Manual do usuário

AWS Application Discovery Service

AWS Application Discovery Service: Manual do usuário

Table of Contents

O que AWS Application Discovery Serviceé 1
VMware Descoberta 2
Descoberta de banco de dados 3
Compare o Agentless Collector e o Discovery Agent 3
Suposições 7
AWS Application Discovery Service mudança de disponibilidade 8
Detalhes da disponibilidade do serviço 8
AWS Transform transição 8
Perguntas frequentes 9
Configurar 11
Cadastre-se na Amazon Web Services 11
Criar usuários do IAM 11
Criação de um usuário administrativo do IAM 12
Criação de um usuário não administrativo do IAM 12
Faça login no Migration Hub e escolha uma região de origem 13
Agente Discovery 14
Como funciona 14
Dados coletados 15
Pré-requisitos 18
Instalação do Discovery Agent 20
Instale no Linux 20
Instalar no Microsoft Windows 24
Gerenciando o processo do Discovery Agent 28
Gerencie o processo no Linux 29
Gerencie o processo no Microsoft Windows 30
Desinstalando o Discovery Agent 31
Desinstalar no Linux 31
Desinstalar no Microsoft Windows 31
Iniciando e interrompendo a coleta de dados 32
Solução de problemas do Discovery 33
Solução de problemas do Discovery Agent no Linux 33
Solução de problemas do Discovery Agent no Microsoft Windows 34
Colecionador sem agente 36
Pré-requisitos 36

Configurar perímetro de dados ... 38
Configurar firewall ... 38
Implantando um coletor ... 40
Criar um usuário do IAM ... 40
Baixe o coletor ... 42
Implante o coletor ... 43
Acessando o console do coletor ... 44
Configurar o coletor ... 45
(Opcional) Configurar um endereço IP estático para a VM do coletor ... 47
(Opcional) Redefina a VM do coletor para usar DHCP ... 52
(Opcional) Configurar o Kerberos ... 54
Usando o módulo de coleta de dados de rede ... 56
Configurando o módulo de coleta de dados de rede ... 56
Tentativas de coleta de dados de rede ... 58
Status do servidor no módulo de coleta de dados de rede ... 58
Usando o módulo VMware de coleta de dados ... 59
Configurando a coleta de dados do vCenter ... 60
Visualizando detalhes da coleta de VMware dados ... 61
Controle do escopo da coleta de dados ... 62
Dados coletados pelo VMware módulo ... 63
Usando o módulo de coleta de dados de banco de dados e análises ... 68
Servidores compatíveis ... 69
Criando o coletor AWS DMS de dados ... 70
Configurando o encaminhamento de dados ... 71
Adicionando seus servidores LDAP e OS ... 72
Descobrindo seus bancos de dados ... 75
Dados coletados pelo módulo de banco de dados e análise ... 80
Visualizando dados coletados ... 81
Acessando o coletor sem agente ... 82
Painel do coletor ... 82
Editando configurações do coletor ... 85
Editando credenciais do vCenter ... 86
Atualizando o Agentless Collector ... 86
Solução de problemas ... 88
Fixação `Unable to retrieve manifest or certificate file error` ... 89
Solucionando problemas de certificação autoassinada ao configurar certificados WinRM ... 89

Corrigindo que o Agentless Collector não pode ser alcançado durante a configuração AWS 90
Corrigindo problemas de certificação autoassinada ao se conectar ao host proxy 92
Encontrando colecionadores insalubres 92
Corrigindo problemas de endereço IP 93
Corrigindo problemas de credenciais do vCenter 94
Corrigindo problemas de encaminhamento de dados 94
Corrigindo problemas de conexão 95
Suporte autônomo ao host ESX 97
Como entrar em contato com o AWS Support 97
Importação de dados para o Migration Hub 99
Formatos de importação compatíveis 100
RVTools 100
Modelo de importação do Migration Hub 100
Configurando permissões de importação 106
Carregando seu arquivo de importação para o Amazon S3 109
Como importar dados 111
Rastreando suas solicitações de importação do Migration Hub 113
Visualize e explore dados 115
Exibir dados coletados 115
Lógica de correspondência 116
Explorando dados no Athena 117
Ativando a exploração de dados 117
Explorar dados 119
Visualizando dados 120
Usando consultas predefinidas 121
Descobrindo dados com o console do Migration Hub 130
Visualizando dados no painel 130
Iniciando e interrompendo coletores de dados 131
Classificação de coletores de dados 131
Visualizando servidores 136
Classificando servidores 137
Marcação de servidores 137
Exportação de dados do servidor 139
Agrupando servidores 141
Usando a API para consultar itens descobertos 143

Usar a ação DescribeConfigurations 143
Usar a ação ListConfigurations 147
Consistência eventual 162
AWS PrivateLink 164
Considerações 164
Como criar um endpoint de interface 164
Criar uma política de endpoint 165
Usando o VPC endpoint para o Agentless Collector e o Application Discovery Agent AWS 166
Segurança 168
Gerenciamento de Identidade e Acesso 169
Público 169
Autenticação com identidades 170
Gerenciar o acesso usando políticas 171
Como AWS Application Discovery Service funciona com o IAM 173
AWS políticas gerenciadas 175
Exemplos de políticas baseadas em identidade 180
Entendendo e usando funções vinculadas a serviços 188
Solução de problemas do IAM 196
Registro de chamadas de API do CloudTrail com 197
Informações do Application Discovery Service em CloudTrail 197
Compreendendo as entradas do arquivo de log do Application Discovery Service 198
Formatos ARN 201
Cotas 202
Solução de problemas 203
Interrompa a coleta de dados por meio da exploração de dados 203
Remova os dados coletados pela exploração de dados 204
Corrija problemas comuns com a exploração de dados no Amazon Athena 206
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 206
Os dados do novo agente não aparecem no Amazon Athena 206
Você não tem permissões suficientes para acessar o Amazon S3, o Amazon Data Firehose ou AWS Glue 208
Solução de problemas de registros de importação com falha 208
Histórico do documento 211
AWS Glossário 216
..... ccxvii

O que AWS Application Discovery Serviceé

AWS Application Discovery Service ajuda você a planejar sua migração para a AWS nuvem coletando dados de uso e configuração sobre seus servidores e bancos de dados locais. O Application Discovery Service é integrado AWS Migration Hub ao AWS Database Migration Service Fleet Advisor. O Migration Hub simplifica o rastreamento da migração, pois agrega as informações do status da migração em um único console. Você pode visualizar os servidores descobertos, agrupá-los em aplicativos e, em seguida, rastrear o status de migração de cada aplicativo no 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 de banco de dados.

Todos os dados descobertos são armazenados em sua região de AWS Migration Hub origem. Portanto, você deve definir sua região de origem no console do Migration Hub ou com os 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 AWS análise como Amazon Athena e Amazon Quick.

Usando o Application Discovery Service APIs, 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 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 três 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 de seu vCenter. VMware Depois que o Agentless Collector é configurado, ele identifica as máquinas virtuais (VMs) e os 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 (Discovery Agent) em cada um de seus servidores 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.
- A importação baseada em arquivos permite que você importe detalhes do seu ambiente local diretamente para o Migration Hub sem usar o Agentless Collector ou o Discovery Agent, para que você possa realizar a avaliação e o planejamento da migração diretamente dos dados importados. Os dados ingeridos dependem dos dados fornecidos.

O Application Discovery Service se integra às soluções de descoberta de aplicativos dos AWS parceiros da 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.

VMware Descoberta

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 no vCenter e permite que ele descubra todos os seus 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 “examinar” cada um deles e VMs, como tal, não consegue descobrir quais processos estão sendo executados em cada VM nem quais conexões de rede existem. Portanto, se você precisar desse nível de detalhe e quiser examinar mais de perto alguns dos seus existentes para ajudar VMs no planejamento de sua migração, você pode instalar o Discovery Agent conforme necessário.

Além disso, se estiver VMs hospedado em VMware, você pode usar o Agentless Collector e o Discovery Agent para realizar a descoberta simultaneamente. Para obter detalhes sobre os tipos exatos de dados que cada ferramenta de descoberta coletará, consulteUsando o módulo de VMware coleta de dados vCenter Agentless Collector.

Descoberta de banco de dados

Se você tiver servidores de banco de dados e análises 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 análises 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 consultas periodicamente 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, consulteDados 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 Usando o módulo de coleta de dados de banco de dados e análises.

Compare o Agentless Collector e o Discovery Agent

A tabela a seguir fornece uma comparação rápida dos métodos de coleta de dados que o Application Discovery Service suporta.

	Colecionador sem agente	Agente Discovery	Modelo do Migration Hub	RVTools exportar
Supported server types				

	Colecionador sem agente	Agente Discovery	Modelo do Migration Hub	RVTools exportar
VMware máquina virtual	Sim	Sim	Sim	Sim
Servidor físico	Não	Sim	Sim	Sim
Deployment				
Por servidor	Não	Sim	N/D	Não
Por vCenter	Sim	Não	N/D	Sim
Por data center na mesma rede	Não	Não	N/D	Não
Collected data				
Dados do perfil do servidor (configuração estática)	Sim	Sim	Sim	Sim
Métricas de utilização do servidor do Hypervisor (CPU, RAM etc.)	Sim	Sim	Sim	Não
Métricas de utilização do servidor a partir do servidor (CPU, RAM etc.)	Sim	Sim	Sim	Não
Conexões de rede do servidor (somente TCP)	Sim	Sim	Não	Não

	Colecionador sem agente	Agente Discovery	Modelo do Migration Hub	RVTools exportar
Processos em execução	Não	Sim	Não	Não
Intervalo de coleta	-60 minutos	-15 segundos	Instantâneo único	Instantâneo único
Server data use cases				
Exibir dados do servidor no Migration Hub	Sim	Sim	Somente perfil	Não
Gere a recomendação do Amazon EC2 com base no perfil do servidor	Sim	Sim	Sim	Sim
Gere a recomendação do Amazon EC2 com base nos dados de utilização	Sim	Sim	Sim	Não
Exportação dos dados instantâneos de utilização mais recentes	Sim	Sim	Sim	Não
Exportação de dados de utilização de séries temporais	Não	Sim	Não	Não
Network data use cases				

	Colecionador sem agente	Agente Discovery	Modelo do Migration Hub	RVTools exportar
Visualização no Migration Hub	Sim	Sim	Não	Não
Exporte para o Amazon Athena para exploração adicional	Não	Sim	Não	Não
Exportar para arquivo CSV	Não	Sim	Não	Não
Database use cases				
Dados do perfil do servidor de banco de dados (configuração estática)	Sim	Não	Não	Não
Mecanismos de banco de dados compatíveis	Oracle, SQL Server, MySQL, PostgreSQL	Nenhum	Nenhum	Nenhum
Complexidade e duplicatas do esquema de banco de dados	Sim	Não	Não	Não
Objetos do esquema do banco de dados	Sim	Não	Não	Não
Platform support				

	Colecionador sem agente	Agente Discovery	Modelo do Migration Hub	RVTools exportar
Sistemas operacionais compatíveis	Qualquer sistema operacional em execução na VMware versão central v5.5 ou mais recente	Qualquer servidor Linux ou Windows	Qualquer servidor Linux ou Windows	Qualquer servidor Linux, servidor Windows ou versão VMware v5.5 ou mais recente

Suposições

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

- Você se inscreveu em 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 de origem.

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 de descoberta, conectores e importações podem ser usados somente na região de origem do Migration Hub selecionada.
- Para obter uma lista de AWS regiões nas quais você pode usar o Application Discovery Service, consulte Referência geral da Amazon Web Servicesso.

AWS Application Discovery Service mudança de disponibilidade

Após uma análise cuidadosa, decidimos fechar novos clientes AWS Application Discovery Service a partir de 7 de novembro de 2025. Se você quiser usar o serviço, inscreva-se antes dessa data. Os clientes atuais podem continuar usando o serviço normalmente.

Este tópico fornece informações sobre a mudança de disponibilidade e orientações para a transição para o. AWS Transform

Detalhes da disponibilidade do serviço

O Application Discovery Service deixará de aceitar novos clientes a partir de 7 de novembro de 2025. AWS Transform é nosso serviço de IA agente de próxima geração que fornece recursos semelhantes e recursos aprimorados de descoberta e avaliação de VMs. Os clientes existentes do Application Discovery Service podem continuar usando o serviço para concluir seus projetos de descoberta em andamento, que normalmente têm um ciclo de vida de 4 meses. A principal funcionalidade do serviço para descobrir e coletar dados sobre servidores e aplicativos locais agora está disponível AWS Transform com recursos aprimorados, sem exigir nenhum esforço do cliente para fazer a transição.

Até 7 de novembro de 2025, continuaremos mantendo a segurança e a confiabilidade do Application Discovery Service. Embora não adicionemos novos recursos ao serviço, continuamos comprometidos em fornecer atualizações de segurança e manter a disponibilidade do serviço para garantir que seus projetos de migração em andamento continuem funcionando sem problemas. Nosso foco é garantir um ambiente estável para que os clientes existentes concluam suas iniciativas de migração em voo enquanto se preparam para os recursos aprimorados disponíveis no AWS Transform.

AWS Transform transição

AWS Transform é nossa solução recomendada que reúne todos os recursos do Application Discovery Service e, ao mesmo tempo, introduz novos recursos poderosos. Ele fornece recursos abrangentes de descoberta e avaliação por meio de coletores baseados em agentes e sem agentes, com análise aprimorada do ambiente. VMware O serviço permite mapeamento automatizado de dependências de aplicativos e planejamento de ondas, ao mesmo tempo que oferece uma lógica de descoberta aprimorada com análise hipotética e estimativas de custo. Com recursos avançados,

incluindo armazenamento integrado e descoberta de banco de dados, integração consolidada de ferramentas 3P e análise abrangente da configuração da VM, foi AWS Transform projetado para tornar o processo de planejamento e avaliação da migração dos clientes mais eficiente e bem-sucedido.

A transição para AWS Transform é simples, sem a necessidade de migração de dados. Os projetos de descoberta existentes no Application Discovery Service continuarão funcionando normalmente até serem concluídos. Quando os clientes estiverem prontos para iniciar novos projetos de descoberta, eles poderão começar a usar AWS Transform diretamente — todos os recursos de descoberta e avaliação do Application Discovery Service estão disponíveis com recursos aprimorados. Para começar a usar AWS Transform , consulte o Guia de introdução. AWS A equipe de suporte está disponível por meio do console AWS Support para ajudar com o AWS Transform acesso ou fazer perguntas sobre projetos de descoberta em andamento.

Perguntas frequentes

O que isso significa para o serviço (você vai encerrar o serviço)?

O Application Discovery Service deixará de aceitar novos clientes a partir de 7 de novembro de 2025. O serviço continuará operando para que os clientes existentes concluam seus projetos de migração em andamento.

Como os clientes existentes serão afetados?

Os clientes existentes não sofrerão nenhuma interrupção em seus projetos de migração atuais. Eles podem continuar usando o Application Discovery Service normalmente até que seus projetos sejam concluídos. Todos os projetos em andamento permanecerão acessíveis e as atualizações de segurança continuarão sendo implantadas para manter a confiabilidade do serviço.

Em 7 de novembro de 2025, o cliente está tendo problemas. Como eles podem escalar?

Clientes com problemas podem entrar em contato com o AWS Support por meio do console do AWS Support. A equipe de AWS Support está disponível para ajudar com qualquer dúvida ou preocupação relacionada ao serviço.

Quais alternativas os clientes podem explorar?

AWS Transform é o serviço alternativo recomendado. Lançado em 2025, AWS Transform inclui recursos similares do Application Discovery Service. Oferece recursos aprimorados com análise

aprimorada VMware do ambiente e mapeamento automatizado de dependências. Fornece recursos integrados de detecção de banco de dados e armazenamento, além de ferramentas abrangentes de avaliação. Não são necessárias ferramentas especiais durante a transição para o. AWS Transform

Como os clientes podem migrar do Application Discovery Service?

Nenhum processo formal de migração é necessário. Os projetos existentes podem continuar no Application Discovery Service até serem concluídos. Para novos projetos, os clientes podem começar diretamente AWS Transform, o que fornece todos os recursos familiares do Application Discovery Service com recursos aprimorados. Nenhuma migração de dados é necessária, e o AWS Support está disponível para ajudar na transição.

Se você tiver outras dúvidas, entre em contato conosco pelo AWS Support ou leia nosso FAQs.

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 a https://portal.aws.amazon.com/billing/inscrição.
2. Siga as instruções online.

   Parte do procedimento de inscrição envolve receber uma chamada telefônica ou uma mensagem de texto e inserir um código de verificação pelo teclado do telefone.

   Quando você se inscreve em um Conta da AWS, um Usuário raiz da conta da AWSé criado. O usuário-raiz tem acesso a todos os Serviços da AWS e recursos na conta. Como prática recomendada de segurança, atribua o acesso administrativo a um usuário e use somente o usuário-raiz para executar tarefas que exigem acesso de 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 Console de gerenciamento da AWS 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, consulteAWS políticas gerenciadas para AWS Application Discovery Service.

Para criar um usuário do IAM não administrador

1. Em Console de gerenciamento da AWS, 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:

   - Na etapa sobre a página Definir permissões, 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, consulteAWS políticas gerenciadas para AWS Application Discovery Service.

- Quando estiver na etapa de visualização das chaves de acesso do usuário (chave de acesso IDs 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.

3. Depois de criar o usuário, forneça a ele acesso programático conforme descrito em Support programatic user access.

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 uma região de origem

1. Usando sua AWS conta, faça login Console de gerenciamento da AWS 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. Você deve registrar 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 `arsenal-discovery.`*`eu-central-1`*`.amazonaws.com` registra no Application Discovery Service.
- Ou substitua sua região de origem, conforme necessário, por 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` 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

Dados coletados pelo Discovery Agent

AWS O Application Discovery Agent (Discovery Agent) é um software que você instala em servidores locais e. VMs 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	Description
agentAssignedProcessIdentificação *	ID dos processos descobertos pelo agente
agentId	ID exclusivo do agente
agentProvidedTimeCarimbo *	Data e hora da observação do agente (mm/dd/yyyy hh:mm:ss am/pm)

Campo de dados	Description
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*	Número da porta para a data/request qual o deve ser enviado
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
netMask*	Prefixo do Endereço IP ao qual um host de rede pertence

Campo de dados	Description
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 da qual data/request se origina
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	Número total de I/O operações de leitura por segundo
totalDiskSize (GB)	Capacidade total do disco em GB
totalDiskWriteOpsPerSecond	Número total de I/O operações de gravação por segundo
totalNetworkBytesReadPerSecond (Kbps)	Total de throughput de bytes lidos por segundo

Campo de dados	Description
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

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).
- Gere as chaves de acesso necessárias para instalar o Discovery Agent.
- 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, 15 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 sua região de origem for`eu-central-1`, você usaria `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.

Instalação do Discovery Agent

Esta página aborda como instalar o Discovery Agent no Linux e no Microsoft Windows.

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 Considerações sobre 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.region.amazonaws.com/aws-discovery-agent.region/linux/latest/aws-discovery-agent.tar.gz
    ```

    b. Para fazer o download do console do Migration Hub, faça o seguinte:

        i. Faça login Console de gerenciamento da AWS e abra o console do Migration Hub em https://console.aws.amazon.com/migrationhub/.

        ii. Na página de navegação à esquerda, em Descobrir, escolha Ferramentas.

        iii. Na caixa AWS Discovery Agent, escolha Baixar agentes e, em seguida, escolha Baixar para Linux. O download começará imediatamente.

3. Verifique a assinatura de criptografia do pacote de instalação com estes três comandos:

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

```
curl -o ./discovery.gpg https://s3.region.amazonaws.com/aws-discovery-agent.region/
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 métodos de instalação a seguir.

Para...	Fazer isso...
Instale Discovery Agent	Para instalar o agente, execute o comando agent install conforme mostrado no exemplo a seguir. No exemplo, *your-home-region* substitua pelo nome da sua região de origem, *aws-access-key-id* pelo ID da chave de acesso e *aws-secret-access-key* pela chave de acesso secreta. `sudo bash install -r your-home-region -k aws-access-key-id -s aws-secret-access-key` Por padrão, os agentes baixam e aplicam automaticamente as atualizações à medida que elas se tornam disponíveis.

Para...	Fazer isso...
	Recomendamos o uso desta configuração padrão. No entanto, se você não quiser que os agentes baixem e apliquem atualizações automaticamente, inclua o `-u false` parâmetro ao executar o comando de instalação do agente.
(Opcional) Instale o Discovery Agent e configure um proxy não transparente	Para configurar um proxy não transpare nte, adicione os seguintes parâmetros ao comando de instalação do agente: • -e A senha do proxy. • -f O número da porta do proxy. • -g O esquema de proxy. • -i O nome de usuário do proxy. Veja a seguir um exemplo do comando agent install usando os parâmetros de proxy não transparentes. `sudo bash install -r your-home-region -k aws-access-key-id -s aws-secret-access-key -d myproxy.mycompany.com -e mypassword -f proxy-port-number -g https -i myusername` Se seu proxy não exigir autenticação, omita `-i` os parâmetros `-e` e. O exemplo de comando install usa`https`, se seu proxy usa HTTP, especifique `http` o valor do `-g` parâmetro.

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 sua região de origem for `eu-central-1`, você usaria `https://arsenal-discovery.eu-central-1.amazonaws.com:443`

Considerações sobre 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
```

Instale o Discovery Agent no Microsoft Windows

Conclua o procedimento a seguir para instalar um agente no Microsoft 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 métodos de instalação a seguir.

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

Para...	Fazer isso...
	Por exemplo, .INSTALLLOCATION=" *C:\install-location* " A hierarquia de pastas resultante será [caminho INSTALLLOCATION]\AWS Discovery. Por padrão, o local de instalação é a `Program Files` pasta. Opcionalmente, você pode usar `LOGANDCONFIGLOCATION` para substituir o diretório padrão (ProgramData) da pasta de registros do agente e do arquivo de configuração. A hierarquia de pastas resultante é [*LOGANDCONFIGLOCATION path*]\AWS Discovery . `.\AWSDiscoveryAgentInstaller.exe REGION=" your-home-region " KEY_ID="aws-access-key-id " KEY_SECRET=" aws-secret-access-key " /quiet` Por padrão, os agentes baixam e aplicam automaticamente as atualizações à medida que elas se tornam disponíveis. Recomendamos o uso desta configuração padrão. 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: `AUTO_UPDATE=false`

Para...	Fazer isso...
	Warning A desativação das atualizações automáticas impede que os patches de segurança mais recentes sejam instalados.

Para...	Fazer isso...
(Opcional) Instale o Discovery Agent e configure um proxy não transparente	Para configurar um proxy não transparente, adicione as seguintes propriedades públicas ao comando de instalação do agente: • 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 Veja a seguir um exemplo do comando agent install usando as propriedades de proxy não transparentes. `.\AWSDiscoveryAgentInstaller.exe REGION=" your-home-region " KEY_ID="aws-access-key-id " KEY_SECRET=" aws-secret-access-key " PROXY_HOST=" myproxy.mycompany.com " PROXY_SCHEME="https" PROXY_PORT=" proxy-port-number " PROXY_USER=" myusername " PROXY_PASSWORD=" mypassword " /quiet` Se seu proxy não exigir autenticação, omita as `PROXY_PASSWORD` propriedades `PROXY_USER` e. O exemplo de comando install usa`https`. Se seu proxy usa HTTP, `http` especifique o `PROXY_SCHEME` valor.

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 for `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 SHA256 certificado. Para atualizações SHA2 automáticas assinadas no Windows Server 2008 SP2, certifique-se de que os hosts tenham um hotfix instalado para oferecer suporte à autenticação por assinatura. SHA2 O hotfix de suporte mais recente da Microsoft ajuda a oferecer suporte à SHA2 autenticação no Windows Server 2008 SP2.

> **Note**
>
> Os hotfixes para SHA256 suporte ao 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 comando a seguir.

```
AWSDiscoveryAgentUpdater.exe /Q
```

Gerenciando o processo do Discovery Agent

Esta página aborda como gerenciar o Discovery Agent no Linux e no Microsoft Windows.

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	`sudo systemctl status aws-discovery-daemon.service`
Iniciar um agente	`sudo systemctl start aws-discovery-daemon.service`
Interromper um agente	`sudo systemctl stop aws-discovery-daemon.service`
Reiniciar um agente	`sudo systemctl restart aws-discovery-daemon.service`

Upstart

Comandos de gerenciamento para o Application Discovery Agent

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

System V init

Comandos de gerenciamento para o Application Discovery Agent

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

Gerencie o processo do Discovery Agent no Microsoft 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 AWS Atualizador Discovery	Iniciou
Iniciar um agente	AWS Agente Discovery AWS Atualizador Discovery	Escolha Iniciar
Interromper um agente	AWS Agente Discovery AWS Atualizador Discovery	Escolha Stop
Reiniciar um agente	AWS Agente Discovery AWS Atualizador Discovery	Selecione Reiniciar.

Desinstalando o Discovery Agent

Esta página aborda como desinstalar o Discovery Agent no Linux e no Microsoft Windows.

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
```

Desinstale o Discovery Agent no Microsoft Windows

Esta seção descreve como desinstalar o Discovery Agent no Microsoft Windows.

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
```

> **Note**
>
> Se o `.exe` arquivo estiver presente no servidor, você poderá desinstalar completamente o agente do servidor usando o comando a seguir. Se você usar esse comando para desinstalar, não precisará usar as `/norestart` opções `/repair` e ao reinstalar o agente.
>
> ```
> .\AWSDiscoveryAgentInstaller.exe /quiet /uninstall
> ```

Iniciar e 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 seguindo as etapas em[Iniciando e parando coletores de dados no console AWS Migration Hub](), ou fazendo

chamadas de API por meio do AWS CLI. Antes de começar, certifique-se de gerar as chaves de acesso necessárias para gerenciar o Discovery Agent.

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 sua região de origem para o nome da região padrão, por exemplo*us-west-2*. (Neste exemplo, presumimos que `us-west-2` seja sua região de origem.)
   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>
```

Solução de problemas do Discovery

Esta página aborda a solução de problemas do Discovery Agent no Linux e no Microsoft Windows.

Solução de problemas do Discovery Agent no Linux

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 diretório a seguir.

  ```
  /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, consultePré-requisitos para o Discovery Agent.

Solução de problemas do Discovery Agent no Microsoft Windows

Se você encontrar problemas ao instalar ou usar o AWS Application Discovery Agent no Microsoft 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.

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 e quantidade de RAM), metadados do banco de dados CPUs, métricas de utilização e dados sobre tráfego de rede entre servidores locais. Você instala o Agentless Collector como uma máquina virtual (VM) em seu ambiente VMware vCenter Server usando um arquivo Open Virtualization Archive (OVA).

O Agentless Collector tem uma arquitetura modular, que permite o uso de vários métodos de coleta sem agente. O Agentless Collector fornece módulos para coleta de dados de VMware VMs e para servidores de banco de dados e análises. Ele também fornece um módulo para coletar dados sobre o tráfego de rede entre seus servidores locais.

O Agentless Collector suporta a coleta de dados para AWS Application Discovery Service (Application Discovery Service) coletando dados de uso e configuração sobre seus servidores e bancos de dados locais, bem como dados sobre o tráfego de rede entre seus servidores locais.

O Application Discovery Service é integrado com AWS Migration Hub, um serviço que simplifica o rastreamento da migração, pois agrega as informações de 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 o. 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.

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, consulteFaça 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 Implantando o Application Discovery Service 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 suporta todas essas versões do VMware, mas atualmente testamos com as versões 6.7 e 7.0.

- Para a configuração VMware do vCenter Server, certifique-se de fornecer as 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, consulteConfigurar 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 Como criar um bucket no Guia do usuário do Amazon S3.
- A versão 2 do Agentless Collector requer ESXi 6.5 ou uma versão posterior.

Configure o perímetro de dados para acesso aos recursos de propriedade dos serviços da AWS

O recurso de atualização automática do Agentless Collector recupera atualizações na forma de imagens do Docker de um AWS repositório ECR público de propriedade do serviço. Se você estiver usando perímetros de dados para controlar o acesso ao Amazon ECR em seu ambiente, talvez seja necessário permitir explicitamente o acesso ao seguinte para usar o recurso de atualização automática:

- Recurso ARNs que requer acesso: `arn:aws:ecr-public::446372222237:repository/6e5498e4-8c31-4f57-9991-13b4b992ff7b`
- Permissões necessárias: `ecr-public:DescribeImages`

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. AWS Os 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 de origem 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.

- `sts.amazonaws.com`— O coletor usa esse domínio para entender com qual conta o coletor foi configurado.

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.
- `sts.amazonaws.com`— O coletor usa esse domínio para entender com qual conta o coletor foi configurado.

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, consulteCorrigindo que o Agentless Collector não pode ser alcançado durante a configuração AWS.

Implantando o Application Discovery Service Agentless Collector

Para implantar o Application Discovery Service Agentless Collector, você deve primeiro criar um usuário do IAM e baixar o coletor. Esta página mostra as etapas a serem seguidas para implantar um coletor.

Crie um usuário do IAM para o Agentless Collector

Para usar o Agentless Collector, na AWS conta em que você usouFaça 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.

  JSON

```
{
    "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.

  JSON

```
{
    "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 Console de gerenciamento da AWS, navegue até o console do IAM usando a AWS conta que você usou para definir a região de origemFaça 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 (chave de acesso IDs 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 acessoConfigurando 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.

Baixe o programa 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 local. VMware 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 VMware administrador 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 usado no ambiente do sistema, faça o download do MD5ou SHA256para obter o arquivo que contém o valor da 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 MD5 comando ou SHA256 comando da versão apropriada para verificar se a assinatura criptográfica do

`ApplicationDiscoveryServiceAgentlessCollector.ova` arquivo corresponde ao valor no respectivo SHA256 arquivo MD5/que você baixou.

```
$ md5sum ApplicationDiscoveryServiceAgentlessCollector.ova
```

```
$ sha256sum ApplicationDiscoveryServiceAgentlessCollector.ova
```

Implemente o coletor sem agente

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

Especificações da máquina virtual Agentless Collector

Agentless Collector version 2

- Sistema operacional — Amazon Linux 2023
- RAM — 16 GB
- CPU — 4 núcleos
- VMware requisitos — Veja os requisitos do VMware host para execução AL2023 em VMware

Agentless Collector version 1

- 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 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. Certifique-se de que as configurações de proxy no painel de gerenciamento do servidor estejam configuradas corretamente.
- 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 VMware Aberta (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.ova
   'vi://username:password@vcenterurl/Datacenter/host/esxi/'
  ```

  A seguir, descrevemos os ***replaceable*** valores 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.
  - Essas username/password são suas credenciais do vCenter.
  - O vcenterurl é o URL do seu vCenter.
  - O caminho vi é o caminho para seu VMware ESXi host.

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.

Acessando 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. Implemente o coletor sem agente
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. Configurando o Agentless Collector Caso contrário, a seguir você veráO painel do Agentless Collector.

Configurando 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, consulteImplantando o Application Discovery Service Agentless Collector.
   a. Em AWS chave 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 AWS chave 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 acessar AWS, 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 para o 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. Atualização manual do Application Discovery Service 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 do 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 do 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 Não suporta IPv6.

Agentless Collector version 2

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 CIDR — Para obter a máscara de rede CIDR, verifique a configuração do endereço IP do host vCenter que hospeda a VMware VM coletora. Por exemplo, /24.
   - Gateway padrão — Para obter o gateway padrão, verifique a configuração do endereço IP do host VMware vCenter que hospeda a VM coletora. Por exemplo, 192.168.1.1.
   - DNS primário — Para obter o DNS primário, verifique a configuração do endereço IP do host vCenter que hospeda a VMware 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.
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. Desative a interface de rede digitando o seguinte comando no terminal remoto.

```
sudo ip link set ens192 down
```

4. Atualize a configuração da interface usando as etapas a seguir.

   a. Abra 10- cloud-init-ens 192.network no editor vi usando o comando a seguir.

   ```
   sudo vi /etc/systemd/network/10-cloud-init-ens192.network
   ```

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

   ```
   [Match]
   Name=ens192

   [Network]
   DHCP=no
   Address=static-ip-value/CIDR-netmask
   Gateway=gateway-value
   DNS=dnsserver-value
   ```

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

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

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

   b. 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 ip link set ens192 up
```

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
```

   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
```

Agentless Collector version 1

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 — Para obter a máscara de rede, verifique a configuração do endereço IP do host VMware vCenter que hospeda a VM coletora. Por exemplo, 255.255.255.0.
   - Gateway padrão — Para obter o gateway padrão, verifique a configuração do endereço IP do host VMware vCenter que hospeda a VM coletora. Por exemplo, 192.168.1.1.
   - DNS primário — Para obter o DNS primário, verifique a configuração do endereço IP do host vCenter que hospeda a VMware 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.
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. Desative a interface de rede digitando o seguinte comando no terminal remoto.

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

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

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

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

   b. 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"
```

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

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

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

   b. 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
```

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.

Agentless Collector version 2

Para configurar a VM coletora para usar DHCP

1. Desative a interface de rede executando o comando a seguir no terminal remoto.

```
sudo ip link set ens192 down
```

2. Atualize a configuração da interface usando as etapas a seguir.

a. Abra o `10-cloud-init-ens192.network` arquivo no editor vi usando o comando a seguir.

```
sudo vi /etc/systemd/network/10-cloud-init-ens192.network
```

b. Atualize os valores conforme mostrado no exemplo a seguir.

```
[Match]
Name=ens192

[Network]
DHCP=yes

[DHCP]
ClientIdentifier=mac
```

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 ip link set ens192 up
```

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

```
sudo reboot
```

Agentless Collector version 1

Para configurar a VM coletora para usar DHCP

1. Desative a interface de rede executando o comando a seguir no terminal remoto.

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

2. Atualize a configuração da 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 comando a seguir.

```
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 `krb5.conf` de configuração com as informações a seguir.

```
[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
```

Usando o módulo de coleta de dados da rede Agentless Collector

O módulo de coleta de dados de rede possibilita que você descubra dependências entre servidores em seu data center local. Esses dados de rede aceleram seu planejamento de migração, fornecendo visibilidade sobre como os aplicativos se comunicam entre os servidores.

O módulo Network Data Collection se conecta aos servidores que o módulo VMware vCenter identifica e analisa o IP de origem para o IP/port tráfego de destino desses servidores.

Tópicos

- Configurando o módulo de coleta de dados de rede
- Tentativas de coleta de dados de rede
- Status do servidor no módulo de coleta de dados de rede

Configurando o módulo de coleta de dados de rede

O módulo Network Data Collection coleta dados de rede para o inventário do servidor que vem do módulo VMware vCenter. Portanto, para usar o módulo Network Data Collection, primeiro configure o módulo VMware vCenter. Para obter instruções, siga as orientações nos tópicos a seguir:

1. the section called “Implantando um coletor”
2. the section called “Acessando o console do coletor”
3. the section called “Configurar o coletor”
4. the section called “Usando o módulo VMware de coleta de dados”

Para configurar o módulo de coleta de dados de rede

1. No painel do Agentless Collector, na seção Coleta de dados de rede, escolha Exibir conexões de rede.
2. Na página Conexões de rede, escolha Editar coletor.
3. Na seção de credenciais, insira pelo menos um conjunto de credenciais. Você pode inserir até 10 conjuntos de credenciais. Na primeira vez que o módulo tenta coletar dados para um servidor, ele tenta todas as credenciais até encontrar um conjunto de credenciais que funcione; em seguida, ele salva esse conjunto e o usa novamente nas tentativas subsequentes. Para obter informações sobre como configurar credenciais, consultethe section called “Configurar credenciais da”.

4. Na seção Preferências de coleta de dados, para começar a coletar dados automaticamente quando um servidor for reinicializado, selecione Iniciar coleta de dados automaticamente.
5. Se você não tiver configurado certificados WinRM, selecione Desabilitar verificações de certificados WinRM.
6. Escolha Salvar.
7. A coleta acontece nos servidores a cada 15 segundos. Para ver os detalhes das tentativas de coleta de um determinado servidor, marque a caixa de seleção à esquerda do servidor na tabela Servidores.

Configurar credenciais da

O módulo de coleta de dados de rede usa o WinRM para coletar dados de servidores Windows. Ele usa SNMPv2 e SNMPv3 coleta dados de servidores Linux.

Credenciais WinRM:

- Especifique o nome de usuário e a senha de uma conta do Windows que tenha o seguinte:
  - Acesso de leitura ao `\root\standardcimv2` namespace
  - Permissões de leitura para a `MSFT_NetTCPConnection` aula
  - Acesso remoto ao WMI
- Recomendamos que você crie uma conta de serviço dedicada com o mínimo de permissões necessárias.
- Evite usar contas de administrador de domínio ou administrador local.
- A porta 5986 (HTTPS) deve estar aberta entre o coletor e os servidores de destino.
- Evite desativar a verificação do certificado WinRM. Para obter informações sobre como configurar certificados WinRM, consulte. the section called “Solucionando problemas de certificação autoassinada ao configurar certificados WinRM”

SNMPv2 credenciais:

- Forneça uma string de comunidade somente para leitura que possa acessar 1.3.6.1.2.1.6.13.* OID
- SNMPv3 é preferível SNMPv2 devido à maior segurança em SNMPv3
- A porta 161/UDP deve estar aberta entre o coletor e os servidores de destino
- Use cadeias de caracteres de comunidade complexas e não padrão

- Evite cadeias de caracteres comuns como “pública” ou “privada”
- Trate as cadeias de caracteres da comunidade como senhas

SNMPv3 credenciais

- Forneça um username/password e auth/privacy detalhes com permissão somente para leitura que possa acessar 1.3.6.1.2.1.6.13.* OID.
- A porta 161/UDP deve estar aberta entre o coletor e os servidores de destino
- Ative a autenticação e a privacidade
- Use protocolos de autenticação fortes (preferencialmente SHA MD5)
- Use protocolos de criptografia fortes (AES preferido ao DES)
- Use senhas complexas para autenticação e privacidade
- Use nomes de usuário exclusivos (evite nomes comuns)

Melhores práticas gerais para gerenciamento de credenciais

- Armazene credenciais com segurança
- Alterne regularmente todas as credenciais
- Use gerenciadores de senhas ou cofres seguros
- Monitore o uso de credenciais
- Siga o princípio do privilégio mínimo e conceda apenas as permissões mínimas necessárias

Tentativas de coleta de dados de rede

Quando um novo servidor é descoberto, o coletor tenta cada credencial configurada para cada endereço IP. Depois que o coletor encontra uma credencial válida, ele usa somente essa credencial. Depois de duas falhas consecutivas, o coletor tenta coletar dados de rede para um servidor após 30 minutos, 2 horas, 8 horas e depois 24 horas. Após 6 tentativas malsucedidas, o coletor continua testando todas as credenciais configuradas uma vez por dia. Para resolver o problema, edite as credenciais atuais ou adicione outras escolhendo Editar coletor ou faça alterações no servidor de destino que está sendo monitorado.

Status do servidor no módulo de coleta de dados de rede

A tabela a seguir explica os valores do status da coleta.

Status	Significado
Coletando ou coletando	A última tentativa de coleta de conexões de rede foi bem-sucedida.
Errando ou errando	A última tentativa de coleta de conexões de rede falhou devido a um problema de rede ou de permissões. Para obter informaçõ es adicionais, marque a caixa de seleção à esquerda do servidor que tem o erro.
Ignorado	Servidores para os quais nenhuma credencia l válida foi fornecida. Atualize ou configure credenciais adicionais do servidor.
Nenhum dado	A coleta de dados para o servidor não foi iniciada. Para começar a coletar dados, escolha Iniciar coletor.
Pendente	A coleta foi iniciada, mas nenhuma tentativa de coleta foi feita. Aguarde alguns minutos e, em seguida, atualize a lista.

Usando o módulo de VMware coleta de dados 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 do seu. VMware VMs

Tópicos

- Configurando o módulo de coleta de dados do Agentless Collector para o vCenter VMware
- Visualizando detalhes da coleta de VMware dados
- Controlando o escopo da coleta de dados do vCenter
- Dados coletados pelo módulo de coleta de dados Agentless Collector VMware vCenter

Configurando o módulo de coleta de dados do Agentless Collector para o vCenter VMware

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

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

Para configurar o módulo de coleta de dados VMware do vCenter

1. Na página do painel do Agentless Collector, em Coleta de dados, escolha Configurar na seção VMware vCenter.
2. Na página Configurar coleta de dados VMware do vCenter, faça o seguinte:
   a. Nas 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 automaticamente a coletar dados imediatamente após uma configuração bem-sucedida, selecione Iniciar coleta de dados automaticamente.
   c. Escolha Configurar.

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

Visualizando detalhes da coleta de VMware dados

A página de detalhes da coleta de VMware dados mostra detalhes sobre o vCenter no qual você configurou. Configurando o módulo de coleta de dados do Agentless Collector para o vCenter VMware

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

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

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

Se você não optou por iniciar a coleta de dados automaticamente, poderá iniciar a coleta de dados usando o botão Iniciar coleta de dados nesta página. Após o início da coleta de dados, o botão Iniciar muda para Interromper a coleta de dados.

Se a coluna Status da coleta 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 VMware do servidor 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, se seu acesso à Internet não estiver bloqueado. Se você escolher esse botão ou não, para obter informações sobre como acessar o console do Migration Hub, consulteVisualizando seus dados coletados.

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

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

Controlando o escopo da coleta de dados do vCenter

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

> **Note**
>
> Como prática recomendada de segurança, não recomendamos a concessão de permissões adicionais desnecessárias ao 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 sob o vCenter atual

1. Em seu cliente VMware vSphere, escolha vCenter e, em seguida, escolha Hosts and Clusters ou and Templates. VMs
2. Escolha um recurso de datacenter e, em seguida, escolha Permissões.
3. Escolha o usuário do vCenter e, em seguida, 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, em seguida, escolha OK.

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

1. Em seu cliente VMware vSphere, escolha vCenter e, em seguida, escolha Hosts and Clusters ou and Templates. VMs
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. Em seu cliente VMware vSphere, escolha vCenter e, em seguida, escolha Hosts and Clusters ou and Templates. VMs
2. Escolha Related Objects.
3. Escolha Hosts (mostrando uma lista de hosts ESX conhecidos pelo vCenter) ou Máquinas virtuais (mostrando uma lista VMs de 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 escolher Propagar para crianças, ainda poderá remover a permissão somente leitura dos hosts ESX e VMs com base nisso. case-by-case Essa opção não tem efeito nas permissões herdadas que se aplicam a outros hosts ESX e. VMs

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 vCenter do Application Discovery Service Agentless Collector (Agentless Collector) VMware . Para obter informações sobre como configurar a coleta de dados, consulteConfigurando o módulo de coleta de dados do Agentless Collector para o vCenter VMware.

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.

- Os 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	Description
applicationConfigurationId*	ID do aplicativo de migração em que a VM está agrupada.
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 I/O operações de leitura por segundo nulo.
avgDiskWriteOpsPerSecond**	Número médio de I/O operações de gravação por segundo.
avgFreeRAM	Média de RAM livre 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.

Campo de dados	Description
Fabricante de computadores	Fornecedor denunciado pelo ESXi anfitrião.
Modelo de computador	Modelo de computador relatado pelo ESXi host.
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.
hostId*	ID do host da VM.
hostName	Nome do host que executa o software de virtualização.
hypervisor	Tipo de hipervisor.
id	ID do servidor.
lastModifiedTimeCarimbo *	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.

Campo de dados	Description
maxDiskBytesWrittenPerSecond	Número máximo de bytes gravados no disco durante o período de pesquisa.
maxDiskReadOpsPerSecond**	Número máximo de I/O operações de leitura por segundo.
maxDiskWriteOpsPerSecond**	Número máximo de I/O operações 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.
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 ESXi host.
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.

Campo de dados	Description
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 VMware ferramentas
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.

Usando o módulo de coleta de dados de banco de dados e análises

Esta seção descreve como instalar, configurar e usar um módulo de coleta de dados de análise e banco de dados de banco de dados. 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 esse módulo, consulteDados coletados pelo banco de dados Agentless Collector e módulo de coleta de dados analíticos.

> **Important**
>
> Aviso de fim do suporte: em 20 de maio de 2026, AWS encerrará o suporte para o AWS Database Migration Service Fleet Advisor. Depois de 20 de maio de 2026, você não poderá mais acessar o console do AWS DMS Fleet Advisor ou os recursos do AWS DMS Fleet Advisor. Para saber mais, consulte Fim do suporte do AWS DMS Fleet Advisor.

Em um alto nível, ao usar o módulo de coleta de dados de banco de dados e análises, você segue as etapas a seguir.

1. Conclua as etapas de pré-requisito, 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 o. 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 Usando o módulo VMware de coleta de dados o.
4. Configure as credenciais de conexão com seus servidores de sistema operacional e, em seguida, use-as para descobrir servidores de banco de dados.
5. Configure as credenciais de conexão com 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 destino para uma migração para Nuvem AWS o. 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
- Criando o coletor AWS DMS de dados
- Configurando o encaminhamento de dados
- Adicionando seus servidores LDAP e OS
- Descobrindo seus servidores de banco de dados
- Dados coletados pelo banco de dados Agentless Collector e módulo de coleta de dados analíticos

Servidores de sistema operacional, banco de dados e análise compatíveis

O módulo de coleta de dados de banco de dados e análises 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 e superior
- Red Hat Enterprise Linux versão 7 e superior
- SUSE Linux Enterprise Server versão 12 e superior
- Ubuntu versão 16.01 e superior
- Windows Server 2012 e superior
- Windows XP e superior

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

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

Criando o coletor AWS DMS de dados

Seu módulo de coleta de dados de banco de dados e análises usa um coletor de AWS DMS 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 de AWS destino do tamanho certo. Para obter mais informações, consulte Usando o recurso de recomendações de destino 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

Para criar uma função do IAM para que seu coletor AWS DMS de dados acesse o Amazon S3

1. Faça login no Console de gerenciamento da AWS e abra o console do IAM em https://console.aws.amazon.com/iam/.
2. No painel de navegação, escolha Funções e, em seguida, escolha Criar função.
3. Na página Selecionar entidade confiável, em Tipo de entidade confiável, escolha Serviço da AWS . Para Casos de uso de outros AWS serviços, escolha DMS.
4. Marque a caixa de seleção DMS e escolha Próximo.
5. Na página Adicionar permissões, escolha FleetAdvisorS3Policy que você criou antes. Escolha Próximo.
6. Na página Nomear, revisar e criar, insira **`FleetAdvisorS3Role`** em Nome do perfil e escolha Criar função.
7. Abra a função que você criou e escolha a guia Relações de confiança. Selecione Edit trust policy (Editar política de confiança).
8. Na página Editar política de confiança, cole o seguinte JSON no editor, substituindo o código existente.

   JSON

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

```
    "dms.amazonaws.com",
    "dms-fleet-advisor.amazonaws.com"
   ]
  },
  "Action": "sts:AssumeRole"
 }]
}
```

9. Escolha Atualizar política.

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

Para criar um coletor AWS DMS de dados

1. Faça login no Console de gerenciamento da AWS e abra o AWS DMS console em https://console.aws.amazon.com/dms/v2/.
2. Escolha Região da AWS aquela 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 coletor de dados.
6. Na seção Conectividade, escolha Procurar S3. Escolha o bucket do Amazon S3 que você criou anteriormente na lista.
7. Para a função do IAM, escolha `FleetAdvisorS3Role` aquela que você criou antes.
8. Escolha Criar coletor de dados.

Configurando o encaminhamento de dados

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

Para configurar o encaminhamento de dados

1. Abra o console do Agentless Collector. Para obter mais informações, consulte Acessando o console do coletor.

2. Escolha Exibir banco de dados e coletor de análise.
3. Na página Painel, escolha Configurar encaminhamento de dados na seção Encaminhamento de dados.
4. Para o Região da AWSID da chave de acesso do IAM e a chave de acesso secreta do IAM, seu coletor sem agente usa os valores que você configurou anteriormente. Para obter mais informações, consulte Faça login no Migration Hub e escolha uma região de origem e Implantando um coletor.
5. Para o coletor de dados Connected DMS, escolha o coletor de dados que você criou no console. AWS DMS
6. Escolha 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 banco de dados e análises exiba

Conect

para acesso ao DMS e acesso ao S3.

Adicionando seus servidores LDAP e OS

O módulo de coleta de dados de banco de dados e análises 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 aplicação de padrão aberto. Você pode usar esse protocolo para acessar e manter serviços distribuídos de informações de diretório 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 de 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 Acessando o console do coletor.
2. Escolha Exibir banco de dados e coletor de análise e, em seguida, escolha servidores LDAP em Descoberta 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 seu 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 tenha adicionado suas credenciais do servidor LDAP corretamente. Como alternativa, você pode verificar suas credenciais de conexão com o 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 análises 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 dos servidores do sistema operacional descobertos escolhendo Exibir servidores do sistema operacional.

Como alternativa, você pode adicionar seus servidores de sistema operacional manualmente ou importar a lista de servidores de um arquivo de valores separados por vírgula (CSV). Além disso, você pode usar o módulo de coleta de dados VMware vCenter Agentless Collector para descobrir seus servidores de sistema operacional. Para obter mais informações, consulte Usando o módulo VMware de coleta de dados.

Para adicionar um servidor de sistema operacional ao seu banco de dados e módulo de coleta de dados analíticos

1. Na página Database and Analytics Collector, escolha servidores OS em Discovery no painel de navegação.
2. Escolha Adicionar servidor de sistema operacional. A página Adicionar servidor OS é aberta.
3. Forneça suas credenciais do servidor do sistema operacional.

a. Para o tipo de sistema operacional, escolha o sistema operacional do seu servidor.

b. Em Hostname/IP, insira o nome do host ou o endereço IP do seu servidor do sistema operacional.

c. Em Porta, insira o número da porta usada para consultas remotas.

d. Em Tipo de autenticação, escolha o tipo de autenticação que seu servidor de sistema operacional usa.

e. Em Nome de usuário, insira o nome de usuário que você usa para se conectar ao servidor do sistema operacional.

f. Em Senha, insira a senha que você usa para se conectar ao servidor do sistema operacional.

g. Escolha Verificar para se certificar de que você adicionou as credenciais do servidor do sistema operacional corretamente.

4. (Opcional) Adicione vários servidores de sistema operacional a partir de um arquivo CSV.

a. Escolha Importar servidores de sistema operacional em massa a partir 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 dos servidores do sistema operacional no arquivo de acordo com o modelo. O exemplo a seguir mostra como você pode fornecer credenciais de conexão do servidor do sistema operacional em um arquivo CSV.

```
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 as credenciais para todos os seus servidores do sistema operacional.

d. Escolha Procurar e, em seguida, escolha seu arquivo CSV.

5. Escolha Adicionar servidor de sistema operacional.

6. Depois de adicionar credenciais para todos os servidores de sistema operacional, selecione seus servidores de sistema operacional e escolha Descobrir servidores de banco de dados.

Descobrindo seus servidores de banco de dados

Esta seção orienta você pelas etapas que você deve seguir para configurar o sistema operacional e os servidores de banco de dados. Em seguida, você descobrirá seus servidores e terá a opção de adicionar um banco de dados ou servidor de análise manualmente.

Para a descoberta do banco de dados, você deve criar 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.

Configurando a configuração

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. Esta página descreve as etapas que você precisa seguir para garantir que seu banco de dados esteja acessível na porta especificada nas configurações de conexão. Você também ativará a autenticação remota em seu servidor de banco de dados e fornecerá permissões ao seu módulo de coleta de dados.

Configurar a configuração no Linux

Conclua o procedimento a seguir para configurar a configuração para descobrir servidores de banco de dados no Linux.

Para configurar o Linux para descobrir servidores de banco de dados

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

   O exemplo de código a seguir concede ao sudo acesso aos `netstat` comandos `ss` 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 os `netstat` comandos `ss` e. Esse caminho pode ser diferente em seu ambiente. Para determinar o caminho para os `netstat` comandos `ss` e, execute os `which ss` `which 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).

Configurar a configuração no Microsoft Windows

Conclua o procedimento a seguir para configurar a configuração para descobrir servidores de banco de dados no Microsoft Windows.

Para configurar o Microsoft Windows para descobrir servidores de banco de dados

1. Forneça credenciais com concessões para executar consultas do Windows Management Instrumentation (WMI) e WMI Query Language (WQL) e ler o registro.
2. Adicione o usuário do Windows que você especificou nas credenciais de conexão do servidor do sistema operacional aos seguintes grupos: Usuários com distribuídos, usuários do log de desempenho, usuários do monitor de desempenho e leitores de log 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 Início local e ativação remota.
   - Para Controle WMI, escolha as permissões Executar Métodos, Ativar Conta, Ativar Remotamente e Ler Segurança para os `DEFAULT` `StandartCimv2` `WMI` namespaces`CIMV2`,, e.
   - Para o plug-in WMI, execute **`winrm configsddl default`** e escolha Ler e Executar.

4. Configure seu host 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 ICPM 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 Negosiate auth usage
winrm set winrm/config/service '@{AllowUnencrypted="true"}' # Allow unencrypted
 connection
```

Descobrindo um servidor de banco de dados

Conclua o seguinte conjunto de tarefas para descobrir e adicionar servidores de banco de dados no console.

Para iniciar a descoberta de seus servidores de banco de dados

1. Na página Database and Analytics Collector, escolha servidores OS em Discovery 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 de 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, insira 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 de 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 análises compatíveis. 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 seu banco de dados e servidores de análise ao inventário manualmente. Além disso, você pode importar a lista de servidores de um arquivo CSV. Você pode pular essa etapa se já tiver adicionado todos os seus servidores de banco de dados e análises ao inventário.

Para adicionar um banco de dados ou servidor de análise manualmente

1. Na página Coletor de banco de dados e análise, 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. Em 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 Nome do host/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 seu servidor.
   f. Em Senha, insira a senha que você usa para se conectar ao seu servidor.
   g. Escolha Verificar para garantir que você tenha adicionado suas credenciais do banco de dados ou do servidor de análise corretamente.

4. (Opcional) Adicione vários servidores a partir de um arquivo CSV.

   a. Escolha servidores de banco de dados de importação em massa a partir 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,h3yCo8nvbEXAMPLE,,,,,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 as 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 de 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 Database and Analytics Collector, escolha Servidores de banco de dados em Discovery no painel de navegação.

2. Selecione o banco de dados e os servidores de 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.

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

O módulo de coleta de dados analíticos e de 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, consulteUsando o módulo de coleta de dados de banco de dados e análises.

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

- Memória disponível nos servidores de SO
- Armazenamento disponível nos servidores de SO
- Versão e edição do banco de dados
- Número de CPUs em seus servidores de sistema operacional
- Número de esquemas
- O número máximo de procedimentos armazenados.
- Número de tabelas
- Número de acionadores
- 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 compatibilidade do banco de dados
- 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 análises para coletar metadados, capacidade do banco de dados e utilização de recursos, ele captura as seguintes métricas.

- Throughput de E/S nos servidores de banco de dados
- Operações de entrada e saída por segundo (IOPS) nos servidores de banco de dados
- Número do CPUs que seus servidores de sistema operacional usam
- Utilização de memória nos servidores de SO
- Utilização de armazenamento nos servidores de SO

Você pode usar o módulo de coleta de dados de banco de dados e análises 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.

Visualizando seus dados coletados

> **Important**
>
> Aviso de fim do suporte: em 20 de maio de 2026, AWS encerrará o suporte para o AWS Database Migration Service Fleet Advisor. Depois de 20 de maio de 2026, você não poderá mais acessar o console do AWS DMS Fleet Advisor ou os recursos do AWS DMS Fleet Advisor. Para saber mais, consulte Fim do suporte do AWS DMS Fleet Advisor.

Você pode visualizar os dados que seu Coletor Sem Agente do Application Discovery Service (Agentless Collector) coletou no console do Migration Hub seguindo as etapas em. Visualizando servidores no AWS Migration Hub console

Você também pode visualizar as métricas coletadas para servidores de banco de dados e análises no AWS DMS console seguindo as etapas a seguir.

Para visualizar os dados descobertos pelo módulo de coleta de dados de banco de dados e análise no AWS DMS console

1. Faça login no Console de gerenciamento da AWS 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.

Acessando o coletor sem agente

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

Tópicos

- O painel do Agentless Collector
- Editando configurações do Agentless Collector
- Editando VMware credenciais do 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 seja necessário editar as configurações do Agentless Collector.

Para editar as configurações do coletor, escolha Editar configurações do coletor e siga as instruções descritas em. Editando configurações do Agentless Collector

Coleta de dados

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

Tópicos

- VMware Coleta de dados do vCenter
- Coleta de dados de banco de dados e análises

VMware Coleta de dados do vCenter

Para coletar dados de inventário, perfil e utilização do servidor VMware VMs, configure conexões com seus servidores vCenter. Para configurar as conexões, escolha Configurar na seção VMware vCenter e siga as instruções descritas em. Usando o módulo de VMware coleta de dados vCenter Agentless Collector

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

- Exibir status da coleta de dados
- Iniciar a 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 VMwarevCenter é substituído pelas informações de status da coleta de dados, pelo botão Parar coleta de dados e pelo botão Exibir e editar.

Coleta de dados de banco de dados e análises

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

Metadados e capacidade do 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 no AWS DMS console. Se seu banco de dados de origem estiver superprovisionado ou subprovisionado, as recomendações de destino também serão superprovisionadas ou subprovisionadas.

Esse é o modo padrão.

Metadados, capacidade do banco de dados e utilização de recursos

Além das informações de metadados e 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 destino mais precisas do que o modo padrão, pois 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 de 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. É possível 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 coleta 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 emVisualizando seus dados coletados.

Editando configurações do Agentless Collector

Você configurou o coletor quando configurou pela primeira vez o Application Discovery Service Agentless Collector (Agentless Collector) conforme descrito em. Configurando o Agentless Collector O procedimento a seguir descreve como editar as configurações do Agentless Collector.

Para editar as configurações do coletor

- Escolha o botão Editar configurações do coletor no painel do coletor sem agente.

  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 AWS Conta de destino para dados de descoberta, insira a chave de AWS acesso e a chave secreta da AWS 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, consulteImplantando o Application Discovery Service Agentless Collector.

     i. Em AWS chave de acesso, insira a chave de acesso do usuário do IAM da AWS conta que você está especificando como a conta de destino.

     ii. Em AWS chave secreta, insira a chave secreta do usuário do IAM da AWS 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 inserir novamente a senha do Agentless Collector, para verificação, insira a senha novamente.

  d. Escolha Salvar configurações.

A seguir, você veráO painel do Agentless Collector.

Editando VMware credenciais do vCenter

Para coletar dados de inventário, perfil e utilização do servidor VMware VMs, configure conexões com seus servidores vCenter. Para obter informações sobre como configurar conexões VMware do vCenter, consulte. Usando o módulo de VMware coleta de dados vCenter Agentless Collector

Esta seção descreve como editar as credenciais do vCenter.

> **Note**
>
> Antes de editar as credenciais do vCenter, certifique-se de fornecer as credenciais do vCenter com as permissões de leitura e visualização definidas para o grupo Sistema.

Para editar as credenciais do VMware vCenter

Na Visualizando detalhes da coleta de VMware dados página, escolha Editar servidores vCenter.

- Na página Editar vCenter, faça o seguinte:
  a. Nas 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 Salvar.

Atualização manual do Application Discovery Service Agentless Collector

Ao configurar o Application Discovery Service Agentless Collector (Agentless Collector), você pode optar por ativar as atualizações automáticas conforme descrito em. Configurando 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. Siga as etapasImplemente o coletor sem agente.

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 vCenter. VMware
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 na sua AL2 instância no Guia do usuário do Amazon Linux 2.

Patching ao vivo do Kernel

Agentless Collector version 2

A máquina virtual Agentless Collector versão 2 usa o Amazon Linux 2023 conforme descrito em. Implemente o coletor sem agente

Para habilitar e usar o Live Patching para Amazon Linux 2023, consulte Kernel Live Patching on AL2023 no Guia do usuário do Amazon EC2.

Agentless Collector version 1

A máquina virtual Agentless Collector versão 1 usa o Amazon Linux 2 conforme descrito em. Implemente o coletor sem agente

Para habilitar e usar o Live Patching para o Amazon Linux 2, consulte Kernel Live Patching on AL2 no Guia do usuário do Amazon EC2.

Para atualizar da versão 1 do Agentless Collector para a versão 2

1. Instale um novo Agentless Collector OVA usando a imagem mais recente.
2. Configure as credenciais da .
3. Exclua o dispositivo virtual antigo.

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

- Fixação Unable to retrieve manifest or certificate file error
- Solucionando problemas de certificação autoassinada ao configurar certificados WinRM
- 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 para problemas com o Agentless Collector

Fixação `Unable to retrieve manifest or certificate file error`

Se você receber esse erro ao tentar implantar o OVA a partir da URL do Amazon S3 na interface do usuário do VMware vCenter, certifique-se de que seu servidor vCenter atenda aos seguintes requisitos:

- VMware vCenter Server versão 8.0, atualização 1 ou posterior
- VMware vCenter Server 7.0 Update 3q (ISO Build 23788036) ou posterior

Solucionando problemas de certificação autoassinada ao configurar certificados WinRM

Se você habilitar as verificações de certificado WinRM, talvez seja necessário importar uma autoridade de certificação autoassinada para o Agentless Collector.

Para importar uma autoridade de certificação autoassinada

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

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

2. Certifique-se de que cada certificado CA autoassinado usado para assinar certificados WinRM esteja sob o diretório. `/etc/pki/ca-trust/source/anchors` Por exemplo:

   ```
   /etc/pki/ca-trust/source/anchors/https-winrm-ca-1.pem
   ```

3. Para instalar os novos certificados, execute o comando a seguir.

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

4. Reinicie o Agentless Collector executando o seguinte comando

   ```
   sudo shutdown -r now
   ```

5. (Opcional) Para verificar se os certificados foram importados com êxito, você pode executar o comando a seguir.

```
sudo trust list --filter=ca-anchors | less
```

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 vCenter. VMware

   b. Abra o console web 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, consulteEntrar em contato com AWS o Support para 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 vCenter. VMware
2. Abra o console web 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 Console de gerenciamento da AWS 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. Configurando 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 VMware credenciais do 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, consulteEntrar em contato com AWS o Support para problemas com o Agentless Collector.

As causas mais comuns de coletores não íntegros são problemas de endereço IP e credenciais. Corrigindo problemas de endereço IPe 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 malformado, 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 vCenter. VMware
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. Implemente o coletor sem agente

3. Escolha Login e, em seguida, insira a senha do Agentless Collector, que foi configurada quando o coletor foi configurado em. Configurando 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 VMware dados, em Servidores vCenter descobertos, anote o endereço IP na coluna vCenter.
6. Usando uma ferramenta de linha de comando separada, como `ping` `outraceroute`, 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 VMware credenciais do 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 obter mais informações, consulte Configurando 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 DMSCollectorpolíticas Policy e FleetAdvisorS3Policy ao seu usuário do IAM. Para obter mais informações, consulte Implantando o Application Discovery Service 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 *`replaceable`* valores por 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 obter mais informações, consulte Descobrindo seus servidores de banco de dados.

Suporte autônomo ao host ESX

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

Entrar em contato com AWS o Support para 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 vCenter. VMware
2. Abra o console web 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 de dados para o Migration Hub

AWS Migration Hub A importação (Migration Hub) permite importar detalhes do seu ambiente local diretamente para o Migration Hub sem usar o Application Discovery Service Agentless Collector (Agentless Collector) ou o AWS Application Discovery Agent (Discovery Agent), para que você possa realizar 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.

Esta página descreve as etapas para concluir uma solicitação de importação. Primeiro, você usa uma das duas opções a seguir para preparar os dados do servidor local.

- Use ferramentas comuns de terceiros para gerar um arquivo que contém os dados do seu servidor local.
- Baixe nosso modelo de importação de valores separados por vírgula (CSV) e preencha-o com os dados do seu servidor local.

Depois de usar um dos dois métodos descritos anteriormente para criar seu arquivo de dados local, você carrega o arquivo no Migration Hub usando o console do Migration Hub ou um dos AWS SDKs. AWS CLI Para obter mais informações sobre as duas opções, consultethe section called “Formatos de importação compatíveis”.

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, por meio do console ou da importação APIs.

Depois de concluída uma solicitação de importação, você pode exibir os detalhes de registros importados individuais. Visualize dados de utilização, tags e mapeamentos de aplicativos diretamente 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.

Tratar 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 AWS Application Discovery Service Cotas.

Formatos de importação compatíveis

O Migration Hub oferece suporte aos seguintes formatos de importação.

- RVTools
- Modelo de importação do Migration Hub

RVTools

O Migration Hub suporta a importação de exportações do VMware RVTools vSphere via. Ao salvar dados de RVTools, primeiro escolha a opção Exportar tudo para csv ou a opção Exportar tudo para o Excel, depois compacte a pasta e importe o arquivo ZIP para o Migration Hub. Os seguintes arquivos são necessários no ZIP: vInfo, vNetwork, vCPU, vMemory, vDisk, vPartition, vSource, vTools, vHost, vNIC, VSC_vmk.

Modelo de importação do Migration Hub

A importação do Migration Hub permite que você importe 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 do nome de um 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.

Um acento circunflexo (^) ao lado do nome do campo de importação na tabela a seguir indica que ele é somente para leitura se um ServerID for fornecido.

> **Note**
>
> Se você estiver usando qualquer um VMware. MoRefId ou VMWare. VCenterId, para identificar um registro, você deve ter os dois campos no mesmo registro.

Nome do campo de importação	Description	Exemplos
ExternalId*^	Identificador personalizado que permite que você marque cada registro como exclusivo. Por exemplo, ExternalIdpode ser o ID do inventário do servidor em seu data center.	ID de inventário 1 Servidor 2 ID CMBD 3
SMBiosIdentificação^	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"
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. VCenterId entificação.	
VMware. VCenterIdentificação*^	Identificador exclusivo da máquina virtual. Deve ser fornecido com um VMware. MoRefId.	
COPO. NumberOfProcessors^	O número de CPUs.	4

Nome do campo de importação	Description	Exemplos
COPO. NumberOfCores^	O número total de núcleos físicos.	8
COPO. NumberOfLogicalCores^	O número total de threads que podem ser executados simultaneamente em todos CPUs em um servidor. Alguns CPUs oferecem suporte a vários threads para serem executados simultaneamente em um único núcleo de CPU. Nesses casos, esse número será maior do que o número de núcleos físicos (ou virtuais).	16
Nome do sistema operacional^	O nome do sistema operacional.	Linux Windows.Hat
Versão do sistema operacional^	A versão do sistema operacional.	16.04.3 NT 6.2.8
VMware.VMName^	O nome da máquina virtual.	Corp1
CARNEIRO. TotalSizeInMB^	O total de RAM disponível no servidor, em MB.	64 128
CARNEIRO. UsedSizeInMB. Média^	A quantidade média de RAM usada no servidor, em MB.	64 128
CARNEIRO. UsedSizeInMB.máx^	A quantidade máxima de RAM usada disponível no servidor, em MB.	64 128

Nome do campo de importação	Description	Exemplos
COPO. UsagePct.Média^	A utilização média da CPU quando a ferramenta de descoberta estava coletando dados.	45 23.9
COPO. 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
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.Média^	O número médio de operações de leitura de disco por segundo.	45 28
DiskWritesOpsPerSecond.Média^	O número médio de operações de gravação de disco por segundo.	8 3

Nome do campo de importação	Description	Exemplos
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
NetworkWritesPerSecondInKB.máx^	O número máximo de operações de gravação de rede por segundo, em KB.	535 71
Aplicativos	Uma lista delimitada por vírgulas de aplicativos que incluem esse servidor, entre aspas. Esse valor pode incluir aplicativos existentes, and/or novos aplicativos criados na importação.	Application1 "Application2, Application3"
ApplicationWave	A onda de migração para esse servidor.	

Nome do campo de importação	Description	Exemplos
Etiquetas^	Uma lista delimitada por vírgulas de tags formatadas como nome:valor. **Important** Não armazene informações confidenciais (como dados pessoais) em tags.	"zone:1, critical:yes" "zone:3, critical:no, zone:1"
ServerId	O identificador do servidor, conforme visto na lista de servidores do Migration Hub.	`d-server-01kk9i6ywwaxmp`

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 oferece suporte a nenhum campo fora dos definidos no modelo de importação. Todos os campos personalizados fornecidos serão ignorados e não serão importados.

Configurando permissões de importação

Antes de importar seus dados, certifique-se de que seu usuário do IAM tenha as permissões necessárias do Amazon S3 para carregar (`s3:PutObject`) seu arquivo de importação para o Amazon S3 e 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 realiza as importações em sua AWS conta.

Console Permissions

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

Para editar as políticas gerenciadas anexadas a um usuário

1. Faça login no Console de gerenciamento da AWS e abra o console do IAM em https://console.aws.amazon.com/iam/.
2. No painel de navegação, escolha Users.
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.

    JSON

```
{
  "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. Selecione Revisar política.

c. Forneça à sua política um novo Name (Nome) e uma descrição opcional antes de revisar o resumo da política.

d. Selecione Criar política.

6. Volte para a página do console do IAM Grant permissions para o usuário que fará solicitações de importação em sua AWS conta.
7. Atualize a tabela de políticas e procure o nome da política que você acabou de criar.
8. Escolha Próximo: revisar.
9. Escolha Adicionar permissões.

Agora que você adicionou a política ao seu 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 dar a um usuário do IAM as permissões para fazer solicitações de importação de dados usando AWS CLI o.

Para criar e anexar as políticas gerenciadas

1. Use o `aws iam create-policy` AWS CLI comando para criar uma política do IAM com as seguintes permissões. 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.

   JSON

   ```
   {
     "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 como usar esse comando, consulte create-policy na Referência de Comandos.AWS CLI

2. Use o `aws iam create-policy` AWS CLI comando para criar uma política adicional do IAM com as seguintes permissões.

   JSON

   ```
   {
       "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. Use o `aws iam attach-user-policy` AWS CLI comando para anexar as políticas que você criou nas duas etapas anteriores ao usuário do IAM que realizará solicitações de importação em sua AWS conta usando AWS CLI o. Para obter mais informações sobre como usar esse comando, consulte attach-user-policyna Referência de AWS CLI Comandos.

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

Lembre-se de que quando o usuário do IAM carrega objetos no bucket do Amazon S3 que você especificou, ele deve deixar as permissões padrão para os objetos definidas para que o usuário possa ler o objeto.

Carregando seu arquivo de importação para o Amazon S3

Em seguida, você deve carregar seu arquivo de importação em formato CSV no Amazon S3 para que ele possa ser importado. Antes de começar, você deve ter um bucket do Amazon S3 que abrigará seu arquivo de importação criado e and/or escolhido com antecedência.

Console S3 Upload

Para fazer o upload do seu arquivo de importação para o Amazon S3

1. Faça login no Console de gerenciamento da AWS 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 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 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. Acesse a página Importar no console do Migration Hub conforme descrito emComo importar dados. Em seguida, cole a URL do objeto no campo URL do objeto do Amazon S3.

AWS CLI S3 Upload

Para fazer o upload do seu arquivo de importação para o Amazon S3

1. Abra uma janela do terminal e navegue até o diretório no qual seu arquivo de importação foi 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 que foi retornado. Você precisará disso ao criar sua solicitação de importação.

Como importar dados

Depois de baixar o modelo de importação do console do Migration Hub e preenchê-lo com os dados existentes do servidor local, você estará 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 fazendo chamadas de API por meio do AWS CLI.

Console Import

Inicie a importação de dados na página 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 baixar o modelo de importação do nosso bucket Amazon S3 em import_template.csv https://s3.us-west-2.amazonaws.com/templates-7cffcf56-bd96-4b1c-b45b-a5b42f282e46/
3. Para abrir a página Importar, escolha Importar na caixa Importar.
4. Em Nome da importação, especifique um nome para a importação.
5. Preencha o campo URL do objeto do Amazon S3. Para fazer essa etapa, você precisará carregar seu arquivo de dados de importação para o Amazon S3. Para obter mais informações, consulte Carregando seu 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. Ao navegar pela página Importações (histórico de importação) selecionando o nome da importação listada na coluna Nome, você é direcionado para a página Servidores, na qual 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 a partir do AWS CLI, o AWS CLI deve primeiro ser instalado em seu ambiente. Para obter mais informações, consulte Instalando a interface de linha de AWS comando no Guia AWS Command Line Interface do usuário.

> **Note**
>
> Se você ainda não tiver um modelo de importação preenchido, você pode baixar o modelo de importação do nosso bucket do Amazon S3 aqui: import_template.csv https://s3.us-west-2.amazonaws.com/templates-7cffcf56-bd96-4b1c-b45b-a5b42f282e46/

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"
    }
}
```

Rastreando suas solicitações de importação do 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

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

- Nome — O nome da solicitação de importação.
- ID de importação — O ID exclusivo da solicitação de importação.
- Hora da 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 — Esse arquivo de dados está sendo importado no momento.
  - Importado — Todo o arquivo de dados foi importado com sucesso.
  - Importado com erros — Falha na importação de um ou mais registros no arquivo de dados. 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 dos registros no 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 sucesso.
- Registros com falha — O número de registros em um arquivo de dados específico que não foram importados.

CLI Tracking

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

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 e explore os dados descobertos

Tanto o Application Discovery Service Agentless Collector (Agentless Collector) quanto o AWS Discovery Agent (Discovery Agent) fornecem dados de desempenho do sistema com base na utilização média e máxima. Você pode usar os dados de desempenho do sistema coletados para realizar um alto nível de custo total de propriedade (TCO). Os agentes Discovery 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 no console e no. AWS CLI

Tópicos

- Visualize os dados coletados usando o console do Migration Hub
- Explorando 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 o AWS 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 usando o. AWS CLI

Para ver os dados coletados sobre os servidores descobertos no console, siga as etapas emVisualizando servidores no AWS Migration Hub console. Para saber mais sobre como usar o console para visualizar, classificar e marcar servidores descobertos por seus coletores sem agente ou agentes de descoberta, consulte. Descobrindo dados com o console AWS Migration Hub

O módulo de coleta de dados analíticos e de banco de dados do Agentless Collector carrega os dados coletados no bucket do Amazon S3. Você pode visualizar os dados desse bucket no console do AWS DMS. Para visualizar os dados coletados sobre servidores de banco de dados e análise descobertos, siga as etapas emVisualizando seus dados coletados.

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 coincidem com as entradas existentes. Quando essa lógica encontra uma correspondência, ela atualiza as informações do servidor descoberto já existente com novos valores.

Essa lógica de correspondência lida com 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 corresponderem ou não.
- IPAddress
- HostName
- MacAddress

- VMware. MoRefIdVMwaree. vCenterId — Esses dois valores devem ser idênticos aos respectivos campos em outra entrada para que o Application Discovery Service realize uma correspondência.

Explorando dados no Amazon 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. Quando a exploração de dados no Amazon Athena é habilitada a partir do console do Migration Hub (ou usando a StartContinousExport 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 Explorando 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 Discovery Agents em um só lugar. Quando a exploração de dados no Amazon Athena é habilitada a partir do console do Migration Hub (ou usando a StartContinousExport 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 de banco de dados de gerenciamento de configuração (CMDB), e associar os servidores descobertos aos aplicativos comerciais reais. Você também pode integrar o banco de dados Athena com o Amazon Quick para visualizar os resultados da consulta e realizar análises adicionais.

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

Ativando a exploração de dados no Amazon Athena

A exploração de dados no Amazon Athena é habilitada ativando 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 ativa a Exportação Contínua, a função vinculada ao serviço `AWSServiceRoleForApplicationDiscoveryServiceContinuousExport` é usada

automaticamente pela sua conta. Para obter mais informações sobre essa função vinculada ao serviço, consulte Permissões de função vinculadas ao serviço para o Application Discovery Service.

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

Turn on 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 na opção “Exploração de dados no Amazon Athena” na página Data Collectors do console do Migration Hub.

Para ativar 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 botão Exploração de dados no Amazon Athena.
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 funcionando no modo de “exportação contínua”, o que permitirá que você veja e trabalhe com seus dados descobertos no Amazon Athena. Na primeira vez em que isso for ativado, poderá 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, o AWS CLI deve primeiro ser instalado em seu ambiente.

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

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. 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 funcionando no modo de “exportação contínua”, o que permitirá que você veja e trabalhe com seus dados descobertos no Amazon Athena. Na primeira vez em que isso for ativado, poderá levar até 30 minutos para que seus dados apareçam no Amazon Athena.

Explorando dados diretamente no Amazon Athena

Depois de ativar 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.

As instruções a seguir explicam como explorar os dados do seu agente diretamente no console do Athena. Se você não tiver dados no Athena ou não tiver habilitado a exploração de dados no Amazon Athena, uma caixa de diálogo solicitará que você habilite a exploração de dados no Amazon Athena, conforme explicado em. Ativando a exploração de dados no Amazon Athena

Para explorar dados descobertos pelo agente diretamente no Athena

1. No AWS Migration Hub console, escolha Servidores no painel de navegação.
2. Para abrir o console do Amazon Athena, escolha Explorar 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 Usando consultas predefinidas no Amazon Athena.

Visualização de dados do Amazon Athena

Para visualizar seus dados, uma consulta pode ser transferida para um programa de visualização, como o Amazon Quick, ou outras ferramentas de visualização de código aberto, como Cytoscape, yEd ou Gelphi. 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 fonte para produzir a visualização.

Para visualizar seus dados do Amazon Athena usando o Quick

1. Faça login no Amazon Quick.

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 caixa de diálogo da fonte de dados New Athena é exibida.
4. Insira um nome no campo Data source name (Nome da fonte de dados).
5. Escolha Criar fonte de dados.
6. Selecione a gents-servers-os tabela A na caixa de diálogo Escolha sua tabela e escolha Selecionar.
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.

Usando consultas predefinidas no Amazon 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 AWS Migration Hub console, escolha Servidores no painel de navegação.
2. Para abrir o console do Amazon Athena, escolha Explorar 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 CREATE VIEW no 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 os 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 CREATE VIEW no 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. Crie a `valid_outbound_ips_helper` exibição 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 CREATE VIEW no 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 a partir do 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 faço upload de arquivos e pastas em um bucket do S3?
3. Crie uma nova tabela em Athena chamada. `iana_service_ports_import` Para obter instruções, consulte Criar uma tabela no 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");
```

Descobrindo dados com o console AWS Migration Hub

AWS Application Discovery Service O (Application Discovery Service) é integrado ao 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 extras de sua parte.

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

Tópicos

- Visualizando dados no painel AWS Migration Hub do console
- Iniciando e parando coletores de dados no console AWS Migration Hub
- Classificando coletores de dados no console AWS Migration Hub
- Visualizando servidores no AWS Migration Hub console
- Classificando servidores no console AWS Migration Hub
- Marcando servidores no console AWS Migration Hub
- Usando AWS Migration Hub para exportar dados do servidor
- Agrupando servidores no console AWS Migration Hub

Visualizando dados no painel AWS Migration Hub do console

Para visualizar o painel principal, escolha Painel no painel de navegação do console AWS Migration Hub (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 o Application Discovery Agent (Discovery Agent).

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 visualizar o painel principal, escolha Painel no painel de navegação, que fica no lado esquerdo da página inicial do console do Migration Hub.

Iniciando e parando coletores de dados no console AWS Migration Hub

O Application Discovery Service Agentless Collector (Agentless Collector) e o AWS Application Discovery Agent (Discovery Agent) são as ferramentas de coleta de dados que (Application Discovery AWS Application Discovery Service Service) usa para ajudá-lo a descobrir sua infraestrutura existente. As etapas a seguir explicam como baixar e implantar essas ferramentas de coleta de dados de descoberta Implemente o coletor sem agente AWS Agente de descoberta de aplicativos e.

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, parar e visualizar os dados coletados no console AWS Migration Hub (Migration Hub).

Depois que o AWS Application Discovery Agent (Discovery Agent) for implantado, você poderá iniciar ou interromper o processo de coleta de dados na página Data Collectors do console AWS Migration Hub (Migration Hub).

Como iniciar ou interromper ferramentas de coleta de dados

1. Usando sua AWS conta, faça login Console de gerenciamento da AWS 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. 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).

Classificando coletores de dados no console AWS Migration Hub

Se você implantou muitos coletores de dados, poderá classificar a lista exibida de coletores implantados na página Coletores de Dados do console. 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 para Agentes, 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 a partir 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 Start scheduled (Início programado): o início da coleta de dados foi programado. Os dados serão enviados para o Application Discovery Service no próximo ping e o status mudará para Started. Interrompido: os dados não estão sendo coletados nem enviados para o Application Discovery Service. Stop scheduled (Interrupção programada): a interrupção da

Critério de pesquisa	Operador	Valor: Definição
		coleta de dados foi programada. Os dados deixarão de ser enviados para o Application Discovery Service no próximo ping e o status mudará para Stopped.

Critério de pesquisa	Operador	Valor: Definição
Integridade	== !=	Healthy (Íntegra): coleta de dados não está ativada. A ferramenta está funcionando normalmente. Unhealthy (Corrompida): ocorreu um erro com a ferramenta. Os dados não estão sendo coletados ou não relatados. Unknown (Desconhecida): nenhuma conexão foi estabelecida em mais de uma hora. Shutdown (Desligada): a ferramenta informou no último comunicado o "desligamento" 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. Running (Em execução): a coleta de dados está ativada. A ferramenta está funcionando normalmente.
IP address (endereço de IP)	== !=	Qualquer endereço IP selecionado na lista pré-preen chida em que uma ferramenta de coleta foi instalada.

A tabela a seguir mostra os critérios de pesquisa que você pode usar para coletores sem agente, 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 a partir 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	== !=	Coleta de dados: a coleta de dados está ativada. A ferramenta está funcionando normalmente. Pronto para configurar — a coleta de dados não está ativada. A ferramenta está funcionando normalmente. Requer atenção— A ferramenta está em um estado de erro e precisa de atenção. Unknown (Desconhecida): nenhuma conexão foi estabelecida em mais de uma hora. Desligar: a ferramenta comunicou o “desligamento”

Critério de pesquisa	Operador	Valor: Definição
		pela última vez devido ao desligamento de um sistema, serviço ou daemon. Se uma reinicialização ou atualizaç ão de ferramenta ocorreu, o status será alterado para outro estado no primeiro ciclo de relatórios.
IP address (endereço de IP)	== !=	Qualquer endereço IP selecionado na lista pré-preen chida em que uma ferramenta de coleta foi instalada.

Como classificar coletores de dados aplicando filtros de pesquisa

1. Usando sua AWS conta, faça login Console de gerenciamento da AWS 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 Data Collectors.
3. Escolha a guia Coletores sem agente ou Agentes.
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.

Visualizando servidores no AWS Migration Hub console

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.

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

Como visualizar servidores descobertos

1. Usando sua AWS conta, faça login Console de gerenciamento da AWS 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 Servers. 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 Usando AWS Migration Hub para exportar dados do servidor.

Classificando servidores no console AWS Migration Hub

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. Usando sua AWS conta, faça login Console de gerenciamento da AWS 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 Servers.
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.

Marcando servidores no console AWS Migration Hub

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. Usando sua AWS conta, faça login Console de gerenciamento da AWS 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 Servers.
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 Adicionar tags e, em seguida, escolha Adicionar nova tag.
5. Na caixa de diálogo, digite uma chave no campo Chave e, opcionalmente, um valor no campo Valor.

   Adicione mais tags escolhendo Adicionar nova tag e adicionando mais informações.
6. Escolha Salvar.

Como remover tags de um ou mais servidores

1. Usando sua AWS conta, faça login Console de gerenciamento da AWS 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 Servers.
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. Escolha Remover tags.
5. Selecione cada tag que você deseja remover.
6. Escolha Confirmar.

Usando AWS Migration Hub para exportar dados do servidor

Este tópico explica como exportar dados do servidor usando a Console de gerenciamento da AWS AWS Command Line Interface, a ou a API.

Para usar o Console de gerenciamento da AWS para exportar dados do servidor para todos os servidores

1. Faça login Console de gerenciamento da AWS e abra o console do Migration Hub em https://console.aws.amazon.com/migrationhub/.
2. No painel de navegação esquerdo, em Descobrir, escolha Servidores.
3. Escolha Ações e, em seguida, escolha Exportar dados de descoberta.
4. Na seção Exports (Exportações), na parte inferior da tela, selecione Export server details (Exportar detalhes do servidor). Essa ação gera um arquivo.zip que inclui os arquivos.csv descritos na tabela a seguir.

Nome do arquivo	Description
{account_id} _Application.csv	Detalhes de cada aplicativo, incluindo a contagem, o nome e a descrição do servidor.
{ID da conta} _ .csv ApplicationResourceAssociation	A relação entre servidores e aplicativos.
{ID da conta} _ ImportTemplate	O resumo do aplicativo e das tags de cada servidor. Esse arquivo pode ser modificado e reimportado para atualizar o aplicativo associado ao servidor.
{ID da conta} _ .csv NetworkInterface	Detalhes de cada interface de rede, incluindo o servidor, endereço e switch associados.
{account_id} _Server.csv	Detalhes de cada servidor, incluindo sistema operacional, nome do host e hipervisor.
{ID da conta} _ .csv SystemPerformance	Detalhes de cada servidor, incluindo CPU, configuração de memória e armazenamento e desempenho.

Nome do arquivo	Description
{account_id} _Tags.csv	Detalhes de cada tag associada a um servidor.
{account_id} _ Info.csv VMware	Detalhes de cada VMware configuração, incluindo MoRef, VMName e vCenter.

Para usar o Console de gerenciamento da AWS para exportar dados do agente para um servidor específico

1. Faça login Console de gerenciamento da AWS e abra o console do Migration Hub em https://console.aws.amazon.com/migrationhub/.
2. No painel de navegação esquerdo, em Descobrir, escolha Servidores.
3. Coloque o cursor no campo de pesquisa em Servidores. Uma lista suspensa aparece. Nessa lista, em Propriedades, escolha Origem, escolha o operador = e escolha Fonte = Agente.
4. Nos resultados da pesquisa, escolha o nome do servidor para o qual você deseja exportar dados. Essa ação leva você à página de detalhes desse servidor.
5. Insira uma hora de início e uma hora de término e escolha Exportar. O arquivo.zip exportado inclui os arquivos.csv descritos na tabela a seguir.

{ID da conta} _ .csv destinationProcess Connection	Detalhes das conexões de entrada no servidor.
{account_id} _networkInterface.csv	Detalhes de cada interface de rede, incluindo endereço, máscara e nome
{account_id} _osInfo.csv	Detalhes do sistema operacional, incluindo tipo de CPU, hipervisor e nome do sistema operacional.
{account_id} _process.csv	Detalhes dos processos em execução no servidor.

{ID da conta} _ .csv sourceProcessConnection	Detalhes da conexão de saída originada do servidor.
{account_id} _systemPerformance.csv	Detalhes da configuração e desempenho da CPU, memória e armazenamento do servidor.

Para usar a AWS Command Line Interface ou a API para exportar dados do servidor

1. Executar start-export-task. A operação de API correspondente é StartExportTask
2. Executar describe-export-tasks. A operação de API correspondente é DescribeExportTasks.

Agrupando servidores no console AWS Migration Hub

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. Usando sua AWS conta, faça login Console de gerenciamento da AWS 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 Servers.
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 servidor selecionado, selecione Add tag (Adicionar tag), digite um valor para Key (Chave) e, opcionalmente, digite um valor para Value (Valor).

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 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 `DescribeConfigurationsListConfigurations`,, e `StartExportTask` podem não conter atualizações recentes. Para obter mais informações, consulte the section called “Consistência eventual”.

Usar a ação **`DescribeConfigurations`**

A `DescribeConfigurations` ação recupera atributos para uma lista de configurações IDs. Todos os fornecidos IDs devem ser do 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
`server.agentId`	
`server.applications`	
`server.applications.hasMoreValues`	
`server.configurationId`	x
`server.cpuType`	
`server.hostName`	
`server.hypervisor`	
`server.networkInterfaceInfo`	
`server.networkInterfaceInfo.hasMoreValues`	
`server.osName`	
`server.osVersion`	
`server.tags`	
`server.tags.hasMoreValues`	
`server.timeOfCreation`	x
`server.type`	
`server.performance.avgCpuUsagePct`	

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

Campo	Obrigatório
server.performance.maxNetworkWritesPerSecondInKB	
server.performance.minFreeRAMInKB	
server.performance.numCores	
server.performance.numCpus	
server.performance.numDisks	
server.performance.numNetworkCards	
server.performance.totalRAMInKB	

Processar ativos

Campo	Obrigatório
process.commandLine	
process.configurationId	x
process.name	
process.path	
process.timeOfCreation	x

Ativos do aplicativo

Campo	Obrigatório
application.configurationId	x

Campo	Obrigatório
application.description	
application.lastModifiedTime	x
application.name	x
application.serverCount	x
application.timeOfCreation	x

Usar a ação **ListConfigurations**

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
server.configurationId	x
server.agentId	
server.hostName	
server.osName	
server.osVersion	
server.timeOfCreation	x
server.type	

Processar ativos

Campo	Obrigatório
process.commandLine	
process.configurationId	x
process.name	
process.path	
process.timeOfCreation	x
server.agentId	
server.configurationId	x

Ativos do aplicativo

Campo	Obrigatório
application.configurationId	x
application.description	
application.name	x
application.serverCount	x
application.timeOfCreation	x
application.lastModifiedTime	x

Ativos de conexão

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

Filtros compatíveis para **ListConfigurations**

As tabelas a seguir, organizadas por tipo de ativo, listam os filtros compatíveis para a ação ListConfigurations. Filtros e valores estão em um key/value relacionamento definido por uma das condições lógicas suportadas. A saída dos filtros indicados pode ser classificada.

Ativos do servidor

Filtro	Condições compatíveis	Valores com suporte	Classificação compatível
`server.configurationId`	• EQUALS • NOT_EQUALS • EQ • NE	• Qualquer ID de configuração de servidor válido	Nenhum
`server.hostName`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• ASC • DESC
`server.osName`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• ASC • DESC
`server.osVersion`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• ASC • DESC
`server.agentId`	• EQUALS • NOT_EQUALS • EQ • NE	• String	Nenhum

Filtro	Condições compatíveis	Valores com suporte	Classificação compatível
`server.connectorId`	• EQUALS • NOT_EQUALS • EQ • NE	• String	Nenhum
`server.type`	• EQUALS • NOT_EQUALS • EQ • NE	String com um dos seguintes valores: • EC2 • OUTRO • VMWARE_VM • VMWARE_HOST • VMWARE_VM_TEMPLATE	Nenhum
`server.vmWareInfo.morefId`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	Nenhum
`server.vmWareInfo.vcenterId`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	Nenhum

Filtro	Condições compatíveis	Valores com suporte	Classificação compatível
`server.vmWareInfo.hostId`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	Nenhum
`server.networkInterfaceInfo.portGroupId`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	Nenhum
`server.networkInterfaceInfo.portGroupName`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	Nenhum
`server.networkInterfaceInfo.virtualSwitchName`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	Nenhum

Filtro	Condições compatíveis	Valores com suporte	Classificação compatível
`server.networkInterfaceInfo.ipAddress`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	Nenhum
`server.networkInterfaceInfo.macAddress`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	Nenhum
`server.performance.avgCpuUsagePct`	• GE • LE • GT • LT	• Porcentagem	Nenhum
`server.performance.totalDiskFreeSizeInKB`	• GE • LE • GT • LT	• Duplo	Nenhum
`server.performance.avgFreeRAMInKB`	• GE • LE • GT • LT	• Duplo	Nenhum

Filtro	Condições compatíveis	Valores com suporte	Classificação compatível
`server.tag.value`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	Nenhum
`server.tag.key`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	Nenhum
`server.application.name`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	Nenhum
`server.application.description`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	Nenhum

Filtro	Condições compatíveis	Valores com suporte	Classificação compatível
`server.application.configurationId`	• EQUALS • NOT_EQUALS • EQ • NE	• Qualquer ID de configuração de aplicativo válido	Nenhum
`server.process.configurationId`	• EQUALS • NOT_EQUALS • EQ • NE	• ProcessId	Nenhum
`server.process.name`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	Nenhum
`server.process.commandLine`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	Nenhum

Ativos do aplicativo

Filtro	Condições compatíveis	Valores com suporte	Classificação compatível
`application.configurationId`	• EQUALS • NOT_EQUALS • EQ • NE	• ApplicationId	Nenhum
`application.name`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• ASC • DESC
`application.description`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• ASC • DESC
`application.serverCount`	Filtragem compatível.	Filtragem compatível.	• ASC • DESC
`application.timeOfCreation`	Filtragem compatível.	Filtragem compatível.	• ASC • DESC
`application.lastModifiedTime`	Filtragem compatível.	Filtragem compatível.	• ASC • DESC

Filtro	Condições compatíveis	Valores com suporte	Classificação compatível
`server.configurationId`	• EQUALS • NOT_EQUALS • EQ • NE	• ServerId	Nenhum

Processar ativos

Filtro	Condições compatíveis	Valores com suporte	Classificação compatível
`process.configurationId`	• EQUALS • NOT_EQUALS • EQ • NE	• ProcessId	
`process.name`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• ASC • DESC
`process.commandLine`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• ASC • DESC

Filtro	Condições compatíveis	Valores com suporte	Classificação compatível
`server.configurationId`	• EQUALS • NOT_EQUALS • EQ • NE	• ServerId	
`server.hostName`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• ASC • DESC
`server.osName`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• ASC • DESC
`server.osVersion`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• ASC • DESC

Filtro	Condições compatíveis	Valores com suporte	Classificação compatível
`server.agentId`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	

Ativos de conexão

Filtro	Condições compatíveis	Valores com suporte	Classificação compatível
`connection.sourceIp`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• IP	• ASC • DESC
`connection.destinationIp`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• IP	• ASC • DESC
`connection.destinationPort`	• EQUALS • NOT_EQUALS • EQ • NE	• Inteiro	• ASC • DESC

Filtro	Condições compatíveis	Valores com suporte	Classificação compatível
`sourceServer.configurationId`	• EQUALS • NOT_EQUALS • EQ • NE	• ServerId	
`sourceServer.hostName`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• ASC • DESC
`destinationServer.osName`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• ASC • DESC
`destinationServer.osVersion`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• ASC • DESC

Filtro	Condições compatíveis	Valores com suporte	Classificação compatível
`destinationServer.agentId`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	
`sourceProcess.configurationId`	• EQUALS • NOT_EQUALS • EQ • NE	• ProcessId	
`sourceProcess.name`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• ASC • DESC
`sourceProcess.commandLine`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• ASC • DESC
`destinationProcess.configurationId`	• EQUALS • NOT_EQUALS • EQ • NE	• ProcessId	

Filtro	Condições compatíveis	Valores com suporte	Classificação compatível
`destinationProcess.name`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• ASC • DESC
`destinationprocess.commandLine`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• 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 StartExportTaskDescribeConfigurations, ListConfigurationse.

- AssociateConfigurationItemsToApplication
- CreateTags
- DeleteApplications
- DeleteTags
- DescribeBatchDeleteConfigurationTask
- DescribeImportTasks
- DisassociateConfigurationItemsFromApplication
- UpdateApplication

Sugestões para gerenciar a consistência eventual:

- Ao invocar as operações de leitura StartExportTaskDescribeConfigurations, ou 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 espera e aumente gradualmente até cerca de cinco minutos de espera.

Acesso AWS Application Discovery Service usando um endpoint de interface ()AWS PrivateLink

Você pode usar AWS PrivateLink para criar uma conexão privada entre sua VPC e. AWS Application Discovery Service Você pode acessar o Application Discovery Service como se estivesse em sua VPC, sem o uso de um gateway de internet, dispositivo NAT, conexão VPN ou conexão. Direct Connect As instâncias em sua VPC não precisam de endereços IP públicos para acessar o Application Discovery Service.

Estabeleça essa conectividade privada criando um endpoint de interface, habilitado pelo AWS PrivateLink. Criaremos um endpoint de interface de rede em cada sub-rede que você habilitar para o endpoint de interface. Essas são interfaces de rede gerenciadas pelo solicitante que servem como ponto de entrada para o tráfego destinado ao Application Discovery Service.

Para saber mais, consulte Acessar os Serviços da AWS pelo AWS PrivateLink no Guia do AWS PrivateLink .

Considerações sobre o Application Discovery Service

Antes de configurar um endpoint de interface para o Application Discovery Service, consulte Acessar um AWS serviço usando um endpoint VPC de interface no Guia.AWS PrivateLink

O Application Discovery Service suporta duas interfaces: uma para fazer chamadas para todas as suas ações de API e outra para o Agentless Collector e o AWS Application Discovery Agent enviarem dados de descoberta.

Como criar um endpoint de interface

Você pode criar um endpoint de interface usando o console do Amazon VPC ou a AWS Command Line Interface (AWS CLI). Para obter mais informações, consulte Acessar um AWS serviço usando uma interface VPC endpoint no Guia.AWS PrivateLink

For Application Discovery Service

- Crie um endpoint de interface para o Application Discovery Service usando o seguinte nome de serviço:

```
com.amazonaws.region.discovery
```

Se você habilitar o DNS privado para o endpoint da interface, poderá fazer solicitações de API ao Application Discovery Service usando seu nome DNS regional padrão. Por exemplo, `.discovery.us-east-1.amazonaws.com`

For Agentless Collector and AWS Application Discovery Agent

Crie um endpoint de interface usando o seguinte nome de serviço:

```
com.amazonaws.region.arsenal-discovery
```

Se você habilitar o DNS privado para o endpoint da interface, poderá fazer solicitações de API ao Application Discovery Arsenal usando seu nome DNS regional padrão. Por exemplo, `.arsenal-discovery.us-east-1.amazonaws.com`

Crie uma política de endpoint para seu endpoint de interface.

Uma política de endpoint é um recurso do IAM que pode ser anexado ao endpoint de interface. A política de endpoint padrão permite acesso total a um AWS serviço por meio do endpoint da interface. Para controlar o acesso permitido a um AWS serviço da sua VPC, anexe uma política de endpoint personalizada ao endpoint da interface.

Uma política de endpoint especifica as seguintes informações:

- As entidades principais que podem realizar ações (Contas da AWS, usuários do IAM e perfis do IAM).
- As ações que podem ser realizadas.

Para obter mais informações, consulte Controlar o acesso aos serviços usando políticas de endpoint no Guia do AWS PrivateLink .

Exemplo: políticas de VPC endpoint

O exemplo a seguir refere-se a uma política de endpoint personalizada. Quando anexada ao endpoint da sua interface, essa política concede acesso às ações do listadas para todas as entidades principais em todos os recursos.

Example policy for Application Discovery Service

```
{
   "Statement": [
      {
         "Principal": "*",
         "Effect": "Allow",
         "Action": [
            "discovery:action-1",
            "discovery:action-2",
            "discovery:action-3"
         ],
         "Resource":"*"
      }
   ]
}
```

Example policy for the Agentless Collector and AWS Application Discovery Agent

```
{
   "Statement": [
      {
         "Principal": "*",
         "Effect": "Allow",
         "Action": [
            "arsenal:RegisterOnPremisesAgent"
         ],
         "Resource":"*"
      }
   ]
}
```

Usando o VPC endpoint para o Agentless Collector e o Application Discovery Agent AWS

O Agentless Collector e o AWS Application Discovery Agent não oferecem suporte a endpoints configuráveis. Em vez disso, use o recurso de DNS privado para o endpoint da `arsenal-discovery` Amazon VPC.

- Configure a tabela de Direct Connect rotas para rotear endereços IP privados da AWS para a VPC. Por exemplo, destino = 10.0.0.0/8 e destino = local. Para essa configuração, você precisa pelo menos rotear os endereços IP privados do endpoint da `arsenal-discovery` Amazon VPC para a VPC.
- Use o recurso DNS privado do endpoint `arsenal-discovery` Amazon VPC porque o Agentless Collector não oferece suporte a endpoints configuráveis do Arsenal.
- Configure o endpoint da `arsenal-discovery` Amazon VPC em uma sub-rede privada com a mesma VPC para a qual você está roteando o tráfego. Direct Connect
- Configure o endpoint da `arsenal-discovery` Amazon VPC com um grupo de segurança que permite tráfego de entrada de dentro da VPC (por exemplo, 10.0.0.0/8).
- Configure um resolvedor de entrada do Amazon Route 53 para rotear a resolução de DNS para o nome DNS privado do endpoint Amazon `arsenal-discovery` VPC, que será resolvido para o IP privado do endpoint VPC. Se você não fizer isso, o coletor executará a resolução de DNS usando o resolvedor local e usará o endpoint público do Arsenal, e o tráfego não passará pela VPC.
- Se você tiver todo o tráfego público desativado, o recurso de atualização automática falhará. Isso ocorre porque o Agentless Collector recupera as atualizações enviando solicitações para o endpoint do Amazon ECR. Para que o recurso de atualização automática funcione sem enviar solicitações pela Internet pública, configure um VPC endpoint para o serviço Amazon ECR e habilite o recurso de DNS privado para esse endpoint.

Segurança em AWS Application Discovery Service

A segurança na nuvem AWS é a maior prioridade. Como AWS cliente, você se beneficia de um data center e de uma arquitetura de rede criados para atender aos requisitos das organizações mais sensíveis à segurança.

A segurança é uma responsabilidade compartilhada entre você AWS e você. O modelo de responsabilidade compartilhada descreve isto como segurança da nuvem e segurança na nuvem.

- Segurança da nuvem — AWS é responsável por proteger a infraestrutura que executa AWS os serviços na AWS nuvem. AWS também fornece serviços que você pode usar 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 na nuvem — Sua responsabilidade é determinada pelo AWS serviço que você usa. Também existe a responsabilidade por outros fatores, incluindo a confidencialidade de dados, os requisitos da 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
- Registrando chamadas da API Application Discovery Service com AWS CloudTrail

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
- Gerenciar o 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
- Usando funções vinculadas a serviços para o 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 com base na sua função:

- Usuário do serviço: solicite permissões ao seu administrador se você não conseguir acessar os atributos (consulte Solução de problemas AWS Application Discovery Service de identidade e acesso).
- Administrador do serviço: determine o acesso do usuário e envie solicitações de permissão (consulte Como AWS Application Discovery Service funciona com o IAM)
- Administrador do IAM: escreva políticas para gerenciar o acesso (consulte AWS Application Discovery Service exemplos de políticas baseadas em identidade)

Autenticação com identidades

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

Você pode fazer login como uma identidade federada usando credenciais de uma fonte de identidade como Centro de Identidade do AWS IAM (IAM Identity Center), autenticação de login único ou credenciais. Google/Facebook Para ter mais informações sobre como fazer login, consulte Como fazer login em sua Conta da AWS no Guia do usuário do Início de Sessão da AWS .

Para acesso programático, AWS fornece um SDK e uma CLI para assinar solicitações criptograficamente. Para ter mais informações, consulte AWS Signature Version 4 para solicitações de API no Guia do usuário do IAM.

Conta da AWS usuário root

Ao criar um Conta da AWS, você começa com uma identidade de login chamada usuário Conta da AWS raiz que tem acesso completo a todos Serviços da AWS os recursos. É altamente recomendável não usar o usuário-raiz em tarefas diárias. Consulte as tarefas que exigem credenciais de usuário-raiz em Tarefas que exigem credenciais de usuário-raiz no Guia do usuário do IAM.

Usuários e grupos do IAM

Um usuário do IAM é uma identidade com permissões específicas para uma única pessoa ou aplicação. É recomendável usar credenciais temporárias, em vez de usuários do IAM com credenciais de longo prazo. Para obter mais informações, consulte Exigir que usuários humanos usem a federação com um provedor de identidade para acessar AWS usando credenciais temporárias no Guia do usuário do IAM.

Um grupo do IAM especifica um conjunto de usuários do IAM e facilita o gerenciamento de permissões para grandes conjuntos de usuários. Para ter mais informações, consulte Casos de uso de usuários do IAM no Guia do usuário do IAM.

Perfis do IAM

Uma perfil do IAM é uma identidade com permissões específicas que oferece credenciais temporárias. Você pode assumir uma função mudando de um usuário para uma função do IAM (console) ou chamando uma operação de AWS API AWS CLI ou. Para saber mais, consulte Métodos para assumir um perfil no Manual do usuário do IAM.

Os perfis do IAM são úteis para acesso de usuário federado, permissões de usuário do IAM temporárias, acesso entre contas, acesso entre serviços e aplicações em execução no Amazon EC2. Consulte mais informações em Acesso a recursos entre contas no IAM no Guia do usuário do IAM.

Gerenciar o acesso usando políticas

Você controla o acesso AWS criando políticas e anexando-as a AWS identidades ou recursos. Uma política define permissões quando associada a uma identidade ou recurso. AWS avalia essas políticas quando um diretor faz uma solicitação. A maioria das políticas é armazenada AWS como documentos JSON. Para ter mais informações sobre documentos de política JSON, consulte Visão geral das políticas JSON no Guia do usuário do IAM.

Por meio de políticas, os administradores especificam quem tem acesso a que, definindo qual entidade principal pode realizar ações em quais recursos e sob quais condições.

Por padrão, usuários e perfis não têm permissões. Um administrador do IAM cria políticas do IAM e as adiciona aos perfis, os quais os usuários podem então assumir. As políticas do IAM definem permissões, independentemente do método usado para realizar a operação.

Políticas baseadas em identidade

As políticas baseadas em identidade são documentos de políticas de permissão JSON que você anexa a uma identidade (usuário, grupo ou perfil). Essas políticas controlam quais ações as identidades podem realizar, em quais recursos e sob quais condições. Para saber como criar uma política baseada em identidade, consulte Definir permissões personalizadas do IAM com as políticas gerenciadas pelo cliente no Guia do Usuário do IAM.

As políticas baseadas em identidade podem ser políticas em linha (incorporadas diretamente em uma única identidade) ou políticas gerenciadas (políticas autônomas anexadas a várias identidades). Para saber como escolher entre uma política gerenciada e políticas em linha, consulte Escolher entre políticas gerenciadas e políticas em linha no Guia do usuário do IAM.

Políticas baseadas em recursos

Políticas baseadas em recursos são documentos de políticas JSON que você anexa a um recurso. Entre os exemplos estão políticas de confiança de perfil do IAM e políticas de bucket do Amazon S3. Em serviços compatíveis com políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. É necessário especificar uma entidade principal em uma política baseada em recursos.

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

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

Outros tipos de política

AWS oferece suporte a tipos de políticas adicionais que podem definir o máximo de permissões concedidas por tipos de políticas mais comuns:

- Limites de permissões: definem o número máximo de permissões que uma política baseada em identidade pode conceder a uma entidade do IAM. Para saber mais sobre limites de permissões, consulte Limites de permissões para identidades do IAM no Guia do usuário do IAM.
- Políticas de controle de serviço (SCPs) — Especifique as permissões máximas para uma organização ou unidade organizacional em AWS Organizations. Para saber mais, consulte Políticas de controle de serviço no Guia do usuário do AWS Organizations .
- Políticas de controle de recursos (RCPs) — Defina o máximo de permissões disponíveis para recursos em suas contas. Para obter mais informações, consulte Políticas de controle de recursos (RCPs) no Guia AWS Organizations do usuário.
- Políticas de sessão: políticas avançadas transmitidas como um parâmetro durante a criação de uma sessão temporária para um perfil ou um usuário federado. Para saber mais, 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 tags 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 e 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 podem ser usadas para permitir ou negar acesso em uma política. 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 oferece suporte à especificação de recursos ARNs 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 tags 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.

Perfis vinculados 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. Usando funções vinculadas a serviços para o Application Discovery Service

Perfis de serviço

Esse atributo permite que um serviço assuma 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 recursos. Esse tipo de atualização afeta todas as identidades (usuários, grupos e funções) em que a política está anexada. É mais provável que os serviços atualizem uma política gerenciada pela AWS quando um novo recurso 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: AWSApplication DiscoveryServiceFullAccess

A `AWSApplicationDiscoveryServiceFullAccess` política concede a uma conta de usuário do IAM acesso ao Application Discovery Service e ao Migration Hub APIs.

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: AWSApplication DiscoveryAgentlessCollectorAccess

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.
- `mgh`— 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.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "arsenal:RegisterOnPremisesAgent"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ecr-public:DescribeImages"
            ],
            "Resource": "arn:aws:ecr-
public::446372222237: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: AWSApplication DiscoveryAgentAccess

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: AWSAgentless DiscoveryService

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: ApplicationDiscoveryServiceContinuousExportServiceRolePolicy

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: AWSDiscovery ContinuousExportFirehosePolicy

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 AWSApplication DiscoveryServiceFirehose função. Para obter um exemplo dessa política, consulte Concedendo permissões para exploração de dados.

Criando a AWSApplication DiscoveryServiceFirehose 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 AWSDiscoveryContinuousExportFirehosePolicye escolha Avançar: Revisão.

8. Insira AWSApplicationDiscoveryServiceFirehose como o nome do perfil e escolha Criar perfil.

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 do documento para 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 `AWSApplicationDiscoveryAgentlessCollectorAccess` que concede ao Agentless Collector acesso para se registrar e se comunicar com o Application Discovery Service e se comunicar com outros serviços. AWS	16 de agosto de 2022
O Application Discovery Service começou a rastrear as alterações	O Application Discovery Service começou a monitorar as alterações em suas políticas AWS gerenciadas.	1.º 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 Console

de gerenciamento da AWS AWS CLI, ou. 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

- Práticas recomendadas 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

Práticas recomendadas 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 sua 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 saber mais, 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 recursos específicos sob condições específicas, também conhecidas como permissões de privilégio mínimo. Para saber mais 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: é possível adicionar uma condição às políticas para limitar o acesso a ações e recursos. Por exemplo, é possível escrever uma condição de política para especificar que todas as solicitações devem ser enviadas usando SSL. Você também pode usar condições para conceder acesso às ações de serviço se elas forem usadas por meio de uma ação específica AWS service (Serviço da AWS), como CloudFormation. Para saber mais, 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 cem verificações de política e recomendações práticas para ajudar a criar políticas seguras e funcionais. Para saber mais, 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 saber mais, consulte Configuração de acesso à API protegido por MFA no Guia do Usuário do IAM.

Para saber mais 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 AWSApplication DiscoveryServiceFullAccess gerenciada concede à conta de usuário do IAM acesso ao Application Discovery Service e ao Migration Hub APIs.

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

JSON

```
{
    "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 AWSApplication DiscoveryAgentAccess 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

JSON

```
{
    "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

JSON

```
{
   "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 AWSDiscovery ContinuousExportFirehosePolicy 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 AWSApplication DiscoveryServiceFirehose função.

Example AWSDiscoveryContinuousExportFirehosePolicy

JSON

```
{
    "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

JSON

```
{
    "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.

Usando funções vinculadas a serviços para o Application Discovery Service

AWS Application Discovery Service usa funções vinculadas ao serviço AWS Identity and Access Management (IAM). Uma 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 exige para chamar outros AWS serviços em seu nome.

Uma função vinculada ao serviço facilita a configuração do Application Discovery Service porque você não precisa adicionar manualmente as permissões necessárias. O Application Discovery Service define as permissões de suas funções vinculadas ao serviço e, a menos que seja 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, que não pode ser anexada a nenhuma outra entidade do IAM.

Um perfil vinculado ao serviço poderá ser excluído somente após excluir seus atributos relacionados. Isso protege seus recursos do Application Discovery Service porque você não pode remover inadvertidamente a permissão para acessar os recursos.

Tópicos

- Permissões de função vinculadas ao serviço para o Application Discovery Service
- Criação de uma função vinculada ao serviço para o Application Discovery Service
- Excluindo uma função vinculada ao serviço para o Application Discovery Service

Para obter informações sobre outros serviços compatíveis com perfis vinculados a serviços, consulte Serviços da AWS compatíveis com o IAM e procure os serviços que contenham Sim na coluna Service-Linked Role. Escolha um Sim com um link para visualizar a documentação do perfil vinculado para esse serviço.

Permissões de função vinculadas ao serviço para o Application Discovery Service

O Application Discovery Service usa a função vinculada ao serviço chamada AWSServiceRoleForApplicationDiscoveryServiceContinuousExport— Permite o acesso aos AWS serviços e recursos usados ou gerenciados por. AWS Application Discovery Service

A função AWSService RoleForApplicationDiscoveryServiceContinuousExport vinculada ao serviço confia nos seguintes serviços para assumir a função:

- `continuousexport.discovery.amazonaws.com`

A política de permissões de 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:

JSON

```
{
    "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 um perfil vinculado a serviço. Para saber mais, consulte Permissões de Função Vinculadas ao Serviço no Guia do Usuário do IAM.

Criação de uma função vinculada ao serviço para o Application Discovery Service

Não é necessário criar manualmente um perfil vinculado ao serviço. A função AWSService RoleForApplicationDiscoveryServiceContinuousExport 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 a API usando a CLI. StartContinuousExport AWS

> **Important**
>
> Esse perfil vinculado ao serviço pode aparecer em sua conta se você concluiu uma ação em outro serviço que usa os atributos compatíveis com esse perfil. Para saber mais, consulte Uma nova função apareceu na minha conta do IAM.

Criando a função vinculada ao serviço a partir do console do Migration Hub

Você pode usar o console do Migration Hub para criar a função AWSService RoleForApplicationDiscoveryServiceContinuousExport vinculada ao serviço.

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 controle deslizante Exploração de dados no Athena para a posição Ativado.
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).

Criando a função vinculada ao serviço a partir do AWS CLI

Você pode usar os comandos do Application Discovery Service do AWS Command Line Interface para criar a função AWSService RoleForApplicationDiscoveryServiceContinuousExport vinculada ao serviço.

Essa função vinculada ao serviço é criada automaticamente quando você inicia a Exportação Contínua a partir do AWS CLI (a primeira AWS CLI deve ser instalada em seu ambiente).

Para criar a função vinculada ao serviço (CLI) iniciando a Exportação Contínua a partir do AWS CLI

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. 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 o caso de uso do Discovery Service - Continuous Export. 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.

Excluindo uma função vinculada ao serviço para o Application Discovery Service

Se você não precisar mais usar um recurso ou serviço que requer um perfil vinculado ao serviço, é recomendável excluí-lo. Dessa forma, você não tem uma entidade não utilizada que não seja monitorada ativamente ou mantida. No entanto, você deve limpar suo perfil vinculado ao serviço para excluí-la manualmente.

Limpar a função vinculada ao serviço

Antes de usar o IAM para excluir um perfil vinculado ao serviço, você deverá excluir qualquer recurso usado pelo perfil.

> **Note**
>
> Se o Application Discovery Service estiver usando a função ao tentar excluir os recursos, a exclusão poderá falhar. Se isso acontecer, espere alguns minutos e tente a operação novamente.

Para excluir os recursos do Application Discovery Service usados pela função AWSService RoleForApplicationDiscoveryServiceContinuousExport 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 o controle deslizante Exploração de dados no Athena para a posição Desligado.

Para excluir os recursos do Application Discovery Service usados pela função AWSService RoleForApplicationDiscoveryServiceContinuousExport vinculada ao serviço do AWS CLI

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. 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. Insira o comando a seguir para garantir que a exportação contínua tenha sido interrompida, verificando se o status de retorno é “INATIVO”:

```
aws discovery describe-continuous-export
```

Excluir manualmente o perfil vinculado ao serviço

Você pode excluir a função AWSService RoleForApplicationDiscoveryServiceContinuousExport vinculada ao serviço usando o console do IAM, a CLI do IAM ou a API do IAM. Se você não precisar mais usar os recursos do Discovery Service - Continuous Export que exigem essa função vinculada ao serviço, recomendamos que você exclua essa função. Dessa forma, você não tem uma entidade não utilizada que não seja monitorada ativamente ou mantida. Para saber mais, consulte Excluir um perfil vinculado ao serviço no Guia do usuário do IAM.

> **Note**
>
> Primeiramente, limpe sua função vinculada ao serviço antes de excluí-la. Consulte Limpar a 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.

Registrando chamadas da API Application Discovery Service com AWS CloudTrail

AWS Application Discovery Service é integrado com AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, função ou AWS serviço no Application Discovery Service. Você pode usar CloudTrail para registrar, monitorar continuamente e reter a atividade da conta para fins de solução de problemas e auditoria. CloudTrail fornece um histórico de eventos da atividade da sua AWS conta, incluindo ações realizadas por meio do AWS Management Console e ferramentas de linha de comando. AWS SDKs

CloudTrail captura todas as chamadas de API para o Application Discovery Service como eventos. As chamadas capturadas incluem chamadas do console do Application Discovery Service e 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 para um bucket do Amazon S3, incluindo eventos para o Application Discovery Service. Se você não configurar uma trilha, ainda poderá ver os eventos mais recentes no CloudTrail console no Histórico de eventos. Usando as informações coletadas por CloudTrail, você pode determinar a solicitação que foi feita ao Application Discovery Service, o endereço IP do qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita e detalhes adicionais.

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

Informações do Application Discovery Service em CloudTrail

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

Para um registro contínuo dos eventos em sua AWS conta, incluindo eventos do Application Discovery Service, crie uma trilha. Uma trilha permite CloudTrail entregar arquivos de log para um bucket do Amazon S3. Por padrão, quando você cria uma trilha no console, a trilha se aplica a todas

as AWS regiões. A trilha registra eventos de todas as regiões na AWS partição e entrega os arquivos de log ao bucket do Amazon S3 que você especificar. Além disso, você pode configurar outros AWS serviços para analisar e agir com base nos dados de eventos coletados nos CloudTrail registros. Para saber mais, consulte:

- Visão Geral para Criar uma Trilha
- CloudTrail Serviços e integrações compatíveis
- Configurando notificações do Amazon SNS para CloudTrail
- Recebendo arquivos de CloudTrail log de várias regiões e recebendo arquivos de CloudTrail log de várias contas

Todas as ações do Application Discovery Service são registradas CloudTrail e documentadas na Referência da API do Application Discovery Service. Por exemplo, chamadas para as `GetDiscoverySummary` ações `CreateTagsDescribeTags`, e geram entradas nos arquivos de CloudTrail log.

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

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

Para obter mais informações, consulte Elemento userIdentity do CloudTrail .

Compreendendo as entradas do arquivo de log do Application Discovery Service

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

O exemplo a seguir mostra uma entrada de CloudTrail registro que demonstra a `DescribeTags` ação.


```
{
    "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"
}
```

AWS Application Discovery Service Formatos ARN

Um Amazon Resource Name (ARN) é uma string que identifica exclusivamente um recurso. AWS AWS requer um ARN quando você deseja especificar um recurso de forma inequívoca em todos os. AWS AWS Application Discovery Service define o seguinte ARNs.

- Agente Discovery: `arn:aws:discovery:region:account:agent/discovery-agent/agentId`
- Colecionador sem agente: `arn:aws:discovery:region:account:agent/agentless-collector/agentId`
- Coletor do Migration Evaluator: `arn:aws:discovery:region:account:agent/migration-evaluator-collector/agentId`
- Conector Discovery: `arn:aws:discovery:region:account:agent/discovery-connector/agentId`

AWS Application Discovery Service Cotas

O console Service Quotas fornece informações sobre AWS Application Discovery Service cotas. É possível usar o console do serviço de cotas para visualizar cotas padrão ou solicitar aumentos de cota para cotas ajustáveis.

Atualmente, a única cota que pode ser aumentada é a importação de servidores por conta.

O Application Discovery Service tem as seguintes cotas padrão:

- 1.000 aplicativos por conta.

  Se você atingir essa cota e quiser importar novos aplicativos, poderá excluir os aplicativos existentes com a ação da `DeleteApplications` API. Para obter mais informações, consulte DeleteApplicationsna Referência da API do Application Discovery Service.
- Cada arquivo de importação pode ter um tamanho máximo de arquivo 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 para o Application Discovery Service.
- 10.000 agentes inativos, que respondem, mas não coletam 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

- Interrompa 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

Interrompa a coleta de dados por meio da exploração de dados

Para interromper a exploração de dados, você pode desligar 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-discover-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 estiver 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.

- Seus servidores locais

  Certifique-se de que seus servidores estejam funcionando, para que assim os seus agentes coletem 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 obter mais informações, consulte AWS Application Discovery Service Cotas.

- 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, como, `CPU.NumberOfCores` devem ter um intervalo de valores que eles suportam. 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 Console de gerenciamento da AWS e abra o console do Migration Hub emhttps://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 Como importar dados.

Histórico do documento para AWS Application Discovery Service

Atualização mais recente da documentação do Guia do Usuário: 16 de maio de 2023

A tabela a seguir descreve mudanças importantes no Guia do Usuário do Application Discovery Service após 18 de janeiro de 2019. Para receber notificações sobre atualizações da documentação, inscreva-se no feed RSS.

Alteração	Descrição	Data
Modo de manutenção	AWS O Application Discovery Service não está mais aberto a novos clientes. Como alternativa, use AWS Transform o que fornece recursos semelhantes. Para obter mais informaçõ es, consulte Alteração de disponibilidade AWS do Application Discovery Service.	7 de novembro de 2025
Transição do Discovery Connector para o Agentless Collector	Recomendamos que os clientes que atualmente usam o Discovery Connector façam a transição para o novo Agentless Collector. A partir de 17 de novembro de 2025, AWS Application Discovery Service deixará de aceitar novos dados dos Discovery Connectors. Para obter mais informações, consulte Discovery Connector.	12 de novembro de 2024

Lançou o módulo de coleta de dados da rede Agentless Collector	O módulo de coleta de dados de rede possibilita que você descubra dependências entre servidores em seu data center local. Para obter mais informações, consulte Usando o módulo de coleta de dados da rede Agentless Collector.	8 de novembro de 2024
Support para coleta sem agente para mapeamento de dependências	Para obter mais informações, consulte Usando o módulo de coleta de dados do VMware vCenter Agentless Collector.	24 de outubro de 2024
Lançou a versão 2 do Agentless Collector com base no Amazon Linux 2023	Para obter mais informações, consulte Pré-requisitos para o Agentless Collector.	26 de setembro de 2024
Pré-requisitos atualizados do Agentless Collector	Para obter mais informações, consulte Pré-requisitos para o Agentless Collector.	9 de setembro de 2024
Consistência eventual na API	Para obter mais informações, consulte Consistência eventual na AWS Application Discovery Service API.	20 de junho de 2024
Atualizações do Agentless Collector	Adicionamos `sts.amazonaws.com` às listas de domínios que exigem acesso externo. Para obter mais informações, consulte Configurar firewall para acesso externo aos domínios da AWS.	20 de junho de 2024

Para separar o acesso, crie e use contas separadas da AWS.	Para obter mais informações, consulte Ações, recursos e chaves de condição para o AWS Application Discovery Service.	5 de abril de 2024
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 do seu banco de dados e servidores de análise locais. 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 para ajudá-lo a planejar com eficiência sua migração para o. Nuvem AWS Para obter mais informações, consulte Agentless Collector.	16 de agosto de 2022

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 de origem do Migration Hub fornece um único repositório de informações de descoberta e planejamento de migração para todo o seu portfólio e uma visão única das migrações em várias AWS regiões.	20 de novembro de 2019
Apresentando o recurso de importação do Migration Hub	A importação do Migration Hub permite que você importe 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 Application Discovery Service User Guide antes de 18 de janeiro de 2019:

Alteração	Descrição	Data
Novo recurso	Documentos atualizados para apoiar a exploração de dados no Amazon Athena e capítulo de solução de problemas adicionado.	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 Console de gerenciamento da AWS foi adicionado.	19 de dezembro de 2016
Descoberta sem agente	Esta versão descreve como definir e configurar a descobert a 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 Guia do Usuário do Application Discovery Service.	12 de maio de 2016

AWS Glossário

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

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.