALS NOT_EQUALS EQ NE CONTAINS NOT_CONTAINS 	<ul style="list-style-type: none"> String 	<ul style="list-style-type: none"> ASC DESC
<code>application.description</code>	<ul style="list-style-type: none"> EQUALS NOT_EQUALS EQ NE CONTAINS NOT_CONTAINS 	<ul style="list-style-type: none"> String 	<ul style="list-style-type: none"> ASC DESC
<code>application.serverCount</code>	Filtragem compatível.	Filtragem compatível.	<ul style="list-style-type: none"> ASC DESC
<code>application.timeOfCreation</code>	Filtragem compatível.	Filtragem compatível.	<ul style="list-style-type: none"> ASC DESC
<code>application.lastModifiedTime</code>	Filtragem compatível.	Filtragem compatível.	<ul style="list-style-type: none"> ASC DESC

Filtro	Condições compatíveis	Valores com suporte	Classificação compatível
<code>server.configurationId</code>	<ul style="list-style-type: none"> EQUALS NOT_EQUALS EQ NE 	<ul style="list-style-type: none"> ServerId 	Nenhum

Processar ativos

Filtro	Condições compatíveis	Valores com suporte	Classificação compatível
<code>process.configurationId</code>	<ul style="list-style-type: none"> EQUALS NOT_EQUALS EQ NE 	<ul style="list-style-type: none"> ProcessId 	
<code>process.name</code>	<ul style="list-style-type: none"> EQUALS NOT_EQUALS EQ NE CONTAINS NOT_CONTAINS 	<ul style="list-style-type: none"> String 	<ul style="list-style-type: none"> ASC DESC
<code>process.commandLine</code>	<ul style="list-style-type: none"> EQUALS NOT_EQUALS EQ NE CONTAINS NOT_CONTAINS 	<ul style="list-style-type: none"> String 	<ul style="list-style-type: none"> ASC DESC

Filtro	Condições compatíveis	Valores com suporte	Classificação compatível
<code>server.configurationId</code>	<ul style="list-style-type: none"> EQUALS NOT_EQUALS EQ NE 	<ul style="list-style-type: none"> ServerId 	
<code>server.hostName</code>	<ul style="list-style-type: none"> EQUALS NOT_EQUALS EQ NE CONTAINS NOT_CONTAINS 	<ul style="list-style-type: none"> String 	<ul style="list-style-type: none"> ASC DESC
<code>server.osName</code>	<ul style="list-style-type: none"> EQUALS NOT_EQUALS EQ NE CONTAINS NOT_CONTAINS 	<ul style="list-style-type: none"> String 	<ul style="list-style-type: none"> ASC DESC
<code>server.osVersion</code>	<ul style="list-style-type: none"> EQUALS NOT_EQUALS EQ NE CONTAINS NOT_CONTAINS 	<ul style="list-style-type: none"> String 	<ul style="list-style-type: none"> ASC DESC

Filtro	Condições compatíveis	Valores com suporte	Classificação compatível
<code>server.agentId</code>	<ul style="list-style-type: none"> EQUALS NOT_EQUALS EQ NE CONTAINS NOT_CONTAINS 	<ul style="list-style-type: none"> String 	

Ativos de conexão

Filtro	Condições compatíveis	Valores com suporte	Classificação compatível
<code>connection.sourceIp</code>	<ul style="list-style-type: none"> EQUALS NOT_EQUALS EQ NE CONTAINS NOT_CONTAINS 	<ul style="list-style-type: none"> IP 	<ul style="list-style-type: none"> ASC DESC
<code>connection.destinationIp</code>	<ul style="list-style-type: none"> EQUALS NOT_EQUALS EQ NE CONTAINS NOT_CONTAINS 	<ul style="list-style-type: none"> IP 	<ul style="list-style-type: none"> ASC DESC
<code>connection.destinationPort</code>	<ul style="list-style-type: none"> EQUALS NOT_EQUALS EQ NE 	<ul style="list-style-type: none"> Inteiro 	<ul style="list-style-type: none"> ASC DESC

Filtro	Condições compatíveis	Valores com suporte	Classificação compatível
sourceServer.configurationId	<ul style="list-style-type: none"> EQUALS NOT_EQUALS EQ NE 	<ul style="list-style-type: none"> ServerId 	
sourceServer.hostName	<ul style="list-style-type: none"> EQUALS NOT_EQUALS EQ NE CONTAINS NOT_CONTAINS 	<ul style="list-style-type: none"> String 	<ul style="list-style-type: none"> ASC DESC
destinationServer.osName	<ul style="list-style-type: none"> EQUALS NOT_EQUALS EQ NE CONTAINS NOT_CONTAINS 	<ul style="list-style-type: none"> String 	<ul style="list-style-type: none"> ASC DESC
destinationServer.osVersion	<ul style="list-style-type: none"> EQUALS NOT_EQUALS EQ NE CONTAINS NOT_CONTAINS 	<ul style="list-style-type: none"> String 	<ul style="list-style-type: none"> ASC DESC

Filtro	Condições compatíveis	Valores com suporte	Classificação compatível
<code>destinationServer.agentId</code>	<ul style="list-style-type: none"> EQUALS NOT_EQUALS EQ NE CONTAINS NOT_CONTAINS 	<ul style="list-style-type: none"> String 	
<code>sourceProcess.configurationId</code>	<ul style="list-style-type: none"> EQUALS NOT_EQUALS EQ NE 	<ul style="list-style-type: none"> ProcessId 	
<code>sourceProcess.name</code>	<ul style="list-style-type: none"> EQUALS NOT_EQUALS EQ NE CONTAINS NOT_CONTAINS 	<ul style="list-style-type: none"> String 	<ul style="list-style-type: none"> ASC DESC
<code>sourceProcess.commandLine</code>	<ul style="list-style-type: none"> EQUALS NOT_EQUALS EQ NE CONTAINS NOT_CONTAINS 	<ul style="list-style-type: none"> String 	<ul style="list-style-type: none"> ASC DESC
<code>destinationProcess.configurationId</code>	<ul style="list-style-type: none"> EQUALS NOT_EQUALS EQ NE 	<ul style="list-style-type: none"> ProcessId 	

Filtro	Condições compatíveis	Valores com suporte	Classificação compatível
<code>destinationProcess.name</code>	<ul style="list-style-type: none">• EQUALS• NOT_EQUALS• EQ• NE• CONTAINS• NOT_CONTAINS	<ul style="list-style-type: none">• String	<ul style="list-style-type: none">• ASC• DESC
<code>destinationProcess.commandLine</code>	<ul style="list-style-type: none">• EQUALS• NOT_EQUALS• EQ• NE• CONTAINS• NOT_CONTAINS	<ul style="list-style-type: none">• String	<ul style="list-style-type: none">• ASC• DESC

Consistência eventual na API AWS Application Discovery Service

Eventualmente, as operações de atualização a seguir são consistentes. As atualizações podem não estar imediatamente visíveis para as operações de leitura [StartExportTask](#), [DescribeConfigurations](#), [ListConfigurations](#).

- [AssociateConfigurationItemsToAplicação](#)
- [CreateTags](#)
- [DeleteApplications](#)
- [DeleteTags](#)
- [DescribeBatchDeleteConfigurationTarefa](#)
- [DescribeImportTarefas](#)
- [DisassociateConfigurationItemsFromApplication](#)
- [UpdateApplication](#)

Sugestões para gerenciar a consistência eventual:

- Ao invocar as operações de leitura [StartExportTask](#), [DescribeConfigurations](#), or [ListConfigurations](#)(ou seus AWS CLI comandos correspondentes), use um algoritmo de recuo exponencial para permitir tempo suficiente para que qualquer operação de atualização anterior se propague pelo sistema. Para fazer isso, execute a operação de leitura repetidamente, começando com um tempo de espera de dois segundos e aumentando gradualmente até cinco minutos de tempo de espera.
- Adicione o tempo de espera entre as operações subsequentes, mesmo que uma operação de atualização retorne uma resposta 200 - OK. Aplique um algoritmo de recuo exponencial começando com alguns segundos de tempo de espera e aumente gradualmente até cerca de cinco minutos de tempo de espera.

Segurança em AWS Application Discovery Service

A segurança para com a nuvem na AWS é a nossa maior prioridade. Como cliente da AWS, você se beneficiará de um datacenter e de uma arquitetura 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 isto como segurança da nuvem e segurança na nuvem:

- Segurança da nuvem: a AWS é responsável pela proteção da infraestrutura que executa produtos da AWS na Nuvem AWS. A AWS também fornece serviços que podem ser usados com segurança. A eficácia da nossa segurança é regularmente testada e verificada por auditores de terceiros como parte dos [Programas de conformidade da AWS](#).
- Segurança da 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 sua organização e as leis e regulamentos aplicáveis.

Para usar o AWS Application Discovery Agent ou o Application Discovery Service Agentless Collector, você deve fornecer as chaves de acesso à sua conta. AWS Essas informações são então armazenadas em sua infraestrutura local. Como parte do modelo de responsabilidade compartilhada, você é responsável por proteger o acesso à sua infraestrutura.

Esta documentação ajudará você a entender como aplicar o modelo de responsabilidade compartilhada ao usar o Application Discovery Service. Os tópicos a seguir mostram como configurar o Application Discovery Service para atender aos seus objetivos de segurança e conformidade. Você também aprenderá a usar outros AWS serviços que podem ajudá-lo a monitorar e proteger seus recursos do Application Discovery Service.

Tópicos

- [Identity and Access Management para AWS Application Discovery Service](#)
- [Registrar em log e monitorar no AWS Application Discovery Service](#)

Identity and Access Management para AWS Application Discovery Service

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 (tem permissões) para usar os recursos do Application Discovery Service. O IAM é um AWS service (Serviço da AWS) que você pode usar sem custo adicional.

Tópicos

- [Público](#)
- [Autenticação com identidades](#)
- [Gerenciamento do acesso usando políticas](#)
- [Como AWS Application Discovery Service funciona com o IAM](#)
- [AWS políticas gerenciadas para AWS Application Discovery Service](#)
- [AWS Application Discovery Service Exemplos de políticas baseadas em identidade](#)
- [Uso de funções vinculadas ao serviço do Application Discovery Service](#)
- [Solução de problemas AWS Application Discovery Service de identidade e acesso](#)

Público

A forma como você usa AWS Identity and Access Management (IAM) difere, dependendo do trabalho que você faz no Application Discovery Service.

Usuário do serviço — Se você usar o serviço Application Discovery Service para fazer seu trabalho, seu administrador fornecerá as credenciais e as permissões de que você precisa. À medida que você usa mais recursos do Application Discovery Service para fazer seu trabalho, talvez precise de permissões adicionais. Entender como o acesso é gerenciado pode ajudar você a solicitar as permissões corretas ao seu administrador. Se você não conseguir acessar um recurso no Application Discovery Service, consulte [Solução de problemas AWS Application Discovery Service de identidade e acesso](#).

Administrador de serviços — Se você é responsável pelos recursos do Application Discovery Service em sua empresa, provavelmente tem acesso total ao Application Discovery Service. É seu trabalho determinar quais recursos e recursos do Application Discovery Service seus usuários do serviço

devem acessar. Assim, você deve enviar solicitações ao administrador do IAM para alterar as permissões dos usuários de seu serviço. Revise as informações nesta página para entender os Introdução ao IAM. Para saber mais sobre como sua empresa pode usar o IAM com o Application Discovery Service, consulte [Como AWS Application Discovery Service funciona com o IAM](#).

Administrador do IAM — Se você for administrador do IAM, talvez queira saber detalhes sobre como criar políticas para gerenciar o acesso ao Application Discovery Service. Para ver exemplos de políticas baseadas em identidade do Application Discovery Service que você pode usar no IAM, consulte. [AWS Application Discovery Service Exemplos de políticas baseadas em identidade](#)

Autenticação com identidades

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

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

Dependendo do tipo de usuário que você é, você pode entrar no AWS Management Console ou no portal de AWS acesso. Para obter mais informações sobre como fazer login em 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.

Independente do método de autenticação usado, também pode ser exigido que você forneça informações adicionais de segurança. Por exemplo, AWS recomenda que você use a autenticação multifator (MFA) para aumentar a segurança da sua conta. Para saber mais, consulte [Autenticação Multifator](#) no Guia do Usuário do AWS IAM Identity Center . [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 puder executar. Para obter a lista completa das tarefas que exigem login como usuário raiz, consulte [Tarefas que exigem credenciais de usuário raiz](#) no Guia do Usuário do IAM.

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 contar com 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 conceder 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 \(em vez de um perfil\)](#) 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 [Utilizar perfis do IAM](#) no Guia do usuário do IAM.

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

- **Acesso de usuário federado:** para atribuir permissões a identidades federadas, você pode criar um perfil e definir permissões para ele. Quando uma identidade federada é autenticada, essa identidade é associada ao perfil e recebe as permissões definidas pelo mesmo. Para obter mais informações sobre perfis para federação, consulte [Criar um perfil para um provedor de identidades de terceiros](#) no Guia do Usuário do IAM. Se você usar o Centro de identidade do IAM, configure um conjunto de permissões. Para controlar o que suas identidades podem acessar após a autenticação, o Centro de identidade do IAM correlaciona o conjunto de permissões a um perfil no IAM. Para obter informações sobre conjuntos de permissões, consulte [Conjuntos de Permissões](#) no Manual do Usuário do AWS IAM Identity Center .
- **Permissões temporárias para usuários do IAM** — um usuário ou um perfil do IAM pode presumir 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 [Acesso a recursos entre contas no IAM](#) 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 aplicativos no Amazon EC2 ou armazene objetos no Amazon S3. Um serviço pode fazer isso usando as permissões do principal de chamada, usando um perfil de serviço ou um perfil vinculado a um 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](#).

- **Função de serviço:** um perfil de serviço é um [perfil do IAM](#) que um serviço assume para realizar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para obter mais informações, consulte [Criar um perfil para delegar permissões a um AWS service \(Serviço da AWS\)](#) no Guia do Usuário do IAM.
- **Função vinculada ao serviço** — Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um AWS service (Serviço da AWS). O serviço pode presumir a função de executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não editar as permissões para funções vinculadas 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 [Utilizar um perfil do IAM para conceder permissões a aplicações em execução nas instâncias do Amazon EC2](#) no Guia do usuário do IAM.

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

Gerenciamento do acesso usando políticas

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

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

Por padrão, usuários e funções não têm permissões. Para conceder aos usuários permissões para executar ações nos recursos 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 presumir os perfis.

As políticas do IAM definem permissões para uma ação independente 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 do IAM, grupo de usuários ou perfil. 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 [Criando políticas do IAM](#) no Guia do Usuário do IAM.

As políticas baseadas em identidade podem ser categorizadas ainda adicionalmente como políticas em linha ou políticas gerenciadas. As políticas em linha são anexadas diretamente a um único usuário, grupo ou perfil. As políticas gerenciadas são políticas autônomas que você pode associar a vários usuários, grupos e funções em seu Conta da AWS. As políticas 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 recursos são documentos de políticas JSON que você anexa a um recurso. São exemplos de políticas baseadas em recursos as políticas de confiança de perfil do IAM e as políticas de bucket do Amazon S3. Em serviços que suportem políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o recurso ao qual a política está anexada, a política define quais ações um principal especificado pode executar nesse recurso e em que condições. Você deve [especificar uma entidade principal](#) em uma política baseada em recursos. Os diretores podem incluir contas, usuários, funções, usuários federados ou. Serviços da AWS

Políticas baseadas em recursos são políticas em linha localizadas nesse serviço. Você não pode usar 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 as políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

O Amazon S3 e o Amazon VPC são exemplos de serviços que oferecem suporte a ACLs. AWS 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 com seus limites de permissões. As políticas baseadas em recurso que especificam o usuário ou o perfil no campo `Principal` não são limitadas pelo limite de permissões. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações sobre limites de permissões, consulte [Limites de permissões para 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 Organizações e SCPs, consulte [Como os SCPs Funcionam](#) no Manual 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 atributo. Uma negação explícita em qualquer uma dessas políticas

substitui a permissão. Para obter mais informações, consulte [Políticas de sessão](#) no Guia do Usuário do IAM.

Vários tipos de política

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

Como AWS Application Discovery Service funciona com o IAM

Antes de usar o IAM para gerenciar o acesso ao Application Discovery Service, você deve entender quais recursos do IAM estão disponíveis para uso com o Application Discovery Service. Para ter uma visão geral de como o Application Discovery Service e outros AWS serviços funcionam com o IAM, consulte [AWS Services That Work with IAM](#) no Guia do usuário do IAM.

Tópicos

- [Políticas baseadas em identidade do Application Discovery Service](#)
- [Políticas baseadas em recursos do Application Discovery Service](#)
- [Autorização baseada em etiquetas do Application Discovery Service](#)
- [Funções do IAM do Application Discovery Service](#)

Políticas baseadas em identidade do Application Discovery Service

Com as políticas baseadas em identidade do IAM, é possível especificar ações ou recursos permitidos ou negados, assim como as condições sob as quais as ações são permitidas ou negadas. O Application Discovery Service oferece suporte a ações, recursos e chaves de condição específicos. Para conhecer todos os elementos usados em uma política JSON, consulte [Referência de elementos de política JSON do IAM](#) no Guia do usuário do IAM.

Ações

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. Algumas operações também exigem várias ações em uma política. Essas ações adicionais são chamadas de ações dependentes.

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

As ações de política no Application Discovery Service usam o seguinte prefixo antes da ação: `discovery:`. As instruções de política devem incluir um elemento `Action` ou `NotAction`. O Application Discovery Service define seu próprio conjunto de ações que descrevem as tarefas que você pode executar com esse serviço.

Para especificar várias ações em uma única instrução, separe-as com vírgulas, como segue:

```
"Action": [  
    "discovery:action1",  
    "discovery:action2"
```

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

```
"Action": "discovery:Describe*"
```

Para ver uma lista de ações do Application Discovery Service, consulte [Actions Defined by AWS Application Discovery Service](#) no Guia do usuário do IAM.

Recursos

O Application Discovery Service não suporta a especificação de ARNs de recursos em uma política. Para separar o acesso, crie e use separadamente Contas da AWS.

Chaves de condição

O Application Discovery Service não fornece nenhuma chave de condição específica do serviço, mas oferece suporte ao uso de algumas chaves de condição globais. Para ver todas as chaves de condição AWS globais, consulte [Chaves de contexto de condição AWS global](#) no Guia do usuário do IAM.

Exemplos

Para ver exemplos de políticas baseadas em identidade do Application Discovery Service, consulte. [AWS Application Discovery Service Exemplos de políticas baseadas em identidade](#)

Políticas baseadas em recursos do Application Discovery Service

O Application Discovery Service não oferece suporte a políticas baseadas em recursos.

Autorização baseada em etiquetas do Application Discovery Service

O Application Discovery Service não oferece suporte à marcação de recursos nem ao controle de acesso com base em tags.

Funções do IAM do Application Discovery Service

Uma [função do IAM](#) é uma entidade dentro da sua AWS conta que tem permissões específicas.

Usando credenciais temporárias com o Application Discovery Service

O Application Discovery Service não oferece suporte ao uso de credenciais temporárias.

Funções vinculadas ao serviço

[As funções vinculadas ao serviço](#) permitem que AWS os serviços acessem recursos em outros serviços para concluir uma ação em seu nome. Os perfis vinculados a serviço aparecem em sua conta do IAM e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não pode editar as permissões para perfis vinculados a serviço.

O Application Discovery Service oferece suporte a funções vinculadas a serviços. Para obter detalhes sobre como criar ou gerenciar funções vinculadas ao serviço do Application Discovery Service, consulte. [Uso de funções vinculadas ao serviço do Application Discovery Service](#)

Perfis de serviço

Esse atributo permite que um serviço assumira um [perfil de serviço](#) em seu nome. O perfil permite que o serviço acesse recursos em outros serviços para concluir uma ação em seu nome. Os perfis de serviço aparecem em sua conta do IAM e são de propriedade da conta. Isso significa que um administrador do IAM pode alterar as permissões para esse perfil. Porém, fazer isso pode alterar a funcionalidade do serviço.

O Application Discovery Service oferece suporte a funções de serviço.

AWS políticas gerenciadas para AWS Application Discovery Service

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. Os serviços ocasionalmente acrescentam permissões adicionais a uma política gerenciada pela AWS para oferecer suporte a novos atributos. Esse tipo de atualização afeta todas as identidades (usuários, grupos e perfis) em que a política está anexada. É mais provável que os serviços atualizem uma política gerenciada pela AWS quando um novo atributo for iniciado ou novas operações se tornarem disponíveis. Os serviços não removem 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: `AWSApplicationDiscoveryServiceFullAccess`

A `AWSApplicationDiscoveryServiceFullAccess` política concede a uma conta de usuário do IAM acesso às APIs do Application Discovery Service e do Migration Hub.

Uma conta de usuário do IAM com essa política anexada pode configurar o Application Discovery Service, iniciar e interromper agentes, iniciar e interromper a descoberta sem agente e consultar

dados do banco de dados do AWS Discovery Service. Para obter um exemplo dessa política, consulte [Concedendo acesso total ao Application Discovery Service](#).

AWS política gerenciada: AWSApplicationDiscoveryAgentlessCollectorAccess

A política `AWSApplicationDiscoveryAgentlessCollectorAccess` gerenciada concede ao Application Discovery Service Agentless Collector (Agentless Collector) acesso para se registrar e se comunicar com o Application Discovery Service e se comunicar com outros serviços. AWS

Essa política deve ser anexada ao usuário do IAM cujas credenciais são usadas para configurar o Agentless Collector.

Detalhes das permissões

Esta política inclui as seguintes permissões.

- `arsenal`— Permite que o coletor se registre no aplicativo Application Discovery Service. Isso é necessário para poder enviar os dados coletados de volta para AWS o.
- `ecr-public`— Permite que o coletor faça chamadas para o Amazon Elastic Container Registry Public (Amazon ECR Public), onde as atualizações mais recentes são encontradas para o coletor.
- `mgm`— Permite que o coletor ligue AWS Migration Hub para recuperar a região inicial da conta usada para configurar o coletor. Isso é necessário para saber para qual região os dados coletados devem ser enviados.
- `sts`— Permite que o coletor recupere um token do portador do serviço para que o coletor possa fazer chamadas para o Amazon ECR Public para obter as atualizações mais recentes.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "arsenal:RegisterOnPremisesAgent"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
```



```

        "Action": [
            "ecr-public:DescribeImages"
        ],
        "Resource": "arn:aws:ecr-
public::44637222237:repository/6e5498e4-8c31-4f57-9991-13b4b992ff7b"
    },
    {
        "Effect": "Allow",
        "Action": [
            "ecr-public:GetAuthorizationToken"
        ],
        "Resource": "*"
    },
    {
        "Effect": "Allow",
        "Action": [
            "mgh:GetHomeRegion"
        ],
        "Resource": "*"
    },
    {
        "Effect": "Allow",
        "Action": [
            "sts:GetServiceBearerToken"
        ],
        "Resource": "*"
    }
]
}

```

AWS política gerenciada: AWSApplicationDiscoveryAgentAccess

A `AWSApplicationDiscoveryAgentAccess` política concede ao Application Discovery Agent acesso para se registrar e se comunicar com o Application Discovery Service.

Você anexa essa política a qualquer usuário cujas credenciais sejam usadas pelo Application Discovery Agent.

Essa política também concede acesso de usuário ao Arsenal. O Arsenal é um serviço de agente gerenciado e hospedado por AWS. O Arsenal encaminha os dados para o Application Discovery Service na nuvem. Para obter um exemplo dessa política, consulte [Concedendo acesso a agentes de descoberta](#).

AWS política gerenciada: AWSAgentlessDiscoveryService

A `AWSAgentlessDiscoveryService` política concede ao AWS Agentless Discovery Connector que está sendo executado em seu VMware vCenter Server acesso para registrar, comunicar-se e compartilhar métricas de integridade do conector com o Application Discovery Service.

Anexe essa política a qualquer usuário cujas credenciais devem ser usadas pelo conector.

AWS política gerenciada: ApplicationDiscoveryServiceContinuousExportServiceRole Política

Se sua conta do IAM tiver a `AWSApplicationDiscoveryServiceFullAccess` política `ApplicationDiscoveryServiceContinuousExportServiceRolePolicy` anexada, ela será automaticamente vinculada à sua conta quando você ativar a exploração de dados no Amazon Athena.

Essa política permite AWS Application Discovery Service criar streams do Amazon Data Firehose para transformar e entregar dados coletados por AWS Application Discovery Service agentes em um bucket do Amazon S3 em sua conta. AWS

Além disso, essa política cria um AWS Glue Data Catalog com um novo banco de dados chamado `application_discovery_service_database` e esquemas de tabela para mapear dados coletados pelos agentes. Para obter um exemplo dessa política, consulte [Conceder permissões para coleta de dados do agente](#).

AWS política gerenciada: AWSDiscoveryContinuousExportFirehosePolicy

A `AWSDiscoveryContinuousExportFirehosePolicy` política é necessária para usar a exploração de dados no Amazon Athena. Ele permite que o Amazon Data Firehose grave dados coletados do Application Discovery Service no Amazon S3. Para obter mais informações sobre como usar essa política, consulte [Criando a AWSApplicationDiscoveryServiceFirehose função](#). Para obter um exemplo dessa política, consulte [Concedendo permissões para exploração de dados](#).

Criando a AWSApplicationDiscoveryServiceFirehose função

Um administrador anexa políticas gerenciadas à sua conta de usuário do IAM. Ao usar a `AWSDiscoveryContinuousExportFirehosePolicy` política, o administrador deve primeiro criar uma função chamada `AWSApplicationDiscoveryServiceFirehoseFirehose` como uma entidade confiável e, em seguida, anexar a `AWSDiscoveryContinuousExportFirehosePolicy` política à função, conforme mostrado no procedimento a seguir.

Para criar o perfil do IAM `AWSApplicationDiscoveryServiceFirehose`

1. No console do IAM, escolha Roles no painel de navegação.
2. Selecione Criar função.
3. Escolha o Kinesis.
4. Escolha o Kinesis Firehose como o seu caso de uso.
5. Escolha Próximo: permissões.
6. Em Políticas de filtro, pesquise por `AWSDiscoveryContinuousExportFirehosePolicy`.
7. Selecione a caixa ao lado `AWSDiscoveryContinuousExportFirehosePolicy` e escolha Avançar: Revisão.
8. Insira `AWSApplicationDiscoveryServiceFirehose` como nome da função e, em seguida, escolha Criar função.

Atualizações do Application Discovery Service para políticas AWS gerenciadas

Veja detalhes sobre as atualizações das políticas AWS gerenciadas do Application Discovery Service desde que esse serviço começou a rastrear essas alterações. Para obter alertas automáticos sobre alterações feitas nesta página, inscreva-se no feed RSS na página [Histórico de documentos do AWS Application Discovery Service](#).

Alteração	Descrição	Data
AWSApplicationDiscoveryAgentlessCollectorAccess — Nova política disponibilizada com o lançamento do Agentless Collector	O Application Discovery Service adicionou a nova política gerenciada <code>AWSApplicationDiscoveryAgentlessCollectorAccess</code> que concede ao Agentless Collector acesso para se registrar e se comunicar com o Application Discovery	16 de agosto de 2022

Alteração	Descrição	Data
	Service e se comunicar com outros serviços. AWS	
O Application Discovery Service começou a rastrear as alterações	O Application Discovery Service começou a monitorar as alterações em suas políticas AWS gerenciadas.	1º de março de 2021

AWS Application Discovery Service Exemplos de políticas baseadas em identidade

Por padrão, os usuários e funções do IAM não têm permissão para criar ou modificar recursos do Application Discovery Service. Eles também não podem realizar tarefas usando a AWS API, o AWS Management Console, o AWS CLI, ou o IAM. Um administrador do IAM deve criar políticas do IAM que concedam aos usuários e perfis permissão para executarem operações de API específicas nos recursos especificados de que precisam. O administrador deve anexar essas políticas aos usuários ou grupos do IAM que exigem essas permissões.

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

Tópicos

- [Melhores práticas de política](#)
- [Concedendo acesso total ao Application Discovery Service](#)
- [Concedendo acesso a agentes de descoberta](#)
- [Conceder permissões para coleta de dados do agente](#)
- [Concedendo permissões para exploração de dados](#)
- [Concedendo permissões para usar o diagrama de rede do console do Migration Hub](#)

Melhores práticas de política

As políticas baseadas em identidade determinam se alguém pode criar, acessar ou excluir recursos do Application Discovery Service em sua conta. Essas ações podem incorrer em custos para

seus 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 funções 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 atributos 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 gravar 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 da política JSON do IAM: Condição](#) 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 100 verificações de política e recomendações acionáveis para ajudá-lo 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 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.

Concedendo acesso total ao Application Discovery Service

A política `AWSApplicationDiscoveryServiceFullAccess` gerenciada concede à conta de usuário do IAM acesso às APIs do Application Discovery Service e do Migration Hub.

Um usuário do IAM com essa política anexada à sua conta pode configurar o Application Discovery Service, iniciar e interromper agentes, iniciar e interromper a descoberta sem agente e consultar dados do banco de dados do AWS Discovery Service. Para obter mais informações sobre essa política, consulte [AWS políticas gerenciadas para AWS Application Discovery Service](#).

Example `AWSApplicationDiscoveryServiceFullAccess` política

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "mgh:*",
        "discovery:*"
      ],
      "Effect": "Allow",
      "Resource": "*"
    },
    {
      "Action": [
        "iam:GetRole"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

Concedendo acesso a agentes de descoberta

A política `AWSApplicationDiscoveryAgentAccess` gerenciada concede ao Application Discovery Agent acesso para se registrar e se comunicar com o Application Discovery Service. Para obter mais informações sobre essa política, consulte [AWS políticas gerenciadas para AWS Application Discovery Service](#).

Anexe essa política a qualquer usuário cujas credenciais sejam usadas pelo Application Discovery Agent.

Essa política também concede acesso de usuário ao Arsenal. O Arsenal é um serviço de agente gerenciado e hospedado por AWS. O Arsenal encaminha os dados para o Application Discovery Service na nuvem.

Example AWSApplicationDiscoveryAgentAccess Política

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "arsenal:RegisterOnPremisesAgent"
      ],
      "Resource": "*"
    }
  ]
}
```

Conceder permissões para coleta de dados do agente

A política `ApplicationDiscoveryServiceContinuousExportServiceRolePolicy` gerenciada permite AWS Application Discovery Service criar fluxos do Amazon Data Firehose para transformar e entregar dados coletados pelos agentes do Application Discovery Service para um bucket do Amazon S3 em sua conta. AWS

Além disso, essa política cria um catálogo de AWS Glue dados com um novo banco de dados chamado `application_discovery_service_database` e esquemas de tabela para mapear dados coletados pelos agentes.

Para obter mais informações sobre como usar essa política, consulte [AWS políticas gerenciadas para AWS Application Discovery Service](#).

Example ApplicationDiscoveryServiceContinuousExportServiceRolePolicy

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
```

```

    "Action": [
      "glue:CreateDatabase",
      "glue:UpdateDatabase",
      "glue:CreateTable",
      "glue:UpdateTable",
      "firehose:CreateDeliveryStream",
      "firehose:DescribeDeliveryStream",
      "logs:CreateLogGroup"
    ],
    "Effect": "Allow",
    "Resource": "*"
  },
  {
    "Action": [
      "firehose>DeleteDeliveryStream",
      "firehose:PutRecord",
      "firehose:PutRecordBatch",
      "firehose:UpdateDestination"
    ],
    "Effect": "Allow",
    "Resource": "arn:aws:firehose:*:*:deliverystream/aws-application-discovery-
service*"
  },
  {
    "Action": [
      "s3:CreateBucket",
      "s3:ListBucket",
      "s3:PutBucketLogging",
      "s3:PutEncryptionConfiguration"
    ],
    "Effect": "Allow",
    "Resource": "arn:aws:s3:::aws-application-discovery-service*"
  },
  {
    "Action": [
      "s3:GetObject"
    ],
    "Effect": "Allow",
    "Resource": "arn:aws:s3:::aws-application-discovery-service/*/*"
  },
  {
    "Action": [
      "logs:CreateLogStream",
      "logs:PutRetentionPolicy"
    ]
  }

```



```

    ],
    "Effect": "Allow",
    "Resource": "arn:aws:logs:*:*:log-group:/aws/application-discovery-service/
firehose*"
  },
  {
    "Action": [
      "iam:PassRole"
    ],
    "Effect": "Allow",
    "Resource": "arn:aws:iam::*:role/AWSApplicationDiscoveryServiceFirehose",
    "Condition": {
      "StringLike": {
        "iam:PassedToService": "firehose.amazonaws.com"
      }
    }
  },
  {
    "Action": [
      "iam:PassRole"
    ],
    "Effect": "Allow",
    "Resource": "arn:aws:iam::*:role/service-role/
AWSApplicationDiscoveryServiceFirehose",
    "Condition": {
      "StringLike": {
        "iam:PassedToService": "firehose.amazonaws.com"
      }
    }
  }
]
}

```

Concedendo permissões para exploração de dados

A `AWSDiscoveryContinuousExportFirehosePolicy` política é necessária para usar a exploração de dados no Amazon Athena. Ele permite que o Amazon Data Firehose grave dados coletados do Application Discovery Service no Amazon S3. Para obter mais informações sobre como usar essa política, consulte [Criando a `AWSApplicationDiscoveryServiceFirehose` função](#).

Example `AWSDiscoveryContinuousExportFirehosePolicy`

```
{
```

```

"Version": "2012-10-17",
"Statement": [
  {
    "Effect": "Allow",
    "Action": [
      "glue:GetTableVersions"
    ],
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "s3:AbortMultipartUpload",
      "s3:GetBucketLocation",
      "s3:GetObject",
      "s3:ListBucket",
      "s3:ListBucketMultipartUploads",
      "s3:PutObject"
    ],
    "Resource": [
      "arn:aws:s3:::aws-application-discovery-service-*",
      "arn:aws:s3:::aws-application-discovery-service-*/*"
    ]
  },
  {
    "Effect": "Allow",
    "Action": [
      "logs:PutLogEvents"
    ],
    "Resource": [
      "arn:aws:logs:*:*:log-group:/aws/application-discovery-service/
firehose:log-stream:*"
    ]
  }
]
}

```

Concedendo permissões para usar o diagrama de rede do console do Migration Hub

Para conceder acesso ao diagrama de rede do AWS Migration Hub console ao criar uma política baseada em identidade que permite ou nega acesso ao Application Discovery Service ou ao Migration Hub, talvez seja necessário adicionar a `discovery:GetNetworkConnectionGraph` ação à política.

Você deve usar a `discovery:GetNetworkConnectionGraph` ação em novas políticas ou atualizar políticas antigas se o seguinte for verdadeiro para a política:

- A política permite ou nega acesso ao Application Discovery Service ou ao Migration Hub.
- A política concede permissões de acesso usando mais uma ação de descoberta específica, como `discovery:action-name` em vez de `discovery:*`.

O exemplo a seguir mostra como usar a `discovery:GetNetworkConnectionGraph` ação em uma política do IAM.

Example

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": ["discovery:GetNetworkConnectionGraph"],
      "Resource": "*"
    }
  ]
}
```

Para obter informações sobre o diagrama de rede do Migration Hub, consulte [Visualizando conexões de rede no Migration Hub](#).

Uso de funções vinculadas ao serviço do Application Discovery Service

O AWS Application Discovery Service usa [funções vinculadas ao serviço](#) do AWS Identity and Access Management (IAM). A função vinculada ao serviço é um tipo exclusivo de função do IAM vinculada diretamente ao Application Discovery Service. As funções vinculadas ao serviço são predefinidas pelo Application Discovery Service e incluem todas as permissões que o serviço requer para chamar outros AWS serviços da em seu nome.

Uma função vinculada ao serviço facilita a configuração do Application Discovery Service porque você não precisa adicionar as permissões necessárias manualmente. O Application Discovery Service define as permissões das funções vinculadas ao serviço e, exceto se definido de outra forma, somente o Application Discovery Service pode assumir suas funções. As permissões definidas incluem a política de confiança e a política de permissões, e essa política não pode ser anexada a nenhuma outra entidade do IAM.

Uma função vinculada ao serviço poderá ser excluída somente após excluir seus recursos relacionados. Isso protege seus recursos do Application Discovery Service, pois você não pode remover por engano as permissões para acessar os recursos.

Tópicos

- [Permissões de função vinculada ao serviço do Application Discovery Service](#)
- [Criar uma função vinculada ao serviço do Application Discovery Service](#)
- [Exclusão de uma função vinculada ao serviço do Application Discovery Service](#)

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 Yes (Sim) na coluna Service-Linked Role (Função vinculada a serviço). Escolha um Sim com um link para visualizar a documentação da função vinculada a serviço desse serviço.

Permissões de função vinculada ao serviço do Application Discovery Service

O Application Discovery Service usa a função vinculada ao serviço chamada `AWSServiceRoleForApplicationDiscoveryServiceContinuousExport`— Permite o acesso a AWS Serviços e recursos usados ou gerenciados por AWS Application Discovery Service.

O `AWSServiceRoleForApplicationDiscoveryServiceContinuousExport` A função vinculada ao serviço confia nos seguintes serviços para assumir a função:

- `continuousexport.discovery.amazonaws.com`

A política de permissões da função permite que o Application Discovery Service conclua as seguintes ações:

glue

`CreateDatabase`

`UpdateDatabase`

`CreateTable`

`UpdateTable`

firehose

`CreateDeliveryStream`

DeleteDeliveryStream

DescribeDeliveryStream

PutRecord

PutRecordBatch

UpdateDestination

s3

CreateBucket

ListBucket

GetObject

logs

CreateLogGroup

CreateLogStream

PutRetentionPolicy

iam

PassRole

Esta é a política completa que mostra a quais recursos as ações acima se aplicam:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "glue:CreateDatabase",
        "glue:UpdateDatabase",
        "glue:CreateTable",
        "glue:UpdateTable",
        "firehose:CreateDeliveryStream",
        "firehose:DescribeDeliveryStream",
        "logs:CreateLogGroup"
      ],
      "Effect": "Allow",
    }
  ]
}
```

```

    "Resource": "*"
  },
  {
    "Action": [
      "firehose:DeleteDeliveryStream",
      "firehose:PutRecord",
      "firehose:PutRecordBatch",
      "firehose:UpdateDestination"
    ],
    "Effect": "Allow",
    "Resource": "arn:aws:firehose:*:*:deliverystream/aws-application-discovery-
service*"
  },
  {
    "Action": [
      "s3:CreateBucket",
      "s3:ListBucket",
      "s3:PutBucketLogging",
      "s3:PutEncryptionConfiguration"
    ],
    "Effect": "Allow",
    "Resource": "arn:aws:s3:::aws-application-discovery-service*"
  },
  {
    "Action": [
      "s3:GetObject"
    ],
    "Effect": "Allow",
    "Resource": "arn:aws:s3:::aws-application-discovery-service/*/*"
  },
  {
    "Action": [
      "logs:CreateLogStream",
      "logs:PutRetentionPolicy"
    ],
    "Effect": "Allow",
    "Resource": "arn:aws:logs:*:*:log-group:/aws/application-discovery-service/
firehose*"
  },
  {
    "Action": [
      "iam:PassRole"
    ],
    "Effect": "Allow",

```

```

    "Resource": "arn:aws:iam::*:role/AWSApplicationDiscoveryServiceFirehose",
    "Condition": {
      "StringLike": {
        "iam:PassedToService": "firehose.amazonaws.com"
      }
    }
  },
  {
    "Action": [
      "iam:PassRole"
    ],
    "Effect": "Allow",
    "Resource": "arn:aws:iam::*:role/service-role/
AWSApplicationDiscoveryServiceFirehose",
    "Condition": {
      "StringLike": {
        "iam:PassedToService": "firehose.amazonaws.com"
      }
    }
  }
]
}

```

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

Criar uma função vinculada ao serviço do Application Discovery Service

Você não precisa criar manualmente uma função vinculada a serviço. O `AWSServiceRoleForApplicationDiscoveryServiceContinuousExport` a função vinculada ao serviço é criada automaticamente quando a Exportação contínua é ativada implicitamente por a) opções de confirmação na caixa de diálogo apresentada na página Coletores de Dados após você escolher “Iniciar coleta de dados”, ou clicar no controle deslizante denominado “Exploração de dados no Athena” ou b) ao chamar o `StartContinuousExport` API usando a `AWSCLI`.

Important

Essa função vinculada ao serviço pode aparecer em sua conta se você concluiu uma ação em outro serviço que usa os recursos compatíveis com essa função. Para saber mais, consulte [Uma nova função apareceu na minha conta do IAM](#).

Criando a função vinculada a serviços a partir do console do Migration Hub

Você pode usar o console do Migration Hub para criar a `AWSServiceRoleForApplicationDiscoveryServiceContinuousExport` função vinculada ao serviço do.

Como criar a função vinculada ao serviço (console)

1. No painel de navegação, selecione Data Collectors (Coletores de dados).
2. Clique na guia Agents (Agentes).
3. Alterne o Exploração de dados no Athenadeslize até a posição Ligado.
4. Na caixa de diálogo gerada a partir da etapa anterior, clique na caixa de seleção para concordar com os custos associados e selecione Continue (Continuar) ou Enable (Habilitar).

Criar uma função vinculada ao serviço a partir da AWS CLI

Você pode usar os comandos do Application Discovery Service do AWS Command Line Interface para criar a `AWSServiceRoleForApplicationDiscoveryServiceContinuousExport` função vinculada ao serviço do.

Essa função vinculada ao serviço é criada automaticamente quando você inicia a Exportação Contínua a partir do AWS CLI (o AWS CLI deve primeiro ser instalado em seu ambiente).

Para criar uma função vinculada ao serviço (CLI) iniciando a Export Contínua da AWS CLI

1. Instale a AWS CLI no sistema operacional (Linux, macOS ou Windows). Consulte a [AWS Command Line Interface Guia do usuário do](#) Para obter instruções.
2. Abra o prompt de comando (Windows) ou o Terminal (macOS/Linux).
 - a. Digite `aws configure` e pressione Enter.
 - b. Insira seu `AWSId` da chave de acesso da `AWS` Chave de acesso secreta.
 - c. Digite `us-west-2` no Default Region Name (Nome padrão da região).
 - d. Digite `text` no Default Output Format (Formato padrão de saída).
3. Digite o seguinte comando:

```
aws discovery start-continuous-export
```


Você também pode usar o console do IAM para criar uma função vinculada ao serviço com aDiscovery Service - Exportação contínuaCaso de uso. Na CLI ou na API do IAM, crie uma função vinculada ao serviço com o nome de serviço `continuousexport.discovery.amazonaws.com`. Para obter mais informações, consulte [Criar uma função vinculada ao serviço](#) no Guia do usuário do IAM. Se você excluir essa função vinculada ao serviço, será possível usar esse mesmo processo para criar a função novamente.

Exclusão de uma função vinculada ao serviço do Application Discovery Service

Se você não precisar mais usar um recurso ou serviço que requer uma função vinculada a serviço, é recomendável excluí-la. Dessa forma, você não tem uma entidade não utilizada que não seja monitorada ativamente ou mantida. No entanto, você deve limpar sua função vinculada ao serviço para excluí-la manualmente.

Limpeza da função vinculada ao serviço

Antes de usar o IAM para excluir uma função vinculada ao serviço, você deverá excluir qualquer recurso usado pela função.

Note

Se o Application Discovery Service estiver usando a função quando você tentar excluir os recursos, a exclusão poderá falhar. Se isso acontecer, espere alguns minutos e tente a operação novamente.

Para excluir recursos do Application Discovery Service usados pelo `AWSServiceRoleForApplicationDiscoveryServiceContinuousExport` função vinculada ao serviço do Console do Migration Hub

1. No painel de navegação, selecione Data Collectors (Coletores de dados).
2. Clique na guia Agents (Agentes).
3. Alterne oExploração de dados no Athenadeslize para a posição Desligado.

Para excluir recursos do Application Discovery Service usados pelo `AWSServiceRoleForApplicationDiscoveryServiceContinuousExport` função vinculada ao serviço da AWS CLI

1. Instale a AWS CLI no sistema operacional (Linux, macOS ou Windows). Consulte a [AWS Command Line Interface Guia do usuário do](#) Para obter instruções.
2. Abra o prompt de comando (Windows) ou o Terminal (macOS/Linux).
 - a. Digite `aws configure` e pressione Enter.
 - b. Insira seu `AWSId` da chave de acesso da `AWS` Chave de acesso secreta.
 - c. Digite `us-west-2` no Default Region Name (Nome padrão da região).
 - d. Digite `text` no Default Output Format (Formato padrão de saída).
3. Digite o seguinte comando:

```
aws discovery stop-continuous-export --export-id <export ID>
```

- Se você não souber o ID de exportação da exportação contínua que deseja interromper, insira o seguinte comando para ver o ID de exportação:

```
aws discovery describe-continuous-exports
```

4. Digite o comando a seguir para garantir que a exportação contínua tenha sido interrompida, verificando se o status de devolução é "INATIVO":

```
aws discovery describe-continuous-export
```

Excluir manualmente a função vinculada ao serviço

Você pode excluir a `AWSServiceRoleForApplicationDiscoveryServiceContinuousExport` Uma função vinculada ao serviço usando o console, a CLI ou a API do IAM. Se você não precisa mais usar os recursos do Discovery Service - Export Contínua que exigem essa função vinculada ao serviço, é recomendável excluí-la. Dessa forma, você não tem uma entidade não utilizada que não seja monitorada ativamente ou mantida. Para obter mais informações, consulte [Excluir uma função vinculada ao serviço](#) no Guia do usuário do IAM.

Note

Primeiramente, limpe sua função vinculada ao serviço antes de excluí-la. Consulte [Limpeza da função vinculada ao serviço](#).

Solução de problemas AWS Application Discovery Service de identidade e acesso

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

Tópicos

- [Não estou autorizado a realizar o meu pedido: PassRole](#)

Não estou autorizado a realizar o meu pedido: PassRole

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

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

O exemplo de erro a seguir ocorre quando um usuário do IAM chamado `marymajor` tenta usar o console para realizar uma ação no Application Discovery Service. 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.

Registrar em log e monitorar no AWS Application Discovery Service

O AWS Application Discovery Service é integrado ao AWS CloudTrail. Você pode usar CloudTrail para registrar, monitorar e reter continuamente a atividade da conta para fins de solução de problemas e auditoria. CloudTrail fornece um histórico de eventos do seu AWS atividade da conta, incluindo ações realizadas por meio do AWS Console de gerenciamento de AWS Os SDKs da e as ferramentas de linha de comando. O tópico desta seção explica como usar CloudTrail Com Application Discovery Service.

Tópicos

- [Registro de chamadas de API do Application Discovery Service com AWS CloudTrail](#)

Registro de chamadas de API do Application Discovery Service com AWS CloudTrail

AWS Application Discovery Service O é integrado ao AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, função ou um AWS Application Discovery Service. CloudTrail captura todas as chamadas de API para Application Discovery Service como eventos. As chamadas capturadas incluem as chamadas do console do Application Discovery Service e as chamadas de código para as operações da API do Application Discovery Service.

Se você criar uma trilha, poderá habilitar a entrega contínua de CloudTrail Eventos em um bucket do Amazon S3, incluindo eventos do Application Discovery Service. Se não configurar uma trilha, você ainda poderá visualizar os eventos mais recentes na CloudTrail Console do Histórico do evento. Usando as informações coletadas por CloudTrail, você pode determinar a solicitação feita ao Application Discovery Service, o endereço IP do qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita e outros detalhes.

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

Application Discovery Service em CloudTrail

CloudTrail está habilitado em sua AWS quando ela é criada. Quando alguma atividade ocorre no Application Discovery Service, essa atividade é registrada em um CloudTrail evento junto com outros AWS Eventos de serviço da em Histórico do evento. É possível visualizar, pesquisar e baixar os eventos recentes em sua conta da AWS. Para obter mais informações, consulte: [Visualizar eventos do com o CloudTrail Histórico do evento](#).

Para obter um registro contínuo de eventos em sua AWS conta da, incluindo eventos do Application Discovery Service, crie uma trilha. Uma trilha ativa CloudTrail para enviar 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 AWS serviços da para analisar mais ainda mais e agir com base nos dados de eventos coletados no CloudTrail troncos. Para obter mais informações, consulte as informações a seguir.

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

Todas as ações do Application Discovery Service CloudTrail e estão documentados na [Application Discovery Service](#). Por exemplo, as chamadas para `CreateTags`, `DescribeTags`, e `GetDiscoverySummary` geram entradas na CloudTrail arquivos de log.

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

- Se a solicitação foi feita com credenciais de usuário raiz 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](#).

Entendendo as entradas do arquivo de log do Applic

Uma trilha é uma configuração que permite a entrega de eventos como arquivos de log a um bucket do Amazon S3 especificado. CloudTrail Os arquivos de log contêm uma ou mais entradas de log. Um evento representa uma única solicitação de qualquer origem e inclui informações sobre a ação solicitada, a data e a hora da ação, os parâmetros de solicitação e assim por diante. CloudTrail Os arquivos de log 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 um CloudTrail entrada de registro que demonstra aDescribeTagsação.

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROAJBHMC4H6EKEXAMPLE:sample-user",
    "arn": "arn:aws:sts::444455556666:assumed-role/ReadOnly/sample-user",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AIDAJQABLZS4A3QDU576Q",
        "arn": "arn:aws:iam::444455556666:role/ReadOnly",
        "accountId": "444455556666",
        "userName": "sampleAdmin"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2020-05-05T15:19:03Z"
      }
    }
  },
  "eventTime": "2020-05-05T17:02:40Z",
  "eventSource": "discovery.amazonaws.com",
  "eventName": "DescribeTags",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "20.22.33.44",
  "userAgent": "Coral/Netty4",
  "requestParameters": {
    "maxResults": 0,
    "filters": [
```

```
    {
      "values": [
        "d-server-0315rfdjreyqsq"
      ],
      "name": "configurationId"
    }
  ]
},
"responseElements": null,
"requestID": "mgh-console-eb1cf315-e2b4-4696-93e5-b3a3b9346b4b",
"eventID": "7b32b778-91c9-4c75-9cb0-6c852791b2eb",
"eventType": "AwsApiCall",
"recipientAccountId": "111122223333"
}
```

Cotas do AWS Application Discovery Service

O console de Cotas de serviço fornece informações sobre as cotas do AWS Application Discovery Service. É possível usar o console do Service Quotas para visualizar as cotas de serviço padrão ou [Aumentos de cota de solicitação](#) para cotas ajustáveis.

Atualmente, a única cota que pode ser aumentada é servidores importados por conta.

O Application Discovery Service tem as cotas padrão a seguir:

- 1.000 aplicativos por conta.

Se você atingir essa cota e quiser importar novos aplicativos, poderá excluir aplicativos existentes com o `DeleteApplications` Ação de API. Para obter mais informações, consulte [DeleteApplications](#) no Referência do Application Discovery Service.

- Cada arquivo de importação pode ter um tamanho máximo de 10 MB.
- 25.000 registros de servidor importados por conta.
- 25.000 exclusões de registros de importação por dia.
- 10.000 servidores importados por conta (você pode solicitar o aumento dessa cota).
- 1.000 agentes ativos, que estão coletando e enviando dados ao Application Discovery Service.
- 10.000 agentes inativos, que são responsivos, mas não ao coletar dados.
- 400 servidores por aplicativo.
- 30 tags por servidor.

Solução de problemas AWS Application Discovery Service

Nesta seção, você encontrará informações sobre como resolver questões frequentes com o AWS Application Discovery Service.

Tópicos

- [Pare a coleta de dados por meio da exploração de dados](#)
- [Remova os dados coletados pela exploração de dados](#)
- [Corrija problemas comuns com a exploração de dados no Amazon Athena](#)
- [Solução de problemas de registros de importação com falha](#)

Pare a coleta de dados por meio da exploração de dados

Para interromper a exploração de dados, você pode desativar a chave seletora no console do Migration Hub, na guia Descobrir > Coletores de dados > Agentes, ou invocar a API.

StopContinuousExport Pode levar até 30 minutos para interromper a coleta de dados e, durante esse estágio, a chave seletora no console e a invocação da DescribeContinuousExport API mostrarão o estado da exploração de dados como “Parada em andamento”.

Note

Se depois de atualizar a página do console, a alternância não for desativada e uma mensagem de erro for lançada ou a API DescribeContinuousExport retornar ao estado de "Stop_Failed", você pode tentar outra vez ao alternar o interruptor ou ligar para a API StopContinuousExport. Se a “exploração de dados” ainda apresentar erros e não for interrompida com sucesso, entre em contato com o AWS suporte.

Como alternativa, a coleta de dados poderá ser interrompida manualmente, como está descrito nas etapas a seguir.

Opção 1: Interromper coleta de dados do agente

Se você já estiver finalizado sua descoberta usando os agentes ADS e não desejar coletar dados adicionais no repositório de banco de dados ADS:

1. No console do Migration Hub, escolha a guia Descobrir > Coletores de dados > Agentes.

2. Selecione todos os agentes em andamento e escolha Stop Data Collection (Interromper coleta de dados).

Isso garantirá que nenhum dado novo seja coletado pelos agentes no repositório de dados ADS e no seu bucket do S3. Seus dados existentes continuarão acessíveis.

Opção 2: excluir o Amazon Kinesis Data Streams da exploração de dados

Se você quiser continuar coletando dados por agentes no repositório de dados do ADS, mas não quiser coletar dados em seu bucket do Amazon S3 usando a exploração de dados, você pode excluir manualmente os streams do Amazon Data Firehose criados pela exploração de dados:

1. Faça login no Amazon Kinesis a partir do AWS console e escolha Data Firehose no painel de navegação.
2. Exclua os seguintes fluxos criados pelo recurso de exploração de dados:
 - `aws-application-discovery-service-id_mapping_agent`
 - `aws-application-discovery-service-inbound_connection_agent`
 - `aws-application-discovery-service-network_interface_agent`
 - `aws-application-discovery-service-os_info_agent`
 - `aws-application-discovery-service-outbound_connection_agent`
 - `aws-application-discovery-service-processes_agent`
 - `aws-application-discovery-service-sys_performance_agent`

Remova os dados coletados pela exploração de dados

Para remover dados coletados pela exploração de dados

1. Remova os dados do agente de descoberta armazenados no Amazon S3.

Os dados coletados pelo AWS Application Discovery Service (ADS) são armazenados em um bucket do S3 chamado `aws-application-discovery-service-uniqueid`.

Note

Excluir o bucket do Amazon S3 ou qualquer um dos objetos nele enquanto a exploração de dados no Amazon Athena está ativada causa um erro. Ele continua enviando novos

dados do agente de descoberta para o S3. Os dados excluídos também não estarão mais acessíveis no Athena.

2. Remover AWS Glue Data Catalog.

Quando a exploração de dados no Amazon Athena é ativada, ele cria um bucket do Amazon S3 em sua conta para armazenar os dados coletados pelos agentes do ADS em intervalos de tempo regulares. Além disso, ele também cria um AWS Glue Data Catalog para permitir que você consulte os dados armazenados em um bucket do Amazon S3 a partir do Amazon Athena. Quando você desativa a exploração de dados no Amazon Athena, nenhum dado novo é armazenado em seu bucket do Amazon S3, mas os dados coletados anteriormente persistirão. Se você não precisar mais desses dados e quiser devolver sua conta ao estado anterior à ativação da exploração de dados no Amazon Athena.

- a. Visite o Amazon S3 a partir do AWS console e exclua manualmente o bucket com o nome "aws-application-discover-discovery-service-uniqueid"
- b. Você pode remover manualmente a exploração de dados AWS Glue Data Catalog excluindo o application-discovery-service-databasebanco de dados e todas essas tabelas:
 - os_info_agent
 - network_interface_agent
 - sys_performance_agent
 - processes_agent
 - inbound_connection_agent
 - outbound_connection_agent
 - id_mapping_agent

Removendo seus dados do AWS Application Discovery Service

Para que todos os seus dados sejam removidos do Application Discovery Service, entre em contato com o [AWS Support](#) e solicite a exclusão total dos dados.

Corrija problemas comuns com a exploração de dados no Amazon Athena

Nesta seção, você pode encontrar informações sobre como corrigir problemas comuns com a exploração de dados no Amazon Athena.

Tópicos

- [A exploração de dados no Amazon Athena não é iniciada porque as funções vinculadas ao serviço e os recursos necessários AWS não podem ser criados](#)
- [Os dados do novo agente não aparecem no Amazon Athena](#)
- [Você não tem permissões suficientes para acessar o Amazon S3, o Amazon Data Firehose ou AWS Glue](#)

A exploração de dados no Amazon Athena não é iniciada porque as funções vinculadas ao serviço e os recursos necessários AWS não podem ser criados

Quando você ativa a exploração de dados no Amazon Athena, ele cria a função vinculada ao serviço em sua conta que permite criar os AWS recursos necessários para tornar os dados coletados pelo agente acessíveis no Amazon Athena, incluindo um bucket do Amazon S3, streams do Amazon Kinesis e `AWSServiceRoleForApplicationDiscoveryServiceContinuousExport` AWS Glue Data Catalog. Se sua conta não tiver as permissões corretas para a exploração de dados no Amazon Athena para criar essa função, ela não será inicializada. Consulte [AWS políticas gerenciadas para AWS Application Discovery Service](#).

Os dados do novo agente não aparecem no Amazon Athena

Se novos dados não fluírem para o Athena, já se passaram mais de 30 minutos desde que um agente foi iniciado e o status da exploração de dados for Ativo, verifique as soluções listadas abaixo:

- AWS Agentes Discovery

Certifique-se de que o status Collection (Coleta) do seu agente esteja marcado como Started (Iniciado) e o estado de Health (Integridade) esteja como Running (Em execução).

- Função do Kinesis

Certifique-se de que você tenha a função `AWSApplicationDiscoveryServiceFirehose` na sua conta.

- Status do Firehose

Verifique se os seguintes fluxos de entrega do Firehose estão funcionando corretamente:

- `aws-application-discovery-service/os_info_agent`
- `aws-application-discovery-service-network_interface_agent`
- `aws-application-discovery-service-sys_performance_agent`
- `aws-application-discovery-service-processes_agent`
- `aws-application-discovery-service-inbound_connection_agent`
- `aws-application-discovery-service-outbound_connection_agent`
- `aws-application-discovery-service-id_mapping_agent`

- AWS Glue Data Catalog

Certifique-se de que o `application-discovery-service-database` banco de dados esteja ativo AWS Glue. Certifique-se de que as seguintes tabelas estejam presentes no AWS Glue:

- `os_info_agent`
- `network_interface_agent`
- `sys_performance_agent`
- `processes_agent`
- `inbound_connection_agent`
- `outbound_connection_agent`
- `id_mapping_agent`

- Bucket do Amazon S3

Certifique-se de ter um bucket do Amazon S3 nomeado `aws-application-discovery-service-uniqueid` em sua conta. Se os objetos no bucket tiverem sido movidos ou excluídos, eles não aparecerão corretamente no Athena.

Certifique-se de que seus servidores estejam funcionando, para que assim os seus agentes colem e enviem dados para o AWS Application Discovery Service.

Você não tem permissões suficientes para acessar o Amazon S3, o Amazon Data Firehose ou AWS Glue

Se você estiver usando AWS Organizations e a inicialização da exploração de dados no Amazon Athena falhar, pode ser porque você não tem permissões para acessar o Amazon S3, o Amazon Data Firehose, o Athena ou AWS Glue.

Você precisará de um usuário do IAM com permissões de administrador para conceder acesso a esses serviços. Um administrador pode usar sua própria conta para conceder este acesso. Consulte [AWS políticas gerenciadas para AWS Application Discovery Service](#).

Para garantir que a exploração de dados no Amazon Athena funcione corretamente, não modifique nem exclua os AWS recursos criados pela exploração de dados no Amazon Athena, incluindo o bucket do Amazon S3, o Amazon Data Firehose Streams e AWS Glue Data Catalog. Se os recursos forem acidentalmente excluídos ou modificados, interrompa e inicie a Exploração de dados. Esta ação criará automaticamente esses recursos outra vez. Se você excluir o bucket do Amazon S3 criado pela exploração de dados, poderá perder os dados que foram coletados no bucket.

Solução de problemas de registros de importação com falha

A importação do Migration Hub permite que você importe detalhes do seu ambiente local diretamente para o Migration Hub sem usar o Discovery Connector ou o Discovery Agent. Assim, você tem a opção de executar a avaliação de migração e o planejamento diretamente de seus dados importados. Você também pode agrupar seus dispositivos como aplicativos e acompanhar seu status de migração.

Na importação de dados, é possível que você encontre erros. Em geral, esses erros ocorrem por um dos seguintes motivos:

- Uma cota relacionada à importação foi atingida — Há uma cota associada às tarefas de importação. Se você fizer uma solicitação de tarefa de importação que exceda as cotas, a solicitação falhará e retornará um erro. Para ter mais informações, consulte [Cotas do AWS Application Discovery Service](#).

- Uma vírgula extra (,) foi inserida no arquivo de importação — vírgulas em arquivos.CSV são usadas para diferenciar um campo do próximo. Não há suporte para vírgulas dentro de um campo porque elas sempre dividirão o campo. Isso pode causar uma cascata de erros de formatação. Certifique-se de usar vírgulas apenas entre campos e não de outra forma em seus arquivos de importação.
- Um campo tem um valor fora do intervalo suportado — alguns campos, por exemplo, CPU.NumberOfCores devem ter um intervalo de valores compatíveis. Se você tiver mais ou menos do que esse intervalo compatível, ocorrerá uma falha na importação do registro.

Se ocorrerem erros com sua solicitação de importação, você poderá resolvê-los fazendo download de seus registros com falha da tarefa de importação e resolver os erros no arquivo CSV de entradas com falha e fazer a importação novamente.

Console

Para fazer download do arquivo de registros com falha

1. 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 lado esquerdo, em Discover (Descobrir), selecione Tools (Ferramentas).
3. Em Discovery Tools (Ferramentas de descoberta), escolha view imports (exibir importações).
4. No painel Imports (Importações), escolha o botão de opção associado a uma solicitação de importação com algum número de Failed records (Registros com falha).
5. Escolha Download failed records (Fazer download de registros com falha) acima da tabela no painel. Isso abrirá a caixa de diálogo de download do navegador para fazer download do arquivo compactado.

AWS CLI

Para fazer download do arquivo de registros com falha

1. Abra uma janela do terminal e digite o seguinte comando, em que *ImportName* is the name of the import task with the failed entries that you want to correct.:

```
aws discovery describe-import-tasks - -name ImportName
```

2. Na saída, copie todo o conteúdo do valor retornado para `errorsAndFailedEntriesZip`, sem aspas.
3. Abra um navegador da web e cole o conteúdo na caixa de texto da URL e pressione ENTER. Isso fará download do arquivo de registros compactado com falha em um formato `.zip`.

Agora que você fez download do arquivo compactado de registros com falha, poderá extrair os dois arquivos internos e corrigir os erros. Se os erros estiverem vinculados a limites com base em serviço, você precisará solicitar um aumento de limite ou excluir recursos associados suficientes para que sua conta fique abaixo do limite. O arquivo compactado tem os seguintes arquivos:

- `errors-file.csv` — Esse arquivo é seu registro de erros e rastreia a linha, o nome da coluna e uma mensagem de erro descritiva para cada registro com falha de cada entrada com falha. `ExternalId`
- `failed-entries-file.csv` — Esse arquivo contém somente as entradas com falha do arquivo de importação original.

Para corrigir os non-limit-based erros encontrados, use o `errors-file.csv` para corrigir os problemas no `failed-entries-file.csv` arquivo e, em seguida, importe esse arquivo. Para obter instruções sobre como importar arquivos, consulte [Importação de dados](#).

Histórico de documentos do AWS Application Discovery Service

Última atualização da documentação do Guia do Usuário: 16 de maio de 2023

A tabela a seguir descreve alterações importantes no Manual do usuário do Application Discovery Service após 18 de junho de 2019. Para receber notificações sobre atualizações da documentação, inscreva-se no feed RSS.

Alteração	Descrição	Data
Apresentando o banco de dados Agentless Collector e o módulo de coleta de dados analíticos	O módulo de coleta de dados de banco de dados e análises é o novo módulo do Application Discovery Service Agentless Collector (Agentless Collector). Você pode usar esse módulo de coleta de dados para se conectar ao seu ambiente e coletar metadados e métricas de desempenho de seu banco de dados local e servidores de análise. Para obter mais informações, consulte Módulo de coleta de dados de banco de dados e análises .	16 de maio de 2023
Apresentando o Application Discovery Service Agentless Collector	O Application Discovery Service Agentless Collector (Agentless Collector) é o novo aplicativo AWS Application Discovery Service local que coleta informações por meio de métodos sem agente sobre seu ambiente local	16 de agosto de 2022

para ajudá-lo a planejar com eficiência sua migração para o. Nuvem AWS Para obter mais informações, consulte [Agentless](#) Collector.

[Atualização do IAM](#)

A `discovery:GetNetworkConnectionGraph` ação AWS Identity and Access Management (IAM) agora está disponível para conceder acesso ao diagrama de rede do AWS Migration Hub console ao criar uma política baseada em identidade. Para obter mais informações, consulte [Conceder permissões para usar o diagrama de rede](#).

24 de maio de 2022

[Apresentando a região de origem](#)

A região inicial do Migration Hub fornece um único repositório de informações de planejamento de descoberta e migração para todo o seu portfólio e uma visão única das migrações para várias AWS regiões.

20 de novembro de 2019

[Apresentando o recurso de importação do Migration Hub](#)

A importação do Migration Hub permite importar informações sobre seus servidores e aplicativos locais para o Migration Hub, incluindo especificações do servidor e dados de utilização. Você também pode usar esses dados para monitorar o status de migrações de aplicativos. Para obter mais informações, consulte [Importação do Migration Hub](#).

18 de janeiro de 2019

A tabela a seguir descreve as versões da documentação do Guia do usuário do Application Discovery Service antes de 18 de janeiro de 2019:

Alteração	Descrição	Data
Novo recurso	Documentos atualizados para apoiar a exploração de dados no Amazon Athena e adicionar um capítulo de solução de problemas.	09 de agosto de 2018
Revisões importantes	Regrava para obter detalhes de uso e saída; o documento inteiro foi reestruturado.	25 de maio de 2018
Discovery Agent 2.0	Há uma versão nova e melhorada do Application Discovery Agent.	19 de outubro de 2017
Console	O AWS Management Console foi adicionado.	19 de dezembro de 2016

Alteração	Descrição	Data
Descoberta sem agente	Esta versão descreve como definir e configurar a descoberta sem agente.	28 de julho de 2016
Novo detalhes para Microsoft Windows Server e correções para problemas de comando	Esta atualização contém detalhes sobre o Microsoft Windows Server. Ela também documenta as correções de vários problemas de comando.	20 de maio de 2016
Publicação inicial	Esta é a primeira versão do Application Discovery Service.	12 de maio de 2016

Glossário do AWS

Para obter a terminologia mais recente da AWS, consulte o [glossário da AWS](#) na Referência do Glossário da AWS.

Apêndice

Esta seção contém informações complementares sobre. AWS Application Discovery Service

Tópicos

- [Apêndice: Transição do Discovery Connector para o Agentless Collector](#)
- [Apêndice: AWS Conector Discovery sem agente](#)

Apêndice: Transição do Discovery Connector para o Agentless Collector

Esta seção descreve como fazer a transição do AWS Agentless Discovery Connector (Discovery Connector) para o Application Discovery Service Agentless Collector (Agentless Collector).

Recomendamos que os clientes que atualmente usam o Discovery Connector façam a transição para o novo Agentless Collector.

Para saber como começar a usar o Agentless Collector, consulte. [Introdução ao Agentless Collector](#)

Depois que o Agentless Collector for implantado, você poderá excluir a máquina virtual do Discovery Connector. Todos os dados coletados anteriormente continuarão disponíveis no AWS Migration Hub (Migration Hub).

Apêndice: AWS Conector Discovery sem agente

Important

Recomendamos que os clientes que atualmente usam o Discovery Connector façam a transição para o novo Agentless Collector. Para ter mais informações, consulte [Apêndice: Transição do Discovery Connector para o Agentless Collector](#).

Tópicos

- [Dados coletados pelo Discovery Connector](#)
- [Coleta de dados Discovery Connector](#)
- [Solução de problemas do Discovery Connector](#)

Dados coletados pelo Discovery Connector

O Discovery Connector coleta informações sobre seus hosts e VMs do VMware vCenter Server. No entanto, você só pode coletar esses dados se as ferramentas do VMware vCenter Server estiverem instaladas. Para garantir que a AWS conta que você está usando tenha a permissão necessária para essa tarefa, consulte [AWS políticas gerenciadas para AWS Application Discovery Service](#).

A seguir, você pode encontrar um inventário das informações coletadas pelo Discovery Connector.

Legenda da tabela dos dados coletados do Discovery Connector:

- Os dados coletados estão em Kilobytes (KB), a menos que especificado de outra forma.
- Dados equivalentes no console do Migration Hub são reportados em megabytes (MB).
- Os campos de dados indicados com um asterisco (*) só estão disponíveis nos arquivos.csv produzidos pela função de exportação da API do conector.
- O período de sondagem ocorre em intervalos de aproximadamente 60 minutos.
- Os campos de dados indicados com um asterisco duplo (**) retornam atualmente um valor nulo.

Campo de dados	Descrição
applicationConfigurationId*	ID do aplicativo de migração na qual a VM está agrupada
avgCpuUsagePct	Porcentagem média de uso da CPU durante o período de sondagem
avgDiskBytesReadPerSecond	Número médio de bytes lidos no disco durante o período de sondagem
avgDiskBytesWrittenPerSecond	Número médio de bytes gravados no disco durante o período de sondagem
avgDiskReadOpsPerSecond**	Número médio de operações de E/S de leitura por segundo nulo
avgDiskWriteOpsPerSecond**	Número médio de operações de E/S de gravação por segundo

Campo de dados	Descrição
avgFreeRAM	Capacidade média da RAM disponível em MB
avgNetworkBytesReadPerSecond	Média de throughput de bytes lidos por segundo
avgNetworkBytesWrittenPerSecond	Média de throughput de bytes gravados por segundo
configId	ID atribuída ao Application Discovery Service à VM descoberta
configType	Tipo de recurso descoberto
connectorId	ID do dispositivo virtual do Discovery Connector
cpuType	vCPU para uma VM, modelo real para um host
datacenterId	ID do vCenter
hostId*	ID do host da VM
hostName	Nome do host que executa o software de virtualização
hypervisor	Tipo de hypervisor
id	ID do servidor
lastModifiedTime ^{Carimbo *}	Data e hora da última coleta de dados antes da exportação dos dados
macAddress	Endereço MAC da VM
manufacturer	Criador do software de virtualização
maxCpuUsagePct	Porcentagem máx. de uso da CPU durante o período de sondagem

Campo de dados	Descrição
maxDiskBytesReadPerSecond	Número máx. de bytes lidos no disco durante o período de sondagem
maxDiskBytesWrittenPerSecond	Número máx. de bytes gravados no disco durante o período de sondagem
maxDiskReadOpsPerSecond ^{**}	Número máx. de operações de E/S de leitura por segundo
maxDiskWriteOpsPerSecond ^{**}	Número máx. de operações de E/S de gravação por segundo
maxNetworkBytesReadPerSecond	Quantidade máx. de transferência de bytes lidos por segundo
maxNetworkBytesWrittenPerSecond	Quantidade máx. de transferência de bytes gravados por segundo
memoryReservation [*]	Limite para evitar a sobrecarga de memória na VM
moRefId	ID exclusiva de referência do objeto gerenciado do VCenter
name [*]	Nome da VM ou rede (usuário especificado)
numCores	Quantidade de unidades de processamento independente dentro da CPU
numCpus	Quantidade de unidades de processamento central na VM
numDisks ^{**}	Quantidade de discos na VM
numNetworkCards ^{**}	Quantidade de placas de rede na VM
osName	Nome do sistema operacional na VM

Campo de dados	Descrição
osVersion	Versão do sistema operacional na VM
portGroupId*	ID do grupo de portas de VLAN
portGroupName*	Nome do grupo de portas de VLAN
powerState*	Status de energia
serverId	ID atribuída ao Application Discovery Service à VM descoberta
smBiosId*	ID/versão do BIOS de gerenciamento de sistemas
estado*	Status do dispositivo virtual do Discovery Connector
toolsStatus	Estado operacional das ferramentas da VMware (Consulte Visualização e classificação de coletores de dados para obter uma lista completa.)
totalDiskSize	Capacidade total do disco em MB
totalRAM	Total de RAM disponível na VM em MB
type	Tipo de host
vCenterId	ID exclusivo de uma VM
vCenterName*	Nome do host do vCenter
virtualSwitchName*	Nome do switch virtual
vmFolderPath	Caminho do diretório de arquivos da VM
vmName	Nome da máquina virtual

Coleta de dados Discovery Connector

Depois que o Discovery Connector for implantado e configurado em seu ambiente VMware, se a coleta de dados for interrompida, você poderá reiniciá-la. Você pode iniciar ou interromper a coleta de dados por meio do console ou fazendo chamadas de API por meio do AWS CLI. Ambos os métodos são descritos nos procedimentos a seguir.

Using the Migration Hub Console

O procedimento a seguir mostra como iniciar ou interromper o processo de coleta de dados do Discovery Connector, na página Coletores de Dados do console do Migration Hub.

Para iniciar ou interromper a coleta de dados

1. No painel de navegação, selecione Data Collectors (Coletores de dados).
2. Clique na a guia Connectors (Conectores).
3. Marque a caixa de seleção do conector que você deseja iniciar ou parar.
4. Selecione Start data collection (Iniciar coleta de dados) ou Stop data collection (Interromper coleta de dados).

Note

Se não for possível visualizar as informações de inventário após o início da coleta de dados com o conector, confira se você registrou o conector com o vCenter Server.

Using the AWS CLI

Para iniciar o processo de coleta de dados do Discovery Connector a partir do AWS CLI, o AWS CLI deve primeiro ser instalado em seu ambiente e, em seguida, você deve configurar a CLI para usar a região de [origem do Migration Hub](#) selecionada.

Para instalar AWS CLI e iniciar a coleta de dados

1. Instale o AWS CLI para seu sistema operacional (Linux, macOS ou Windows). Consulte o [Guia AWS Command Line Interface do usuário](#) para obter instruções.
2. Abra o prompt de comando (Windows) ou o Terminal (macOS/Linux).
 - a. Digite `aws configure` e pressione Enter.

- b. Insira o ID da chave de AWS acesso e a chave de acesso AWS secreta.
 - c. Insira sua região de origem para o nome da região padrão. Por exemplo, us-west-2.
 - d. Digite `text` no Default Output Format (Formato padrão de saída).
3. Para encontrar o ID do conector para o qual você deseja iniciar ou interromper a coleta de dados, digite o seguinte comando para ver o ID do conector:

```
aws discovery describe-agents --filters  
condition=EQUALS,name=hostName,values=connector
```

4. Para iniciar a coleta de dados pelo conector, digite o seguinte comando:

```
aws discovery start-data-collection-by-agent-ids --agent-ids <connector ID>
```

Note

Se não for possível visualizar as informações de inventário após o início da coleta de dados com o conector, confira se você registrou o conector com o vCenter Server.

Para interromper a coleta de dados pelo conector, digite o seguinte comando:

```
aws discovery stop-data-collection-by-agent-ids --agent-ids <connector ID>
```

Solução de problemas do Discovery Connector

Esta seção contém tópicos que podem ajudá-lo a solucionar problemas conhecidos com o Application Discovery Service Discovery Connector.

A correção que o Discovery Connector não pode alcançar AWS durante a configuração

Ao configurar o AWS Agentless Discovery Connector no console, você pode receber a seguinte mensagem de erro:

i Não foi possível alcançar AWS

AWS não pode ser acessado (conexão redefinida). Verifique as configurações de rede e proxy.

Esse erro ocorre devido a uma tentativa fracassada do Discovery Connector de estabelecer uma conexão HTTPS com um AWS domínio com o qual o conector precisa se comunicar durante o processo de configuração. A configuração do Discovery Connector falhará se uma conexão não puder ser estabelecida.

Para corrigir a conexão com AWS

1. Verifique com seu administrador de TI se o firewall da sua empresa está bloqueando o tráfego de saída na porta 443 para qualquer um dos AWS domínios que precisam de acesso externo.

Os seguintes AWS domínios precisam de acesso externo:

- `awsconnector.Migration Hub home Region.amazonaws.com`
- `sns.Migration Hub home Region.amazonaws.com`
- `arsenal-discovery.Migration Hub home Region.amazonaws.com`
- `iam.amazonaws.com`
- `aws.amazon.com`
- `ec2.amazonaws.com`

Se seu firewall estiver bloqueando o tráfego de saída, desbloqueie-o. Depois de atualizar o firewall, reconfigure o conector.

2. Se a atualização do firewall não resolver o problema de conexão, verifique se a máquina virtual do conector tem conectividade de rede de saída com os domínios listados. Se a máquina virtual tiver conectividade de saída, teste a conexão com os domínios listados executando o telnet nas portas 443, conforme mostrado no exemplo a seguir.

```
telnet ec2.amazonaws.com 443
```

3. Se a conectividade de saída da máquina virtual estiver ativada, você deverá entrar em contato com o [AWS Support](#) para solucionar problemas adicionais.

Corrigindo conectores não íntegros

As informações de saúde de cada Discovery Connector podem ser encontradas na página [Data Collectors](#) do console do Migration Hub. É possível identificar conectores com problemas localizando os conectores com status de Health (Integridade) de Unhealthy (Não íntegro). O procedimento a seguir descreve como acessar o console do conector para identificar problemas de integridade.

Acessar um console de conector

1. Abra o console do Migration Hub em um navegador da Web e escolha Data Collectors na navegação à esquerda.
2. Na guia Connectors (Conectores) anote o IP address (Endereço IP) de cada conector com um status de integridade Unhealthy (Não íntegro).
3. Abra um navegador em qualquer computador que possa se conectar à máquina virtual do conector e insira a URL do console do conector, `https://ip_address_of_connector`, onde `ip_address_of_connector` está o endereço IP de um conector não íntegro.
4. Insira a senha do console de gerenciamento do conector, que foi configurada durante a configuração do conector.

Depois de acessar o console do conector, é possível tomar medidas para resolver um status não íntegro. Aqui é possível selecionar View Info (Visualizar informações) para vCenter connectivity (Conectividade do vCenter), e você receberá uma caixa de diálogo com uma mensagem de diagnóstico. O link View Info (Visualizar informações) só está disponível em conectores da versão 1.0.3.12 ou posterior.

Depois de corrigir os problemas de integridade, o conector vai restabelecer a conectividade com o servidor vCenter, e o status do conector será alterado para o estado HEALTHY (Íntegro). Se os problemas persistirem, entre em contato com o [AWS Support](#).

As causas mais comuns para conectores não íntegros são problemas de endereço IP e problemas de credenciais. As seções a seguir podem ajudar a resolver esses problemas e a retornar um conector para um estado íntegro.

Tópicos

- [Problemas de endereço IP](#)
- [Problemas de credenciais](#)

Problemas de endereço IP

Um conector pode entrar em um estado não íntegro se o endpoint do vCenter fornecido durante a configuração do conector estiver malformatado, inválido ou se o servidor vCenter estiver inativo e inacessível. Nesse caso, ao selecionar View Info (Visualizar informações) para vCenter connectivity (Conectividade do vCenter) você receberá uma caixa de diálogo com a mensagem "Confirm the operational status of your vCenter server, or choose Edit Settings to update the vCenter endpoint." (Confirme o status operacional do servidor vCenter ou selecione Edit Settings (Editar configurações) para atualizar o endpoint do vCenter).

O procedimento a seguir pode ajudar a resolver problemas de endereço IP.

1. No console do conector (https://ip_address_of_connector), selecione Edit Settings (Editar configurações).
2. Na navegação à esquerda, selecione Step 5: Discovery Connector Set Up (Etapa 5: Configuração do conector de descoberta).
3. Em Configure vCenter credentials (Configurar credenciais do vCenter), anote o endereço IP de vCenter Host (Host do vCenter).
4. Usando uma ferramenta de linha de comando separada, como ping ou traceroute, valide se o servidor vCenter associado está ativo e se o IP pode ser acessado pela VM do conector.
 - Se o endereço IP estiver incorreto e o serviço vCenter estiver ativo, atualize o endereço IP no console do conector e selecione Next (Próximo).
 - Se o endereço IP estiver correto, mas o servidor vCenter estiver inativo, ative-o.
 - Se o endereço IP estiver correto e o servidor vCenter estiver ativo, verifique se ele está bloqueando conexões de rede de entrada devido a problemas de firewall. Em caso afirmativo, atualize as configurações de firewall para permitir conexões de entrada a partir da VM do conector.

Problemas de credenciais

Os conectores podem entrar em um estado não íntegro se as credenciais de usuário do vCenter fornecidas durante a configuração do conector forem inválidas ou não tiverem privilégios de leitura e de visualização de conta do vCenter. Nesse caso, ao selecionar View Info (Visualizar informações) para vCenter connectivity (Conectividade do vCenter) você receberá uma caixa de diálogo com a mensagem "Choose Edit Settings to update your vCenter username and password for your account

with read and view privileges." (Selecione Edit Settings (Editar configurações) para atualizar o nome de usuário e a senha do vCenter para a conta com privilégios de leitura e de visualização).

O procedimento a seguir pode ajudar a resolver problemas de credenciais. Como pré-requisito, verifique se você criou um usuário do vCenter com permissões de leitura e de visualização de conta no servidor vCenter.

1. No console do conector (https://ip_address_of_connector), selecione Edit Settings (Editar configurações).
2. Na navegação à esquerda, selecione Step 5: Discovery Connector Set Up (Etapa 5: Configuração do conector de descoberta).
3. Em Configure vCenter credentials (Configurar credenciais do vCenter), atualize o vCenter Username (Nome de usuário do vCenter) e a vCenter Password (Senha do vCenter) fornecendo as credenciais para um usuário do vCenter com permissões de leitura e de visualização.
4. Selecione Next (Próximo) para concluir a configuração.

Suporte autônomo ao host ESX

O Discovery Connector não oferece suporte a um host ESX independente. O host ESX deve fazer parte da instância do vCenter Server.

Obter suporte adicional para problemas de conectores

Se você encontrar problemas e precisar de ajuda, entre em contato com o [AWS Support](#). Você será contatado, e o envio dos logs do conector pode ser solicitado. Para obter os logs, faça o seguinte:

- Faça login novamente no console do AWS Agentless Discovery Connector e escolha Baixar pacote de registros.
- Assim que o download do pacote de log estiver concluído, o envie conforme as instruções do AWS Support.

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.